შოთა რუსთაველის ეროვნული სამეცნიერო ფონდი
SHOTA RUSTAVELI NATIONAL SCIENCE FOUNDATION
SCIENTIA POTESTAS EST.

კიბერუსაფრთხოების გამოწვევები, კონცეფციები და პრაქტიკა

წ. არაბული, ა. შეყელაძე,
ვ. ადამია, ზ. ცირამუა

2024

პროექტი განხორციელდა „შოთა რუსთაველის საქართველოს ეროვნული სამეცნიერო ფონდის ფინანსური მხარდაჭერით.
გრანტის ნომერი: SP-23-392

კიბერუსაფრთხოების გამოწვევები, კონცეფციები და პრაქტიკა

ავტორები:

ნანი არაბული

აკაკი შეყელაძე

ვლადიმერ ადამია

ზაზა ცირამუა

2024 წელი

მოცემულ წიგნში განხილულია ინფორმაციული უსაფრთხოების საფუძვლები, კიბერსივრცის თანამედროვე გამოწვევები და მათთან გამკლავების მეთოდები და ინსტრუმენტები. მკითხველს საშუალება ეძლევა ქართულ ენაზე შეისწავლოს კიბერუსაფრთხოების იურიდიული, თეორიული და პრაქტიკული კომპონენტები, რაც მას სამომავლოდ შეუქმნის მყარ საფუძველს აღნიშნულ სფეროში მოღვაწეობისთვის.

წიგნში წარმოდგენილი საკითხები და თანდართული მდიდარი პრაქტიკული მასალა მკითხველის გამოცდილებას კიბერუსაფრთხოების სფეროში ახალი, უნიკალური უნარ-ჩვევებით გაამდიდრებს.

წიგნის გამოყენება შესაძლებელია უმაღლეს საგანმანათლებლო დაწესებულებაში ინფორმაციული ან/და კიბერუსაფრთხოების სასწავლო დისციპლინების როგორ ძირითად, ასევე დამხმარე ლიტერატურად ბაკალავრიატის, მაგისტრატურისა და დოქტორანტურის საფეხურებზე.

სამეცნიერო რედაქტორები: პროფ. დავით გულუა

პროფ. სალომე ონიანი

შინაარსი

დანართი: პრაქტიკული დავალებები

თავი 1: კიბერუსაფრთხოება - ექსპერტებისა და კრიმინალების სამყარო

მსოფლიოში პირველი ჰაკერები იყვნენ კომპიუტერის მოყვარულები, პროგრამისტები და სტუდენტები XX საუკუნის 60-იან წლებში. თავდაპირველად, ტერმინი ჰაკერი აღწერდა პირების პროგრამირების მოწინავე უნარებს. ჰაკერებმა ეს პროგრამირების უნარი გამოიყენეს ადრეული სისტემების საზღვრებისა და შესაძლებლობების შესამოწმებლად. ეს ადრეული ჰაკერები ასევე ჩართულნი იყვნენ პირველი კომპიუტერული თამაშების განვითარებაში.

ჰაკერთა საქმიანობის განვითარების კვალდაკვალ ეს ტერმინი დამკვიდრდა კიბერკულტურაში. ამ კულტურის გარეთ მყოფმა სამყარომაც კი შეცდომით მიიღო ყოვლისმომცველ ვიზარდთა ჰაკერული სამყარო. წიგნებ, რომლებიც 1996 წლისთვის გამოვიდა, ინტერნეტის საწყისებზე, უკვე აღწერდა ჰაკერული კულტურის მისტიკას. ჩამოყალიბდა ერთგვარი ჰაკერული იმიჯი და ლექსიკა. დღეისათვის ბევრი ჰაკერული ჯგუფი ირგებს ამ იმიჯს. ერთ-ერთი ყველაზე ცნობილი ჰაკერული ჯგუფის სახელია Legion of Doom. მნიშვნელოვანია კიბერკულტურის გაგება, რათა ჩავწვდეთ კიბერსამყაროს დამნაშავეების გეგმებსა და მათ მოტივაციას.

სუნ ცზი ჩინელი ფილოსოფოსი და მეომარი იყო ძველი წელთაღრიცხით მე-6 საუკუნეში. სუნ ცზიმ დაწერა წიგნი სახელწოდებით ომის ხელოვნება, რომელიც კლასიკური ნამუშევარია მტრის დასამარცხებლად არსებული სტრატეგიების შესახებ. მისმა წიგნმა დიდი სამსახური გაუწია ომის ტაქტიკოსებს საუკუნეების განმავლობაში. სუნ ცზის მოძღვრების ერთ-ერთი მთავარი პრინციპია მოწინააღმდეგის საფუძვლიანი შესწავლა. მიუხედავად იმისა, რომ იგი კონკრეტულად გულისხმობდა ომს, მისი რჩევა ასევე მიესადაგება ცხოვრების სხვა ასპექტებსაც, მათ შორის კიბერუსაფრთხოების გამოწვევებს. ეს თავი იწყება კიბერუსაფრთხოების სამყაროს სტრუქტურისა და მისი განვითარების აუცილებლობის მიზეზების ახსნით.

1.1. კიბერუსაფრთხოების ოპერაციების არეალი

არსებობს მრავალი ჯგუფი, რომლებიც ქმნიან „კიბერსამყაროს“ სხვადასხვა დომენებს. როდესაც ჯგუფებს შესაძლებლობა ეძლევათ, გაერთიანდნენ და მოიპოვონ წვდომა დიდი რაოდენობით მონაცემებზე, ისინი გარდაიქმნებიან საკმაოდ გავლენიან ძალად. ეს მონაცემები შეიძლება არსებობდეს ტექსტის, სურათების, ვიდეოს, აუდიო ან ნებისმიერი ტიპის ინფორმაციის სახით, რომელიც შეიძლება მოპოვებულ იქნას ციფრულ სამყაროში. ეს ჯგუფები შეიძლება იმდენად გაძლიერდნენ, რომ მიუხედავად მათი განცალკევებული ძალებისა, შესაძლოა მიეცეთ შესაძლებლობა, შექმნან საკმაოდ ძლიერი კიბერუსაფრთხოების დომენები.

კომპანიები, როგორიცაა Google, Facebook და LinkedIn, შეიძლება ჩაითვალონ მონაცემთა დომენებად ჩვენს კიბერსამყაროში. მოცემული ანალოგიის განვრცობით, ადამიანები, რომლებიც დასაქმებულნი არიან ზემოთხსენებულ კომპანიებში ინფორმაციის დაცვის მიმართულებით, შეიძლება განხილულ იქნენ, როგორც კიბერუსაფრთხოების სპეციალისტები, ან ექსპერტები.

სიტყვა 'დომენი' შესაძლოა განხილულ იქნას მრავალი მნიშვნელობით. ყველა ის სფერო, სადაც არსებობს მართვა, გარკვეული ტიპის კანონმდებლობა და დაცვა, შესაძლოა განხილულ იქნას, როგოც ოპერაციების არეალი, ანუ დომენი. წარმოიდგინეთ, როგორ დაიცავდა ველური ცხოველი საკუთარ დეკლარირებულ "დომენს". მოცემულ კურსში, განვიხილოთ დომენი, როგორც ერთგვარი დაცული ტერიტორია. იგი შეიძლება შეზღუდულ იქნას ლოგიკური ან ფიზიკური საზღვრით. ეს დამოკიდებული იქნება რეალიზებული სისტემის ზომაზე. ბევრ რამეში კიბერუსაფრთხოების ექსპერტებმა არსებული დომენები საკუთარი ქვეყნის კანონების შესაბამისად უნდა დაიცვან.

Google-ის ექსპერტებმა ინტერნეტის ფართო კიბერსამყაროში ერთერთი პირველი და ყველაზე ძლიერი დომენი შექმნეს. მილიარდობით ადამიანი Google-ს ყოველდღიურად იყენებს სასურველი ინფორმაციის მოსაძიებლად. Google-მა უდავოდ შექმნა მსოფლიოში უდიდესი მონაცემთა შეგროვების ინფრასტრუქტურა. Google-მა შეიმუშავა Android - ოპერაციული სისტემა, რომელიც დაინსტალირებულია ინტერნეტთან დაკავშირებული ყველა მობილური მოწყობილობის დაახლოებით 80%-ზე. თითოეული მოწყობილობა მოითხოვს

მომხმარებლებისაგან Google ანგარიშის შექმნას, რომელსაც შეუძლია სანიშნეების და ანგარიშის ინფორმაციის შენახვა, ძიების შედეგების შენახვა და მოწყობილობის დამახსოვრება.

Facebook წარმოადგენს კიდევ ერთი მძლავრ დომენს ინტერნეტსივრცეში. ადამიანები ყოველდღიურად ქმნიან პირად ანგარიშებს ოჯახთან და მეგობრებთან კომუნიკაციისთვის. ამით, თქვენ ნებაყოფლობით განათავსებთ პირად მონაცემებს საჯარო სივრცეში. Facebook-ის შემქმნელებმა ჩამოაყალიბეს მასიური მონაცემთა დომენი, რომლის მეშვეობითაც ადამიანებს საშუალება მიეცათ დაკავშირებოდნენ ერთმანეთს, რაც წარსულში წარმოუდგენელი ჩანდა. ფეისბუქი ყოველდღიურად მილიონობით ადამიანს აკავშირებს ერთმანეთთთან და აძლევს კომპანიებს და ორგანიზაციებს ადამიანებთან კომუნიკაციის საშუალებას პერსონალურ და სხვადასხვა ტიპის ფოკუსირებულ გარემოში.

LinkedIn არის კიდევ ერთი მონაცემთა დომენი ინტერნეტში. LinkedIn-ის დამფუძნებლებმა აღნიშნეს, რომ მათი წევრები უზიარებენ ერთმანეთს ინფორმაციას პროფესიული კავშირების მშენებლობის პროცესში. LinkedIn-ის მომხმარებლები ახდენენ ამ ინფორმაციის ატვირთვას ონლაინ პროფილების შესაქმნელად და სხვა წევრებთან დასაკავშირებლად. LinkedIn აკავშირებს თანამშრომლებს დამსაქმებლებთან და კომპანიებს ერთმანეთთან მთელი მსოფლიოს მასშტაბით. ცხადია, არსებობს გარკვეული მსგავსება LinkedIn -სა და Facebook-ს შორის.

ამ დომენების შიდა სტრუქტურის განხილვა ცხადყოფს, თუ როგორ არიან ისინი რეალიზებულნი. ფუნდამენტურ დონეზე, ეს დომენები წარმოადგენენ მძლავრ სტრუქტურას იმის გამო, რომ მონაცემების შეგროვება ხდება თვით მომხმარებელთა მიერ. ეს მონაცემები ხშირად მოიცავს მომხმარებელთა პირად ინფორმაციას, მათ სხვადასხვა ტიპის ინტერესებს, მეგობრებს და ოჯახის წევრებს, პროფესიებს, ჰობებსა და სამუშაო და პირად გრაფიკებს. ექსპერტები, სოციალურ ქსელებში ატვირთული მონაცემების დაცვით, უზრუნველყოფენ პრესტიჟს და მნიშვნელობას იმ პირებისა და ორგანიზაციებისთვის, რომლებიც დაინტერესებულნი არიან ამ დომენების გამოყენებით.

ინტერნეტში შეგროვებული მონაცემები გაცილებით აღემატება იმ მონაცემებს, რომლებსაც მომხმარებლები ნებაყოფლობით აზიარებენ. კიბერდომენები განაგრძობენ მეცნიერებისა და ტექნოლოგიების

განვითარებას, რაც საშუალებას აძლევს ექსპერტებსა და მათ დამსაქმებლებს (Google, Facebook, LinkedIn და ა. შ.), თავი მოუყარონ ინფორმაციის სხვადასხვა ტიპებს. კიბერექსპერტებს ახლა გააჩნიათ ტექნოლოგიები მსოფლიო ამინდის ტენდენციების გასაკონტროლებლად, ოკეანეების მონიტორინგისათვის, ასევე ადამიანების, ცხოველებისა და ობიექტების გადაადგილებისა და ქცევის შესასწავლად რეალურ დროში.

გაჩნდა ახალი ტექნოლოგიები, როგორიცაა გეოსივრცითი საინფორმაციო სისტემები (GIS) და ნივთების (საგანთა) ინტერნეტი (IoT), მოხდა მათი დაკავშირება. ამ ახალ ტექნოლოგიებს შეუძლიათ თვალყური ადევნონ ხეების ჯანმრთელობას სამეზობლოში. მათ შეუძლიათ განახორციელონ ავტომობილების, მოწყობილობების, ფიზიკური პირებისა და მასალების ადგილმდებარეობის მონიტორინგი. ამ ტიპის ინფორმაციას შეუძლია ენერგიის დაზოგვა, ეფექტურობის გაუმჯობესება და უსაფრთხოების რისკების შემცირება. თითოეულ ამ ტექნოლოგიას ასევე შეუძლია უზრუნველყოს შეგროვებული მონაცემების გაანალიზება და გამოყენებული ინფორმაციის ექსპონენციალურად გაფართოება და ანალიზი გარემომცველი სამყაროს უკეთ შესაცნობად. GIS-ისა და IoT-ს მიერ შეგროვებული მონაცემები კიბერუსაფრთხოების სპეციალისტებისთვის უზარმაზარ გამოწვევას ქმნის. ამ მოწყობილობების მიერ გენერირებული მონაცემების ტიპს აქვს პოტენციალი, რომ კიბერდამნაშავეებს ყოველდღიური ცხოვრების ძალიან ინტიმურ ასპექტებზე წვდომა მისცენ.

1.2 კიბერკრიმინალები კიბერუსაფრთხოების სპეციალისტების წინააღმდეგ

კიბერდამნაშავეები

კიბერუსაფრთხოების სამყაროს ადრეულ წლებში ტიპური კიბერდამნაშავეები იყვნენ მოზარდები ან მოყვარულები, რომლებიც მუშაობდნენ სახლის კომპიუტერიდან, თავდასხმებით ძირითადად შემოიფარგლებოდნენ ხუმრობებით და ვანდალიზმით. დღეს კიბერდამნაშავეთა სამყარო უფრო საშიში გახდა. თავდამსხმელები არიან ფიზიკური პირები ან ჯგუფები, რომლებიც ცდილობენ გამოიყენონ მოწყვლადობა პირადი ან ფინანსური მოგებისთვის. კიბერდამნაშავეები დაინტერესებულნი არიან საქმიანობის სფეროს

ფართო სპექტრით, დაწყებული საკრედიტო ბარათებიდან პროდუქტის დიზაინამდე, ასევე ნებისმიერი ფასეული ინფორმაციით.

მოყვარულები

მოყვარულებს, იგივე script kiddies, გააჩნიათ მცირე გამოცდილება და ხშირად იყენებენ ინტერნეტში მოძიებულ ინსტრუქციებსა და პროგრამებს ქსელური შეტევების განსახორციელებლად. ზოგი უბრალოდ ინტერესდება ამ თემით, ზოგი კი ცდილობს თავიანთი უნარ-ჩვევების დემონსტრირებას და ზიანს აყენებს გარშემომყოფთ. ისინი შეიძლება შემოიფარგლებოდნენ ბაზური ინსტრუმენტებით, მაგრამ შედეგები მაინც დამანგრეველი იყოს.

ჰაკერები

კრიმინალების ეს ჯგუფი ცდილობს შეაღწიოს კომპიუტერებსა და ქსელებში სხვადასხვა მიზეზების გამო. ჰაკერთა ტიპების კლასიფიკაცია ფართოდ განსხვავდება. ხშირად მათ ყოფენ მხოლოდ 3 კატეგორიად: თეთრ, ნაცრისფერ და შავქუდიანებად, თუმცა, სფეროს სპეციფიკამ აჩვენა, რომ ჰაკერის გამოცდილების, შესაძლებლობის, მიზნისა და ჯგუფის წევრობის მიხედვით, ჰაკერთა განსხვავებული ტიპებია წარმოდგენილი.

უპირველესად უნდა აღვნიშნოთ, რომ ჰაკერების საქმიანობა შეიძლება იყოს როგორც სასარგებლო, ასევე მავნე. მავნე ზემოქმედებაში მოიაზრება კომპიუტერულ სისტემებში უნებართვო შეღწევა, ფინანსური რესურსის დაუფლება, ინფორმაციის მოპარვა. ხოლო სასარგებლო მიზნებით მოქმედი ჰაკერები პოულობენ სისტემების მოწყვლადობებს და მათი საბოლოო მიზანი სწორედ ამ სისუსტეების აღმოფხვრაა.

ჰაკერები შავი ქუდით

მოიცავს (კლასიკურ) შავქუდიან ჰაკერებს და სუიციდ-ჰაკერებს.

შავქუდიანი ჰაკერები

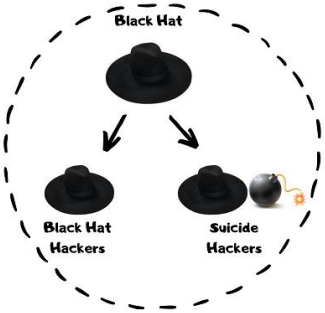
კლასიკური შავქუდიანი ჰაკერები ჰაკერთა ყველაზე საშიშ კატეგორიად მიიჩნევა. ისინი არიან სხვადასხვა კომპეტენციის მაღალკვალიფიციური სპეციალისტები: პროგრამისტები, ქსელის და მონაცემთა ბაზის ადმინისტრატორები. მათი მიზანია საკუთარი

ცოდნისა და გამოცდილების გამოყენება სახელმწიფო და კერძო სექტორის ინფრასტრუქტურის წინააღმდეგ.

სწორედ შავქუდიანი ჰაკერები დგანან ყველაზე მასშტაბური და ცნობილი კიბერდანაშაულების უკან.

სუიციდ-ჰაკერი

სუიციდ-ჰაკერი არის ჰაკერი, რომელიც აცნობიერებს, რომ მისი ვინაობის დადგენას კიბერუსაფრთხოების სპეციალისტები შეძლებენ. ამის ცოდნის მიუხედავად, ის მაინც უტევს კომპიუტერულ სისტემებს და მისი ძირითადი მიზანი ფინანსური რესურსის დაუფლება ან შურისძიებაა.



სურ.1. 1. ჰაკერები შავი ქუდით

<u>ჰაკერები თეთრი ქუდით</u>

ჰაკერები თეთრი ქუდით, თავის მხრივ, იყოფა 2 კატეგორიად: თეთრქუდიანი ჰაკერები და წითელქუდიანი ჰაკერები.

თეთრქუდიანი ჰაკერები

თეთრქუდიანი ჰაკერები არიან ეთიკური ჰაკერები, რაც ნიშნავს იმას, რომ მათი საქმიანობა არის კანონიერი და ამოძრავებთ მხოლოდ დადებითი მიზნები. ისინი ამა თუ იმ პროგრამული უზრუნველყოფის მოწყვლადობის აღმოჩენისას, ინფორმაციას აწვდიან მწარმოებლებს სისუსტეების შესახებ, რათა მოხდეს პრობლემების აღმოფხვრა.

თეთრქუდიანი ჰაკერები, მსგავსად შავქუდიანებისა, გამოირჩევიან ძალიან ძლიერი ტექნიკური შესაძლებლობებით. ნებისმიერი სამთავრობო და კერძო დაწესებულება, საკუთარ კიბერუსაფრთხოებას, სწორედ თეთრქუდიან ჰაკერებს ანდობს.

წითელქუდიანი ჰაკერები

წითელქუდიანი ჰაკერები, მსგავსად თეთრქუდიანებისა, იცავს სისტემებს, ცდილობს სისტემების სისუსტეების პოვნას და ჰაკერებისგან დაცვას, თუმცა, ამასთანავე, ისინი, ასევე, უტევენ ბოროტმოქმედ ჰაკერებს. მათი დევიზი შეიძლება ჩამოყალიბდეს შემდეგნაირად: „საუკეთესო თავდაცვა თავდასხმაა“.

ჰაკერები ნაცრისფერი ქუდით

მოიცავს 2 ქვეკატეგორიას: ნაცრისფერქუდიან ჰაკერებს და განგაშის ამტეხებს.

ნაცრისფერქუდიანი ჰაკერები

ნაცრისფერქუდიანი ჰაკერები შავ და თეთრქუდიან ჰაკერთა გაერთიანებაა. ისინი არ არიან შავქუდიანები, ვინაიდან საკუთარ ცოდნასა და უნარებს არ იყენებენ პირადი მიზნებისთვის. თუმცა, არც თეთრქუდიანები არიან, ვინაიდან სენსიტიურ ინფორმაციაზე წვდომის მიღება ნებართვის გარეშე არ არის კანონიერი. მათი ძირითადი საქმიანობაა ე.წ.”Zero-Day” კატეგორიის სისუსტეების აღმოჩენა სახელმწიფო სპეცსამსახურებისთვის, რათა მოხდეს ამ მოწყვლადობების გამოყენება სხვა სახელმწიფოების ან კომპანიების წინააღმდეგ. მათი ძირითადი სამიზნე არის მონაცემები (მოპარვა, შეცვლა, განადგურება...).

განგაშის ამტეხები

განგაშის ამტეხები დასაქმებულები არიან ორგანიზაციების მიერ, რათა მოიპოვონ ინფორმაცია მეტოქეებზე. ისინი იყენებენ ჰაკინგის საშუალებებს იმისთვის, რომ წვდომა მიიღონ კონკურენტი კომპანიის სენსიტიურ მონაცემებზე, მათ შორის, საკუთარი დამსაქმებელი კომპანიის შესახებ. ისინი საშიშები არიან მეტოქეებისთვის.

სამთავრობო დაფინანსების ჰაკერთა დაჯგუფება

ასეთ დაჯგუფებებში შემავალი ჰაკერები გამოირჩევიან მძლავრი კომპიუტერული ინფრასტრუქტურით, მდიდარი რესურსებით და ასრულებენ დაკვეთას სახელმწიფოს მხრიდან. მათი სამიზნე მოწინააღმდეგე ქვეყნის ინფრასტრუქტურა, სამხედრო და საფინანსო ინსტიტუტებია.

უმცროსი ჰაკერები

უმცროსი ჰაკერები შეიძლება იყვნენ სკრიპტერები, ლურჯქუდიანი ჰაკერები და მწვანექუდიანი ჰაკერები.

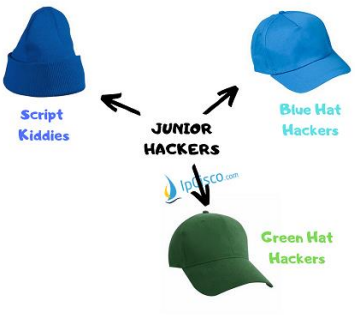
სკრიპტერები

სკრიპტერები არიან თინეიჯერები, რომლებსაც გააჩნიათ საბაზისო უნარები კომპიუტერულ პროგრამირებაში და ამ ცოდნას იყენებენ

გართობისა და პოპულარობის მოსახვეჭად. ისინი ძირითადად მიმართავენ DOS ან DDOS შეტევის ტიპებს.

<u>მწვანექუდიანი ჰაკერები</u>

მწვანექუდიანი ჰაკერების მთავარი მიზანია გახდნენ ექსპერტი ჰაკერები. მათ აქვთ გარკვეული ცოდნა პროგრამირებაში, კომპიუტერულ სისტემებში და ცდილობენ ამ ცოდნის გაღრმავებას. მათი მიზანი შეუძლებელია შეფასდეს ცალსახად დადებითად ან უარყოფითად. ვინაიდან მათი გადასაწყვეტია რა ფერის ქუდს აირჩევენ მოგვიანებით - შავს, თუ თეთრს.



სურ.1. 2. ფერადქუდიანი ჰაკერები

<u>ლურჯქუდიანი ჰაკერები</u>

ლურჯქუდიანი ჰაკერები აგრესიულ დამწყებ ჰაკერებს აერთიანებს და მათი ძირითადი მიზანი შურისძიებაა. ისინი ცდილობენ ინფორმაციულ სისტემებზე შეტევით შური იძიონ ან ადამიანებზე, ან სხვადასხვა ორგანიზაციებზე. მათი მოქმედება, როგორც წესი, მარტივი ტიპის შეტევებს მოიცავს.

<u>ჰაკტივისტები</u>

სურ.1. 3.ჰაკტივისტების ილუსტრაცია

ჰაკტივისტები საერთო სოციალური ან პოლიტიკური მოტივების მქონე ჰაკერთა ჯგუფია, რომელთა საქმიანობაც, ძირითადად, დაკავშირებულია კონსტიტუციური წესწყობილების რღვევასთან. ისინი, როგორც წესი, მიმართავენ შეტევებს სამთავრობო ინფრასტრუქტურის წინააღმდეგ და ღიად ასაჯაროებენ შეტევის განხორციელების შესახებ ინფორმაციას.

სოციალური მედიის ჰაკერები

სოციალური მედიის ჰაკერი იპარავს სოციალური ქსელის ანგარიშებს. მისი მიზანი შეიძლება იყოს შურისძიება, ან ინფორმაციის მიღება კონკრეტულ პირ(ებ)ზე.

იისფერქუდიანი ჰაკერები

იისფერქუდიანი ჰაკერების მიზანი საკუთარი ჰაკერული შესაძლებლობების შემოწმებაა. ამისათვის ისინი საკუთარი ერთი მოწყობილობიდან უტევენ მეორეს. აღნიშნული ითვლება საკმაოდ კარგ პრაქტიკად უნარ-ჩვევების განვითარების კუთხით.

ავტომატიზებული ინსტრუმენტები

ავტომატიზებული ინსტრუმენტი არის ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც ავტომატურ რეჟიმში ასრულებს იგივე ფუნქციას, რასაც ჰაკერი. წარმოდგენილია სხვადასხვა მავნე პროგრამული უზრუნელყოფის, ძირითადად ბოტნეტის, სახით.

ორგანიზებული ჰაკერები

ეს კრიმინალური სამყარო მოიცავს კიბერკრიმინალების, ჰაკტივისტების, ტერორისტებისა და სახელმწიფოს მიერ დაფინანსებული ჰაკერების ორგანიზაციებს. კიბერკრიმინალები, როგორც წესი, პროფესიონალი კრიმინალების ჯგუფები არიან, რომლებიც ორიენტირებულნი არიან კონტროლზე, ძალასა და სიმდიდრეზე. ეს კრიმინალები მოქმედებენ ძალიან დახვეწილად და ორგანიზებულად და შესაძლოა კიბერდანაშაულის მომსახურებაც კი უზრუნველყონ. ჰაკერი-აქტივისტები პოლიტიკურ განცხადებებს აკეთებენ იმისთვის, რომ მათთვის მნიშვნელოვანი საკითხები წინ წამოწიონ და მოახდინონ გავლენა ადამიანთა ცნობიერებაზე. ჰაკერი-აქტივისტები მსხვერპლთა შესახებ უხერხულ ინფორმაციას საჯაროდ აქვეყნებენ. სახელმწიფოს მიერ დაფინანსებული თავდამსხმელები იკრიბებიან დაზვერვის ან საბოტაჟის ჩადენის სახელით. ეს თავდამსხმელები, როგორც წესი, წარმოადგენენ მაღალკვალიფიციურ და კარგად ფინანსირებულ ძალას. მათი თავდასხმები ფოკუსირებულია კონკრეტულ მიზნებზე, რაც მათი ხელისუფლებისთვის სასარგებლოა. ზოგიერთი სახელმწიფოს მიერ დაფინანსებული ჰაკერი კი ამ ქვეყნის შეიარაღებული ძალების წევრიც კი შეიძლება იყოს.

კიბერკრიმინალური მოტივები

კიბერკრიმინალური პროფილები და მოტივები წლების განმავლობაში შეიცვალა. ჰაკეროზა დაიწყო გასული საუკუნის 60-იან წლებში, როდესაც ხდებოდა ტელეფონის სიხშირეებით მანიპულირება (phone freaking). 80-იანი წლების შუა რიცხვებში კრიმინალებმა გამოიყენეს dial-up მოდემები კომპიუტერულ ქსელებთან დაკავშირების მიზნით და შექმნეს პაროლის გატეხვის პროგრამები მონაცემთა ხელმისაწვდომობის მისაღებად. ამჟამად კრიმინალები მხოლოდ ინფორმაციის ქურდობას არ კმაყოფილდებიან. დამნაშავეებს ახლა შეუძლიათ გამოიყენონ მავნე პროგრამები და ვირუსები, როგორც მაღალტექნოლოგიური იარაღი. თუმცა, ყველაზე დიდი მოტივაცია კიბერდამნაშავეთა უმრავლესობისთვის ფინანსური მოგების მიღებაა. კიბერდანაშაული უფრო მომგებიანი გახდა, ვიდრე უკანონო ნარკოტიკებით ვაჭრობა.

კიბერუსაფრთოების სპეციალისტები

კიბერუსაფრთხოების სპეციალისტებზე მოთხოვნა უფრო მეტია, ვიდრე სხვა IT სამუშაო ადგილებზე. ყველა ტექნოლოგია, რომელიც გარდაქმნის სამყაროს და აუმჯობესებს ხალხის ცხოვრების წესს, უფრო დაუცველს ხდის თავდასხმების წინააღმდეგ. მხოლოდ ტექნოლოგია ვერ ახერხებს კიბერუსაფრთხოების ინციდენტების თავიდან აცილებას, გამოვლენას, რეაგირებას და აღდგენას. განვიხილოთ შემდეგი სარგებელი ამ სფეროში მოღვაწეობის შემთხვევაში:

კიბერუსაფრთხოების ეფექტური სპეციალისტისთვის საჭირო უნარ-ჩვევების დონე და კიბერუსაფრთხოების კვალიფიციური პროფესიონალების დეფიციტი მოითხოვს უფრო მაღალ მოსაპოვებელ პოტენციალს.

საინფორმაციო ტექნოლოგია მუდმივად იცვლება. ეს ასევე ეხება კიბერუსაფრთხოებას. კიბერუსაფრთხოების სფეროს უაღრესად დინამიური ხასიათი შეიძლება იყოს რთული და მომხიბლავი.

კიბერუსაფრთხოების სპეციალისტის კარიერა ასევე უაღრესად მოთხოვნადია. ამ სფეროში სამუშაო ადგილები მსოფლიოს ყველა რეგიონში არსებობს.

კიბერუსაფრთხოების სპეციალისტები უზრუნველყოფენ საჭირო მომსახურებას თავიანთი ორგანიზაციებისათვის, ქვეყნებისა და საზოგადოებისათვის, რითაც ისინი ძალიან ჰგვანან სამართალდამცავ ან საგანგებო რეაგენტებს.

კიბერუსაფრთხოების სპეციალისტად გახდომა გარკვეული ჯილდოა კარიერულ გამოწვევებში.

კიბერკრიმინალის აღკვეთა

კიბერდამნაშავეთა გამოვლენა რთული ამოცანაა და არ არსებობს მასთან ბრძოლის უნივერსალური მეთოდი. თუმცა, კომპანიებმა მთავრობებმა და საერთაშორისო ორგანიზაციებმა დაიწყეს კოორდინირებული ქმედებების განხორციელება კიბერდამნაშავეების შეზღუდვისა და აღკვეთის მიზნით. კოორდინირებული ქმედებები მოიცავს:

- ცნობილი სისტემის მოწყვლადობის და თავდასხმის ხელმოწერების ყოვლისმომცველი მონაცემთა ბაზების შექმნა (ინფორმაციის უნიკალური პლატფორმები, რომელიც გამოიყენება თავდამსხმელის მცდელობის იდენტიფიცირებისთვის ცნობილი მოწყვლადობის გამოყენების მიზნით). ორგანიზაციები აზიარებენ ამ მონაცემთა ბაზებს მსოფლიოს მასშტაბით, რათა დაეხმარონ სხვებს საბაზისო შეტევების თავიდან აცილებაში.
- ადრეული გაფრთხილების სისტემის ჩამოყალიბება ხდის ქსელებს ნაკლებად მოწყვლადად. ყველა არსებული ქსელის მონიტორინგის მაღალი ღირებულებისა და სირთულის გამო, ორგანიზაციები აკვირდებიან მაღალი ღირებულების მიზნებს ან ქმნიან ე.წ. იმპოსტერებს, რომლებიც ქმნიან მაღალი ღირებულების ცრუ სამიზნეებს. იმის გამო, რომ ეს მაღალი ღირებულების სამიზნეები უფრო მეტი ალბათობით არიან თავდასხმის ობიექტები, ისინი აფრთხილებენ სხვა კომპანიებს პოტენციური თავდასხმების თავისებურებების შესახებ.
- კიბერდაზვერვის ინფორმაციის გაზიარება. ბიზნესი, სამთავრობო უწყებები და ქვეყნები დღეისათვის თანამშრომლობენ კრიტიკულ სამიზნეებზე სერიოზული თავდასხმების შესახებ, რათა თავიდან აიცილონ მსგავსი

თავდასხმები სხვა ადგილებში. ბევრმა ქვეყანამ ჩამოაყალიბა კიბერსადაზვერვო სააგენტოები მსოფლიო მასშტაბით მსხვილი კიბერშეტევების წინააღმდეგ ბრძოლის მიზნით.

- ინფორმაციული უსაფრთხოების მართვის სტანდარტების დამკვიდრება ეროვნულ და საერთაშორისო ორგანიზაციებს შორის. ISO 27000 წარმოადგენს ამ საერთაშორისო ძალისხმევის კარგ მაგალითს.
- ახალი კანონების შემუშავება კიბერშეტევებისა და მონაცემების დარღვევის წინააღმდეგ. ეს კანონები ითვალისწინებს საკმაოდ დიდ ჯარიმებს კიბერდამნაშავეების წინააღმდეგ მათ მიერ განხორციელებული არალეგალური ქმედებების გამო.

1.3 კიბერსაფრთხეები ფიზიკურ პირების, ბიზნესისა და სახელმწიფო ორგანიზაციების წინაშე

საერთო საფრთხეები საბოლოო მომხმარებლებისთვის

არსებობენ ექსპერტები, რომლებიც ინოვატორები არიან. ისინი ქმნიან ინტერნეტის სხვადასხვა კიბერდომენებს. მათ აქვთ უნარი შეაფასონ მონაცემთა ძალა და გამოიყენონ ის გარკვეული მიზნით. შემდეგ ისინი ქმნიან თავიანთ ორგანიზაციებს და უზრუნველყოფენ მომსახურებას, ასევე იცავენ ადამიანებს კიბერშეტევებისგან. იდეალურ შემთხვევაში, კიბერუსაფრთხოების პროფესიონალებმა უნდა შეაფასონ საფრთხე, რომელიც იწვევს მონაცემების დაკარგვას და გამოიყენება ხალხის წინააღმდეგ.

საფრთხეებისა და მოწყვლადობის აღმოცენა კიბერუსაფრთხოების პროფესიონალების მთავარი საზრუნავია. ორი გარემოება განსაკუთრებით კრიტიკულია:

- როდესაც არსებობს შესაძლებლობა, რომ მავნე მოვლენა, როგორიცაა თავდასხმა, მოხდება;
- როდესაც დაუცველობა ხდის სამიზნეს პოტენციურ თავდასხმის ობიექტად.

მაგალითად, "ცუდ ხელში" მოხვედრილმა მონაცემებმა შეიძლება გამოიწვიოს მფლობელების კონფიდენციალურობის დაკარგვა, ასევე შეიძლება გავლენა იქონიოს მათი ინფორმაციის დაცვაზე ან საფრთხე შეუქმნის მათ კარიერას ან პირად ურთიერთობებს. პიროვნების

ქურდობა საკმაოდ გავრცელებული ბიზნესია. თუმცა, ეს არ არის აუცილებლად იყოს Googles და Facebook, რომლებიც დგანან ყველაზე დიდი რისკის წინაშე. სკოლები, საავადმყოფოები, ფინანსური ინსტიტუტები, სამთავრობო უწყებები, სამუშაო ადგილი და ელექტრონული კომერცია კიდევ უფრო დიდი რისკების ქვეშ არიან მოქცეულნი. ორგანიზაციებს, როგორიცაა Google და Facebook, გააჩნიათ რესურსი, რომ დაიქირავონ კიბერუსაფრთხოების საუკეთესო პროფესიონალები, რათა დაიცვან თავიანთი პლატფორმები. რაც უფრო მეტი ორგანიზაცია ქმნის დიდ მონაცემთა ბაზებს, რომლებიც შეიცავს ყველა ჩვენს პერსონალურ მონაცემს, მით უფრო იზრდება კიბერუსაფრთხოების პროფესიონალების საჭიროება. ეს შედარებით მცირე შანსს უტოვებს ბიზნესს და ორგანიზაციებს, რომლებიც იბრძვიან კიბერუსაფრთხოების პროფესიონალების დარჩენილი ნაწილისათვის. კიბერსაფრთხეები განსაკუთრებით საშიშია გარკვეული ინდუსტრიებისთვის და მათი მონაცემებისათვის.

პირადი ჩანაწერების სახეები

შემდეგი მაგალითები წარმოადგენენ მხოლოდ რამდენიმე წყაროს იმ მონაცემებისა, რომლებიც შეიძლება გენერირებულ იქნან არსებული ორგანიზაციების მიერ.

სამედიცინო ჩანაწერები

ექიმის კაბინეტში ყოველი ვიზიტის შედეგად იქმნება ელექტრონულ ჯანმრთელობის ჩანაწერი (EHR) გარკვეული ინფორმაციის დამატებით. ოჯახის ექიმისმიერ გამოწერილი რეცეპტი ხდება EHR-ის ნაწილი. EHR მოიცავს ინფორმაციას ფიზიკურ ჯანმრთელობის, ფსიქიკურ ჯანმრთელობისა და სხვა პერსონალურ ინფორმაციას, რომელიც შეიძლება არ იყოს დაკავშირებული სამედიცინო მონაცემებთან. მაგალითად, ადამიანი შესაძლოა მივიდეს ექიმთან ბავშვთან დაკავშირებული რეკომენდაციის მისაღებად. ეს შეიძლება აისახოს მის სამედიცინო ჩანაწერებში. სამედიცინო ისტორიისა და პირადი ინფორმაციის გარდა, EHR ასევე შეიძლება მოიცავდეს ინფორმაციას ამ პირის ოჯახის შესახებ. რამდენიმე კანონი უზრუნველყოფს პაციენტის მონაცემთა დაცვას.

სამედიცინო მოწყობილობები იყენებენ ღრუბლოვან პლატფორმას, რათა შესაძლებელი გახდეს მონაცემების უკაბელო გადაცემა, შენახვა და ჩვენება, როგორიცაა გულისცემის, სისხლის წნევა და შაქარი. ამ მოწყობილობებს შეუძლიათ შექმნან უზარმაზარი რაოდენობის მონაცემები, რომლებიც შეიძლება გახდეს სამედიცინო ჩანაწერის ნაწილი.

განათლების ჩანაწერები

განათლების ჩანაწერებში შედის ინფორმაცია ტესტირების ქულების, დასწრების, კურსების, ჯილდოების, ხარისხებისა და დისციპლინური ანგარიშების შესახებ. ეს ჩანაწერი ასევე შეიძლება მოიცავდეს საკონტაქტო ინფორმაციას, ჯანმრთელობისა და იმუნიზაციის ჩანაწერებს და სპეციალური განათლების ჩანაწერებს, მათ შორის ინდივიდუალური განათლების პროგრამებს.

დასაქმება და ფინანსური ჩანაწერები

დასაქმების ინფორმაცია შეიძლება შეიცავდეს ინფორმაციას წარსული დასაქმებისა და საქმიანობის შესახებ. დასაქმების ჩანაწერები ასევე შეიძლება შეიცავდეს მონაცემებს ხელფასისა და სადაზღვევო ინფორმაციის შესახებ. ფინანსური ჩანაწერები შეიძლება შეიცავდეს ინფორმაციას შემოსავლებისა და ხარჯების შესახებ. საგადასახადო ჩანაწერები შეიძლება შეიცავდეს ტრანზაქციებს, საკრედიტო ბარათის განცხადებებს, ბარათის დეტალებს და, ზოგადად, საბანკო ინფორმაციას.

ინტერნეტსერვისების საფრთხეები

არსებობს მრავალი ტექნიკური მომსახურება, რომელიც აუცილებელია ქსელის, და საბოლოო ჯამში, ინტერნეტის ფუნქციონირების უზრუნველსაყოფად. ეს მომსახურება მოიცავს მარშრუტიზაციას, მისამართებს, დომენის დასახელებას და მონაცემთა ბაზის მართვას. ეს მომსახურებები წარმოადგენენ მთავარ სამიზნეებს კიბერდამნაშავეებისთვის.

დამნაშავეები იყენებენ ე.წ. პაკეტურ მზვერავ პროგრამებს და მათ ინსტრუმენტებს ქსელში არსებულ მონაცემთა ნაკადების გასაკონტროლებლად. ეს იმას ნიშნავს, რომ ყველა სენსიტიური მონაცემი, როგორიცაა სახელები, პაროლები და საკრედიტო ბარათის ნომრები, რისკის ქვეშ იმყოფება. ე.წ.პაკეტური სნიფერები ახდენენ

ქსელის მონიტორინგს მასში არსებული მონაცემთა ტრაფიკის ხელში ჩაგდების მიზნით. კრიმინალებს ასევე შეუძლიათ გამოიყენონ rogue მოწყობილობები, როგორიცაა დაუცველი უსადენო (Wi-Fi) წვდომის წერტილები. თუ კრიმინალი მოქმედებს რომელიმე საჯარო ადგილის მახლობლად, როგორიცაა ყავის მაღაზია, მას შეუძლია მოიპაროს იმ ადამიანის პერსონალური ინფორმაცია, რომელიც უერთდება ქსელს და წარმოდგენა არ აქვს, რომ ხდება კრიმინალის მსხვერპლი..

დომენური სახელის სერვისი (DNS) ახდენს დომენური სახელის ტრანსლაციას, როგორიცაა www.facebook.com, მის რიცხვითი IP მისამართში. თუ DNS სერვერმა არ იცის IP მისამართი, ის აგზავნის მოთხოვნას სხვა DNS სერვერთან. DNS spoofing ნიშნავს, რომ კრიმინალი წარუდგენს ცრუ მონაცემების DNS-ის ქეშში. ეს ზიანის მომტანი თავდასხმები იყენებენ სისუსტეებს DNS პროგრამულ უზრუნველყოფაში, რომელნიც იწვევენ DNS სერვერების გადამისამართებას კრიმინალის მფლობელობაში მყოფი კონკრეტული დომენის კომპიუტერში, ნაცვლად ავთენტური დომენისა.

ზემოთ მოყვანილი მაგალითები მხოლოდ მცირე ნაწილია იმ კიბერდანაშაულებისა, რომელთაც კრიმინალები ჩადიან ინტერნეტსა და სხვა ქსელურ სერვისებში.

საფრთხეები მრეწველობის ძირითადი სექტორებისთვის

ძირითადი ინდუსტრიის სექტორები მოიცავენ ქსელის ინფრასტრუქტურულ სისტემებს, როგორიცაა წარმოება, ენერგია, კომუნიკაცია და ტრანსპორტირება. მაგალითად, ჭკვიანი ქსელი (smart grid) არის ელექტრული გენერაციისა და განაწილების სისტემის გაფართოება. ელექტრული ქსელი (electrical grid) მოიცავს ცენტრალურ გენერატორებს დიდი რაოდენობით მომხმარებელისათვის. ჭკვიანი ქსელი იყენებს ინფორმაციას ავტომატური მოწინავე ენერგომომარაგების ქსელის შესაქმნელად. მსოფლიო ლიდერები აღიარებენ, რომ მათი ინფრასტრუქტურის დაცვა კრიტიკულია საკუთარი ქვეყნების ეკონომიკის დასაცავად.

ბოლო ათწლეულის განმავლობაში, Stuxnet-ის მსგავსმა კიბერშეტევებმა დაამტკიცა, რომ კიბერშეტევას შეუძლია კრიტიკული ინფრასტრუქტურების წარმატებით განადგურება ან შეწყვეტა. კერძოდ, Stuxnet-ის თავდასხმა მიზნად ისახავდა სამეთვალყურეო კონტროლისა და მონაცემთა შეძენის (SCADA) სისტემასთან წვდომის

მოპოვებას, რომელიც გამოიყენება სამრეწველო პროცესების კონტროლისა და მონიტორინგის მიზნით. SCADA შეიძლება იყოს სხვადასხვა სამრეწველო პროცესების ნაწილი წარმოების, წარმოების, ენერგეტიკისა და საკომუნიკაციო სისტემებში.

კიბერშეტევას შეეძლო ჩამოეშალა ან საგრძნობლად დაეზიანებინა ინდუსტრიული სექტორები, როგორიცაა სატელეკომუნიკაციო, ტრანსპორტირების ან ელექტროენერგიის გამომუშავებისა და განაწილების სისტემები. მას ასევე შეეძლო საფრთხე შეექმნა ფინანსური მომსახურების სექტორისათვის. ერთ-ერთი პრობლემა გარემოში, რომელიც მოიცავს SCADA-ს არის ის ფაქტი, რომ შემქმნელებმა SCADA არ დაუკავშირეს ტრადიციულ IT გარემოსა და ინტერნეტს. აქედან გამომდინარე, ამ სისტემების განვითარების ფაზაში ისინი სათანადოდ არ განიხილავდნენ კიბერუსაფრთხოებას. სხვა ინდუსტრიების მსგავსად, SCADA სისტემების გამოყენებით ორგანიზაციები აღიარებენ მონაცემთა შეგროვების ღირებულებას ოპერაციების გაუმჯობესებისა და ხარჯების შემცირების მიზნით. შედეგად მიღებული ტენდენციაა SCADA სისტემების ტრადიციული IT სისტემებთან დაკავშირება. თუმცა, ეს ზრდის მრეწველობის მოწყვლადობას SCADA სისტემების გამოყენების გამო.

თანამედროვე საფრთხის პოტენციალთან გამკლავება, რომელიც დღეს არსებობს, კიბერუსაფრთხოების ექსპერტთა სპეციალურ განსწავლას ითხოვს.

ადამიანებს ცხოვრების გზაზე თან სდევს გარკვეული საფრთხეები

კიბერუსაფრთხოება მუდმივად მოქმედი ძალისხმევაა ქსელური სისტემებსა და მონაცემებზე არასანქცირებული წვდომისგან დასაცავად. პირად დონეზე, ყველას უნდა დაიცვას თავისი იდენტობა, მონაცემები და კომპიუტერული მოწყობილობები. კორპორატიულ დონეზე დასაქმებულთა პასუხისმგებლობაა ორგანიზაციის რეპუტაციის, მონაცემებისა და მომხმარებლების დაცვა. სახელმწიფო დონეზე, ეროვნული უსაფრთხოება და მოქალაქეთა უსაფრთხოება და კეთილდღეობა შესაძლოა აღმოჩნდეს საფრთხეში.

კიბერუსაფრთხოების სპეციალისტები ხშირად მონაწილეობენ სამთავრობო უწყებებთან მუშაობის პროცესში მონაცემების იდენტიფიცირებისა და შეგროვების მიზნით.

აშშ-ში, ეროვნული უსაფრთხოების სააგენტო (NSA) პასუხისმგებელია სადაზვერვო ინფორმაციის შეგროვებასა და სათვალთვალო საქმიანობაზე. NSA-მ შექმნა ახალი მონაცემთა ცენტრი მზარდი მოცულობის ინფორმაციის დამუშავების მიზნით. 2015 წელს აშშ-ს კონგრესმა გამოსცა აქტი, რომელიც აღკვეთს აშშ-ს მოქალაქეთა სატელეფონო ჩანაწერების შეგროვების პრაქტიკას. პროგრამა ითვალისწინებდა მეტამონაცემებს, რომლის მეშვეობითაც NSA ინფორმაციას იღებდა გაცემული და მიღებული კომუნიკაციების შესახებ.

ხალხის ცხოვრების წესის დაცვის მცდელობა ხშირად ეწინააღმდეგება მათ კონფიდენციალურობის უფლებას. საინტერესო იქნება იმის დანახვა, თუ როგორია ბალანსი ამ უფლებებსა და ინტერნეტმომხმარებელთა უსაფრთხოებას შორის.

1.4 კიბერდანაშაულის გავრცელებისა და ზრდის ტენდენციები

შიდა და გარე საფრთხეები

შიდა უსაფრთხოების საფრთხეები

თავდასხმები შეიძლება წარმოიშვას ორგანიზაციის ფარგლებში ან ორგანიზაციის გარეთ. შიდა მომხმარებელი, როგორიცაა თანამშრომელი ან კონტრაქტორი, შეიძლება შემთხვევით ან განზრახ:

- ვერ გაუმკლავდეს კონფიდენციალური მონაცემების დაცვის მოთხოვნებს.
- საფრთხე შეუქმნას შიდა სერვერების ან ქსელური ინფრასტრუქტურული მოწყობილობების ოპერირებას.
- ხელი შეუწყოს გარე თავდასხმებს, ინფიცირებული USB მედია მატარებლის კორპორატიულ კომპიუტერულ სისტემაში გამოყენებით.
- შემთხვევით შემოუშვას სისტემაში ზიანის მომტანი პროგრამა ან გახსნას ვირუსული გზავნილი ელექტრონული ფოსტით.

შიდა საფრთხეებს აქვთ იმის პოტენციალი, რომ უფრო მეტი ზიანი მიაყენოს სისტემას, ვიდრე გარე საფრთხეებმა, რადგან შიდა მომხმარებლებს აქვთ პირდაპირი წვდომა შენობაში შიდა ინფრასტრუქტურულ მოწყობილობებზე. შიდა თავდამსხმელებს, როგორც წესი, გააჩნიათ კორპორატიული ქსელის ცოდნა და წვდომა

აქვთ მის კონფიდენციალურ მონაცემებზე. მათ ასევე შეიძლება ჰქონდეთ უსაფრთხოების კონტრზომების, პოლიტიკისა და ადმინისტრაციული პრივილეგიების უმაღლესი დონის ცოდნა.

გარე შეტევათა საფრთხეები

გარე საფრთხეები შესაძლოა შექმნან მოყვარულებმა ან გამოცდილმა თავდამსხმელებმა, გამოიყენონ რა ქსელში არსებული მოწყვლადობა ან გამოიყენონ სოციალური ინჟინერია ქსელურ რესურსებზე წვდომისათვის. გარე თავდასხმელები იყენებენ ქსელში არსებულ სისუსტეებს ან ხარვეზებს შიდა რესურსებზე ხელმისაწვდომობის მისაღებად.

ტრადიციული მონაცემები

კორპორატიული მონაცემები მოიცავს პერსონალის ინფორმაციას, ინტელექტუალურ საკუთრებას და ფინანსურ მონაცემებს. პერსონალის ინფორმაცია მოიცავს განაცხადის მასალებს, სახელფასო, შეთავაზების წერილებს, თანამშრომლის შეთანხმებებს და დასაქმების გადაწყვეტილებების მიღებისას გამოყენებულ ნებისმიერ ინფორმაციას. ინტელექტუალური საკუთრება, როგორიცაა პატენტები, სავაჭრო ნიშნები და ახალი პროდუქტის გეგმები, საშუალებას აძლევს ბიზნესს მოიპოვოს ეკონომიკური უპირატესობა მის კონკურენტებზე. განვიხილოთ ეს ინტელექტუალური საკუთრება, როგორც სავაჭრო საიდუმლო - ამ ინფორმაციის დაკარგვა შეიძლება დამღუპველი იყოს კომპანიის მომავლისთვის. ფინანსური მონაცემებია, მაგალითად, შემოსავლის ანგარიშგება, ბალანსი და ფულადი სახსრების ანგარიშგება.

მობილური მოწყობილობების მოწყვლადობა

წარსულში, თანამშრომლები, როგორც წესი, იყენებდნენ კომპანიის მიერ მიწოდებულ კომპიუტერებს, რომლებიც დაკავშირებული იყო კორპორატიულ LAN- თან. ადმინისტრატორები მუდმივად აკონტროლებდნენ და ანახლებდნენ ამ კომპიუტერებს უსაფრთხოების მოთხოვნების დასაკმაყოფილებლად. დღეს, მობილური მოწყობილობები, როგორიცაა სმარტფონები, ტაბლეტები და ათასობით სხვა მოწყობილობა, ნელ-ნელა ანაცვლებენ ტრადიციულ პერსონალურ კომპიუტერებს. უფრო და უფრო მეტი ადამიანი იყენებს ამ მოწყობილობებს ინფორმაციის დამუშავებისთვის. საკუთარი

მოწყობილობების გამოყენება (BYOD) წარმოადგენს მზარდ ტრენდს. მობილური მოწყობილობების ცენტრალიზებული მართვისა და განახლების უუნარობა საფრთხეს უქმნის ორგანიზაციებს, რომლებიც საშუალებას აძლევენ დასაქმებულ პერსონალს, გამოიყენოს მობილური მოწყობილობები თავიანთ ქსელებში.

ნივთების ინტერნეტის (Internet of Things) გამოჩენა

ნივთების (საგანთა) ინტერნეტი (IoT) არის ტექნოლოგიების ერთობლიობა, რომელიც საშუალებას გვაძლევს, დავაკავშიროთ ინტერნეტში სხვადასხვა მოწყობილობები. IoT-ის სამყაროსთან დაკავშირებული ტექნოლოგიური პროცესები ვითარდება კომერციულ და სამომხმარებლო გარემოში. IoT ტექნოლოგიები საშუალებას აძლევს ადამიანებს დაუკავშირდნენ მილიარდობით მოწყობილობას ინტერნეტში. ეს მოწყობილობები მოიცავს ტექნიკას, ბლოკებს, ძრავებს და გასართობ მოწყობილობებს, და ეს მხოლოდ მცირე ნაწილია. ეს ტექნოლოგია გავლენას ახდენს მონაცემთა რაოდენობაზე, რომელიც საჭიროებს დაცვას. მომხმარებლები ამ მოწყობილობებს დისტანციურად უკავშირდებიან, რაც ზრდის ქსელების რაოდენობას, რომელიც მოითხოვს დაცვას.

IoT- ის წარმოქმნით, ბევრად უფრო მეტი მონაცემების მართვა და უზრუნველყოფა ხდება საჭირო. ყველა ეს კავშირი, პლუს გაფართოებული შენახვის მოცულობა და შენახვის მომსახურება, რომელიც იყენებს Cloud ტექნოლოგიებსა და ვირტუალიზაციას, იწვევს მონაცემების ექსპონენციალურ ზრდას. ამ მონაცემების გაფართოებამ შექმნა ტექნოლოგიებისა და ბიზნესის ინტერესის ახალი სფერო სახელწოდებით „დიდი მონაცემები“.

დიდი მონაცემების გავლენა

დიდი მონაცემები არის რთულად დასამუშავებელ მონაცემთა დაგროვების შედეგი, რომლისთვისაც დამუშავების მეთოდები ტრადიციული შეუსაბამოა. დიდი მონაცემები ქმნიან გამოწვევას და შესაძლებლობებს სამი განზომილების საფუძველზე:

- მონაცემთა მოცულობა
- მონაცემთა დაგროვების სიხშირე ან სიჩქარე
- მონაცემთა ტიპებისა და წყაროების მრავალფეროვნება და სპექტრი

არსებობს უამრავი მაგალითი დიდ კორპორატიულ კომპანიებზე ჰაკერული შეტევებისა. კომპანიები, როგორიცაა Target, Home Depot და PayPal ხშირად ხდებიან სუბიექტები სახიფათო თავდასხმებისა. შედეგად, მათი სისტემები საჭიროებს სიღრმისეულ ცვლილებებს უსაფრთხოების პროდუქტის შემუშავებაში და მნიშვნელოვან განახლებებს ტექნოლოგიებსა და პრაქტიკებში. გარდა ამისა, მთავრობები და მეწარმეები უფრო მეტ რეგულაციებსა და მანდატებს ახორციელებენ, რომლებიც საჭიროებენ მონაცემთა დაცვასა და უსაფრთხოების კონტროლს, რათა გაუმჯობესდეს დიდი მონაცემების სრულფასოვანი დაცვა.

საფრთხის სირთულე

პროგრამული უზრუნველყოფის მოწყვლადობას დღეს იწვევს პროგრამირების შეცდომები, პროტოკოლის ხარვეზები ან სისტემური შეცდომები. კიბერკრიმინალები, როგორც წესი, იყენებენ ერთ-ერთ ზემოთხსენებულ მიზეზს. მაგალითად, შეტევათა დიდი რაოდენობა ეყრდნობა პროგრამულ კოდში წვდომას მისი გაუმართაობის მისაღწევად. ეს გაუმართაობა უზრუნველყოფს წვდომას პროგრამულ კოდში და იწვევს ინფორმაციის გაჟონვას.

დღეს კიბერშეტევები სულ უფრო და უფრო დახვეწილი ხდება. მოწინავე მუდმივი საფრთხე (APT) არის უწყვეტი კომპიუტერული ჰაკერული შეტევების სერია, რომელიც ხორციელდება სპეციფიურ ობიექტზე სკურპულოზური დაკვირვების ქვეშ. დამნაშავეები, როგორც წესი, ახორციელებენ APT-ს ბიზნეს ან პოლიტიკური მოტივებით. APT ხორციელდება ხანგრძლივი პერიოდის განმავლობაში მაღალი ხარისხის საიდუმლოების დაცვითა და დახვეწილი ზიანის მომტანი პროგრამული პროდუქტის გამოყენებით.

ალგორითმის შეტევებს შეუძლიათ თვალყური ადევნონ სისტემის თვითანგარიშგების მონაცემებს, როგორიცაა კომპიუტერის მიერ გამოყენებული ენერგია და მოპოვებულ ინფორმაციაზე დაყრდნობით შეარჩიონ სამიზნეები სისტემისათვის ზიანის მისაყენებლად. ალგორითმულ შეტევებს ასევე შეუძლიათ კომპიუტერის გადატვირთვა, დატვირთონ რა მაქსიმალურად მისი ოპერატიული მეხსიერება ან ცენტრალური პროცესორი. ალგორითმული თავდასხმები უფრო ძნელად გასაშიფრია, ვინაიდან ისინი იყენებენ

პროგრამებს, რომლებიც შემუშავებულნი არიან ენერგიის დაზოგვისა და სისტემის ეფექტურობის გაზრდის მიზნით.

საბოლოოდ, ახალი თაობის თავდასხმები მოიცავს მსხვერპლთა ინტელექტუალურ შერჩევას. წარსულში თავდასხმები მიმართული იყო ადვილად გასაშიფრ ან ყველაზე დაუცველ მსხვერპლისადმი. თუმცა, ვინაიდან კიბერშეტევების გამოვლენასა და იზოლაციას უფრო დიდი ყურადღება ექცევა, კიბერდამნაშავეებს მართებთ უფრო დიდი სიფრთხილე. ისინი ვერ რისკავენ ადრეულ გამოვლენას, ვინაიდან კიბერუსაფრთხოების სპეციალისტები აღკვეთენ მათ ქმედებებს. შედეგად, ბევრი უფრო დახვეწილი თავდასხმა დაიწყება მხოლოდ იმ შემთხვევაში, თუ თავდამსხმელი შეძლებს შეუსაბამოს თავისი ქმედება დასახულ მიზანს.

ფართო მასშტაბი და კასკადის ეფექტი

საზიარო ავტორიზაციის მართვა ეხება სერვისებზე იმ ტიპის ავტორიზაციას, როდესაც მომხმარებლები გამოიყენონ იგივე საიდენტიფიკაციო მონაცემებს, რომლითაც სარგებლობენ სხვა სერვისებზე. მაგ.: YouTube სისტემაში ავტორიზაცია Google ანგარიშით.

საზიარო ავტორიზაციის მართვის მიზანია ავტორიზაციის ინფორმაციის გავრცელება სხვადასხვა პოპულარულ და მძლავრ სისტემებში ინდივიდუალური მომხმარებლის პერსპექტივით.

უსაფრთხოების შედეგები და მათი ამოცნობა

აშშ-ში გადაუდებელი დახმარების სატელეფონო ცენტრები მოწყვლადნი არიან კიბერშეტევების გამო, რომლებსაც შეუძლიათ გამოიწვიონ 911 ქსელის დაზიანება და საფრთხე შეუქმნან საზოგადოებრივ უსაფრთხოებას. სატელეფონო მომსახურების წყვეტის (TDoS) თავდასხმა იყენებს სატელეფონო ზარებს სამიზნე სატელეფონო ქსელის წინააღმდეგ, რომელიც ზღუდავს სისტემას და ხელს უშლის ავთენტური ზარების მიღებას. ახალი თაობის 911 სატელეფონო ცენტრები დაუცველნი არიან, რადგან ისინი იყენებენ Voice-over-IP (VoIP) სისტემებს, ნაცვლად ტრადიციული landlines სისტემებისა. გარდა TDoS თავდასხმებისა, ეს სატელეფონო ცენტრები ასევე შეიძლება აღმოჩნდნენ რისკის ქვეშ განაწილებული მომსახურების წყვეტის (DDoS) თავდასხმების გამოც, რომლებიც ცდილობენ გახადონ სამიზნე მიუწვდომელი ლეგიტიმური

მომხმარებლებისათვის. დღეს უკვე მრავალი გზა არსებობს 911 დახმარების მოთხოვნისა, მაგ.:სმარტფონის აპლიკაციის გამოყენებით, სახლის უსაფრთხოების სისტემის გამოყენებით და სხვა.

კიბერშეტევათა ეპოქის დაწყებისას კიბერშეტევების წინააღმდეგ თავდაცვა დაბალი დონის იყო. ჭკვიანი საშუალო სკოლის მოსწავლეს ან სკრიპტერის მიერ შექმნილ აპლიკაციას ადვილად შეეძლო სისტემაში შეღწევა. ქვეყნები მთელს მსოფლიოში უფრო მეტად აცნობიერებენ კიბერშეტევების საფრთხეს. კიბერშეტევებით გამოწვეული საფრთხე ახლა მსოფლიოს უმეტეს ქვეყნებში ეროვნული და ეკონომიკური უსაფრთხოების უდიდესი გამოწვევების ჩამონათვალში შედის.

1.5 ორგანიზაციების ძალისხმევა კიბერუსაფრთხოების წინააღმდეგ

აშშ-ში სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST) კიბერუსაფრთხოების პროფესიონალების საჭიროების მქონე კომპანიებისა და ორგანიზაციებისთვის ჩარჩო შექმნა. ჩარჩო საშუალებას აძლევს კომპანიებს გამოავლინონ ძირითადი ტიპის პასუხისმგებლობა, სამუშაო პოზიციები და სამუშაო ძალის უნარები. კიბერუსაფრთხოების სამუშაო ძალის ეროვნული ჩარჩო აღწერს კიბერუსაფრთხოების სპეციალობებს. იგი წარმოადგენს საერთო მონახაზს, რომელიც განსაზღვრავს ცოდნასა და უნარებს, რომლებიც აუცილებელია კიბერუსაფრთხოების სპეციალისტად ჩამოყალიბებისათვის. ჩარჩო ხელს უწყობს კიბერუსაფრთხოების სფეროში პროფესიული მოთხოვნების განსაზღვრას.

კიბერუსაფრთხოების ეროვნული სამუშაო ძალის ჩარჩო

სამუშაო ძალის ჩარჩო ჰყოფს კიბერუსაფრთხოების სამუშაოებს შვიდ კატეგორიად.

- ფუნქციონირება და შენარჩუნება მოიცავს მხარდაჭერას, ადმინისტრაციას და შენარჩუნებას, რომელიც საჭიროა IT სისტემის მუშაობისა და უსაფრთხოების უზრუნველსაყოფად.
- დაცვა და უსაფრთხოება მოიცავს შიდა სისტემებისა და ქსელების საფრთხეების იდენტიფიცირებას, ანალიზს და შემსუბუქებას.

- გამოძიება მოიცავს კიბერინციდენტების და კიბერდანაშაულების გამოძიებას.
- შეგროვება და ფუნქციონირება მოიცავს სპეციალიზებულ მომსახურებაზე უარის თქმის და მოტყუებითი ოპერაციების გამოვლენას და კიბერუსაფრთხოების ინფორმაციის შეგროვებას.
- ანალიზი მოიცავს მაღალკვალიფიციურ მიმოხილვას და ინფორმაციის შეფასებას, რათა დადგინდეს, არის თუ არა ეს სასარგებლო დაზვერვისთვის.
- ზედამხედველობა და განვითარება უზრუნველყოფს კიბერუსაფრთხოების მუშაობის ეფექტურად წარმართვას და ზედამხედველობას.
- უსაფრთხოების უზრუნველყოფა მოიცავს უსაფრთხო IT სისტემების კონცეპტუალიზაციას, დაპროექტებას და მშენებლობას.

თითოეულ კატეგორიაში არსებობს რამდენიმე სპეციალობის სფერო. სპეციალობის სფეროები შემდეგ განსაზღვრავენ კიბერუსაფრთხოების საერთო ტიპებს.

კიბერუსაფრთხოების ონლაინ საზოგადოებები

კიბერუსაფრთხოების სპეციალისტებმა ხშირად უნდა ითანამშრომლონ კოლეგებთან. საერთაშორისო ტექნოლოგიური ორგანიზაციები ხშირად აფინანსებენ და სპონსორობას უწევენ სამუშაო შეხვედრებსა და კონფერენციებს. ეს ორგანიზაციები ხშირად ახდენენ კიბერუსაფრთხოების პროფესიონალების შთაგონებასა და მოტივირებას.

CERT – Computer Emergency Response Team

სურ.1. 4.CERT

კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CERT) არის აშშ-ის ფედერალური ბიუროს მიერ დაფინანსებული ინიციატივა, რომელიც მიზნად ისახავს ინტერნეტსაზოგადოებასთან მუშაობას კომპიუტერული უსაფრთხოების ინციდენტების გამოვლენისა და მოგვარების მიზნით. CERT საკოორდინაციო ცენტრი (CERT/CC) კოორდინაციას

უწევს ექსპერტებს უსაფრთხოების საგანგებო სიტუაციების დროს, რათა მომავალში თავიდან იქნას აცილებული არასასიამოვნო ინციდენტები. CERT ასევე ახდენს რეაგირებას უსაფრთხოების ინციდენტებზე და ახორციელებს პროდუქტის მოწყვლადობის ანალიზს. CERT მართავს ცვლილებებს, რომლებიც ეხებიან განვითარებად შეღწევის სისტემებს და თავდასხმათა აღმოჩენის სირთულეებს და თავდამსხმელთა დაკავებას. ის ასევე ავითარებს შესაბამისი ტექნოლოგიებისა და სისტემების გამოყენებას ქსელებზე თავდასხმათა წინააღმდეგ ბრძოლაში, დანაკარგის შესამცირებლად და სერვისის შესანარჩუნებლად.

SANS

სურ.1. 5.SANS

სისტემური ადმინისტრირების, აუდიტის, ქსელის, უსაფრთხოების (SANS) ინსტიტუტის რესურსები დიდწილად უფასოა და მოიცავს პოპულარულ პლატფორმას, რომელიც აერთიანებს სიახლეებს, ადრეული გაფრთხილების სისტემას, ყოველკვირეულ საინფორმაციო დაიჯესტს, სერტიფიცრების სისტემას, კვლევით ნაშრომებს, უსაფრთხოების კურსებს და სხვა.

MITRE

სურ.1. 6.MITRE

Mitre Corporation შეიმუშავებს და მხარს უჭერს საერთო მოწყვლადობის და გამოვლინებების ჩამონათვალს (CVE), რომელიც გამოიყენება ცნობილი უსაფრთხოების ორგანიზაციების მიერ.

FIRST

სურ.1. 7.FIRST

ინციდენტებზე რეაგირებისა და უსაფრთხოების ჯგუფების ფორუმი (FIST) წარმოადგენს ორგანიზაციას, რომელიც აერთიანებს კომპიუტერული უსაფრთხოების ინციდენტების რეაგირების სხვადასხვა ჯგუფებს სამთავრობო, კომერციულ და საგანმანათლებლო ორგანიზაციებს შორის, რათა ხელი შეუწყოს თანამშრომლობას და კოორდინაციას ინფორმაციის გაზიარების, ინციდენტების პრევენციისა და სწრაფი რეაქციის მიზნით..

INFOSYSSEC

სურ.1. 8.INFOSYSSEC

ინფორმაციული სისტემების უსაფრთხოება (InfoSysSec) — ქსელური უსაფრთხოების ორგანიზაციაა, რომელიც განათავსებს უსაფრთხოების საინფორმაციო პორტალს, რომელიც, თავის მხრივ, უზრუნველყოფს შეტყობინებების, ექსპლოიტებისა და მოწყვლადობის უახლეს ამბებს.

ISC²

სურ.1. 9.ISC₂

საერთაშორისო საინფორმაციო სისტემების უსაფრთხოების სერტიფიცირების კონსორციუმი (ISC)² უზრუნველყოფს მწარმოებელზე დამოუკიდებელ განათლების პროდუქტებსა და კარიერულ მომსახურებას 135-ზე მეტ ქვეყანაში, 75,000+ სერტიფიცირებული ინდუსტრიის პროფესიონალებისთვის. მათი მისიაა კიბერსამყარო უსაფრთხო ადგილად გახადოს საზოგადოებრივ დომენში ინფორმაციული უსაფრთხოების ამაღლებითა და ქსელის უსაფრთხოების პროფესიონალების მხარდაჭერითა და განვითარებით მთელს მსოფლიოში. ისინი ასევე უზრუნველყოფენ ინფორმაციული უსაფრთხოების სერტიფიცირებას, მათ შორის სერტიფიცირებული საინფორმაციო სისტემების უსაფრთხოების პროფესიულ სერტიფიკატს (CISSP).

MS-ISAC

სურ.1. 10.MS-ISAC

MS-ISAC არის ამოსავალი წერტილი კიბერსაფრთხის პრევენციის, დაცვის, რეაგირებისა და აღდგენისა სახელმწიფო დონეზე, ადგილობრივი და ტერიტორიული (SLTT) მთავრობებისთვის. MS-ISAC 24x7 კიბერუსაფრთხოების ოპერაციების ცენტრი უზრუნველყოფს რეალურ დროში ქსელის მონიტორინგს, ადრეული კიბერსაფრთხის გაფრთხილებებსა და რჩევებს, მოწყვლადობის იდენტიფიცირებასა და შემსუბუქებას და ინციდენტზე რეაგირებას.

კიბერუსაფრთხოების სპეციალისტებს უნდა ჰქონდეთ იგივე უნარები, როგორც ჰაკერებს, განსაკუთრებით შავქუდიან ჰაკერებს, რათა დაიცვან თავიანთი ორგანიზაციები კიბერთავდასხმებისგან. როგორ უნდა გამოიმუშაოს სპეციალისტმა პრაქტიკაში საჭირო უნარ-ჩვევები და გახდეს კიბერუსაფრთხოების სპეციალისტი? სტუდენტური უნარების კონკურსები კარგი გზაა კიბერუსაფრთხოების ცოდნის, უნარებისა და შესაძლებლობების მისაღებად. კიბერუსაფრთხოების უნარების მქონე სტუდენტებისთვის ხელმისაწვდომია კიბერუსაფრთხოების მრავალი შეჯიბრება.

კიბერუსაფრთხოების სერტიფიკატები

კიბერსაფრთხეების სამყაროში არსებობს დიდი მოთხოვნა გამოცდილი და მცოდნე ინფორმაციული უსაფრთხოების პროფესიონალებზე. IT ინდუსტრიამ კიბერუსაფრთხოების სპეციალისტებისთვის დაამკვიდრა სტანდარტები და პროფესიული სერტიფიკატები, რომლებიც უზრუნველყოფენ უნარ-ჩვევებისა და ცოდნის დონის დადასტურებას.

CompTIA-ს უსაფრთხოები+

Security + არის CompTIA-ს მიერ დაფინანსებული ტესტირების პროგრამა, რომელიც ადასტურებს IT ადმინისტრატორების კომპეტენციას ინფორმაციის უზრუნველყოფის სფეროში. Security+ ტესტი მოიცავს ქსელის უზრუნველყოფისა და რისკის მართვის უმნიშვნელოვანეს პრინციპებს, მათ შორის ღრუბლოვან გამოთვლებთან დაკავშირებულ საკითხებს.

EC-საბჭოს მიერ სერტიფიცირებული ეთიკური ჰაკერი (CEH)

ეს შუალედური დონის სერტიფიცირება ამტკიცებს, რომ ამ სერტიფიკატის მქონე კიბერუსაფრთხოების სპეციალისტები ფლობენ სხვადასხვა ჰაკერულ პრაქტიკაში არსებულ უნარ-ჩვევებსა და ცოდნას. კიბერუსაფრთხოების ეს სპეციალისტები იყენებენ იგივე უნარებსა და ტექნიკას, რომელსაც კიბერდამნაშავეები იყენებენ სისტემის მოწყვლადობის და სისტემაში წვდომის წერტილების იდენტიფიცირების მიზნით.

SANS GIAC უსაფრთხოების სერტიფიცირება (GSEC)

GSEC სერტიფიცირება კარგი არჩევანია საწყისი დონის კიბერუსაფრთხოების სპეციალისტებისთვის, რომლებსაც შეუძლიათ იმის დემონსტრირება, რომ მათ ესმით უსაფრთხოების ტერმინოლოგია და ცნებები და აქვთ „პრაქტიკული“ უსაფრთხოების როლებისთვის საჭირო უნარ-ჩვევები და ექსპერტიზის უნარები. SANS GIAC პროგრამა გთავაზობთ დამატებით სერტიფიკატებს უსაფრთხოების ადმინისტრირების, სასამართლო ექსპერტიზის და აუდიტის სფეროებში.

(ISC)^2 სერტიფიცირებული ინფორმაციული სისტემების უსაფრთხოების პროფესიონალი (CISSP)

CISSP-ის სერტიფიცირება არის მწარმოებელზე დამოუკიდებელი სერტიფიცირება იმ კიბერუსაფრთხოების სპეციალისტებისთვის, რომლებსაც აქვთ დიდი ტექნიკური და მენეჯერული გამოცდილება. მას ასევე ფორმალურად ამტკიცებს აშშ-ის თავდაცვის დეპარტამენტს (DoD) და წარმოადგენს ინდუსტრიის გლობალურად აღიარებულ სერტიფიცირებას უსაფრთხოების სფეროში.

ISACA სერტიფიცირებული ინფორმაციული უსაფრთხოების მენეჯერი (CISM)

კიბერსპეციალისტებს, რომლებიც პასუხისმგებელნი არიან ინფორმაციული უსაფრთხოების სისტემების მართვაზე, განვითარებასა და ზედამხედველობაზე ორგანიზაციის მასშტაბით ან უსაფრთხოების საუკეთესო პრაქტიკის შემუშავებაზე, შეუძლიათ ისარგებლონ CISM-ით. ამ სერტიფიცირების მქონე სპეციალისტები ფლობენ მოწინავე უნარებს ინფორმაციული უსაფრთხოების რისკების მართვაში.

წარმატებული კიბერუსაფრთხოების სპეციალისტად გახდომისთვის პოტენციურმა კანდიდატმა უნდა შეისწავლოს ზოგიერთი უნიკალური მოთხოვნა. კანდიდატებმა უნდა შეძლონ საფრთხეებზე რეაგირება რაც შეიძლება სწრაფად. ეს იმას ნიშნავს, რომ სამუშაო საათები შეიძლება გარკვეულწილად არანორმირებული იყოს.

კიბერსპეციალისტები ასევე აანალიზებენ პოლიტიკას, ტენდენციებს და სადაზვერვო ინფორმაციას, რათა გაიგონ, რას ფიქრობენ კიბერდამნაშავეები.

შემდეგი რეკომენდაციები დაეხმარება კიბერუსაფრთხოების სპეციალისტებს მათი მიზნების მისაღწევად:

- სწავლა: შეისწავლეთ საფუძვლები IT კურსების გავლით. განაგრძეთ სწავლა სიცოცხლის ბოლომდე. კიბერუსაფრთხოება მუდმივად ცვალებადი სფეროა და კიბერუსაფრთხოების სპეციალისტებმა უნდა შეინარჩუნონ ცოდნის შესაბამისი დონე.
- სერტიფიკატები: ინდუსტრიის და კომპანიის მიერ დაფინანსებული სერტიფიკატები ორგანიზაციებისგან, როგორიცაა Microsoft და Cisco, ადასტურებს, რომ პირი ფლობს ცოდნას, რომელიც საჭიროა კიბერუსაფრთხოების სპეციალისტად დასაქმებისთვის.
- სტაჟირება: უსაფრთხოების სტაჟირების ძიება სტუდენტის მიერ მომავალი შესაძლებლობების მოძიების მიზნით.
- გაწევრიანდით პროფესიულ ორგანიზაციებში: ჩაერთეთ კომპიუტერული უსაფრთხოების ორგანიზაციებში, დაესწარით შეხვედრებს, კონფერენციებს და ფორუმებს და გაეცანით ექსპერტების ბლოგებს ცოდნის გასაღრმავებლად.

თავი 2: კიბერუსაფრთხოების „კუბი“

კიბერუსაფრთხოების პროფესიონალები საუკეთესოდ აღიწერებიან, როგორც კიბერსივრცის დამცველი ექსპერტები. ჯონ მაკკუმბერი წარმოადგენს ერთ-ერთ პირველ კიბერუსაფრთხოების ექსპერტს, რომელმაც განავითარა საყოველთაოდ გამოყენებული ჩარჩო სახელწოდებით McCumber Cube ან Cybersecurity Cube. ეს ჩარჩო გამოიყენება როგორც ინსტრუმენტი, ქსელების, დომენებისა და ზოგადად ინტერნეტის დაცვის მართვაში. კიბერუსაფრთხოების კუბი გარკვეულწილად რუბიკის კუბს ჰგავს.

კიბერუსაფრთხოების კუბის პირველი განზომილება მოიცავს ინფორმაციული უსაფრთხოების სამ პრინციპს. კიბერუსაფრთხოების პროფესიონალები განიხილავენ სამ პრინციპს, როგორც CIA-ს პირამიდას (ტრიადა). მეორე განზომილება განსაზღვრავს ინფორმაციის ან მონაცემების სამ მდგომარეობას. კუბის მესამე განზომილება განსაზღვრავს ექსპერტიზას, რომელიც აუცილებელია დაცვის უზრუნველსაყოფად. მათ ხშირად უწოდებენ კიბერუსაფრთხოების მცველთა სამ კატეგორიას.

2.1 კიბერუსაფრთხოების კუბის სამი განზომილება

უსაფრთხოების პრინციპები

კიბერუსაფრთხოების კუბის პირველი განზომილება განსაზღვრავს კიბერსივრცის დაცვის მიზნებს. პირველ განზომილებაში გამოვლენილი მიზნები ფუძემდებლურ პრინციპებს წარმოადგენს. ეს სამი პრინციპია კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა. პრინციპები უზრუნველყოფს ფოკუსირებას და საშუალებას აძლევს კიბერუსაფრთხოების ექსპერტს პრიორიტეტული გახდეს ნებისმიერი ქსელური სისტემის დაცვისას.

კონფიდენციალობა ხელს უშლის ინფორმაციის გამჟღავნებას არასანქცირებული ადამიანების, რესურსების ან პროცესების მიმართ. მთლიანობა ეხება მონაცემების სიზუსტეს, თანმიმდევრულობას და სანდოობას. საბოლოოდ, ხელმისაწვდომობა უზრუნველყოფს, რომ ინფორმაცია წვდომადი იქნება უფლებამოსილი მომხმარებლების მიერ

საჭიროების შემთხვევაში. გამოვიყენოთ აკრონიმი CIA, რათა დავიმახსოვროთ ეს სამი პრინციპი.

მონაცემთა მდგომარეობები

კიბერსივრცე არის დომენი, რომელიც შეიცავს კრიტიკულად მნიშვნელოვანი მონაცემების მნიშვნელოვან რაოდენობას. შესაბამისად, კიბერუსაფრთხოების ექსპერტები ყურადღებას ამახვილებენ მონაცემთა დაცვაზე. კიბერუსაფრთხოების კუბის მეორე განზომილება ყურადღებას ამახვილებს კიბერსივრცეში არსებული მონაცემების მდგომარეობის დაცვის პრობლემებზე. მონაცემებს აქვს სამი შესაძლო მდგომარეობა:

- მონაცემები გადაცემაში (ტრანზიტში)
- დროებით გამოუყენებელი ან შენახული მონაცემები
- მიმდინარე მონაცემები

კიბერსივრცის დაცვა მოითხოვს კიბერუსაფრთხოების სპეციალისტების არსებობას, რათა მათ უზრუნველყონ სამივე მდგომარეობაში არსებული მონაცემების დაცვა.

კიბერუსაფრთხოების გარანტიები

კიბერუსაფრთხოების კუბის მესამე განზომილება განსაზღვრავს კიბერუსაფრთხოების პროფესიონალის უნარებსა და მოთხოვნებს, რომელსაც შეუძლია კიბერსივრცის დაცვა. კიბერუსაფრთხოების პროფესიონალებმა უნდა გამოიყენონ კიბერსივრცეში არსებული მონაცემების დაცვისას მათთვის ხელმისაწვდომი სხვადასხვა უნარებისა და დისციპლინების სპექტრი. მათ ეს უნდა გააკეთონ კანონის სრული დაცვით.

კიბერუსაფრთხოების კუბი განსაზღვრავს სამი სახის უნარებსა და დარგებს, რომლებიც გამოიყენება დაცვის უზრუნველსაყოფად. პირველი უნარი მოიცავს საინფორმაციო სისტემების დასაცავად არსებულ ტექნოლოგიებს, მოწყობილობებსა და პროდუქტებს კიბერდამნაშავეების გამოსავლენად. კიბერუსაფრთხოების პროფესიონალებს გააჩნიათ რეპუტაცია მათ ხელთ არსებული ტექნოლოგიური ინსტრუმენტების დაუფლებისთვის. თუმცა მაკკუმბერი შეახსენებს მათ, რომ მხოლოდ ტექნოლოგიური იარაღები საკმარისი არ არის კიბერდამნაშავეების დასამარცხებლად. კიბერუსაფრთხოების პროფესიონალებმა ასევე უნდა შექმნან ძლიერი

დაცვა პოლიტიკის, პროცედურებისა და სახელმძღვანელოების დადგენის გზით, რაც საშუალებას აძლევს კიბერსივრცის მომხმარებლებს უსაფრთხოდ დარჩნენ და იმოქმედონ ოპტიმალური მეთოდებით. საბოლოოდ, კიბერსივრცის მომხმარებლებმა უნდა გაიღონ მეტი ძალისხმევა, რათა გაიღრმავონ ცოდნა კიბერსივრცის დაცვის საკითხებში და დაამკვიდრონ წინსვლისა და განვითარების კულტურა.

2.2 CIA ტრიადა - კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის პრინციპები

კონფიდენციალურობის პრინციპი

კონფიდენციალურობა აღკვეთს ინფორმაციის გამჟღავნებას არასანქცირებული ადამიანების, რესურსებისა და პროცესების მიმართ. ორგანიზაციები ზღუდავენ ხელმისაწვდომობას იმის უზრუნველსაყოფად, რომ მხოლოდ ავტორიზებულ პირებს შეეძლოთ გამოიყენონ მონაცემები ან სხვა ქსელური რესურსები. მაგალითად, პროგრამისტს არ უნდა ჰქონდეს წვდომა ყველა თანამშრომლის პირად ინფორმაციაზე.

ორგანიზაციებმა უნდა მოამზადონ თანამშრომლები საუკეთესო პრაქტიკის შესაბამისად, რაც უზრუნველყოფს მგრძნობიარე ინფორმაციის დაცვას საკუთარ თავსა და ორგანიზაციაზე თავდასხმებისგან დასაცავად. კონფიდენციალურობის უზრუნველსაყოფად გამოყენებული მეთოდები მოიცავს მონაცემთა დაშიფვრის, ავტორიზაციისა და წვდომის მართვას.

მონაცემთა კონფიდენციალურობის დაცვა

ორგანიზაციები აგროვებენ დიდი რაოდენობით მონაცემებს. ამ მონაცემების დიდი ნაწილი არ არის სენსიტიური, რადგან საჯაროდ ხელმისაწვდომია, როგორც სახელები და ტელეფონის ნომრები. თუმცა, სხვა მონაცემები შესაძლოა იყოს, სენსიტიური. სენსიტიური ინფორმაცია წარმოადგენს მონაცემებს, რომლებიც დაცულნი არიან არასანქცირებული წვდომისგან, რათა უზრუნველყონ ინდივიდის ან ორგანიზაციის დაცვა. არსებობს სამი სახის სენსიტიური ინფორმაცია:

- ✓ პერსონალური ინფორმაცია წარმოადგენს პირადად ამოცნობად ინფორმაციას (PII), რომელიც შესაძლებლობას იძლევა განხორციელდეს ინდივიდის თვალთვალი.
- ✓ სამსახურებრივი ინფორმაცია არის ინფორმაცია, რომელიც მოიცავს ყველაფერს, რაც საფრთხეს უქმნის ორგანიზაციას, თუ ის აღმოჩენილი იქნება არაავტორიზებული პირის ან კონკურენტის მიერ.
- ✓ საიდუმლო ინფორმაცია წარმოადგენს ინფორმაციას, რომელიც მიეკუთვნება სახელმწიფო ორგანოს და კლასიფიცირებულია მისი სენსიტიურობის დონის მიხედვით.

წვდომის მართვა

წვდომის მართვა განსაზღვრავს რიგი დაცვის სქემებს, რომლებიც აღკვეთენ კომპიუტერის, ქსელის, მონაცემთა ბაზის ან სხვა მონაცემთა რესურსების არასანქცირებულ წვდომას. AAA-ს ცნებები მოიცავს უსაფრთხოების სამ დონეს: ავთენტიფიკაცია, ავტორიზაცია და აღრიცხვა. ეს მომსახურება უზრუნველყოფს ხელმისაწვდომობის კონტროლის ძირითად ჩარჩოებს.

პირველი “A” AAA-ში წარმოადგენს ავთენტიფიკაციას. ავთენტიფიკაცია ადასტურებს მომხმარებლის ვინაობას არასანქცირებული წვდომის თავიდან ასაცილებლად. მომხმარებელი ადასტურებს თავის ვინაობას მომხმარებლის პაროლით ან პირადობის მოწმობით. გარდა ამისა, მომხმარებლებს ესაჭიროებათ გადაამოწმონ მათი ვინაობა შემდეგი ნაბიჯებით:

- რაიმე, რაც მათ იციან (როგორიცაა პაროლი)
- რაიმე, რაც მათ აქვთ (როგორიცაა ბარათი)
- რაიმე, რაც მხოლოდ მათი პირადულია (როგორიცაა თითის ანაბეჭდი)

მაგალითად, თუ ბანკომატიდან ნაღდი ფულის ასაღებად მიდიხართ, საჭიროა თქვენი საბანკო ბარათი (რაღაც გაქვთ) და თქვენ უნდა იცოდეთ PIN. ეს ასევე წარმოადგენს მულტიფაქტორული ავტორიზაციის მაგალითს. მულტიფაქტორული ავტორიზაცია მოითხოვს ერთზე მეტი ტიპის ავტორიზაციას. ავტორიზაციის ყველაზე პოპულარული ფორმა პაროლების გამოყენებაა.

ავტორიზაციის მომსახურება განსაზღვრავს, თუ რომელი რესურსების მომხმარებლებს შეუძლიათ ისარგებლონ იმ ოპერაციებთან ერთად, რომლებიც მომხმარებლებს შეუძლიათ შეასრულონ. ზოგიერთი სისტემა ამას ახორციელებს წვდომის მართვის სიის ან ACL(Access Control List)-ის გამოყენებით. ACL განსაზღვრავს, გააჩნია თუ არა მომხმარებელს გარკვეული წვდომის პრივილეგიები ავტორიზაციის განხორციელების შემდეგ. მხოლოდ იმიტომ, რომ თქვენ გაგაჩნიათ უფლება შეხვიდეთ კორპორატიულ ქსელში, არ ნიშნავს იმას, რომ თქვენ გაქვთ მაღალსიჩქარიანი ფერადი პრინტერის გამოყენების ნებართვა. ავტორიზაციის პროცესს ასევე შეუძლია გააკონტროლოს, რა შემთხვევაში აქვს მომხმარებელს კონკრეტულ რესურსთან ხელმისაწვდომობა. მაგალითად, თანამშრომლებს შეიძლება ჰქონდეთ სამუშაო საათებში გაყიდვების მონაცემთა ბაზის ხელმისაწვდომობა, მაგრამ სისტემა გააუქმებს ამ წვდომას რამდენიმე საათის შემდეგ.

აღრიცხვა თვალს ადევნებს იმას, რასაც მომხმარებლები აკეთებენ, მათ შორის, გარკვეულ რესურსებზე წვდომას, რესურსებზე ხელმისაწვდომობას მოცემულ საათებში და ნებისმიერ განხორციელებულ ცვლილებას. მაგალითად, ბანკი ინახავს თითოეული მომხმარებლის მიერ განხორციელებული მოქმედების შესახებ ინფორმაციას. ამ სისტემის აუდიტს შეუძლია გამოავლინოს ყველა ტრანზაქციის დრო და ოდენობა და სისტემის თანამშრომელი, რომელმაც განახორციელა მოცემული ტრანზაქცია. კიბერუსაფრთხოების აღრიცხვითი მომსახურება ანალოგიურად მუშაობს. სისტემა აკონტროლებს მონაცემთა თითოეულ ტრანზაქციას და უზრუნველყოფს აუდიტის შედეგებს. ადმინისტრატორს შეუძლია შექმნას კომპიუტერული პოლიტიკა, სისტემის აუდიტის გასააქტიურებლად.

AAA კონცეფცია მსგავსია საკრედიტო ბარათის გამოყენების სისტემისა. საკრედიტო ბარათი განსაზღვრავს, ვინ იყენებს მას, რა თანხა იქნა რეალიზებული და რა სერვისი იქნა გამოყენებული.

კიბერუსაფრთხოების სააღრიცხვო ოპერაციები ახდენს ქმედების მართვას და მონიტორინგს რეალურ დროში. საიტები, როგორიცაა Norse, აჩვენებენ თავდასხმებს რეალურ დროში შეგროვებული მონაცემების საფუძველზე, როგორც ნაწილს აღრიცხვის ან თვალთვალის სისტემისა.

კანონები და პასუხისმგებლობა

კონფიდენციალურობა და პრივატულობა ერთი შეხედვით, ურთიერთშემცვლელია, მაგრამ სამართლებრივი თვალსაზრისით, ისინი სხვადასხვა რამეს გულისხმობენ. პრივატული მონაცემების უმრავლესობა კონფიდენციალურია, მაგრამ ყველა კონფიდენციალური მონაცემი საკუთარი არაა. კონფიდენციალური ინფორმაციის ხელმისაწვდომობა ხდება სათანადო ავტორიზაციის დადასტურების შემდეგ. ფინანსური ინსტიტუტები, საავადმყოფოები, სამედიცინო მუშაკები, იურიდიული ფირმები და ბიზნესი კონფიდენციალურ ინფორმაციას ამუშავებენ. კონფიდენციალურ ინფორმაციას გააჩნია არასაჯარო სტატუსი. კონფიდენციალურობის შენარჩუნება უფრო ეთიკური მოვალეობაა.

კონფიდენციალურობა არის მონაცემების შესაბამისი გამოყენება. როდესაც ორგანიზაციები აგროვებენ მომხმარებელთა ან თანამშრომლების მიერ მოწოდებულ ინფორმაციას, მათ უნდა გამოიყენონ ეს ინფორმაცია მხოლოდ შესაბამისი მიზნებისათვის. ორგანიზაციების უმრავლესობა თხოვს მომხმარებელს ან თანამშრომელს, ხელი მოაწეროს განაცხადის ფორმას, რომელიც აძლევს ორგანიზაციის ნებართვას მონაცემების გამოყენების შესახებ.

ყველა კანონი, რომელიც ჩამოთვლილია ქვრმოთ, მოიცავს დებულებას კონფიდენციალურობის შესახებ, მიღებულს აშშ კანონების შესაბამისად. ამ კანონების უმრავლესობა არის მონაცემთა შეგროვების მასიური ზრდის პასუხი.

- 1974 წლის კონფიდენციალურობის აქტი
- ინფორმაციის თავისუფლების აქტი (FOAI)
- საოჯახო განათლების ჩანაწერები და კონფიდენციალურობის აქტი (FERОA)
- აქტი აშშ კომპიუტერული თაღლითობისა და ძალადობის შესახებ (CFAA)
- აშშ ბავშვთა კონფედენციალურობის დაცვის აქტი (COPPA)
- ვიდეოს კონფიდენციალურობის დაცვის აქტი (VPPA)
- ჯანმრთელობის დაზღვევის პორტაბელურობა და ანგარიშვალდებულება
- გრამ-ლეჩ-ბლილის აქტი (GLBA)
- აშშ საბანკო წესები და რეგულაციები

- გადახდის ბარათის ინდუსტრიის მონაცემთა უსაფრთხოების სტანდარტი (PCI DSS)
- სამართლიანი საკრედიტო ანგარიშგების აქტი (FCRA)

კონფიდენციალურობასთან დაკავშირებული წესების მზარდი რაოდენობა უწესებს დიდ პასუხისმგებლობას იმ ორგანიზაციებს, რომლებიც აგროვებენ და აანალიზებენ მონაცემებს. საერთო პოლიტიკების შემუშავება საუკეთესო საშუალებაა ორგანიზაციისთვის, რათა მათ მოახერხონ შეესაბამებოდნენ კონფიდენციალურობასთან დაკავშირებული კანონების მზარდ რაოდენობას.

- პერსონალური ინფორმაციის დაცვისა და ელექტრონული დოკუმენტების აქტი (კანადა)
- პერსონალური ინფორმაციის დაცვის აქტი (ჩინეთი)
- აქტი პერსონალური ინფორმაციის დაცვის შესახებ (იაპონია)
- მუხლი 8. ადამიანის უფლებათა ევროპული კონვენცია (გაერთიანებული სამეფო)

ამ პოლიტიკების შემუშავება ორგანიზაციებს საშუალებას აძლევს, განახორციელონ კონკრეტული წესები, პროცედურები და პროცესები მონაცემთა შეგროვების, შენახვისა და გაზიარების დროს.

მონაცემთა მთლიანობის პრინციპი

მთლიანობა არის მთელი სასიცოცხლო ციკლის განმავლობაში შეგროვებული მონაცემების სიზუსტე, თანმიმდევრულობა და სანდოობა. მთლიანობის კიდევ ერთი ტერმინია ხარისხი. მონაცემები განიცდიან შემდეგ ოპერაციებს, როგორიცაა მოძიება, შეცვლა, შენახვა, განახლება და გადაცემა. მონაცემები უნდა დარჩნენ შეუცვლელნი არასანქცირებული პირების მიერ ამ ოპერაციების განხორციელებისას.

მონაცემთა მთლიანობის უზრუნველსაყოფად გამოყენებული მეთოდები მოიცავს ჰეშირებას, მონაცემთა ვალიდურობის შემოწმებას, მონაცემთა სიზუსტის შემოწმებას და წვდომის მართვას. მონაცემთა მთლიანობის სისტემები შეიძლება შეიცავდეს ზემოთ ჩამოთვლილ მეთოდებს.

მონაცემთა მთლიანობის საჭიროება

მონაცემთა მთლიანობა ინფორმაციული უსაფრთხოების ფუნდამენტური კომპონენტია. მონაცემთა მთლიანობის საჭიროება

მერყეობს იმის მიხედვით, თუ როგორ იყენებს ორგანიზაცია მონაცემებს. მაგალითად, Facebook, როგორც წესი, არ ამოწმებს მონაცემებს, რომლებსაც მომხმარებლები აქვეყნებენ კედელზე. ბანკი ან ფინანსური ორგანიზაცია უფრო მაღალ მნიშვნელობას ანიჭებს მონაცემთა მთლიანობას, ვიდრე Facebook. გარიგებები და კლიენტების ანგარიშები უნდა იყოს ზუსტი. ჯანდაცვის ორგანიზაციაში მონაცემთა მთლიანობა შეიძლება იყოს სასიცოცხლოდ მნიშვნელოვანი.

მონაცემთა მთლიანობის დაცვა წარმოადგენს მუდმივ გამოწვევას ყველა ორგანიზაციისათვის. მონაცემთა მთლიანობის დაკარგვას შეუძლია გამოიწვიოს მთლიან მონაცემთა რესურსის არასაიმედოობა და საერთოდაც უსარგებლობა.

კრიტიკული დონე

ჯანდაცვისა და გადაუდებელი დახმარების სამსახურები:

- ყველა მონაცემი დამტკიცებულია და შემოწმებულია
- მონაცემები დამოწმებულია, რათა უზრუნველყოფილი იყოს სანდოობა
- მაგალითები მოიცავს ჯანდაცვისა და ფინანსურ ჩანაწერებს

მაღალი დონე

ელექტრონული კომერცია და ანალიტიკა:

- ყველა მონაცემი დამოწმებულია
- მონაცემები შემოწმებულია სანდოობის უზრუნველსაყოფად
- მაგალითები მოიცავს ორგანიზაციების მონაცემთა ბაზებს

საშუალო დონე

ონლაინ გაყიდვები და საძიებო სისტემები:

- შესრულებულია მცირე გადამოწმება
- მონაცემები არ არის სრულიად სანდო
- მონაცემები შეგროვებულია საჯაროდ გამოქვეყნებულ ფორმებთან

დაბალი დონე

დღიურები და პირადი განთავსების საიტები:

- მონაცემები შეიძლება არ იყოს დამოწმებული

- შინაარსის ნდობის დაბალი დონე
- მაგალითები მოიცავს საზოგადოებრივ აზრს და საჯარო ინფორმაციას

მთლიანობის შემოწმება

მთლიანობის შემოწმება არის მონაცემთა შეგროვების თანმიმდევრულობა (ფაილი, სურათი ან ჩანაწერი). მთლიანობის შემოწმება ახორციელებს პროცესს, რომელსაც ეწოდება hash ფუნქცია, და რომელიც ასრულებს მონაცემთა "სნეფშოთს" მცირე დროში. მთლიანობის შემოწმება იყენებს მიღებულ Snapshot-ს, რათა შეამოწმოს მონაცემების უცვლელობა.

საკონტროლო ჯამი წარმოადგენს hash ფუნქციის ერთ-ერთ მაგალითს. საკონტროლო ჯამი ადასტურებს ფაილების მთლიანობას ან სიმბოლოების სტრიქონებს, მას შემდეგ, რაც მოხდა მათი გადატანა ერთი მოწყობილობიდან მეორეზე ლოკალურ ქსელში ან ინტერნეტში. საკონტროლო ჯამი უბრალოდ აკონვერტირებს ინფორმაციის თითოეულ პორციას მის რიცხობრივ ღირებულებაში. მონაცემთა მთლიანობის შესამოწმებლად, მიმღები სისტემა მხოლოდ იმეორებს პროცესს. თუ ორი ჯამი თანაბარია, მონაცემები ითვლება ვალიდურად. თუ ისინი არ არიან თანაბარი, ეს აჩვენებს, რომ ცვლილება მოხდა გადაცემისას.

ბაზური ჰეშ-ფუნქციები მოიცავს: MD5, SHA-1, SHA-256, და SHA-512. ეს ჰეშ-ფუნქციები იყენებს კომპლექსურ მათემატიკურ ალგორითმებს. ჰეშირებული ჯამი გამოიყენება მხოლოდ შედარების მიზნით. მაგალითად, ფაილის გადმოტვირთვის შემდეგ, მომხმარებელს შეუძლია შეამოწმოს ფაილის მთლიანობა წყაროს ჰეშ ღირებულებების შედარებით ნებისმიერი ჰეშ კალკულატორის მიერ გენერირებული მიმღების ჰეშის ჯამთან.

ორგანიზაციები იყენებენ ვერსიის კონტროლს ავტორიზებული მომხმარებლების მიერ შემთხვევითი ცვლილებების თავიდან ასაცილებლად. ორ მომხმარებელს არ შეუძლია ერთი და იგივე ობიექტის განახლება. ობიექტები შეიძლება იყოს ფაილები, მონაცემთა ბაზის ჩანაწერები ან ოპერაციები. მაგალითად, დოკუმენტის გახსნისას პირველი მომხმარებელი უფლებამოსილია შეცვალოს ეს დოკუმენტი; მეორე პირს აქვს მხოლოდ წაკითხვის უფლება..

ზუსტი სარეზერვო ასლის შექმნა ხელს უწყობს მონაცემთა მთლიანობის შენარჩუნებას მონაცემების დაზიანების შემთხვევაში. ორგანიზაციამ უნდა დაადასტუროს თავისი სარეზერვო პროცესი, რათა უზრუნველყოს სარეზერვო ასლის მთლიანობა მონაცემთა დაკარგვამდე.

ავტორიზაცია განსაზღვრავს, თუ ვის აქვს ორგანიზაციის რესურსებზე წვდომა მათი საჭიროების მიხედვით. მაგალითად, ფაილზე ნებართვები და მომხმარებლის წვდომის მართვა უზრუნველყოფს იმ ფაქტს, რომ მხოლოდ გარკვეულ მომხმარებლებს შეუძლიათ შეცვალონ მონაცემები. ადმინისტრატორს შეუძლია შექმნას ნებართვა მხოლოდ ფაილის წაკითხვისთვის (read-only). შედეგად, ამ ფაილზე წვდომის პროცესში მომხმარებელი ვერ მოახდენს ფაილში რაიმე ცვლილებას.

ხელმისაწვდომობის პრინციპი

მონაცემთა ხელმისაწვდომობა არის პრინციპი, რომელიც აღწერს საინფორმაციო სისტემებისა და მომსახურების ხელმისაწვდომობის მხარდაჭერას ნებისმიერ დროს. კიბერშეტევები და სისტემური მტყუნებები ხელს უშლის საინფორმაციო სისტემებსა და სერვისებზე წვდომას. მაგალითად, კონკურენტის ვებ-გვერდზე ხელმისაწვდომობის შეწყვეტამ მასზე შეტევით შეიძლება უპირატესობა მიანიჭოს მის კონკურენტს. ეს მომსახურების წვდომის შეფერხების (DoS) თავდასხმები საფრთხეს უქმნის სისტემის ხელმისაწვდომობას და ხელს უშლის ლეგიტიმურ მომხმარებლებს ინფორმაციის სისტემებზე წვდომასა და გამოყენებაზე საჭიროების შემთხვევაში.

მეთოდები, რომლებიც გამოიყენება ხელმისაწვდომობის უზრუნველსაყოფად, მოიცავს სისტემის მხარდაჭერას, სისტემის სარეზერვო ასლების შექმნას, მის გაზრდილ მდგრადობას, ტექნიკის მხარდაჭერას, უახლესი ოპერაციული სისტემებსა და პროგრამულ უზრუნველყოფას, და ნათლად შემუშავებულ გეგმას შეტევის შედეგად დაზიანებული სისტემის უსწრაფესი აღდგენისა.

ხუთი ცხრიანი

ადამიანები ყოველდღიურ ცხოვრებაში იყენებენ სხვადასხვა საინფორმაციო სისტემებს. კომპიუტერები და საინფორმაციო სისტემები აკონტროლებენ კომუნიკაციებს, ტრანსპორტირებას და

პროდუქციის წარმოებას. ინფორმაციული სისტემების უწყვეტი ხელმისაწვდომობა აუცილებელია თანამედროვე ცხოვრებისათვის. ტერმინი მაღალი ხელმისაწვდომობა აღწერს სისტემებს, რომლებიც განკუთვნილია იმისათვის, რომ თავიდან იქნას აცილებული დროის მოცდენა სამუშაო პროცესში (downtime). მაღალი ხელმისაწვდომობა უზრუნველყოფს შედარებით მაღალ მწარმოებლობას. მაღალი ხელმისაწვდომობის სისტემები, როგორც წესი, მოიცავს სამ დიზაინის პრინციპს:

- აღმოფხვრავს ერთეულ მტყუნებებს

განსაზღვრეთ ყველა მოწყობილობა და კომპონენტი სისტემაში, რომელნიც გამოიწვევენ სისტემის გათიშვას, თუ ეს მოწყობილობა ან კომპონენტი დაზიანდება.

- უზრუნველყოფს საიმედო გადართვებს (crossover)

გადაჭარბებული დენის წყაროები, სარეზერვო დენის სისტემები და სარეზერვო საკომუნიკაციო სისტემები უზრუნველყოფენ საიმედო გადართვებს.

- გამოავლენს მტყუნებებს მათი მოხდენის შემთხვევაში

მოწყობილობათა და სისტემის აქტიური მონიტორინგი უზრუნველყოფს მრავალი სახის მოვლენის აღმოჩენას, მათ შორის სისტემისა და მოწყობილობის მტყუნებებს. მონიტორინგის სისტემებმა შეიძლება ასევე უზრუნველყონ სარეზერვო სისტემის ასლის შექმნის საჭიროება მარცხის შემთხვევაში.

მისი მიზანია ისეთ ექსტრემალურ პირობებში მუშაობის გაგრძელების უზრუნველყოფა, როგორიცაა მაგალითად კიბერთავდასხმა. ერთ-ერთი ყველაზე პოპულარული მაღალი ხელმისაწვდომობის პრაქტიკა ხუთი ცხრიანი (five nines). ხუთი ცხრიანი ნიშნავს 99.999% -ს. ეს იმას ნიშნავს, რომ სისტემის მოცდენა (downtime) უნდა იყოს ნაკლები, ვიდრე 5.26 წუთი წელიწადში.

ხელმისაწვდომობის უზრუნველყოფა

ორგანიზაციებს შეუძლიათ უზრუნველყონ ხელმისაწვდომობა შემდეგი ქმედებების განხორციელების გზით:

- ტექნიკური აპარატურის მხარდაჭერა
- ოპერაციული სისტემების განახლებები

- სარეზერვო ასლების ტესტირება
- კატასტროფიდან აღდგენის დაგეგმვა
- ახალი ტექნოლოგიების დანერგვა
- უჩვეულო აქტივობების მონიტორინგი
- ხელმისაწვდომობის ტესტირება

2.3 მონაცემთა შენახვა და დაცვა

შენახული მონაცემები ეხება მონაცემებს, რომელიც დროებით არაა გამოყენებული. დროებით გამოუყენებელი მონაცემები ნიშნავს იმას, რომ შესანახი მოწყობილობის ტიპი ინახავს მონაცემებს, როდესაც მომხმარებელი ან პროცესი არ იყენებს მას. შესანახი მოწყობილობა შეიძლება იყოს ადგილობრივი (კომპიუტერული მოწყობილობაზე) ან ცენტრალიზებული (ქსელში). არსებობს რიგი პარამეტრები მონაცემთა შენახვისთვის.

უშუალოდ მიმაგრებული შენახვა (DAS) არის კომპიუტერთან დაკავშირებული შენახვა. მყარი დისკი ან ელ.მედია მატარებელი არის უშუალოდ მიმაგრებული შენახვის მაგალითი.

დამოუკიდებელი დისკების ჭარბი მასივი (RAID) იყენებს მრავალრიცხოვან მყარ დისკს მასივში, რაც წარმოადგენს მრავალჯერადი დისკების კომბინაციის მეთოდს ისე, რომ ოპერაციული სისტემა ხედავდეს მათ, როგორც ერთ საერთო დისკს. RAID სისტემა უზრუნველყოფს გაუმჯობესებულ მწარმოებლობას და მეტ უსაფრთხოებას.

ქსელის თანდართული შენახვის (NAS) მოწყობილობა არის ქსელთან დაკავშირებული შენახვის მოწყობილობა, რომელიც იძლევა მონაცემთა შენახვისა და მოძიების საშუალებას ცენტრალიზებული ადგილმდებარეობიდან ავტორიზებული ქსელის მომხმარებლების მიერ. NAS მოწყობილობები მოქნილი და მასშტაბირებადია, რაც საშუალებას აძლევს ადმინისტრატორს, გაზარდოს მისი მოცულობა საჭიროების შემთხვევაში.

შენახვის არეალის ქსელი (SAN)-ს არქიტექტურა წარმოადგენს ქსელზე დაფუძნებულ შენახვის სისტემას. SAN სისტემები დაკავშირებულია ქსელთან მაღალსიჩქარიანი ინტერფეისების გამოყენებით, რაც უზრუნველყოფს მაღალ მწარმოებლობას და ცენტრალიზებული შენახვის საცავთან და მრავალ სერვერთან სწრაფ მიერტებას.

ღრუბლოვანი შენახვის სისტემა (Cloud Storage) არის დისტანციური შენახვის ვარიანტი, რომელიც იყენებს ინტერნეტსივრცეში მონაცემთა ცენტრის პროვაიდერს და ხელმისაწვდომია ნებისმიერი კომპიუტერიდან ინტერნეტის მეშვეობით. Google Drive, iCloud და Dropbox წარმოადგენენ ღრუბლოვანი შენახვის სერვისების მაგალითებს.

ორგანიზაციები დგანან რთული გამოწვევების წინაშე შენახული მონაცემების დაცვის უზრუნველყოფაში. მონაცემთა შენახვის გაუმჯობესების მიზნით, ორგანიზაციებს შეუძლიათ მონაცემთა სარეზერვო სისტემის ავტომატიზება და ცენტრალიზება.

პირდაპირი თანდართული შენახვა (NAS) შეიძლება იყოს მონაცემთა შენახვის ერთ-ერთი ყველაზე რთული ტიპი მისი მართვისა და კონტროლიდან გამომდინარე. პირდაპირი თანდართული შენახვა (NAS) დაუცველია ლოკალურ ჰოსტზე მავნე თავდასხმებისაგან. შენახული მონაცემები შეიძლება ასევე შეიცავდეს სარეზერვო ასლებს. სარეზერვო ასლები შეიძლება იყოს შექმნილი ხელით ან ავტომატურად. ორგანიზაციებმა უნდა შეზღუდონ პირდაპირი თანდართული შენახვისას მონაცემთა ტიპები. კერძოდ, ორგანიზაციამ თავი უნდა აარიდოს კრიტიკული მონაცემების შენახვას პირდაპირი თანდართული შენახვის მოწყობილობებზე.

შენახვის არეალის ქსელი (SAN) გთავაზობთ უფრო უსაფრთხო ვარიანტს. შენახვის არეალის ქსელი, მათ შორის RAID და SAN უზრუნველყოფს უფრო მეტ მწარმოებლობასა და სიჭარბის უზრუნველყოფას. თუმცა, ეს გადაწყვეტა უფრო რთულია კონფიგურაციისა და მართვისთვის. ისინი ამუშავებენ უფრო მეტ მონაცემს, შესაბამისად მეტია რისკი მათი ორგანიზებისათვის იმ შემთხვევაში, თუ მოხდება აპარატურული მტყუნება. ქსელის შენახვის სისტემების უნიკალური გამოწვევები მოიცავს სისტემის კონფიგურაციას, ტესტირებას და მონიტორინგს.

მონაცემთა გადაცემის მეთოდები

მონაცემთა გადაცემა მოიცავს ინფორმაციის გაგზავნას ერთი მოწყობილობიდან მეორეზე. მოწყობილობებს შორის ინფორმაციის გადაცემის მრავალი მეთოდი არსებობს, მათ შორის:

- Sneaker net — იყენებს მოსახსნელ მედიას მონაცემების ფიზიკურად გადაადგილებისათვის ერთი კომპიუტერიდან მეორეში.
- სადენიანი ქსელები — იყენებს კაბელებს მონაცემთა გადაცემისთვის
- უსადენო ქსელები — იყენებს რადიო ტალღებს მონაცემთა გადაცემისთვის

ორგანიზაციები, როგორც წესი, ვერასდროს ვერ ახერხებენ აღკვეტონ sneaker net მეთოდის გამოყენება.

სადენიანი ქსელები მოიცავს სპილენძის სადენიან და ბოჭკოვან მედიას. სადენიანი ქსელები შეიძლება ემსახურებოდეს ადგილობრივ გეოგრაფიულ არეალს (ლოკალური ქსელი) ან შესაძლოა ისინი მოიცავდნენ დიდ მანძილსაც (ფართო არეალის ქსელი).

უსადენო ქსელები ნელ-ნელა ანაცვლებენ სადენიან ქსელებს. უსადენო ქსელები უფრო სწრაფად მოქმედებენ და ქმნიან შედარებით მაღალ გამტარუნარიანობას. უსადენო ქსელები იძლევა სტუმრების რაოდენობას გაზრდის შესაძლებლობას მობილური მოწყობილობებით მცირე ზომის ოფისში (SOHO) და საწარმოო ქსელებში.

როგორც სადენიანი, ასევე უსადენო ქსელები იყენებენ პაკეტებს ან მონაცემთა ერთეულებს. ტერმინი პაკეტი აღწერს მონაცემთა ერთეულს, რომელიც გადაიცემა ქსელში მისი წყაროსა და დანიშნულების ადგილს შორის. სტანდარტული პროტოკოლები, როგორებიცაა ინტერნეტ პროტოკოლი (IP) და ჰიპერტექსტის გადაცემის პროტოკოლი (HTTP) განსაზღვრავენ მონაცემთა პაკეტების სტრუქტურას და ფორმირებას. ეს სტანდარტები ღია წყაროა და საზოგადოებისთვის ხელმისაწვდომია. გადაცემული მონაცემების კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვა კიბერუსაფრთხოების სპეციალისტის ერთ-ერთი უმნიშვნელოვანესი პასუხისმგებლობაა.

ტრანზიტში არსებული მონაცემების უსაფრთხოების გამოწვევები

გადაცემული მონაცემების დაცვა კიბერუსაფრთხოების სპეციალისტის ერთ-ერთი ყველაზე რთული სამუშაოა. მობილური და უსადენო მოწყობილობების ზრდასთან ერთად, კიბერუსაფრთხოების პროფესიონალები პასუხისმგებელნი არიან ყოველდღიურად მათ

ქსელში გადაცემული დიდი რაოდენობის მონაცემთა დაცვაზე. კიბერუსაფრთხოების პროფესიონალი ვალდებულია გაუმკლავდეს ამ მონაცემების დაცვის რამდენიმე გამოწვევას:

- მონაცემთა კონფიდენციალურობის დაცვა - კიბერდამნაშავეებს შეუძლიათ ტრანზიტის მონაცემების ხელში ჩაგდება, შენახვა და მოპარვა. კიბერუსაფრთხოების სპეციალისტმა უნდა გადადგას ნაბიჯები ამ გამოწვევების დასაძლევად
- მონაცემთა მთლიანობის დაცვა - კიბერდამნაშავეებს შეუძლიათ შეზღუდონ და შეცვალოთ მონაცემები ტრანზიტში. კიბერუსაფრთხოების პროფესიონალები ახდენენ მონაცემთა მთლიანობის სისტემების გამოყენებას, რომლებიც ამოწმებენ გადაცემული მონაცემების მთლიანობასა და ავთენტურობას მავნე ქმედებების საწინააღმდეგოდ.
- მონაცემთა ხელმისაწვდომობის დაცვა - კიბერდამნაშავეებს შეუძლიათ გამოიყენონ rogue ან არასანქცირებული მოწყობილობები მონაცემთა ხელმისაწვდომობის შეზღუდისათვის. მარტივმა მობილურმა მოწყობილობამ შეიძლება შეასრულოს ადგილობრივი უსადენო წვდომის წერტილის როლი და დააკავშიროს არასასურველი მომხმარებლები rogue მოწყობილობასთან. კიბერკრიმინალს შეუძლია შეაღწიოს დაცული მომსახურების ან მოწყობილობის ქსელში. ქსელის უსაფრთხოების პროფესიონალებს შეუძლიათ გამართონ ურთიერთ-ავთენტიფიკაციის სისტემები ამ ქმედებების საწინააღმდეგოდ. ურთიერთ-ავთენტიფიკაციის სისტემები მოითხოვენ მომხმარებლის ავტორიზაციას სერვერზე და ასევე მოითხოვენ სერვერის მიერ მომხმარებლის ავთენტიფიკაციას.

მონაცემთა დამუშავებისა და გამოთვლების ფორმები

მონაცემთა მესამე მდგომარეობა არის მონაცემები დამუშავების პროცესში. ეს ეხება მონაცემების მდგომარეობას თავდაპირველი შეტანის, მოდიფიკაციის, გამოთვლების ან გამოტანის დროს.

მონაცემთა მთლიანობის დაცვა იწყება მონაცემების საწყისი შეტანის დროს. ორგანიზაციები იყენებენ რამდენიმე მეთოდს მონაცემების შესაგროვებლად, როგორიცაა მექანიკური მონაცემების შეყვანა,

სკანირების ფორმები, ფაილის ატვირთვები და სენსორებისგან შეგროვებული მონაცემები. თითოეული ეს მეთოდი პოტენციურ საფრთხეს უქმნის მონაცემთა მთლიანობას. შეტანის პროცესში მონაცემთა დაზიანების მაგალითი მოიცავს მონაცემთა შეტანის შეცდომებს ან გათიშულ, გაუმართავ ან უმოქმედო სისტემურ სენსორებს. სხვა მაგალითები შეიძლება შეიცავდეს არასწორი მარკირების ან არათავსებად მონაცემთა ფორმატებს.

მონაცემთა მოდიფიკაცია ეხება თავდაპირველ მონაცემებში ნებისმიერ ცვლილებას, რომელიც, მაგალითისთვის, მოიცავს მომხმარებლების მიერ ხელით შეცვლილ მონაცემებს, პროგრამების დამუშავების დროს მონაცემების მოდიფიცირებასა და აპარატურის მტყუნებას, რაც იწვევს მონაცემთა შეცვლას. პროცესები, როგორიცაა კოდირება/დეკოდირება, კომპრესია/დეკომპრესია და შიფრაცია/დეშიფრაცია არის მონაცემთა მოდიფიკაციის რამდენიმე მაგალითი. მავნე კოდი (Malicious code) ასევე იწვევს მონაცემთა დაზიანებას.

მონაცემთა დაზიანება ასევე ხდება მონაცემთა გამოტანის პროცესში. მონაცემთა გამოტანა ეხება პრინტერებს, ელექტრონულ მონიტორებს ან უშუალოდ სხვა მოწყობილობებს. გამომავალი მონაცემების სიზუსტე კრიტიკულად მნიშვნელოვანია, რადგან ის უზრუნველყოფს ინფორმაციას და გავლენას ახდენს გადაწყვეტილების მიღებაზე. გამომავალი მონაცემების კომპრომეტირების მაგალითები მოიცავს მონაცემთა დელიმიტერების არასწორ გამოყენებას, არასწორ კომუნიკაციის კონფიგურაციებს და არასწორად კონფიგურირებულ პრინტერებს.

დამუშავების დროს არასწორი მონაცემების მოდიფიკაციისგან დაცვამ შესაძლოა უარყოფითი გავლენა იქონიოს პროცესზე. პროგრამული შეცდომები შესაძლოა იყოს მიზეზი მრავალი არასასურველი პროცესისა. მაგალითად, შობამდე ორი კვირით ადრე ზოგიერთმა Amazon-ის მესამე მხარის საცალო მოვაჭრემ აღმოაჩინა, რომ მათი მათ პროდუქციაზე ფასი შეცვლილი იყო სულ რაღაც ერთი ცენტით. ეს მტყუნება გაგრძელდა ერთი საათის განმავლობაში. აღნიშნული შეცდომის შედეგად ათასობით მომხმარებელი დარჩა უკმაყოფილო, ხოლო კომპანიამ განიცადა მნიშვნელოვანი დანაკარგი. 2016 წელს, Nest-ის თერმოსტატის გაუმართაობის გამო მომხმარებლები დარჩნენ გათბობის გარეშე. Nest-ის თერმოსტატი წარმოადგენს Google-ის საკუთრებაში არსებულ ჭკვიან ტექნოლოგიას. პროგრამულმა

მტყუნებამ დატოვა მომხმარებლები, პირდაპირი მნიშვნელობით, სიცივეში. პროგრამული განახლებისას დაშვებულმა შეცდომამ მწყობრიდან გამოიყვანა მოწყობილობის ბატარეები, რის შედეგადაც ტემპერატურის კონტროლი გახდა შეუძლებელი. შედეგად, მომხმარებლებმა ვერ შეძლეს საკუთარი სახლების გათბობა და ცხელი წყლის მიღება წლის ერთ-ერთ ყველაზე ცივ შაბათ-კვირას.

დამუშავების დროს მონაცემების დაცვა მოითხოვს კარგად შემუშავებულ სისტემებს. კიბერუსაფრთხოების პროფესიონალები შეიმუშავებენ პოლიტიკასა და პროცედურებს, რომლებიც საჭიროებენ ტესტირების, შენარჩუნებისა და განახლების სისტემებს, რათა უზრუნველყონ შეცდომათა მაქსიმალურად ნაკლები რიცხვი.

2.4 კიბერუსაფრთხოების ზომები და კიბერუსაფრთხოების კონტრზომების ტიპები

პროგრამულ უზრუნველყოფაზე დაფუძნებული ტექნოლოგიების დაცვა

პროგრამული უზრუნველყოფის გარანტიები მოიცავს პროგრამებსა და მომსახურებას, რომელიც იცავს ოპერაციულ სისტემებს, მონაცემთა ბაზებს და სხვა სერვისებს, რომლებიც მუშაობენ სამუშაო მოწყობილობებზე, პორტატულ მოწყობილობებსა და სერვერებზე. ადმინისტრატორები აინსტალირებენ პროგრამაზე დაფუძნებულ კონტრზომებს ან დაცვებს ინდივიდუალურკვანძებზე ან სერვერებზე. არსებობს რამდენიმე პროგრამულ პროდუქტზე დაფუძნებული ტექნოლოგია, რომელიც გამოიყენება ორგანიზაციის აქტივების დასაცავად:

- პროგრამული დამცავი ეკრანები აკონტროლებენ დისტანციურ წვდომას სისტემაზე. ოპერაციული სისტემები, როგორც წესი, მოიცავს firewall-ს, თუმცა მომხმარებელს ასევე შეუძლია შეიძინოს ან ჩამოტვირთოს დამცავი ეკრანის პროგრამული უზრუნველყოფა მესამე მხარის ვებგვერდიდან.
- ქსელისა და პორტის სკანერები აღმოაჩენენ და აკონტროლებენ ღია პორტებს ქსელში ან სერვერზე.
- პროტოკოლის ანალიზატორები, ან ხელმოწერის ანალიზატორები წარმოადგენენ მოწყობილობებს, რომლებიც აგროვებენ და

შეისწავლიან ქსელურ ტრაფიკს. ისინი განსაზღვრავენ მწარმოებლობის პრობლემებს, აღმოაჩენენ არასწორ კონფიგურაციებს, ახდენენ არასწორი აპლიკაციების იდენტიფიცირებას, საბაზისო და ნორმალური მუშაობის ნიმუშების ჩამოყალიბებას და კომუნიკაციის პრობლემების გამართვას.

- მოწყვლადობის სკანერები წარმოადგენენ კომპიუტერულ პროგრამებს, რომლებიც განკუთვნილია კომპიუტერების ან ქსელების სისუსტეების შესაფასებლად.
- ინდივიდუალურ ჰოსტზე დაფუძნებული შეღწევის გამოვლენის სისტემები (IDS) შეისწავლიან მხოლოდ ჰოსტის სისტემების აქტივობას. IDS აგენერირებს log ფაილებსა და განგაშის შეტყობინებებს, გამოავლენს რა უჩვეულო აქტივობებს სისტემაში. IDS-ს ამოცანაა სენსიტიური მონაცემების დაცვა და კრიტიკული სერვისების უზრუნველყოფა.

აპარატურაზე დაფუძნებული ტექნოლოგიების დაცვა

არსებობს რამდენიმე აპარატურაზე დაფუძნებული დაფუძნებული ტექნოლოგია, რომელიც გამოიყენება ორგანიზაციის აქტივების დასაცავად:

ქსელური დაცვის ეკრანი (Firewall) ახდენს არასასურველი ტრაფიკის ბლოკირებას. დამცავი ეკრანები აყალიბებენ წესებს, რომლებიც განსაზღვრავენ ქსელში დაშვებულ შემომავალ და გამავალ ტრაფიკს.

- შეღწევის აღმომჩენი სისტემა (IDS) აღმოაჩენს უჩვეულო ტრაფიკს ან შეტევის ნიშნებს და აგზავნის განგაშის შეტყობინებას.
- შეღწევის პრევენციის სისტემები (IPS) გამოავლენს უჩვეულო ტრაფიკს ან შეტევის ნიშნებს, აგზავნის განგაშის შეტყობინებას და ახდენს მაკორექტირებელ ქმედებას.
- კონტენტის ფილტრაციის სერვისი აკონტროლებს მიუღებელი ან მავნე შინაარსის მქონე კონტენტის მიღებასა და გადაცემას.

ქსელზე დაფუძნებული ტექნოლოგიების დაცვა

არსებობს რამდენიმე ქსელზე დაფუძნებული დაცვის ტექნოლოგია, რომელიც გამოიყენება ორგანიზაციის აქტივების დასაცავად:

- ვირტუალური კერძო ქსელი (VPN) არის უსაფრთხო ვირტუალური ქსელი, რომელიც იყენებს საყოველთაო ქსელს

(მაგ., ინტერნეტი). VPN-ის უსაფრთხოება მდგომარეობს იმაში, რომ ხდება პაკეტის შინაარსის დაშიფვრა საბოლოო წერტილებს შორის, რომლებიც განსაზღვრავენ VPN- ს.

- ქსელზე წვდომის მართვა (NAC) მოითხოვს შემოწმებათა კომპლექტს, რომელიც საშუალებას მისცემს მოწყობილობას ქსელთან დაკავშირებისა. ზოგიერთი შემოწმება მოითხოვს განახლებული ანტივირუსული პროგრამული უზრუნველყოფის ან ოპერაციული სისტემის განახლებას.
- უსადენო წვდომის წერტილის უსაფრთხოება მოიცავს ავთენტიფიკაციისა და დაშიფვრის განხორციელებას.

Cloud-ზე დაფუძნებული ტექნოლოგიების დაცვა

Cloud-ზე დაფუძნებული ტექნოლოგიები ხორციელდება ორგანიზაციისგან ტექნოლოგიური კომპონენტის გადატანით Cloud პროვაიდერთან. სამი ძირითადი ღრუბლოვანი გამოთვლის კომპიუტერული მომსახურება მოიცავს:

- პროგრამული უზრუნველყოფა, როგორც სერვისი (SAAs) საშუალებას აძლევს მომხმარებლებს, მიიღონ წვდომა პროგრამულ უზრუნველყოფასა და მონაცემთა ბაზებზე. Cloud პროვაიდერები მართავენ ინფრასტრუქტურას. მომხმარებელი ინახავს მონაცემებს Cloud პროვაიდერის სერვერებზე.
- ინფრასტრუქტურა, როგორც სერვისი (IAs) უზრუნველყოფს ვირტუალიზებულ კომპიუტერულ რესურსებს ინტერნეტში. პროვაიდერი სთავაზობს ტექნიკის, პროგრამული უზრუნველყოფის, სერვერებისა და შენახვის კომპონენტებს.
- პლატფორმა როგორც სერვისი (PaaS) ახორციელებს წვდომას ინსტრუმენტებთან და სერვისებთან, რომლებიც უზრუნველყოფენ აპლიკაციებს.

Cloud სერვისის პროვაიდერებმა გააფართოვეს ეს პარამეტრები, რათა ჩართონ IT როგორც სერვისი (ITAAs), რომელიც უზრუნველყოფს IAAS, PaAs და SaaAs სერვისის მოდელების IT მხარდაჭერას. ITaaS (ინფორმაციული ტექნოლოგიები (IT) როგორც სერვისი) მოდელში, ორგანიზაცია დებს კონტრაქტს ღრუბლოვანი სერვისების მომწოდებელთან, ინდივიდუალურ ან ურთიერთდაკავშირებულ მომსახურებაზე.

Cloud სერვის პროვაიდერები იყენებენ ვირტუალურ უსაფრთხოების ტექნიკას, რომლებიც ვირტუალურ გარემოში იყენებენ ვირტუალურ

გარემოში წინასწარ შეფუთული, საიმედო ოპერაციული სისტემის გაშვებას ვირტუალიზებული აპარატურით.

კიბერუსაფრთხოების განათლებისა და ტრენინგის განხორციელება

ტექნოლოგიაში ფინანსების ინვესტირება არ მოიტანს სათანადო შედეგს, თუ ორგანიზაციაში დასაქმებულ პერსონალს არ გააჩნია მაღალი დონის ცოდნა კიბერუსაფრთხოებაში. თანამედროვე კიბერუსაფრთხოების საფუძვლების ცოდნა ძალიან მნიშვნელოვანია ორგანიზაციისათვის. თანამშრომელი შეიძლება არ იყოს მიზანმიმართულად მავნე, მაგრამ უბრალოდ არ იცოდეს, რა არის სწორი პროცედურა. არსებობს ფორმალური სასწავლო პროგრამის განხორციელების რამდენიმე გზა:

- გადააქციეთ უსაფრთხოების ცნობიერების ამაღლების ტრენინგი თანამშრომლისათვის სამუშაო პროცესის ნაწილად
- მიაბით უსაფრთხოების ცნობიერების ამაღლება სამუშაო მოთხოვნებს
- ჩაატარეთ ინდივიდუალური ტრენინგები
- უზრუნველყავით ონლაინ კურსები

ინფორმაციული უსაფრთხოების ცნობიერება უნდა იყოს მიმდინარე პროცესი, რადგან ახალი საფრთხეები და ტექნიკა ყოველთვის სახეზეა.

კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლების კულტურის ჩამოყალიბება

ორგანიზაციის თანამშრომლებს უნდა გააჩნდეთ ცოდნა უსაფრთხოების პოლიტიკის შესახებ და გახადონ ის მათი ყოველდღიური საქმიანობის ნაწილად.

უსაფრთხოების ცნობიერების აქტიური პროგრამა დამოკიდებულია:

- ორგანიზაციის გარემოზე
- საფრთხის დონეზე

კიბერუსაფრთხოების ცნობიერების კულტურის შექმნა მიმდინარე ძალისხმევაა, რომელიც მოითხოვს TOP მენეჯმენტისa და ყოველი მომხმარებლისა და თანამშრომლის ვალდებულებას. ორგანიზაციის კიბერუსაფრთხოების კულტურის ჩამოყალიბება იწყება მართვის პოლიტიკისა და პროცედურების შექმნით. მაგალითად, ბევრ ორგანიზაციას აქვს დაწესებული ინფორმაციული უსაფრთხოების

ცნობიერების დღეები. ორგანიზაციებს ასევე შეუძლიათ განათავსონ ბანერები და ლოზუნგები, რათა მოხდეს ზოგადი კიბერუსაფრთხოების შესახებ ცნობიერების ამაღლება. კიბერუსაფრთხოებაზე ორიენტირებული სამუშაო შეხვედრებისა და სემინარების ჩატარება ხელს უწყობს ცნობიერების ამაღლებას.

ადამიანური ფაქტორები კიბერუსაფრთხოებაში

ჯერომი ზალცერმა და მაიკლ შრედერმა თავიანთ 1975 წლის ფუნდამენტურ ნაშრომში „ინფორმაციის დაცვა კომპიუტერულ სისტემებში“, შეადგინეს უსაფრთხოების დიზაინის ათი პრინციპი. ათიდან სამი დამყარებულია ქცევითი მეცნიერებების ცოდნაზე:

• ფსიქოლოგია: უსაფრთხოების მექანიზმები უნდა იყოს „ფსიქოლოგიურად მისაღები“ იმ ადამიანებისთვის, ვინც უნდა გამოიყენონ ისინი;

• ადამიანური ფაქტორები და ეკონომიკა: თითოეული ინდივიდუალური მომხმარებელი და ორგანიზაცია უნდა გაუმკლავდეს რაც შეიძლება ნაკლებ განსხვავებულ უსაფრთხოების მექანიზმებს;

• კრიმინალური მეცნიერება და ეკონომიკა: უსაფრთხოების ზომების დასაძლევად საჭირო ძალისხმევამ უნდა გადააჭარბოს თავდამსხმელის რესურსებს და მისთვის არსებულ პოტენციურ დადებით შედეგებს.

შრედერსა და ზალცერზე ერთი საუკუნით ადრე კრიპტოგრაფიის მამამ, ავგუსტე კერჩკოფსმა შეიმუშავა ექვსი პრინციპი უსაფრთხო კომუნიკაციის სისტემისთვის, რომელიც გათვალისწინებულია ადამიანურ ფაქტორებზე. მათგან სამი ეხება “ისეთ სისტემას, რომლის გამოყენება მარტივი არის და არ სჭირდება მაღალფარდოვანი განათლება და სტრესი”.

ამ ორივე ფუნდამენტალმა ტექსტმა აღნიშნა ის ფაქტი, რომ თავდაცვითი ზომები ვერ იქნება შედეგიანი, თუ ადამიანებს მისი გამოყენება არ სურთ ან არ შეუძლიათ. ერთ-ერთი კარგი მაგალითია ელ-ფოსტის დაშიფვრა. უკვე 20 წელია, რაც არსებობს დაშიფვრის შესაძლებლობა, თუმცა დღევანდელი ელ-ფოსტის მხოლოდ 0.1% თუ არის დაშიფრულად გადაგზავნილი. ეს სავარაუდი შედეგი გახლავთ, რადგან ვითენმა და ტაიგარმა აღმოაჩინეს უკვე 1999-ში, რომ

მოტივირებული და ნასწავლი პიროვნებებიც ვერ ახერხებდნენ ელ-ფოსტის სწორად დაშიფვრას. ეს სიტუაცია დღესაც არ შეცვლილა მნიშვნელოვნად - თუმცა ახლანდელი კვლევები გვაძლევენ მისი შეცვლის შესაძლებლობებს. უკვე 20 წელია, რაც მიმდინარეობს შესწავლა თავდაცვითი ზომების წარუმატებლობაზე და ადამიანური ფაქტორის როლზე. კვლევების შედეგად ნათელია, რომ თავდაცვითი ზომები იმიტომ არაა მიღებული, რომ ადამიანები კომპონენტებად არიან მიჩნეულები, რომელთა ქცევის დაკონკრეტება და გაკონტროლება შეიძლება უსაფრთხოების ზომებით და თავდავითი მექანიზმებით და სანქციებით. თუმცა აქ უმთავრესი ბრალი არ მიუძღვით მომხმარებლებს იმ შეხედულების მიუხედავად, რომ ადამიანები "ყველაზე სუსტ ჯაჭვს" წარმოადგენენ.

ერთ-ერთი მაგალითი მოცემულ პრობლემაზე არის პაროლებზე მიღებული ზომები. ადამსმა და სასემ აჩვენეს, რომ ექსპერტების მიერ მიღებული ზომები პაროლების უსაფრთხოებაზე და მექანიზმებზე პრაქტიკაში თითქმის არ მუშაობდა. შესაბამისად, თანამშრომლები რეგულარულად ახერხებდნენ მათთვის გვერდის ავლას. ნაიაკშინამ აჩვენა, რომ არამხოლოდ მომხმარებლებს უჭირთ კომპლექსური პაროლების გამოყენება, არამედ დეველოპერებსაც. დეველოპერებს ცალსახად უნდა მოეთხოვოთ უსაფრთხოების ჩართვა და, მაშინაც კი, როდესაც ეს ყველაფერი კეთდება, ისინი ხშირად იყენებენ მოძველებულ და გაუმართავ უსაფრთხოების მექანიზმებს. ცოდნის ეს სფერო ასევე აჩვენებს უსაფრთხოების უფრო ფართო ორგანიზაციულ და სოციალურ პერსპექტივას, რომელიც გაჩნდა გასული ათწლეულის განმავლობაში: ნდობისა და თანამშრომლობის მნიშვნელობა ეფექტური კიბერუსაფრთხოებისთვის, რაც მიიღწევა მხოლოდ დაინტერესებული მხარეების ჩართულობით და უსაფრთხოების გადაწყვეტების მოლაპარაკებით, რომლებიც აკმაყოფილებს მათ საჭიროებებს. ეს მოითხოვს იმ უნარებს, რომელიც ტრადიციულად არ იყო უსაფრთხოების ექსპერტებისთვის გათვალისწინებული. ამ განათლების მხარის მიზანია, რომ ამ ექსპერტებმა მიიღონ შესაბამისი ცოდნა ამ საკითებზე

ადამიანური ქცევა, რომელსაც განსაზღვრავს შინაგანი და გარეგანი ფაქტორები

ცოდნის ეს სფერო ორგანიზებულია: იწყება შიგნიდან და შემდგომ გარეთ ინაცვლებს: თავდაპირველად მოცემულია ინდივიდუალური

და შინაგანი ფაქტორები, რომლებიც განაპირობებს ადამიანის ქცევას (შესაძლებლობები და შეზღუდვები, გონებრივი მოდელები), შემდგომ გადადის უფრო ფართო კონტექსტის ასპექტებზე, რომელშიც ხდება ურთიერთობა უსაფრთხოებასთან. შემდეგ ჩვენ განვიხილავთ სხვა უშუალო ფაქტორებს, რომლებსაც გავლენა გააჩნიათ.

მოწინააღმდეგე აქტიურად მუშაობს, რათა შეცვალოს მომხმარებლების შეხედულებები სისტემის შესაძლებლობებისა და საზღვრების შესახებ, და ასევე გამოიყენოს სოციალური და ორგანიზაციული კონტექსტების სპეციფიკა (მაგ. უსაფრთხოების ზომები, სამუშაო პრაქტიკა, გადაწყვეტილების მიღების იერარქია) უსაფრთხოებაზე ზემოქმედების მიზნით. გამოყენებადი უსაფრთხოების შესწავლა აქტიური თავდამსხმელის მოდელის მეშვეობით და მომხმარებელთა ცნობიერების ამაღლება უსაფრთხოების საკითხებთან დაკავშირებით, რომლებიც აერთიანებს ასეთ მოდელებს, მაგ. ანტი-ფიშინგის სიმულაციები, არის ამ კვლევის მიმდინარე სფერო. ეს მექანიზმები გთავაზობთ გარკვეულ დაცვას, მაგრამ მოითხოვს მომხმარებლის დროსა და ძალისხმევას, ამიტომ უსაფრთხოების მთლიანი დატვირთვა უნდა იყოს ზედამხედველობის ქვეშ, რათა პროდუქტიულობა არ შემცირდეს. გარდა ამისა, მათ აქვთ გავლენა მომხმარებელთა ნდობაზე ორგანიზაციისადმი და პირველ-ხარისხოვანი (უსაფრთხოებასთან დაუკავშირებელი) ამოცანის შესრულებაზე – ნებისმიერი ასეთი ჩარევისა თუ კამპანიის დიზაინი უნდა ითვალისწინებდეს მოცემულ რისკებს.

როდესაც მომხმარებლები არ იქცევიან ისე, როგორც ეს განსაზღვრულია უსაფრთხოების ზომებით, უსაფრთხოების სპეციალისტების უმეტესობა მიიჩნევს, რომ მომხმარებლები არიან დამნაშავე ამაში: რომ მათ „უბრალოდ არ ესმით რისკების მნიშვნელობა ან „უბრალოდ ზარმაცები არიან“. მაგრამ კვლევებმა აჩვენა, რომელსაც „წესების დარღვევები” ძირითადად გამოწვეულია იმ ადამიანების მიერ, რომლებიც არჩევანის წინაშე დგანან უსაფრთხოების თვალსაზრისით სწორი ქმედების გაკეთებისა და მათი პროდუქტიულობის გაზრდას შორის. უმეტესობა ამ ადამიანებიდან ირჩევს პროდუქტიულობას, რადგან სწორედ ამას აკეთებენ ორგანიზაციებიც. ასეთი წესების დარღვევების მოგვარებაზე ძირითადად პასუხობენ უსაფრთხოების ინფორმირებულობისა და განათლების ამაღლების მცდელობით. მაგრამ ადამიანის ფაქტორების

კვლევამ დაადგინა ათწლეულების წინ: როდესაც ჩვენ გავითვალისწინებთ ყველა ძალისხმევას და შედეგად მიღებულ შედეგს, ადამიანის დავალებისთვის მორგების ტექნიკა გაცილებით უფრო ეფექტურია. უსაფრთხოების ინფორმირებულობისა და ტრენინგს გააჩნია გარკვეული როლი, მაგრამ ის უნდა ჩაითვალოს, როგორც ერთ-ერთ ვარიანტად, მაგრამ არა ერთადერთ გამოსავალად. შესაბამისი ცოდნის მიღების შემდეგაც ადამიანს არ შეუძლია, გაუმკლავდეს ისეთ უსაფრთხოების პრობლემებს, რომლებიც შეუძლებელია ან ბერვ ინდივიდუალურ ან ორგანიზაციულ მსხვერპლს მოითხოვს. გაერთიანებული სამეფოს კიბერუსაფრთხოების ეროვნული ცენტრის (NCSC) მიხედვით, „უსაფრთხოების მუშაობის ეფექტურ გზას წარმოადგენს უსაფრთხოება, რომელიც მუშაობს ადამიანებისთვის". სხვა სიტყვებით რომ ვთქვათ, უსაფრთხოება უნდა იყოს მარტივად გამოყენებადი. ISO განსაზღვრავს გამოყენებადობას (ISO 9241–11:2018), როგორც „ეფექტურობა და კმაყოფილება, რომლითაც შესაბამისი მომხმარებლები აღწევენ განსაზღვრული მიზნებს კონკრეტულ გარემოებებში".

კრიტერიუმები, რომლითაც ფასდება პრაქტიკულობა არის:

1. ეფექტურობა: სიზუსტე და სისრულე, რომლითაც მომხმარებლებს შესაძლებლობა აქვთ, რომ მიაღწიონ განსაზღვრული მიზნებს კონკრეტულ გარემოში;
2. ეფექტიანობა: დახარჯული რესურსები სიზუსტესა და სისრულეზე;
3. კმაყოფილება: სამუშაო სისტემის კომფორტი და ხელმისაწვდომობა მისი მომხმარებლებისთვის და სხვა ადამიანებისთვის.

დავალების ადამიანთან მისადაგება

პრაქტიკული თვალსაზრისიდან გამომდინარე, უსაფთხოების ამოცანების მისადაგება და მათი გამარტივება მოიცავს ოთხ მთავარ ნაწილს:

1. სამიზნე მომხმარებლების შესაძლებლობები და შეზღუდვები;
2. მომხმარებლების მიზნები, და მათ მიერ შესრულებული ამოცანები ამ მიზნების მისაღწევად;

3. ფიზიკური და სოციალური გარემოებების გათვალისწინება;
4. იმ მოწყობილობების შესაძლებლობების გათვალისწინება, სადაც ეს უსაფრთხოების მექანიზმები გამოიყენება.

ჩვენ ახლა განვიხილავთ თითოეულ მათგანს, და თუ როგორ გამოიყენება ისინი ეფექტური უსაფრთხოების მექანიზმების შექმნაში.

ძირითადი ადამიანური შესაძლებლობები და შეზღუდვები: არსებობს ზოგადი შესაძლებლობები და შეზღუდვები - ფიზიკური და გონებრივი - რაც ადამიანების უმეტესობას ეხება. ადამიანებისთვის ისეთი დავალების მიცემა, რომელიც აღემატება მის შესაძლებლობას, ნიშნავს იმას, რომ ჩვენ მათ წარუმატებლობისთვის ვწირავთ. როდესაც მათ წინაშე არსებული დავალება მათი შესაძლებლობის ზღვართან ახლოსაა, ადამიანთა უმეტესობა ცდილობს მის შესრულებას, თუმცა ეს მათგან მნიშვნელოვან ძალისხმევას მოითხოვს, რაც საბოლოოდ შეიძლება არამდგრადი აღმოჩნდეს. დღეს გამოთვლით მოწყობილობებს შეუძლიათ ფიზიკურ შესაძლებლობებს მასობრივად გადააჭარბონ უსაფრთხოების ამოცანებში. უსაფრთხოების მრავალი სისტემა უზრუნველყოფს სტატუსის შეტყობინებებს, შეხსენებებს ან გაფრთხილებებს. ადამიანებს ძირითადად შეუძლიათ თავიანთი ყურადღების მიპყრობა მხოლოდ ერთ ამოცანაზე ერთ კონკრეტულ დროს. ეს ყურადღება გამახვილებულია მათ მთავარ საქმიანობებზე და ამავდროულად უსაფრთხოების ბევრი მექანიზმი მოითხოვს მეტ დროსა და ყურადღებას, ვიდრე მომხმარებლებს შეუძლიათ, რომ გამოყონ მისთვის. ეს ნიშნავს, რომ ცვლილებები პასიურ უსაფრთხოების ინდიკატორებში ხშირად არ შეიმჩნევა, განსაკუთრებით თუ ისინი ეკრანის კიდეებზეა გამოსახული. მომხმარებლებისთვის ამ ინდიკატორების გადამოწმების მოთხოვნა მათ წარუმატებლობას განაპირობებს, თუნდაც მათ შეგნებულად სცადონ მათი შემოწმება. მათი ყურადღება კვლავ მთავარ ამოცანაზე იქნება გამახვილებული. თუ უსაფრთხოების მაჩვენებლებისათვის საჭიროა დაკვირვება, ისინი უნდა იყოს მიმართული პირდაპირ, და მოითხოვდეს პასუხს. ეს ხერხი გამოსადეგია, თუმცა მხოლოდ იშვიათი და სანდო ინდიკატორებისთვის.

მოკლევადიანი მეხსიერება და ერთჯერადი პაროლები (OTP) - ერთჯერადი PIN-ების ან პაროლების (OTP) გამოყენება გაზრდილია, რადგან ორდონიანი ავთენტიფიკაცია (2FA) უფრო გავრცელებული

არის ახლა მსოფლიოში. ჩვენ ყურადღებას ვამახვილებთ გამოტანილ რიცხვზე და ვუმეორებთ საკუთარ თავს (გონებაში ან ხმამაღლა). შემდეგ ჩვენ ვიღებთ ახლად დამახსოვრებულ ინფორმაციას STM ციკლიდან და საკუთარ თავს ვუმეორებთ. მნიშვნელოვანია იმის აღნიშვნა, რომ ეს მეთოდი ადამიანების უმეტესობისთვის მხოლოდ ექვს-ელემენტიანი ინფორმაციის დასამახსოვრებლად კმარა. ისეთი კოდები, რომლებიც მეტ ელემენტებს შეიცავენ, ზედმეტ დატვირთვას აძლევენ STM ციკლს. ადამიანებმა ასეთ შემთხვევაში უნდა დაიწყონ წინ და უკან ყურება ეკრანებს შორის, რათა წაიკითხონ სიმბოლოები და შეიყვანონ ისინი. ეს ზრდის როგორც შესვლის დროს, ასევე შეცდომის ალბათობასაც. ასოებისა და ციფრების შერევაც ასევე უარყოფით გავლენას ახდენს.

შეძლებს თუ არა მომხმარებელი გაიხსენოს ის, თუ რაც ინახება გრძელვადიან მეხსიერებაში დამოკიდებულია იმაზე, თუ რამდენად ღრმად არის ის ჩანერგული მეხსიერებაში.

ინფორმაცია, რომლის გახსენებაც ხშირადაა საჭირო, უფრო კარგად არის დამახსოვრებული, ვიდრე ის, რომლის მოგონებაც იშვიათად გვიწევს. ეს ნიშნავს, რომ შეიძლება ველოდოთ პრობლემებს იშვიათად გასახსენებელ ინფორმაციასთან (მაგალითად, საკუთარი სურათების ამოცნობა სურათების ერთობლიობაში უფრო ადვილია, ვიდრე უცხო ფოტოების). LTM იყოფა ორად განსხვავებული სფეროდ: ზოგადი ცოდნა ინახება სემანტიკურ მეხსიერებაში (LTM-SM), ხოლო ის ინფორმაცია, რომელიც პირად ისტორიასთან არის დაკავშირებული, ინახება ეპიზოდურ მეხსიერებაში (LTM-EM): ავტობიოგრაფიული მეხსიერება.

TM-SM-ში შენახული ნივთები უფრო სწრაფად ქრებიან, ვიდრე LTM-EM-ში, რადგან ამ უკანასკნელ შემთხვევაში ტვინი იმახსოვრებს არამხოლოდ ინფორმაციას, არამედ მასთან დაკავშირებულ ემოციებსა და სურათებსაც.

LTM და პაროლები: LTM-SM იყოფა ზონებად, რომლებშიც ინახება მსგავსი ინფორმაცია. როდესაც პიროვნება ცდილობს რაიმეს გახსენებას, განყოფილება, რომელშიც ის ინახება, აქტიურდება და იქ მყოფი ელემენტები ერთმანეთს კონკურენციას უწევენ, შესაბამისად, უკვე მოძიებული ინფორმაცია უფრო ხშირად გვაგონდება. ეს ჩარევის ეფექტი საკმაოდ ძლიერი და დამაზიანებელია განსაკუთრებით

იმიტომ, რომ ის ინფორმაცია, რომლის გახსენებაც ადამიანს აღარ სჭირდება (როგორიცაა ძველი პაროლები), რჩებიან და კონკურენციას უწევენ იმ ინფორმაციას, რომლის გახსენება საჭიროა. ამრიგად, მსგავსი სახის მონაცემების სიმრავლის მართვა შეუძლებელია განსაკუთრებით მაშინ, თუ მათ შორის რამდენიმე მათგანი იშვიათადაა გასახსენებელი. ამიტომ ადამიანებს სჭირდებათ ამ ეფექტის დაძლევის საშუალებები, მაგალთად პაროლების ამოწერის, პაროლის მენეჯერის ან ერთჯერადი მონაცემების მეშვეობით. შეგვიძლია შევთანხმდეთ, რომ 123456 ან P@SSword არ წარმოადგენს უსაფრთხო პაროლს, მაგრამ რადგან მომხმარებელთა უმეტესობას ახლა უკვე მრავალი პაროლი ერთდროულად აქვს, მუდმივად ძლიერი პაროლების შექმნა ადამიანურად შეუძლებელი ამოცანაა. ადამიანების უმეტესობას უჭირს 2–3-ზე მეტი პაროლის ან PIN-კოდის დამახსოვრება – და რაც უფრო გრძელი და ძლიერია ისინი, მით უფრო რთული იქნება მათი შემდგომში გამოყენება

NCSC პაროლის სახელმძღვანელო გვაძლევს მრავალი და რთული პაროლების მარტივად მართვის საშუალებას: 2FA მეთოდის და/ან პაროლის მენეჯერების გამოყენება, და თუ შეუძლებელია ამის გამოყენება, მაშინ რთული პაროლებისათვის ვადის ხანგრძლივობის გაზრდა. თუ პაროლის გამოყენება უნდა შეწყდეს (მაგ., რადგან ის გატეხილია), მაშინ შეიძლება დაგვეხმაროს გარკვეული დროის გამოყენება დღის განმავლობაში პაროლის შესაცვლელად.

უსაფრთხოების ერთ-ერთი მნიშვნელოვანი კრიტერიუმი ცოდნაზე დაფუძნებული ავთენტიფიკაციისთვის არის ავტორიზაციის მონაცემების კარგი დაცვა. ადამიანის ფიზიკური და გონებრივი მახასიათებლების გამო, უმეტესად ეს მონაცემები მარტივად გამოსარჩევი და ნაცნობი ხასიათისაა.

1. პაროლებით ადამიანები ცდილობენ აირჩიონ ისეთი პაროლები, რომლებიც მათთვის ადვილად დასამახსოვრებელია, მაგალითად სახელები ან თარიღები.
2. როდესაც მომხმარებლებს უწევთ სურათების არჩევა, როგორც ავტორიზაციის მონაცემის, ისინი უპირატესობას ანიჭებენ მკვეთრ ფერებსა და ფორმებს.
3. როდესაც ადამიანების სურათებთან გვაქვს საქმე, უმეტესად ადამიანები აირჩევენ "უფრო მიმზიდველი" ადამიანების სურათებს და მსგავსი ეთნიკური ჯგუფის პიროვნებას.

4. როდესაც ავტორიზაციის მონაცემი არის კონკრეტული ადგილი სურათზე, ადამიანები უპირატესობას ანიჭებენ მახასიათებლებს, რომლებიც გამოირჩევა.
5. მდებარეობაზე დაფუძნებული სისტემის შემთხვევაში ადამიანები ირჩევენ დასამახსოვრებელ ადგილებს.
6. ავტორიზაციის მონაცემთა ელემენტების თანმიმდევრობა პროგნოზირებადია, რადგან მათი არჩევისას არსებობს ძლიერი კულტურული გავლენები. მაგალითად, ადამიანები, რომლებიც საუბრობენ ენებზე, რომლებიც კითხულობენ მარცხნიდან მარჯვნივ, აირჩევენ მსგავს ფორმატს.
7. Android ტელეფონებზე თითის გასრიალების პაროლების შემთხვევაში ადამიანები ირჩევენ ფორმებს ძალიან შეზღუდული დიაპაზონიდან.

ეს ადამიანური მიკერძოებებები ამცირებენ პაროლებში მრავალფეროვნებას (სხვადასხვა პაროლების რაოდენობას) მონაცემთა ბაზაში და ზრდიან თავდამსხმელის მიერ პაროლის გამოცნობის ალბათობას. ამ პრობლემის გადასაჭრელად უსაფრთხოების ზომები კრძალავენ ყველაზე მარტივ და აშკარა პაროლების არჩევას. მიუხედავად იმისა, რომ ხშირად ეს ზომები აუცილებელია, ძალიან ბევრი შეზღუდვის ქონა ზრდის პაროლის შექმნის ამოცანასთან დაკავშირებულ დატვირთვებს. მაგალითად ისეთი შემოწმების სისტემა, რომელიც 5-ზე მეტ პაროლს ძალიან სუსტის კატეგორიას მისცემს, მომხმარებლებს დააყენებს მნიშვნელოვანი სტრესის ქვეშ და, სავარაუდოდ უბიძგებს მათ პაროლის ხელახლა გამოყენებისკენ.

ანალოგიურად, პაროლის სიმძლავრის შესაფასებელი სისტემები ხშირად გამოიყენება მომხმარებლის პაროლის არჩევანზე ზემოქმედების მიზნით. მაგალითად, Ur et al-მა განიხილა პაროლების კომბინაციის სხვადასხვა დიზაინის გავლენა მომხმარებელთა პაროლების არჩევანზე. მან ასევე ხაზი გაუსვა მომხმარებლებზე არსებულ გაზრდილ დატვირთვას და გაღიზიანებას, როდესაც ისინი აწყდებიან უფრო მკაცრი პაროლის შემთხვევაში. გოლასა და დურმუთის ბოლო ნაშრომში გამოკვლეულია 45 პაროლის სიძლიერე, მათ შორის რამდენიმე პრაქტიკაში გამოყენებულიც და აკადემიური შემოთვაზებებიც. მათი ნამუშევარი გვიჩვენებს ცვალებადობის ხარისხს სიზუსტის თვალსაზრისით და გვიჩვენებს, რომ ისინი მნიშვნელოვნად არ გაუმჯობესებულან ბოლო ხუთი წლის

განმავლობაში. ასე რომ, მაშინაც კი, თუ ჩვენ უგულებელვყოფთ მომხმარებლებზე ზედმეტ დატვირთვას, ამ მიდგომებს ყოველთვის არ გააჩნიათ ის სიზუსტის დონე, რომელიც საჭიროა პაროლებზე არსებული ზომების ეფექტურად განსახორციელებლად. ეს მოსაზრებები მხედველობაში უნდა იყოს გათვალისწინებული უსაფრთხოების პოლიტიკის განსახორციელებლად. ზოგჯერ ჩნდება კითხვა თუ არსებობს ისეთი ტრენინგი, რომელიც მომხმარებლებს ეხმარება უსაფრთხოების სერთიტიკატების გახსენებაში. მეხსიერების სპეციალისტები იყენებენ სპეციალურ ვარჯიშებს მეხსიერების მუშაობის გასაუმჯობესებლად. მწერალი ჯოშუა ფოერი თავის ბესტსელერში “Moonwalking with Einstein” დეტალურად აღწერს, რომ ეს ყველაფერი მოითხოვს დროის დიდ ხარჯს (რამდენიმე თვე), მაგრამ ასევე ვარჯიშის გაგრძელებასაც (მინიმუმ 30 წუთი დღეში), დამატებით კი დრო, რომელიც საჭიროა გახსენებისა და შესვლისთვის. პაროლები (რომლებიც თავისთავად ადამიანებს უკვე ზედმეტი მიაჩნიათ).

ჩვენ აქამდე განვიხილეთ შესაძლებლობები და შეზღუდვები, რომლებიც ადამიანების უმეტესობას ეხება. მაგრამ, კონკრეტულ მომხმარებელთა ჯგუფებს ექნებათ დამატებითი საჭიროებები, რომელიც უნდა განსაზღვრავდეს უსაფრთხოების სისტემის ან პროცესის არჩევას. მაგალითად, ბავშვებსა და ხანდაზმულ მოქალაქეებს შეიძლება ჰქონდეთ შესაძლებლობები და შეზღუდულობები (მაგ. საავტომობილო უნარები), რომლებიც განსხვავდება სამუშაო ასაკის მოზრდილებისგან. მაგ., უფრო დიდი თითების მქონე ადამიანებს გაუჭირდებათ თითის დაჭერა პატარა კლავიშებზე. გასათვალისწინებელია კულტურული ღირებულებები და ნორმები და მომხმარებლების ფიზიკური და ფსიქიკური მდგომარეობაც. ყველა მომხმარებელს არ შეუძლია მოწყობილობის ხელით მართვა, ეკრანიდან წაკითხვა ან აუდიოს მოსმენა. ისეთი პირობები, როგორიცაა მაგალითად ფერთა სიბრმავე, დიდ გავლენას ახდენს ადამიამიანთა მნიშვნელოვან ნაწილზე. ამიტომ გრაფიკული ავთენტიფიკაციისთვის გამოყენებული სურათები უნდა შემოწმდეს, რათა ის ამ ჯგუფებისთვის გამოსაყენებლად ვარგისი იყოს. ზოგიერთმა აუდიო ან ვიდეო ეფექტმა შეიძლება ზიანი მიაყენოს აუტიზმის ან ეპილეფსის მქონე პიროვნებებს.

CAPTCHA - გარკვეული ნაშრომები განიხილავენ სენსორული დარღვევების მქონე მომხმარებლების მხარდაჭერას. თუმცა, უნდა

გვახსოვდეს, რომ CAPTCHA უფრო მეტ ძალისხმევას მოითხოვს ლეგიტიმური მომხმარებლისგან, რაც ხელს უშლის დასახული მიზნის მიღწევას, ანუ წვდომის მიღწევას. შეზღუდვები იმ მექანიზმებისა, რომლებიც მიზნად ისახავენ ლეგიტიმური მომხმარებლების „შემოწმებას“ - და მათი წვლილი “უსაფრთხოების შიმშილში” - მეტად გასათვალისწინებელია.

ადამიანის ქცევის მიზნები და ამოცანები

ადამიანის ქცევა ძირითადად მიზნებზეა ორიენტირებული. ადამიანები ასრულებენ დავალებებს გარკვეული მიზნების მისაღწევად სამსახურში ან პირად ცხოვრებაში. ამ მიზნების მისაღწევად ადამიანები ასრულებენ ამოცანებს. სამუშაოს შესასრულებლად საჭიროა შესაბამისი მასალების და მათი რესურსის მოძიება, საჭირო საათების რაოდენობის და შესაბამის გადასახადების დადგენა და ა.შ. თუ სამუშაო რამდენიმე ნაწილისგან შედგება, ის შესაძლოა დავყოთ შედარებით მცირე სამუშაოებად. მაგალითად, სამუშაოზე მოთხოვნილი საათების დამუშავება შეიძლება დაიყოს შემდგომ ამოცანებად:

1. ყველა სამუშაო ეტაპის განხილვა;
2. შესაფერისი მონაწილეების მოძიება კონკრეტული დავალების შესასრულებლად;
3. მონაწილეებისთვის გარკვეული რაოდენობის დროის გამოყოფა;
4. მონაწილეების მიერ საკუტარი დავალებისადმი შესაფერისი მომზადება.

ასეთ ამოცანებს ეწოდებათ პირველადი ან წარმოებადი ამოცანები ადამიანური ფაქტორების ტერმინოლოგიაში. გარკვეული ტექნოლოგიური ხელსაწყოების შემუშავება, რათა ადამიანებს შეეძლოთ ამოცანების ეფექტურად და ეფექტურად შესრულება, არის გამოყენებადობის ყველაზე მთავარი ნაწილი. იმის უზრუნველსაყოფად, რომ ადამიანებმა დავალებები ეფექტურად შეასრულონ, ტექნოლოგიის (და უსაფრთხოების) დიზაინერებმა უნდა იცოდნენ მოთხოვნები მათ მიერ შესრულებულ ამოცანებზე

ურთიერთქმედების კონტექსტი

კონტექსტური კვლევა იყენებს დაკვირვებისა და ინტერვიუს ერთობლივად, რათა დაადგინოს ის ძირითადი ამოცანები, რომლებსაც ადამიანები ასრულებენ და რა განაპირობებს ამას.

როგორც ფიზიკური გარემო, ასევე სოციალური გარემო, რომელშიც ადამიანებს უწევთ უსაფრთხოების ამოცანების შესრულება, გავლენას ახდენს ამ ამოცანების შესრულებაზე. სამუშაო ასაკის ადამიანების უმეტესობა ახლა უფრო ხშირად ურთიერთობს ტექნოლოგიასთან მოძრაობისას, ვიდრე სამუშაო მაგიდასთან, ტრადიციულ სამუშაო გარემოში. გამოყენების კონტექსტში ეს ცვლილება გავლენას ახდენს უსაფრთხოების უამრავ მექანიზმზე. თუნდაც გავიხსენოთ CIA-ს ყოფილი დირექტორის მაიკლ ჰეიდენიზე დასმენის შემთხვევა მატარებელში მგზავრობის დროს. მოსმენის რისკი ახლა გათვალისწინებულია ბევრ კორპორატიულ ტრენინგის პაკეტებში, მაგრამ უსაფრთხოების რამდენიმე მექანიზმი ჯერ კიდევ გამოიყენება, რომლებიც დაუცველია დასმენის შემთხვევაში. ზოგიერთ თავდამსხმელს ასევე შეუძლია სცადოს ავტორიზაციის მონაცემების მოპოვება თვალთვალის ან ფარული კამერების მეშვეობით. მთლიანობაში, ერთჯერადი პაროლის (OTP) გამოყენებამ შეიძლება უზრუნველყოს უსაფრთხოება. თავდაცვის მექანიზმების გამოყენებაზე შეიძლება გავლენა იქონიოს შემდეგმა ფიზიკურმა ფაქტორებმა:

1. სინათლე: კაშკაშა შუქზე ეკრანზე გამოსახული ინფორმაცია ძნელად აღსაქმელია, რამაც შეიძლება გავლენა მოახდინოს კონკრეტულად გრაფიკულ ავთენტიფიკაციაზე. ბიომეტრიული სისტემები, როგორიცაა ირისი და სახის ამოცნობა, ეყრდნობა კამერებს. კაშკაშა შუქმა შეიძლება გამოიწვიოს სიკაშკაშე, რაც ნიშნავს, რომ გადაღებული სურათები საკმარისად კარგად არ არის დასამუშავებლად.

2. ხმაური ყველაზე აშკარად ხელს შეუშლის ხმის ამომცნობი სისტემების მუშაობას. მაგრამ ხმაურის მაღალი დონე ასევე გავლენას ახდენს ადამიანის მუშაობაზე ზოგადად გაზრდილი სტრესის გამო და, თავის მხრივ, გაზრდილი შეცდომის ალბათობის გამო.

3. გარემოს ტემპერატურამ შეიძლება გავლენა მოახდინოს როგორც ტექნოლოგიების, ასევე ადამიანების მუშაობაზე. თითის

ანაბეჭდის სენსორები წყვეტენ მუშაობას, როდესაც ცივა, ხოლო ადამიანები უფრო ნელა მოქმედებენ. მათ ასევე შეიძლება დასჭირდეთ დამცავი ტანსაცმლის ტარება, როგორიცაა ხელთათმანები, რომლებიც შეუძლებელს ან რთულს ხდის სენსორულ ეკრანზე მუშაობას. ანალოგიურად, ძალიან ცხელმა გარემომ შეიძლება გამოიწვიოს დისკომფორტი და ოფლმა შესაძლოა ხელი შეუშალოს სენსორებს.

4. დაბინძურებამ შეიძლება გავლენა მოახდინოს მოწყობილობებზე. ეს განსაკუთრებით ეხება თითის ანაბეჭდის სენსორებსა და სენსორულ ეკრანებს. დარჩენილი ლიპიდები გაერთიანდება ნაწილაკებთან და მიღებული მუქი ცხიმი ბლოკავს სენსორებს ან ტოვებს აშკარად შესამჩნევი ნიმუშს სენსორულ ეკრანზე.

სოციალური კონტექსტი, რომელშიც ადამიანები აღმოჩნდებიან, ძლიერ გავლენას ახდენს ქცევაზე ღირებულებების მეშვეობით: საერთო რწმენა იმის შესახებ, თუ რა არის მნიშვნელოვანი და ღირებული, და ნორმები: წესები და მოლოდინები ქცევის შესახებ. თუ თავდავცის მოსალოდნელი ქცევა ეწინააღმდეგება ყოველდღიური ქცევის ნორმებს, შესაძლოა გაჩნდეს პრობლემები. მაგალითად, თუ ორგანიზაცია აფასებს მომხმარებელთა კმაყოფილებას და მეგობრულ ურთიერთობებს, მაშინ უსაფრთხოების პოლიტიკა, რომელიც მოითხოვს, რომ პერსონალმა კლიენტის ნებისმიერ შეკითხვას ინფორმაციის მოპოვების პოტენციურ მცდელობად ჩათვალოს, შეუსაბამოა. უსაფრთხოების პოლიტიკასთან შეურიგებლობის მიზეზების გაგებამ შეიძლება ნათელი მოჰფინოს ამ კონფლიქტებს.

ნდობა კიდევ ერთი ძირითადი ნორმაა. ადამიანებს არ უყვართ უნდობლობის გრძნობა - და ნაჩვენებია, რომ თანამშრომლებისადმი უნდობლობის გამოხატვა ხელს უწყობს უარყოფით დამოკიდებულებებს. საჭიროა სხვა ასპექტების გათვალისწინება, რათა გავიგოთ, თუ როგორ ყალიბდება უსაფრთხოების რწმენა და ნორმები. მაგალითად, მომხმარებლები ხშირად იღებენ ცოდნას სოციალური ქსელებიდან და ისინი ასევე წარმოადგენენ მხარდაჭერისა და დახმარების წყაროს, როდესაც ისინი აწყდებიან გამოწვევებს.

მოწყობილობის შესაძლებლობები და შეზღუდვები

ჩვენ უკვე განვიხილეთ, რომ მოწყობილობის ფიზიკურმა მახა-სიათებლებმა შეიძლება გაართულოს უსაფრთხოების მექანიზმებთან

ურთიერთქმედება გარკვეულ გარემოებებში. მოწყობილობის ზოგიერთმა მახასიათებელმა შეიძლება გაართულოს უსაფრთხოების მექანიზმების გამოყენება ნებისმიერ ვითარებაში. მობილურ ტელეფონზე რბილ კლავიატურაზე გრძელი და რთული პაროლების შეყვანას გაცილებით მეტი დრო სჭირდება, ვიდრე ჩვეულებრივ კლავიატურაზე. მიუხედავად იმისა, რომ კლავიატურაზე ხშირი გამოყენების შემთხვევაში, ადამიანების უმეტესობას შეუძლია პაროლის დამახსოვრება, მათი ტემპი არ გაუმჯობესდება, როდესაც ისინი ხვდებან შეზღუდვას. განსაკუთრებით შემაშფოთებელია უსაფრთხოების თვალსაზრისით ის, რომ (შეთანხმების გარეშე) მომხმარებლები იწყებენ პაროლების მცირე რაოდენობის გამოყენებას, რომელთა შეყვანა ყველაზე ადვილია. ეს კი ამარტივებს თავდამსხმელების მიერ პაროლების გატეხვის ალბათობას. მიუხედავად იმისა, რომ 2FA-ს აქვს უსაფრთხოების უპირატესობები და ამცირებს ძლიერი პაროლების საჭიროებას, 2FA-ს ყველა უპირატესობის გამოყენება ერთრდოულად რთულია. ბევრ მომხმარებელს უჭირს ფართოდ გამოყენებული 2FA token-ების გამოყენება, როგორიცაა Digipass. ისინი აფასებენ იმას, რომ ის ჯდება მათ საფულეში, მაგრამ საბოლოო ჯამში მათთვის ეს „ზედმეტად დისკომფორტულია“. ონლაინ ბანკინგის მომხმარებელთა ნახევარზე მეტს აქვს ანგარიშები ერთზე მეტ ფინანსურ პროვაიდერთან. ის ფაქტი, რომ ისინიც კი, ვინც იყენებენ 2FA-ს, განსხვავებულად ახორციელებენ (რომელი ტოკენი გამოიყენება, როდესაც ის უნდა იქნას გამოყენებული, და როგორ არის მოხსენიებული ავტორიზაციის სხვადასხვა ელემენტები (ფრაზა, პაროლი, საკვანძო ფრაზა) იწვევს მომხმარებლებში დაბნეულობას. ანალოგიურად, სხვადასხვა Chip-ისა და PIN-ის დანერგვა ქმნის ოდნავ განსხვავებულ ვარიაციებს ამოცანებში, რაც იწვევს შეცდომების გაზრდილ ალბათობას. ახალი მოწყობილობების გაზრდის გამო, ჭკვიანი საათებიდან დაწყებული და სახლის მოწყობილობებით დამთავრებული, და კიდევ უფრო მცირე ეკრანის ზომითა და იმპლიციტური ურთიერთქმედებით).

ადამიანური შეცდომა

უბედური შემთხვევებისა და უსაფრთხოების შესახებ 30 წელზე მეტი ხნის კვლევისას, ფსიქოლოგმა ჯეიმს რეისონმა დაადგინა, რომ ადამიანების თითქმის ყველა შეცდომა პროგნოზირებადია. ისინი წარმოიქმნება გაუცნობიერებელი შეცდომებისა (ორგანიზაციის და

ადგილობრივი სამუშაო ადგილის პირობები) და ცნობიერი შეცდომების შედეგად (ადამიანის შეცდომები და დარღვევები). უსაფრთხოების ინციდენტი ხდება იმის გამო, რომ საფრთხე აღწევს ორგანიზაციის თადაცვის მექანიზმების სისუსტეების გამოყენების მეთოდს. მართალია, პიროვნება შეიძლება იყოს ის, ვინც დააჭირა არასწორ ღილაკს ან დააჭირა ბმულს და გამოიწვია ინციდენტი, თუმცა, ამას წინ უძღოდა რამდენიმე სხვა შეცდომა, რამაც გამოიწვია ის, რომ ადამიანი მოხვდა ისეთ მდგომარეობაში, რომ სწორი არჩევანის გაკეთება არასწორი აღმოჩნდა.

ასევე არ შეიძლება ვივარაუდოთ, რომ ყველა სისტემა შექმნილია უსაფრთხოების სისტემების გათვალისწინებით. ყველაზე ხშირად, სისტემები, ფაქტობრივად, სისტემათა სისტემებია (SoS), რომლებიც წარმოიქმნება სხვაგვარად დამოუკიდებელი სისტემების შედგენისგან, რომლებიც გაერთიანებულია კონკრეტული სერვისის ან ამოცანის შესრულებისთვის. SoS-ში ინტეგრაციის პრობლემები შესწავლილია და გასათვალისწინებელია გაუცნობიერებელი შეცდომები, რომლებიც წარმოიქმნება ინტეგრაციის დროს მიღებული გადაწყვეტილებების გამო. ცუდი გამოყენებადობა და ამოცანებისგან გამოწვეული გადაღლა წარმოადგენს იმდენად სერიოზულ რისკს SoS-ის უსაფრთხოებისთვის, რომ მნიშვნელოვანია მოხდეს წინასწარი ინვესტიცია, რათა თავიდან იქნას აცილებული ფარული წარუმატებლობა.

უსაფრთხოების კუთხით, თანამშრომლის მიერ უსაფრთხოების პროცედურებს არშესრულება წარმოადგენს წარუმატებლობას და უნდა მოხდეს მისი გამოსწორება. ხშირად უსაფრთხოების შეუსაბამობა გაუთვალისწინებელი რჩება გარკვეულ ინციდენტამდე. ფსიქოლოგმა დანიელ კანემანმა, 2002 წლის ნობელის პრემიის ლაურეატმა ეკონომიკაში ადამიანური მიკერძოების შესახებ გადაწყვეტილების მიღების პროცესში მუშაობისთვის აღწერა ორი სფერო: სისტემა 1 და სისტემა 2 (სწრაფი და ნელი აზროვნება). ერთი ძალიან მნიშვნელოვანი ფაქტია ის, რომ ადამიანების მიერ განხორციელებული აქტივობების უმეტესობა ხორციელდება პირველი სისტემის რეჟიმში, რომელიც ეფექტურს გვხდის. ადამიანები თავიანთი საქმიანობის უმეტეს ნაწილს მეორე სისტემის რეჟიმში რომ ასრულებდნენ. მოწოდება „Take Five“ არარეალურია, როდესაც ადამიანები იღებენ ათობით სამუშაო წერილს ბმულებით. გარდა ამისა, თუ ამ ბმულზე დაწკაპუნების გარეშე ან პერსონალური ინფორმაციის მიწოდების გარეშე არ არსებობს

ძირითადი ამოცანის შესრულების გზა, პროდუქტიულობა სერიოზული საფრთხის ქვეშ ექცევა.

გარდა ამისა, თავდავცის ზომების დატვირთვის გათვალისწინებით, თავდაცვის ექსპერტებმა უნდა განიხილონ ის გავლენა, რაც მათი რჩევების დაცვას აქვს ადამიანების უნარზე, რომ შეასრულონ თავიანთი დავალებები, ისევე როგორც გავლენა ორგანიზაციასა და თანამშრომლებს შორის კომუნიკაციის ეფექტურობაზე. მაგალითად, დომენზე დაფუძნებული შეტყობინებების ავთენტიფიკაციის მოხსენებისა და შესაბამისობის (DMARC) გამოყენებამ თანამშრომლებს უნდა მისცეს საშუალება, განასხვავონ ნამდვილი შიდა კომუნიკაციები პოტენციური ფიშინგის მცდელობებისაგან. DMARC-ის გამოყენებამ „უსაფრთხო“ გამომგზავნის საიმედო მითითების უზრუნველსაყოფად შესაძლოა შეამციროს ელექტრონული წერილების რაოდენობა, რომლებიც საფრთხეს შეიცავენ. ულტრა უსაფრთხო დათვალიერების ტექნოლოგიის უზრუნველყოფა, რომელიც ახლა უკვე ხელმისაწვდომია, ნიშნავს, რომ ბმულებზე დაწკაპუნებას არ გააჩნია უარყოფითი შედეგები, ამიტომ მომხმარებლის განათლება და ტრენინგი შეიძლება მოხმარდეს სოციალური ინჟინერიისა და მანიპულაციის ტექნიკის ახსნას.

კომპლექსურ პრობლემებთან გამკლავებისას ადამიანებს ხშირად უწევთ როგორც სწრაფი, ისე ნელი პროცესების გაერთიანება და შედეგად შედიან ე.წ შერეული რეჟიმში, სადაც დავალების შესრულება არ ხდება სრულად ავტომატურად: ზოგიერთი ქცევა ავტომატურია, მაგრამ აუცილებელია შეგნებულად მუშაობაც. პროდუქტიულობის ხარჯების გარდა, ის უსაფრთხოების ექსპერტები, რომლებიც ურჩევენ ადამიანებს “შეჩერებას და ფიქრს” თვლიან, რომ „ნელი რეჟიმი“ „უსაფრთხო რეჟიმს“ წარმოადგენს. მაგალითად, ნელი რეჟიმშ ყოფნამ ასევე შეიძლება გამოიწვიოს ზედმეტი ფიქრი, მტკიცებულებების რაციონალიზაცია, არასწორ მიზნებზე ფოკუსირება (მაგ. წარმოების მიზნები) და დროისა და ენერგიის დაკარგვა. ფაქტობრივად, ოპერაციის თითოეულ ამ რეჟიმს გააჩნია საკუთარი ტიპის ადამიანური ნაკლი.

შეგნებულ რეჟიმშიც კი, ადამიანები ცდილობენ იყვნენ ეფექტურები. ისინი მიჰყვებიან იმ ქცევებს, რომლებსაც ხშირად იყენებენ, ან ისეთ ქცევას, რომლებიც ყველაზე მეტად შესაფერისი ჩანს იმ სიტუაციაში, რომელშიც ისინი ხვდებიან. თავდამსხმელები ამას საკუთარი

მიზნებისთვის იყენებენ მსგავსი ვებსაიტების შექმნით, ან უსაფრთხოების შეტყობინებების ჩართვით მათ ფიშინგ ელ-ფოსტაში. Reason განსაზღვრავს გაუცნობიერებელი წარუმატებლობის ოთხ ტიპს:

1. ინდივიდუალური ფაქტორები, რომელიც მოიცავს დაღლილობას, ასევე გამოუცდელობასა და რისკისადმი არასწორ მიდგომას.

2. ადამიანური ფაქტორები მოიცავს მეხსიერების შეზღუდვებს, საერთო ჩვევებსა და გავრცელებულ ცრურწმენებს.

3. სამუშაო ფაქტორები მოიცავს დროის ზეწოლას, დიდ დატვირთვას და მრავალ დავალებას, მაგრამ ერთფეროვნება და მოწყენილობა ერთნაირად იწვევს შეცდომებს, რადგან ადამიანების ყურადღება იფანტება. როლების, პასუხისმგებლობისა და წესების შესახებ გაურკვევლობა ასევე იწვევს არასწორ არჩევანს.

4. სამუშაო გარემოს ფაქტორები მოიცავს ამოცანების შეფერხებას, ცუდ აღჭურვილობასა და ინფორმაციას. ადამიანები ასევე მეტ შეცდომებს უშვებენ, როდესაც იცვლება წესები და პროცედურები.

ამოცანები და სამუშაო გარემო ფაქტორები ორგანიზაციის პასუხისმგებლობას წარმოადგენს. რეგულარული მიმოხილვები უნდა იყოს იმის შესახებ, თუ რამდენად კარგად არის დაცული უსაფრთხოების მექანიზმები. თუ ეს არ ხდება, მაშინ უნდა მოხდეს გამომწვევი მიზეზების იდენტიფიცირება და აღმოფხვრა. ის შეცდომებიც კი, რომელთაც ინციდენტი არ მოჰყოლიათ, ანალოგიურად უნდა იქნას გამოყენებული გამომწვევი მიზეზების იდენტიფიცირებისთვის. ჩვენ ასევე უნდა გავიგოთ, თუ როგორ რეაგირებენ ადამიანები სტრესის პირობებში, მაგალითად, როდესაც განვითარებული თავდასხმის წინაშე დგანან.

„არასოდეს მიიღოთ ისეთი უსაფრთხოების პოლიტიკა, რომლის შესრულებაც შეუძლებელია“. მეორე მსოფლიო ომის ცნობილმა სამხედრო ლიდერმა გენერალმა დუგლას მაკართურმა გაავრცელა ფრაზა „არასოდეს გასცეთ ბრძანება, რომლის შესრულებაც შეუძლებელია“. მან აღიარა იმ ბრძანების დამანგრეველი გავლენა, რომლის შესრულებაც შეუძლებელია - რადგან ის ძირს უთხრის ყველა ბრძანების და ზემდგომების სანდოობას, რომლებიც მას გასცემენ და ბადებს გაურკვევლობას და ეჭვს. ეს იგივეა უსაფრთხოების

პოლიტიკის შემთხვევაშიც, როდესაც თანამშრომლები არიან ისეთი უსაფრთხოების პროტოკოლის წინაშე, რომლის დაცვა შეუძლებელია ან არაეფექტურია, ისინი უსაფრთხოების ყველა პოლიტიკაში ეჭვის შეიტანენ. ამიტომ უსაფრთხოების სწორი პოლიტიკა აუცილებელია. როდესაც უსაფრთხოების პროტოკოლები არაა დაცული, უსაფრთხოების პროფესიონალებმა უნდა გამოიკვლიონ არაკონფრონტაციული გზით, თუ რატომ არ ხდება მათი სწორად შესრულება. კირლაპოსმა და სხვებმა აღნიშნეს, რომ უმეტეს შემთხვევაში, თანამშრომლები პირდაპირ არ უგულებელყოფენ უსაფრთხოებას, მაგრამ ცდილობენ მართონ რისკი ისე, როგორც მათ იციან. ამ მეთოდს ჩრდილოვან უსაფრთხოებას უწოდებენ. მათ მიერ მიღებული გადაწყვეტილებები უსაფრთხოების საკითხში შეიძლება არ იყოს ეფექტური, მაგრამ რადგან ის "მუშაობს", კითხვა „როგორ შევძლოთ ეს უსაფრთხოდ" კარგი საწყისი წერტილია იმ მეთოდის მოსაძებნად, რომელიც პიროვნებების ინტერესებსაც გაითვალისწინებს.

კიბერუსაფრთხოების ინფორმირებულობა და განათლება

უსაფრთხოების ცნობიერების მიზანია ხალხის ყურადღების მიპყრობა და მათი დარწმუნება, რომ ღირს უსაფრთხოების გათვალისწინება. იმის გათვალისწინებით, რომ ბევრ ორგანიზაციაში გავრცელებულია თავდაცვის ზომების მიმართ ზერელე დამოკიდებულება, შეგვიძლია დავესესხოთ კორმაკ ჰერლეის ციტატას: მეტი არაა პასუხი: ბევრი კომუნიკაციის დამიზნება უკუშედეგს მოიტანს. ჩვენ უნდა მივიპყროთ ხალხის ყურადღება და გავაცნობიერებინოთ, რომ (ა) კიბერუსაფრთხოება მათთვისაა მნიშვნელოვანია და (ბ) არსებობს შესაძლებელი ნაბიჯები, რომელთა გადადგმაც შეუძლიათ რისკის შესამცირებლად. ეფექტურად ცნობიერების ამაღლება არ არის ადვილი ამოცანა უსაფრთხოების სპეციალისტებისთვის.

უსაფრთხოების განათლება - მას შემდეგ, რაც ადამიანებს სურთ, რომ მეტი გაიგონ კიბერუსაფრთხოების შესახებ, ჩვენ შეგვიძლია მივაწოდოთ ინფორმაცია მათ რისკების შესახებ და თუ რა შეუძლიათ გააკეთონ მათგან თავის დასაცავად. ადამიანთა უმეტესობას ამჟამად ძალიან არასრული და ხშირად არასწორი წარმოდგენები აქვს

კიბერრისკებზე. სწორი წარმოდგენების ჩამოყალიბება საშუალებას გვაძლევს კიბერუსაფრთხოების უნარების ჩამოყალიბებისთვის.

უსაფრთხოების ტრენინგი.

ტრენინგი ეხმარება ადამიანებს, რომ შეიძინონ უნარები, მაგალითად, თუ როგორ გამოიყენონ უსაფრთხოების კონკრეტული მექანიზმი სწორად, როგორ ამოიცნონ და უპასუხონ სოციალური ინჟინერიის შეტევას. გარდა იმისა, რომ ვაჩვენოთ ადამიანებს, როგორ გააკეთონ რაღაც, ჩვენ უნდა დავუჭიროთ მხარი უნარების შეძენას და მათ გამოყენებას ისეთ გარემოში, სადაც შესაძლოა უსაფრთხოების გადაწყვეტილების მიღებაზე „ექსპერიმენტირება" და მიკერძოებების ასახვა. უნარების ათვისების წახალისება შესაძლებელია ონლაინ, ის ბევრად უფრო ეფექტურია სოციალური საზოგადოებაში.

გავრცელებული ცრურწმენაა, რომ ადამიანები ზემოთ მოცემული საფეხურების გავლის შემდგომ სხვანაირად მოიქცევიან. მაგრამ მხოლოდ იმის ცოდნა, თუ რა და როგორ უნდა გავაკეთოთ, საკმარისი არ არის. ადამიანის მოქმედებების 90% ავტომატურია. უსაფრთხოებაზე ორიენტირებული ქმედებები ადამიანის ტვინში უნდა იყოს მოთავსებული, მაგრამ მის განკუთვნილ ადგილზეა არსებული ქცევა (ძველი პაროლის მსგავსად). გამონათქვამი, რომ „ძველი ჩვევები მარტივად არ კვდება" ზუსტად აღწერს იმ ფაქტს, რომ სანამ არ მოვახერხებთ ძველი ქცევის ახლით ჩანაცვლებას, ცნობიერება, განათლება და ტრენინგი უაზროა. ამის მიღწევა რთულია, ვინაიდან პროდუქტიული აქტივობა უნდა მიმდინარეობდეს ამ ცვლილებების პროცესში. ჩვენ შეგვიძლია უყრადღება ერთდრულოად მხოლოდ ერთ-ორ ქცევას მივაქციოთ და მხოლოდ მათი მთლიანად ჩანაცვლების შემდეგ მივხედოთ დანარჩენებს. ასევე არ უნდა ავურიოთ უსაფრთხოების ცნობიერება და განათლება უსაფრთხოების კულტურასთან. ეს შეიძლება იყოს უსაფრთხოების კულტურის განვითარების ერთ-ერთი ელემენტი, მაგრამ თავისთავად არ არის ეფექტური უსაფრთხოების კულტურის მაგალითი. RISCS White Paper „ცნობიერება მხოლოდ პირველი ნაბიჯია", წარმოადგენს მხარდაჭერის მოდელს, რომელიც ორგანიზაციებმა უნდა გამოიყენონ უსაფრთხოებასთან დაკავშირებული ქცევის ცვლილების მისაღწევად.

ახალი მიდგომები უსაფრთხოების ინფორმირებულობისა და ქცევის ცვლილების მხარდასაჭერად

სიმულაციები და თამაშები სულ უფრო ხშირად გამოიყენება, არამარტო როგორც უსაფრთხოების ცნობიერების ამაღლების შედარებით მიმზიდველ მეთოდებად, არამედ ასევე უფრო კომპლექსური საგანმანათლებლო ზომებისა და ქცევის ცვლილების ჩამოსაყალიბებლად. ფიშინგის საწინააღმდეგო სიმულაციები დღეს ფართოდ გამოიყენება ორგანიზაციებში. მათი პოპულარობა გამომდინარეობს იქიდან, რომ ისინი გვაძლევენ ამ შეფერხებების გავლენის გაზომვის უნარს და ისინი, როგორც წესი, მართლაც ეფექტურები არიან ამ შეფერხებების რაოდენობის შემცირებაში. არგუმენტი იმაში მდგომარეობს, რომ ფიშინგის გამოცდილება არის „სასწავლო მომენტი“, რომელიც იპყრობს თანამშრომლების ყურადღებას და არწმუნებს მათ ამ საგანმანათლებლო პროგრამაში მონაწილეობის მნიშვნელობას. თუმცა, ფოგგი, რომელმაც პირველად შემოიტანა კონცეფცია „გამომწვევი მომენტები“ ცხადადაა დარწმუნებული, რომ ისი გამოიწვევს ქცევათა ცვლილებას მხოლოდ იმ შემთხვევაში, თუ ადამიანს აქვს ტრენინგში ჩართვის მოტივაცია და ნასწავლი უნარების გამოყენების უნარი. ჯოინსონი ამტკიცებს, რომ სოციალური ინჟინერიის გამომყენებელი თავდამსხმელების მიერ გარკვეული ემოციური და კონტექსტური გამომწვევები იმდენად მიზანმიმართული და მძლავრია (მაგალითად, შეტყობინება, რომელიც ამტკიცებს, რომ ინფორმაციას აქვს მოძრაობის ან საზოგადოებრივი ტრანსპორტის შეფერხების შესახებ სამუშაო დღის დასრულებამდე ცოტა ხნით ადრე), რომ მათი თავიდან აცილება შეუძლებელია ტრენინგით.

ადამიანური ფაქტორის პერსპექტივიდან, ფიშინგის საწინააღმდეგო სიმულაციები შეიძლება პრობლემური აღმოჩნდეს, რადგან: 1) რადგან თანამშრომლებმა შეიძლება აღიქვან ეს, როგორც თავდასხმა საკუთარი ორგანიზაციის მიერ, რაც ამცირებს ნდობას და 2) მათ შეუძლიათ იმდენად დააშინონ თანმშრომლები, რომ ისინი უკვე ნამდვილ ელფოსტასაც არ პასუხობენ. ეს ფაქტორები გულდასმით უნდა იქნას გათვალისწინებული ნებისმიერი ასეთი სიმულაციის დიზაინში. გარდა ამისა, როგორც ზემოთ განვიხილეთ, ისეთი მექანიზმების გამოყენებამ, როგორიცაა DMARC, შეიძლება შეამციროს საეჭვო ელწერილების რაოდენობა, რომლებზეც მომხმარებლებმა უნდა გაამახვილონ ყურადღება, რაც საშუალებას მოგვცემს მიმართული

სოციალური ინჟინერიისა და მანიპულაციის ტექნიკის უკეთესად ახსნაზე კონცენტრაციის შესაძლებლობას.

უსაფრთხოების ცნობიერების ასამაღლებელი თამაშები

Capture The Flag (CTF) თამაშები შექმნილია მოწყვლადობის შესახებ ცნობიერების ასამაღლებლად. მათი იდეა იმაში მდგომარეობს, რომ იმის დანახვით, თუ როგორ შეიძლება დაუცველობის გამოყენება სისტემაზე თავდასხმისთვის, დამცველები ისწავლიან თავდაცვის სწორი მეთოდების გამოყენებას საკუთარ სისტემებში. თუმცა, აქცენტი ამ თამაშებში ძირითადად კეთდება ორგანიზაციის უსაფრთხოებაზე პასუხისმგებელი პირების მომზადებაზე და არა მომხმარებელთა და თანამშრომელთა უფრო ფართო ჯგუფზე. არსებობს მაგიდის კარტის თამაშები, რომლებიც მიზნად ისახავს უსაფრთხოების ცნობიერების ამაღლებას ორგანიზაციებში მყოფ ფართო მომხმარებელთა ჯგუფებში. მაგალითად, Ctrl-Alt-Hack, dox3d!a და სხვა, რომლებიც სპეციალურად შექმნილი ICT სპეციალისტებისა და დეველოპერებისთვის. ასევე არსებობს სამაგიდო თამაშები, რომლებიც შექმნილია კიბერუსაფრთხოების საფრთხეებისა და კიბერრისკების შესახებ ცნობიერების ასამაღლებლად, მაგ., "გადაწყვეტილებები და შეფერხებები". ყველა ამ თამაშს აქვს სოციალური სწავლის გამოცდილების შეთავაზების პოტენციური უპირატესობა ჯგუფში თამაშის შემთხვევაში. მაგრამ, თუ ისინი შვიათად გამოიყენება, ნაკლებად სავარაუდოა, რომ მათ ექნებათ ხანგრძლივი ეფექტი. მთლიანობაში, თამაშებსა და სიმულაციებს აქვთ შესაძლებლობა, რომ შესთავაზონ ინდივიდებს ახალი ელემენტები, რომლებიც შეიძლება გამოყენებულ იქნას ქცევის ცვლილების მოდელის სხვადასხვა ეტაპზე, მაგრამ ისინი უნდა იყვნენ ქცევის შეცვლის დაგეგმილი პროგრამის ნაწილი და არა ერთჯერადი ინტერვენციები.

პოზიტიური უსაფრთხოება

რა არის კიბერუსაფრთხოების მიზანი? ამ კითხვაზე ადამიანების უმრავლესობის პირველი პასუხი არის კიბერშეტევების თავიდან აცილება ან თავდასხმების წარმატებისა და ზარალის რისკის შემცირება. როგორც ფლორენციომ და სხვებმა აღნიშნეს, იმ პირებს,

ვისაც სურთ, რომ ორგანიზაციებმა უფრო სერიოზულად აღიქვან უსაფრთხოება, მიმართავენ „შიშის, გაურკვევლობის და ეჭვის" (FUD) მეთოდს - ისინი ბადებენ შიშს შესაძლო თავდასხმებსა და მათ შედეგებზე, შემოაქვთ გაურკვევლობა შედეგების შესახებ და ბადებენ ეჭვს ორგანიზაციის უნარში, რათა დაიცვას საკუთარი თავი.

უსაფრთხოების პრაქტიკოსები დღეს ჩივიან, რომ ადამიანებისა და ბიზნესების უმეტესობა სერიოზულად არ იღებს კიბერრისკებს. პრობლემა ის არის, რომ შიშის გამოყენება არ არის კარგი საფუძველი თავდაცვითი უნარების გასაუმჯობესებლად: როდესაც უსაფრთხოების სფეროში მიღებული ინვესტიცია არაეფექტურია, მომხმარებლები სკეპტიკურად უყურებენ კიბერუსაფრთხოების სარგებელს.

ახალი საფრთხეებისგან თავის დასაცავად, კომპანიებს სჭირდებათ მეტი, ვიდრე პასიური მორჩილება - მათ სჭირდებათ თანამშრომლები, რომლებსაც სურთ ორგანიზაციის დაცვა და იმ პასუხისმგებლობის გათვალისწინება, რომლებიც მათ ეკისრებათ თავდაცვის სფეროში. ამის მისაღწევად აუცილებელია თავდაცვის, როგორც სანდო და საიმედო ზომის წარმოჩენა. პოზიტიური უსაფრთხოება გვთავაზობს უფრო მეტს, ვიდრე უბრალოდ რაიმეეს დაცვას. ის საშუალებას გვაძლევს, რომ ჩავერთოთ აქტივობებში, რომლებსაც ვაფასებთ. რო ამტკიცებს, რომ უსაფრთხოების პოზიტიური კონცეფცია იდეებს შემოიტანს ახალი პოლიტიკის ვარიანტებისა და ინტერვენციებისთვის და წაახალისებს ინდივიდებს ან ჯგუფებს, რომ უფრო მეტად ჩაერთონ ამ პროცესში.

პოზიტიური უსაფრთხოების კიდევ ერთი მთავარი ასპექტი არის ენა, რომელსაც ვიყენებთ მასთან დაკავშირებით. როგორც პირველი ნაბიჯი, ჩვენ უნდა შევწყვიტოთ იმ ადამიანების დემონიზაციის პრაქტიკა, რომლებსაც არ სურთ ან არ შეუძლიათ დაიცვან უსაფრთხოების ზომები: ამ ადამიანებისათვის „ყველაზე სუსტი რგოლის" იარლიყის მიკერება მათ წარმოაჩენს, როგორც უვიც პიროვნებებს.

დაინტერესებული მხარეების ჩართულობა

გასული ათწლეულის განმავლობაში კიბერუსაფრთხოებაში ადამიანის ქცევის შესახებ ჩატარებული გამოკვლევიდან ერთი ძალიან მკაფიო თემა გამოიკვეთა: თანამშრომლებისთვის უსაფრთხოების ფუნქციონირების გზების პოვნაში ჩართულობის მნიშვნელობა. ამ

მხრივ მნიშვნელოვანია კომუნიკაცია და ლიდერობა. ლიზი კოულზ-კემპმა და მისმა კოლეგებმა შეიმუშავეს მიდგომა, რომელიც თანამშრომლების ჩართულობაზე კიდევ უფრო გამახვილებულია. ისინი იყენებენ პროექციულ ტექნიკას (მაგალითად, ნახატებს და კოლაჟებს) ყოველდღიური აქტივობების წარმოდგენის შესაქმნელად და უსაფრთხოების შესახებ დისკუსიის დასაბადებლად. კვლევები აჩვენებს, თუ როგორ ეხმარება ეს მერყევი ქცევების ძირეული მიზეზების იდენტიფიცირებას. ხშირ შემთხვევაში ეს ცუდად შემუშავებული უსაფრთხოების ზომებია (Beautement et al. შედეგების ეხმიანება), მაგრამ ასევე გვხვდება უფრო ფუნდამენტური პრობლემებიც, რომელიც ორგანიზაციაში არსებობს.

კრეატიული უსაფრთხოების ჩართულობები (პირველად ნახსენები Dunphy-ს მიერ.) მოუწოდებს მონაწილეებს (თანამშრომლებს კომპანიის კონტექსტში ან მომხმარებლებს ან მოქალაქეებს უფრო ფართო ჩართულობით) დაფიქრდნენ:

- მათი გარემოზე;
- ემოციებზე, რომლებსაც ისინი განიცდიან;
- შეზღუდვებზე, რომელიც მათ აქვთ;
- მათზე არსებულ ზეწოლაზე;
- მოქმედებებზე და ამოცანებზე, რომლებსაც ისინი ასრულებენ ინფორმაციის შექმნისა და გაზიარებისას.

ინფორმაციული უსაფრთხოების საფრთხეების ფიზიკური მოდელირებისთვის Lego-ს გამოყენებით შემოქმედებითი ჩართულობის ერთი კონკრეტული ტექნიკა შეიმუშავა EU Trespass Project-მა. ფიზიკური მოდელირების ეს მეთოდი აკავშირებს ტიპიურ დიაგრამებს (ნაკადის დიაგრამები და ერთიანი მოდელირების ენის (UML) დიაგრამები), რომლებზეც ჩვეულებრივ მუშაობენ უსაფრთხოების პრაქტიკოსები და მომხმარებლების ყოველდღიურ პრაქტიკას, რომლებზეც გავლენას ახდენს უსაფრთხოების დიზაინი. Heath, Hall & Coles-Kemp-მა აღნიშნეს ამ მეთოდის წარმატებული შემთხვევის შესწავლას ბანკინგის აპლიკაციის უსაფრთხოების მოდელირებისთვის, რომელმაც გამოავლინა ის სფეროები, სადაც ადამიანის ჩარევა და მხარდაჭერა იყო საჭირო იმისათვის, რომ უსაფრთხოებამ მთლიანობაში იმუშაოს. ეს კვლევები იძლევა

უსაფრთხოების საკითხებში თანამშრომლებთან, მომხმარებლებთან და მოქალაქეებთან ურთიერთობის სხვადასხვა გზების მაგალითებს. ისინი წარმოადგენენ კვლევის მზარდი ტენდენციების ნაწილს, რომლებიც შორდებიან ინდივიდებში თვისებების ძიების მექანიკურ მიდგომას. ამ მიდგომების ყურადღება გამახვილებულია უსაფრთხოების დიზაინის შეცვლაზე მომხმარებლისა და ორგანიზაციის სასარგებლოდ.

პროგრამული უზრუნველყოფის შემქმნელები და უსაფრთხოება

საბოლოო მომხმარებლები არ არიან ერთადერთები, რომლებსაც აქვთ პაროლებთან პრობლემები. იმ დეველოპერებს, რომლებიც წერენ კოდებს, რომელთა მეშვეობითაც პაროლები ინახება, აუცილებლად უსაფრთხოდ უნდა იმოქმედონ. მიუხედავად ამისა, ხშირად ვხდებით ფაქტის წინაშე, რომ ეს რთული ამოცანა ხშირად კატასტროფული შედეგებით მთავრდება. თუ დეველოპერებს დაავიწყდებათ პაროლის მონაცემთა ბაზის სათანადოდ დაცვა, ამან შეიძლება გამოიწვიოს საბოლოო მომხმარებლთა მილიონობით პაროლის გატეხვა. ნაიაკშინამ და სხვ, ჩაატარა შემთხვევითი ბუნების საკონტროლო ტესტი კომპიუტერული მეცნიერების სტუდენტებთან და თავისუფალ დეველოპერებთან და დაადგინა, რომ საბოლოო მომხმარებლების მსგავსად, დეველოპერები ძირითადად ამოცანის შესრულებაზე მუშაობენ და უსაფრთხოებას მეორეხარისხოვნად მიიჩნევენ. არცერთი სტუდენტი და მხოლოდ თავისუფალი დეველოპერების მცირე ნაწილი იღებდა რაიმე სახის უსაფრთხოების ზომებს, თუ ამის შესახებ აშკარა მოთხოვნა არ არსებობდა. საინტერესოა, რომ იმ მონაწილეთაგან, რომლებმაც მიიღეს უსაფრთხოების გარკვეული ზომები, სტუდენტების მიერ მიღებული ზომები უკეთესად იყო შესრულებული, ვიდრე თავისუფალ დეველოპერებსა, რომლებიც უფრო მოძველებულ და არასწორ კრიპტოგრაფიულ მექანიზმებს იყენებდნენ თავიანთი პაროლების შესანახად.

Acar-მა და სხვ. შეისწავლეს ონლაინ სოციალური ქსელების გავლენა (როგორიცაა StackOverflow) იმ კოდის უსაფრთხოებაზე, რომელსაც დეველოპერები ქმნიან. დეველოპერების ორმა მესამედმა, რომლებიც იყენებდნენ StackOverflow-ს ან სახელმძღვანელოს, მოახერხა გამოყოფილი დროის განმავლობაში სწორი გამოსავლის პოვნა, მაშინ

როცა ოფიციალურ დოკუმენტაციის მომხამრებლების მხოლოდ 40%-მა შეძლო ამის გაკეთება. უსაფრთხოების ამოცანების თვალსაზრისით კი შედეგები სხვაგვარი აღმოჩნდა. ისინი, ვინც იყენებდნენ ოფიციალურ დოკუმენტაციას, აწარმოებდნენ ყველაზე სანდო კოდებს, ხოლო StackOverflow-ს მომხმარებლები კი ყველაზე ნაკლებად უსაფრთხოს. ამ შედეგზე ტრადიციული პასუხი იქნება, რომ „StackOverflow-ის გამოყენება უნდა აიკრძალოს“. მაგრამ ცხადია, რომ ეს პროდუქტიულობას მეტად დააზარალებს. მაგალითად, ბოლოდროინდელმა სამუშაოებმა აჩვენა, რომ დეველოპერები იყენებენ ასეთ ფორუმებს ინფორმაციის გაცვლისა და ურთიერთდახმარების შეთავაზებისთვის. ეს არ ნიშნავს, რომ ასეთი რჩევები ყოველთვის ეფექტურია (როგორც ზემოთ აღინიშნა), მაგრამ ფორუმები უზრუნველყოფს პრაქტიკული საზოგადოების არსებობას, რომელშიც დეველოპერებს შეუძლიათ თავიანთი პრობლემების გაზიარება და დახმარების ძებნა. ასეთი ფორუმების პირდაპირი აკრძალვა მათი შესაბამისი მხარდაჭერით ჩანაცვლების გარეშე, შესაბამისად, არ გადაწყვეტს იმ პრობლემას, რის გამოც ეძებენ დეველოპერები ასეთ მხარდაჭერას.

პოლიტიკა

უსაფრთხოების პოლიტიკა არის უსაფრთხოების მიზნების კომპლექტი კომპანიისთვის, რომელიც მოიცავს მომხმარებელთა და ადმინისტრატორთა ქცევის წესებს და განსაზღვრავს სისტემის მოთხოვნებს. ეს მიზნები, წესები და მოთხოვნები ერთობლივად უზრუნველყოფენ ორგანიზაციის ფარგლებში ქსელის, მონაცემებისა და კომპიუტერული სისტემების უსაფრთხოებას.

უსაფრთხოების ყოვლისმომცველი პოლიტიკა ასრულებს რამდენიმე ამოცანას:

- ახდენს ორგანიზაციის ვალდებულების დემონსტრაციას უსაფრთხოების მიმართ;
- იგი ადგენს წესების გარკვეულ ჩამონათვალს მოსალოდნელი მოვლენებისადმი რეაგირების მიმართ;
- იგი უზრუნველყოფს სისტემური ოპერაციების, პროგრამული უზრუნველყოფის და აპარატურის შეძენისა და გამოყენების თანმიმდევრულობასა და მხარდაჭერას;

- იგი განსაზღვრავს დარღვევების სამართლებრივ შედეგებს;
- იგი აძლევს უსაფრთხოების პერსონალს მენეჯმენტის მხარდაჭერას.

უსაფრთხოების პოლიტიკა აცნობს მომხმარებლებს, თანამშრომლებს და მენეჯერებს ორგანიზაციის მოთხოვნებს ტექნოლოგიისა და ინფორმაციული აქტივების დაცვის შესახებ. უსაფრთხოების პოლიტიკა ასევე განსაზღვრავს უსაფრთხოების მოთხოვნების დასაკმაყოფილებლად საჭირო მექანიზმებს.

უსაფრთხოების პოლიტიკა, როგორც წესი, მოიცავს:

- იდენტიფიკაციისა და ავტორიზაციის პოლიტიკა - განსაზღვრავს ავტორიზებულ პერსონალს, რომელსაც გააჩნია წვდომა ქსელის რესურსებთან და მართავს ვერიფიკაციის პროცესს;
- პაროლების პოლიტიკა - უზრუნველყოფს პაროლთა სირთულის პოლიტიკას და განსაზღვრავს მათი ცვლილების სიხშირეს;
- დასაშვები გამოყენების პოლიტიკა - ახდენს ქსელის რესურსების იდენტიფიცირებას და მათი გამოყენების მიზანშეწონილობას ორგანიზაციისათვის. მან ასევე შესაძლოა განსაზღვროს სახდელი უსაფრთხოების პოლიტიკის დარღვევისათვის;
- დისტანციური წვდომის პოლიტიკები - განსაზღვრავს დისტანციური მომხმარებლის ქსელის რესურსებთან წვდომის წესს;
- ქსელის მხარდაჭერის პოლიტიკა - განსაზღვრავს ქსელური ოპერაციული სისტემის ტიპს და მომხმარებელთა აპლიკაციების განახლების პროცესს;
- ინციდენტებზე რეაგირების პოლიტიკა - განსაზღვრავს ინციდენტთა აღმოფხვრის წესებს.

ერთ-ერთი ყველაზე გავრცელებული უსაფრთხოების პოლიტიკის კომპონენტს წარმოადგენს დასაშვები გამოყენების წესები (AUP). ეს კომპონენტი განსაზღვრავს, რომელ მომხმარებლებს აქვთ ან არ აქვთ წვდომა სისტემის სხვადასხვა კომპონენტებზე. AUP-ის წესები უნდა იყოს მაქსიმალურად გამჭვირვალე, რათა თავიდან იქნას აცილებული გაუგებრობა. მაგალითად, AUP-ში ჩამოთვლილი უნდა იყოს

კონკრეტული ვებგვერდები, საინფორმაციო ჯგუფები, ან პროგრამები, რათა მომხმარებლებს არ შეეძლოთ მათზე წვდომა ორგანიზაციის კომპიუტერების ან ქსელის გამოყენებით.

მკაცრად გაწერილი სტანდარტები საშუალებას აძლევს IT თანამშრომლებს შეინარჩუნონ თანმიმდევრულობა ქსელის ფუნქციონირებაში. სტანდარტების დოკუმენტები უზრუნველყოფს იმ ტექნოლოგიებს, რომლებიც სპეციფიკურ მომხმარებლებს ან პროგრამებს სჭირდებათ დამატებით ნებისმიერი პროგრამის მოთხოვნებსა ან კრიტერიუმებზე, რომლებიც ორგანიზაციამ უნდა დაიცვას. ეს ხელს უწყობს IT პერსონალს, გაუმჯობესოს ეფექტიანობა და უფრო მარტივი გახადოს სისტემის მხარდაჭერა და გაუმართაობების აღმოფხვრის პროცესი.

ერთ-ერთი ყველაზე მნიშვნელოვანი უსაფრთხოების პრინციპია თანმიმდევრულობა. ამისათვის აუცილებელია ორგანიზაციებისთვის სტანდარტების დამკვიდრება. თითოეული ორგანიზაცია ავითარებს სტანდარტებს თავისი უნიკალური საოპერაციო გარემოს მხარდასაჭერად. მაგალითად, ორგანიზაცია ადგენს პაროლის პოლიტიკას. სტანდარტის თანახმად პაროლები მოითხოვენ მინიმუმ რვა მაღალი და დაბალი რეგისტრის სიმბოლოებს, მათ შორის მინიმუმ ერთს უნიკალურ სიმბოლოს. მომხმარებელმა უნდა შეიცვალოს პაროლი ყოველ 30 დღეში, ხოლო 12 წინა პაროლის ისტორია უზრუნველყოფს მომხმარებლის მიერ უნიკალური პაროლების შექმნას ერთი წლის განმავლობაში.

სახელმძღვანელო წარმოადგენს მითითებების ჩამონათვალს, როგორ ვიმოქმედოთ უფრო ეფექტურად და უსაფრთხოდ. ისინი სტანდარტების მსგავსია, მაგრამ უფრო მოქნილია და ჩვეულებრივ, სავალდებულო არ არის. სახელმძღვანელო პრინციპები განსაზღვრავენ, თუ როგორ ვითარდება სტანდარტები და უზრუნველყოფენ უსაფრთხოების ზოგადი პოლიტიკის დაცვას.

ზოგიერთ შემთხვევაში ყველაზე სასარგებლო სახელმძღვანელო პრინციპებს ქმნის ორგანიზაციის პრაქტიკა. ორგანიზაციის მიერ განსაზღვრული საუკეთესო პრაქტიკის გარდა, სახელმძღვანელო მითითებები ასევე შესაძლოა ხელმისაწვდომი იყოს შემდეგნაირად:

- სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტი (NIST) კომპიუტერული უსაფრთხოების რესურსცენტრი

- ეროვნული უსაფრთხოების სააგენტოს (NSA) უსაფრთხოების კონფიგურაციის მითითებები
- საერთო კრიტერიუმების სტანდარტი

პაროლის პოლიტიკის მაგალითის გამოყენებით, სახელმძღვანელოში მითითებულია, რომ მომხმარებელმა აარჩიოს ფრაზა, როგორიცაა „I have dream" და დააკონვერტიროს ის ძლიერ პაროლში, "Ihv @dr3 @m". მომხმარებელს შეუძლია შექმნას სხვა პაროლები ამ ფრაზისგან ნომრის შეცვლით, სიმბოლოების გადაადგილებით ან პუნქტუაციის ნიშნის შეცვლით.

პროცედურული დოკუმენტები უფრო დიდი მოცულობის და უფრო დეტალურია, ვიდრე სტანდარტები და სახელმძღვანელო მითითებები. პროცედურული დოკუმენტები მოიცავს განხორციელების დეტალებს, რომლებიც, როგორც წესი, შეიცავენ ნაბიჯ-ნაბიჯ ინსტრუქციებს

მსხვილმა ორგანიზაციებმა უნდა გამოიყენონ პროცედურული დოკუმენტები, რათა შეინარჩუნონ რეალიზაციის თანმიმდევრულობა, რაც აუცილებელია უსაფრთხო გარემოსთვის.

2.5 ISO ინფორმაციული უსაფრთხოების მოდელი

მოდელის მიმოხილვა

უსაფრთხოების სპეციალისტებმა უნდა უზრუნველყონ ინფორმაციის დაცვა ორგანიზაციის ფარგლებში მისი გენერირების წყაროდან დანიშნულების ობიექტამდე. ეს საკმაოდ მოცულობითი ამოცანაა და ძნელად წარმოსადგენია, რომ ერთი ადამიანის ცოდნა ეყოს მის სათანადო განხორციელებას. სტანდარტიზაციის საერთაშორისო ორგანიზაცია (ISO)/საერთაშორისო ელექტროტექნიკური კომისია (IEC)-მ შეიმუშავა ყოვლისმომცველი ჩარჩო ინფორმაციული უსაფრთხოების მართვისთვის. ISO/IEC კიბერუსაფრთხოების მოდელი კიბერუსაფრთხოების პროფესიონალებისთვის არის ის, რაც OSI ქსელის მოდელია ქსელის ინჟინრებისთვის. ორივე უზრუნველყოფს კომპლექსური ამოცანების გააზრებას და არ სცილდება გარკვეულ ჩარჩოებს.

კიბერუსაფრთხოების დომენები

ISO/IEC 27000 წარმოადგენს ინფორმაციული უსაფრთხოების სტანდარტს, რომელიც პირველად გამოქვეყნდა 2005 წელს და ბოლოს განახლდა 2022 წელს. ISO აქვეყნებს ISO 27000 სტანდარტებს. მიუხედავად იმისა, რომ სტანდარტები სავალდებულო არ არის, ქვეყნების უმრავლესობა მათ ინფორმაციული უსაფრთხოების განსახორციელებლად დე-ფაქტო ჩარჩოდ იყენებს.

ISO 27000 სტანდარტი აღწერს ყოვლისმომცველი ინფორმაციული უსაფრთხოების მართვის სისტემის (ISMS) განხორციელებას. ISMS შეიცავს ყველა ადმინისტრაციულ, ტექნიკურ და საოპერაციო კონტროლის მექანიზმს, რათა დაცული იქნას ინფორმაცია ორგანიზაციის ფარგლებში. ISO 27000 სტანდარტის კომპონენტები ემსახურება ინფორმაციული უსაფრთხოების ქოლგის ქვეშ ინფორმაციის ფართო სპექტრის მაღალ დონეზე ორგანიზებას.

ISO კიბერუსაფრთხოების მოდელის სტრუქტურა განსხვავდება OSI მოდელისგან, რომელიც იყენებს დომენებს და არა შრეებს უსაფრთხოების კატეგორიების აღსაწერად. ამის მიზეზი ის არის, რომ ISO კიბერუსაფრთხოების მოდელში არ არის გათვალისწინებული იერარქიული ურთიერთობა. ეს არის თანასწორობის მოდელი, რომელშიც თითოეული დომენი პირდაპირ ურთიერთობაშია სხვა დომენებთან. ISO 27000 კიბერუსაფრთხოების მოდელი ძალიან ჰგავს OSI-ს მოდელს, შესაბამისად, კიბერუსაფრთხოების სპეციალისტებისთვის მნიშვნელოვანია ამის გააზრება წარმატებული საქმიანობისათვის.

თორმეტი დომენი წარმოადგენს უსაფრთხოების ორგანიზაციული სტანდარტებისა და უსაფრთხოების ეფექტური მართვის პრაქტიკის შემუშავების საერთო საფუძველს. ისინი ასევე ხელს უწყობენ ორგანიზაციებს შორის კომუნიკაციას.

მართვის მიზნები

თორმეტი დომენი შეიცავს მართვის მიზნებს, რომლებიც აღწერილნი არიან სტანდარტის 27001 ნაწილში. მართვის მიზნები განსაზღვრავენ ყოვლისმომცველი ISMS-ის მაღალი დონის მოთხოვნებს. ორგანიზაციის მმართველი გუნდი იყენებს ISO 27001 კონტროლის მიზნებს ორგანიზაციის უსაფრთხოების პოლიტიკის განსაზღვრასა და

გამოსაქვეყნებლად. მართვის მიზნები უზრუნველყოფენ ჩამონათვალს, რომელიც გამოიყენება უსაფრთხოების მართვის აუდიტის დროს. ბევრ ორგანიზაციას ესაჭიროება ISMS აუდიტის გავლა, რათა მიიღოს ISO 27001 შესაბამისი სერტიფიკატი.

სერტიფიცირება და შესაბამისობა უზრუნველყოფს ნდობას ორი ორგანიზაციისთვის, რომლებიც უნდა გააჩნდეთ ნდობა ერთმანეთის მიმართ კონფიდენციალურ მონაცემებსა და ოპერაციებზე. შესაბამისობის და უსაფრთხოების აუდიტი ადასტურებს, რომ ორგანიზაციები მუდმივად აუმჯობესებენ ინფორმაციული უსაფრთხოების მართვის სისტემას.

შემდეგი მაგალითი წარმოგვიდგენს მართვის მიზანს:

ქსელებზე ხელმისაწვდომობის კონტროლის განხორციელება მომხმარებლებისა და აპარატურის შესაბამისი ავტორიზაციის მექანიზმების გამოყენებით.

მართვის სისტემები

ISO/IEC 27002 განსაზღვრავს ინფორმაციული უსაფრთხოების სისტემის მართვას. მართვა უფრო დეტალურია, ვიდრე მიზნები. მართვის მიზნები უსახავს ორგანიზაციას სამოქმედო გეგმებს. ისინი განსაზღვრავს, თუ როგორ უნდა იქნეს მიღწეული მიზანი.

მართვის ობიექტზე დაყრდნობით, იმისათვის, რომ განხორციელდეს ქსელებზე წვდომის მართვა მომხმარებლებისა და აპარატურის შესაბამისი ავტორიზაციის მექანიზმების გამოყენებით:

გამოიყენეთ ძლიერი პაროლები. ძლიერი პაროლი შედგება მინიმუმ რვა სიმბოლოსაგან, რომელიც არის ასოების, ნომრებისა და სიმბოლოების კომბინაცია (@, #, $,% და ა. შ.). პაროლები მგრძნობიარეა, ამიტომ ძლიერი პაროლი შეიცავს სიმბოლოებს ორივე - ზედა და ქვედა რეგისტრში.

ISO კიბერუსაფრთხოების მოდელი და CIA ტრიადა

ISO 27000 არის უნივერსალური ჩარჩო ყველა ტიპის ორგანიზაციისთვის. ჩარჩოს ეფექტურად გამოყენების მიზნით, ორგანიზაციამ მკაცრად უნდა განსაზღვროს, თუ რომელი დომენები, კონტროლის მიზნები და კონტროლის მექანიზმები ვრცელდება მის გარემოსა და ოპერაციებზე.

ISO 27001 მართვის მიზნები შეიძლება განხილულ იქნას, როგორც ერთგვარი ჩამონათვალი. ორგანიზაციის პირველი ნაბიჯი არის იმის განსაზღვრა, თუ მართვის მიზნების რა ჩამონათვალის გამოიყენებაა მიზანშეწონილი ორგანიზაციისთვის. ორგანიზაციების უმრავლესობა ქმნის დოკუმენტს, რომელსაც ეწოდება გამოყენებადობის განაცხადი (SOA). SOA განსაზღვრავს კონტროლის მექანიზმებს, რომელთა გამოყენებაც ორგანიზაციას ესაჭიროება.

სხვადასხვა ორგანიზაციები უფრო დიდ პრიორიტეტს ანიჭებენ კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის მხარდაჭერას, რაც დამოკიდებულია ინდუსტრიის ტიპზე. მაგალითად, Google ანიჭებს ყველაზე მაღალ მნიშვნელობას მომხმარებლის მონაცემების კონფიდენციალურობასა და ხელმისაწვდომობას და ნაკლებს - მთლიანობას. Google არ ამოწმებს მომხმარებლის მონაცემებს. Amazon აქცენტს აკეთებს მონაცემთა ხელმისაწვდომობაზე. თუ საიტი არ არის ხელმისაწვდომი, Amazon ვერ გაყიდის პროდუქტს. ეს არ ნიშნავს იმას, რომ Amazon უგულებელყოფს კონფიდენციალურობას ხელმისაწვდომობის სასარგებლოდ. Amazon-ისათვის უბრალოდ უმაღლესი პრიორიტეტი ხელმისაწვდომობაა. აქედან გამომდინარე, Amazon-ს შეუძლია მეტი რესურსის დახარჯვა უზრუნველყოს, რათა რაც შეიძლება მეტი სერვერი გახადოს ხელმისაწვდომი მომხმარებელთათვის.

ორგანიზაცია ახორციელებს თავისი მართვის მიზნების ადაპტაციას და მიმართავს ძალისხმევას მაქსიმალური კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის მისაღწევად.

ორგანიზაციის ფარგლებში თითოეული სხვადასხვა ჯგუფი შეიძლება პასუხისმგებელი იყოს სხვადასხვა ტიპის მონაცემებზე. მაგალითად, ქსელის უსაფრთხოების ჯგუფი პასუხისმგებელია მონაცემებზე მისი გადაცემის დროს. პროგრამისტები და მონაცემთა შეტანის პერსონალი პასუხისმგებელნი არიან მონაცემებზე მისი დამუშავების დროს. აპარატურისა და სერვერის მხარდაჭერის სპეციალისტები პასუხისმგებელნი არიან შენახულ მონაცემებზე. ISO მართვა კონკრეტულად მიმართავს უსაფრთხოების კონტროლის მექანიზმებს თითოეული სამი ტიპის მონაცემისთვის.

მოცემულ მაგალითში, თითოეული წარმომადგენელი სამი ჯგუფის ხელს უწყობს მართვის იდენტიფიცირებას და თითოეული მართვის

პრიორიტეტს მათ საპასუხისმგებლო სექტორში. ქსელის უსაფრთხოების ჯგუფის წარმომადგენელი განსაზღვრავს მართვას, რომელიც უზრუნველყოფს ყველა მონაცემის კონფიდენციალურობას, მთლიანობასა და ხელმისაწვდომობას.

ISO 27001 მართვის მიზნები უშუალოდ ეხება ორგანიზაციის კიბერუსაფრთხოების პოლიტიკას, პროცედურებსა და სახელმძღვანელო პრინციპებს, რომლებსაც TOP მენეჯმენტი განსაზღვრავს. ISO 27002 მართვა უზრუნველყოფს ტექნიკურ მიმართულებას. მაგალითად, TOP მენეჯმენტი ადგენს პოლიტიკას, რომელიც განსაზღვრავს ორგანიზაციის შიგნით ან გარეთ არსებული ყველა მონაცემის დაცვას. პოლიტიკის მიზნების დასაკმაყოფილებლად ტექნოლოგიის დანერგვა არ მოითხოვს ზედა მენეჯმენტის ჩართულობას. IT პროფესიონალების პასუხისმგებლობაა, სწორად შეარჩიონ და გამართონ აპარატურა, რომელიც გამოიყენება TOP მენეჯმენტის მიერ დადგენილი პოლიტიკის შესასრულებლად.

ინფორმაციული უსაფრთხოების რისკი და მართვის საჭიროება

ხანძარი, წყალდიდობა, ძლიერი ყინვა, აფეთქება და ვულკანის ამოფრქვევა იმ მოვლენათა არასრული ჩამონათვალია, რაც საუკუნეების განმავლობაში კაცობრიობის მიერ ფიზიკური ინფრასტრუქტურის წინაშე მდგარ საფრთხეებად მიიჩნეოდა. თუმცა, 21-ე საუკუნეში, თითოეულ მათგანს უკვე ინფორმაციისა და ინფორმაციული სისტემების საფრთხედაც მიიჩნევენ და ისინი განგაშის საფუძველსაც ხშირად ქმნიან. ამას ემატება უშუალოდ კიბერსივრცეში არსებული საფრთხეები, როგორიცაა: შპიონაჟი, ფინანსური თაღლითობები, საბოტაჟი, ინფორმაციის მოპარვა, დაკარგვა და სხვა.

მართლაც, ინფორმაციის მნიშვნელობამ დღეს უმაღლეს ნიშნულს მიაღწია, რითაც ის გახდა ყველაზე კრიტიკული აქტივი, რომელსაც ორგანიზაცია იღებს, ამუშავებს, ცვლის და ინახავს.

ორგანიზაციის ინფორმაციულ სისტემებში არსებული პერსონალური და კონფიდენციალური ინფორმაცია მოწყვლადია როგორც ზემოაღნიშნული ფიზიკური, ასევე კიბერსაფრთხეების წინაშე, რის გამოც ინფორმაციული უსაფრთხოების რისკების მართვას უფრო და უფრო დიდი მნიშვნელობა ენიჭება როგორც კერძო, ასევე საჯარო სექტორში.

ინფორმაციული უსაფრთხოების რისკების მართვა არის უსაფრთხოების წინაშე მდგარი საფრთხეების იდენტიფიცირების, შეფასებისა და მართვის უწყვეტი პროცესი. ის წარმოადგენს ორგანიზაციის მიერ რისკების მართვის განუყოფელ, მნიშვნელოვან ნაწილს, ვინაიდან მის საფუძველზე უნდა იყოს შეთავაზებული უსაფრთხოების ადეკვატური გადაწყვეტები ინფორმაციული სისტემებისა და მონაცემებისთვის.

სხვადასხვა საერთაშორისო სტანდარტები, როგორიცაა ISO, NIST წარმოგვიდგენენ ინფორმაციული უსაფრთხოების რისკის მართვის მეთოდოლოგიას, რომელთაც მსოფლიოში ფართოდ იყენებენ და მათგან მიღებულ სარგებელს დადებითად აფასებენ. თუმცა, ამ სტანდარტების დანერგვას სჭირდება გარკვეული რესურსი და ძალისხმევა, დაწყებული მმართველი რგოლის მხარდაჭერით და დასრულებული ფინანსური ინვესტიციით.

ინფორმაციული უსაფრთხოების რისკი, საერთაშორისო სტანდარტების თანახმად, განიმარტება როგორც შესაძლებლობა იმისა, რომ კონკრეტული საფრთხე, ინფორმაციული აქტივ(ებ)ის სისუსტის გამოყენებით, ზიანს მიაყენებს აქტივს ან აქტივთა ჯგუფს და აღნიშნულით ზიანი მიადგება ორგანიზაციას.

ცხადია, იმ ეპოქაში, როდესაც კიბერთაღლითობას უამრავი მსხვერპლი ჰყავს, ერთ კიბერშეტევას კი შეუძლია ორგანიზაციას ასი ათასობით დოლარის ზარალი მოუტანოს, რეპუტაცია შეულახოს და, უფრო მეტიც, ინფრასტრუქტურა ფიზიკურად გაანადგუროს, საჯარო არეულობა გამოიწვიოს, ან ეროვნული უსაფრთხოების საკითხი კითხვის ნიშნის ქვეშ დააყენოს, საფრთხეების პრევენციის საჭიროებაზე ყურადღების გამახვილების საჭიროება აღარ დგას.

მართლაც, შეუძლებელია 21-ე საუკუნეში კერძო თუ საჯარო დაწესებულება ფუნქციონირებდეს შესაბამისი საფრთხეების იდენტიფიცირებისა და რისკების შეფასების გარეშე. ინფორმაციას და ინფორმაციულ სისტემებს შეიძლება საფრთხე შეუქმნას ფიზიკურმა ზიანმა (ხანძარი, ნგრევა, ყინვა), ბუნებრივმა პროცესებმა (წყალდიდობა, მიწისძვრა), ძირითადი სერვისების შეფერხებამ (კონდიცირების სისტემა დაზიანება, კვების შეწყვეტა), ინფორმაციის კომპრომეტირებამ (შპიონაჟი, დეზინფორმაცია, არასანქცირებული შეღწევა სისტემებში), ტექნიკურმა გაუმართაობებმა (მოწყობილობის

გაუმართაობა, პროგრამის შეფერხებით მუშაობა), მესამე პირის არაავტორიზებულმა ქმედებებმა თუ სხვა.

ინფორმაციული უსაფრთხოების რისკების მართვა კი გულისხმობს როგორც ამ საფრთხეების, ასევე ამ საფრთხეების შესაბამისი მოწყვლადობის იდენტიფიცირებას. მაგალითისთვის, თუკი საფრთხედ მივიჩნევთ შპიონაჟს და ორგანიზაციას ქსელის დაუცველი არქიტექტურა აქვს, ამ შემთხვევაში, მან იცის, რომ ეს პრობლემა დაუყოვნებლივ გადასაჭრელია.

ინფორმაციული უსაფრთხოების რისკების მართვას აქვს რიგი სარგებელი, კერძოდ:

- ✓ ის ორგანიზაციას უჩენს კონკურენტულ უპირატესობას, ზრდის მის რეპუტაციას და მის მიმართ ნდობას, რაც საბოლოოდ ბიზნესის შედეგებზე აისახება;
- ✓ ის ამცირებს ინფორმაციული უსაფრთხოების ინციდენტის მოხდენის ალბათობას, ვინაიდან ორგანიზაციას აქვს ინფორმაცია შესაბამის საფრთხეზე და ამ საფრთხის თავიდან ასარიდებელ საშუალებებს იყენებს;
- ✓ ის საშუალებას აძლევს ორგანიზაციას მიიღოს სწორი გადაწყვეტილება, რომელიც ემყარება რეალურ რისკებს;
- ✓ ის ზოგავს ორგანიზაციის ხარჯებს ეფექტური და ეფექტიანი კონტროლის მექანიზმების დანერგვით;
- ✓ ის არის საქმიანობის უწყვეტობის წინაპირობა;
- ✓ ის ორგანიზაციას აძლევს სრულ ხედვას ინფორმაციული აქტივების წინაშე მდგარი გამოწვევების შესახებ.

უნდა აღინიშნოს ისიც, რომ მხოლოდ ამ პროცესის წარმატებით განხორციელების შემთხვევაში შეუძლია ორგანიზაციას იყოს სრულად თავსებადი ისეთ საერთაშორისო სტანდარტებთან, როგორიც არის ISO27001, NIST და სხვა. მეტიც, ინფორმაციული უსაფრთხოების რისკების მართვა ISO სტანდარტის ერთ-ერთი ძირითადი მოთხოვნაა და მის გარეშე ორგანიზაცია შესაბამის სერტიფიკატს ვერ მოიპოვებს.

ვინაიდან „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი ავალდებულებს კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომ მათი ინფორმაციული უსაფრთხოების პოლიტიკა იყოს თავსებადი სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ISO), აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნული

ინსტიტუტის (NIST) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებთან, ნაკლებად სავარაუდოა, რომ საქართველოს კრიტიკული ინფორმაციული სისტემის რომელიმე სუბიექტის ინფორმაციული უსაფრთხოების რისკების მართვის პროცესმა ამ სტანდარტებს გვერდი აუაროს.

ინფორმაციული უსაფრთხოების რისკების მართვისთვის მნიშვნელოვანია განისაზღვროს მეთოდოლოგია. თითოეული ორგანიზაცია განსხვავდება თავისი შიდა და გარე გარემოს მიხედვით, სტრატეგიული მიზნებით, ამოცანებით, სტრუქტურით, ინფორმაციული სისტემებით, ქსელის არქიტექტურით. შესაბამისად, ზოგი საჭიროებს საბაზისო მიდგომას, ზოგი კი უფრო სიღრმისეული მეთოდოლოგიის გამოყენებას. არსებობს ამ პროცესის მართვის რამდენიმე საერთაშორისოდ აღიარებული სტანდარტი, თუმცა რომელიმე მათგანის გამოყენება ვალდებულება ნამდვილად არ არის. ორგანიზაციას შეუძლია შექმნას საკუთარიც. მთავარი ისაა, რომ მეთოდოლოგია იყოს შესატყვისი ორგანიზაციასთან, მის მიზნებსა და სამუშაო პროცესებთან. წარმოგიდგენთ ყველაზე გავრცელებული მეთოდოლოგიებიდან რამდენიმეს:

OCTAVE: 2001 წელს შექმნილი OCTAVE Allegro კონცენტრირდება ინფორმაციულ აქტივებზე. ორგანიზაციის კრიტიკული აქტივები იდენტიფიცირდება და ფასდება მასთან დაკავშირებულ სხვა აქტივებთან მიმართებაში. ამ მეთოდოლოგიის დადებით მხარედ მიიჩნევა მორგებისა და დოკუმენტირების შესაძლებლობა, ხოლო უარყოფით მხარედ მისი სირთულე. ის შედგება 3 ფაზისგან:

ფაზა 1: ორგანიზაცია ახდენს აქტივების იდენტიფიცირებას და განსაზღვრავს მათ მნიშვნელობას თავისი ბიზნესის მიზნებისთვის. აქტივად შეიძლება განისაზღვროს ნებისმიერი ინფორმაცია, ქონება ან ადამიანური რესურსი, ან ორგანიზაციის ფუნქციონირებისთვის კრიტიკული მონაცემები, როგორიცაა ნოუ-ჰაუ და მონაცემები. შემდეგ ორგანიზაცია განსაზღვრავს საფრთხეებს ამ აქტივებისთვის და აჯგუფებს მათ თემატიკის (პროფილების) მიხედვით.

ფაზა 2: ამ ფაზაზე ორგანიზაცია აფასებს დაუცველობას თავის ინფრასტრუქტურაში, რომელიც შეიძლება იდენტიფიცირებული საფრთხეების დადგომის მიზეზი. ეს მოიცავს სისუსტეების

იდენტიფიცირებას ორგანიზაციის ფიზიკურ, ტექნიკურ და ადმინისტრაციულ ოპერაციებში.

ფაზა 3: ამ ფაზაზე ორგანიზაცია შეიმუშავებს უსაფრთხოების სტრატეგიას და განხორციელების გეგმას გამოვლენილი რისკების მართვისთვის. გეგმა მოიცავს რისკების პრიორიტეტიზაციას ორგანიზაციაზე მათი გავლენის საფუძველზე და მათი მართვის კონცეპტუალური ჩარჩოს შემუშავებას.

FAIR: არის რისკის ანალიზის რაოდენობრივი შეფასების მოდელი. ის სპეციალიზდება ფინანსურ შედეგებზე და არ მოიაზრებს ხარისხობრივ შეფასებას. მისი დადებითი მხარეა საფრთხეების, მოწყვლადობებისა და რისკების დონეების დაყოფა, ხოლო უარყოფითი მხარეა სირთულე.

COBIT: „კონტროლის მექანიზმები ინფორმაციისა და ტექნოლოგიებისთვის“, რომელიც შეიქმნა ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ, ფოკუსირდება კონტროლის მექანიზმების იდენტიფიცირებაზე (Simplelearn, 2023). ის შედგება 37 პროცესისგან, რომლითაც იმართება და კონტროლდება ინფორმაცია და მასთან დაკავშირებული ტექნოლოგიები. COBIT არ გვთავაზობს რისკების შეფასების მეთოდოლოგიას, მაგრამ ქმნის ინფორმაციული ტექნოლოგიების ორგანიზაციის საფუძველს. COBIT მოიცავს ინფორმაციული ტექნოლოგიების რისკების შემცირების კონტროლის მექანიზმებს.

გარდა ამისა, COBIT 5 რისკისთვის ხაზს უსვამს ძირითად დამხმარე პროცესებს. მიიჩნევა, რომ ორგანიზაციებს შეუძლიათ მიიღონ მნიშვნელოვანი დოკუმენტები, როგორიცაა რისკის მართვის სტრატეგია, რისკის მართვის საკომუნიკაციო გეგმა და ფინანსური და საბიუჯეტო მოთხოვნები რისკის რეაგირებისა და შემცირების მიზნით.

დოკუმენტების შექმნისთვის საჭირო პროცედურები მოიცავს, მაგრამ არ შემოიფარგლება შემდეგით:

- ✓ უზრუნველყოს მმართველობის ჩარჩოს დანერგვა და შენარჩუნება
- ✓ უპირატესობების მიწოდების უზრუნველყოფა
- ✓ სტრატეგიის მართვა
- ✓ ბიუჯეტისა და ხარჯების მართვა
- ✓ კომუნიკაციის მართვა
- ✓ მონიტორინგი, შეფასება და შესრულება, შესაბამისობა

- ✓ მონიტორინგი, შეფასება და მესამე მხარის მოთხოვნებთან შესაბამისობის შეფასება

ISACA წარმოადგენს ოფიციალურ რჩევებს მოცემული რისკის მართვის მეთოდოლოგიის დანერგვისთვის:

- ✓ უმაღლესი რგოლის მენეჯმენტის წახალისება, გამოავლინოს მხარდაჭერა რისკის მართვის პროგრამის მიმართ;
- ✓ ძირითადი ორგანიზაციული სტრუქტურები/როლების განსაზღვრა, რომლებიც საჭიროა ორგანიზაციაში რისკების ეფექტიანი და ეფექტური მართვისა და შესანარჩუნებლად;
- ✓ თითოეული როლისა და სტრუქტურის კონკრეტული აღწერის განსაზღვრა;
- ✓ რისკის მენეჯმენტი უნდა იყოს ჩართული ბიზნეს-პროცესში და იყოს ყოველდღიური მართვის ნაწილი;
- ✓ რისკის გაცნობიერების კულტურის ჩამოყალიბება ყველა თანამშრომელს შორის, ყველა დონეზე;
- ✓ მუდმივი კომუნიკაცია თანამშრომლებთან;
- ✓ რისკისა და რისკების მართვაში ადამიანური რესურსის როლის შესახებ ცნობიერების ამაღლება;
- ✓ ძირითადი რისკის ინდიკატორების (KRI) შემუშავება, რათა სწორად იდენტიფიცირდეს და იმართოს ინფორმაციული უსაფრთხოების რისკები.

NIST RMF: NIST საერთაშორისო სტანდარტის რისკების მართვის ჩარჩო (RMF) არის სტრუქტირებული პროცესი, რომელიც მოიცავს ინფორმაციული უსაფრთხოებისა და რისკების მართვის პროცედურებს. კერძოდ, რისკების მართვა ხორციელდება შემდეგი ეტაპებით (NIST, 2018) (ნახ.19):

- ✓ მომზადება - პირველ ეტაპზე ხდება იმგვარი პროცედურების განხორციელება ორგანიზაციაში, რითაც ის მოემზადება საკუთარი უსაფრთხოების რისკების მართვისთვის RMF ჩარჩოს გამოყენებით. ეს, მაგალითისთვის, მოიცავს როლებისა და პასუხისმგებლობების განსაზღვრას;
- ✓ კატეგორიზება - ხდება მოვლენების შეფასება ინფორმაციის ხელმისაწვდომობას, მთლიანობასა და კონფიდენციალურობასთან მიმართებაში, საფრთხეების კლასიფიცირება და შესაბამისი პირების ინფორმირება;

- ✓ შერჩევა/აღმოჩენა - ორგანიზაცია აღრიცხავს მოვლენებს, რომლებიც უქმნის საფრთხეს ინფორმაციის უსაფრთხოებას;
- ✓ დანერგვა - ამ ეტაპზე ინერგება კონტროლის მექანიზმები შესაბამისი რისკების საპასუხოდ;
- ✓ შეფასება - ამ დროს ფასდება დანერგილი კონტროლის მექანიზმების ეფექტურობა და სისწორე, რომ ის პასუხობს უსაფრთხოების პრობლემებს და შესაბამის მოთხოვნებს;
- ✓ ავტორიზება - მენეჯმენტის მხრიდან ხდება უსაფრთხოების რისკებისთვის დანერგილი კონტროლის მექანიზმების დამოწმება;
- ✓ მონიტორინგი - მოიცავს აღწერილი ეტაპების მონიტორინგის უწყვეტ პროცესს.

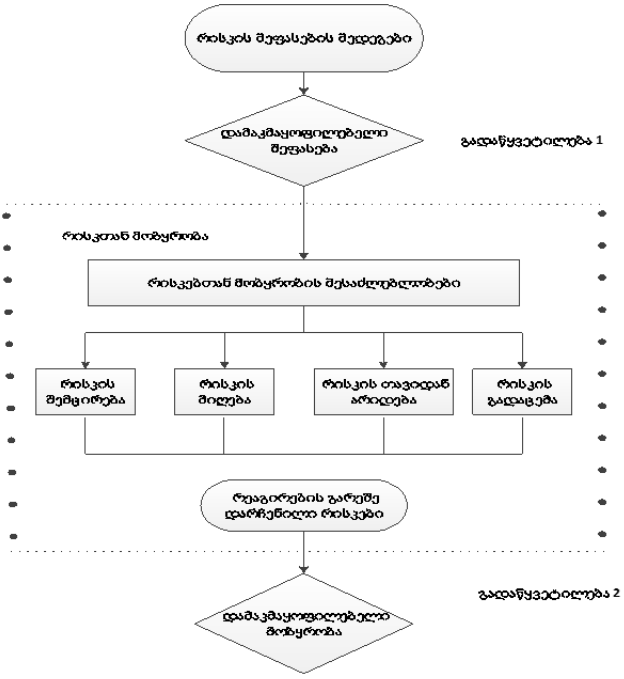
ISO 27001/27005: ISO ინფორმაციული უსაფრთხოების სტანდარტის თანახმად, ინფორმაციული უსაფრთხოების რისკების მართვის პროცესი შედგება შემდეგი პროცესებისგან:

- ✓ ორგანიზაციული გარემოს განსაზღვრა - მოიცავს საჭირო კრიტერიუმების დადგენას ინფორმაციული უსაფრთხოების რისკების მართვის გამოყენების სფეროსა და ჩარჩოების განსაზღვრას, ასევე ორგანიზაციული სტრუქტურის შექმნას, რომელიც განახორციელებს ინფორმაციული უსაფრთხოების რისკების მართვას. ამ პროცესში ხდება შიდა და გარე პროცესების, შეზღუდვების, საჭიროებების, მიზნების გათვალისწინება;
- ✓ რისკების შეფასება - მოიცავს რისკის ანალიზს (შედგება რისკების იდენტიფიცირებისგან და რისკების მიახლოებითი შეფასებისგან) და რისკის დონის დადგენას;
- ✓ რისკებთან მოპყრობა - მოიცავს არჩევანს რისკებთან მოპყრობის შესახებ (ნახ.20);
- ✓ რისკების შესახებ ინფორმირება;
- ✓ რისკების მონიტორინგი და განხილვა.

რისკების შეფასებისთვის პირველ ეტაპს წარმოადგენს რისკების იდენტიფიკაცია. ამ პროცესში შემავალ ინფორმაციას წარმოადგენს ორგანიზაციის ინფორმაციული აქტივები. თითოეული აქტივისთვის უნდა დადგინდეს შესაბამისი საფრთხე. საფრთხე, წარმოშობის წყაროს მიხედვით, შეიძლება იყოს შიდა, გარე და ბუნებრივი. აუცილებელია მოწყვლადობების იდენტიფიკაცია, რომელი სისუსტეებით

სარგებლობაც წარმოადგენს საფრთხეს აქტივებისთვის ან ორგანიზაციისთვის.

შემდეგ ხდება რისკების მიახლოებითი შეფასება. ის შეიძლება ჩატარდეს დეტალურობის სხვადასხვა დონეზე და დამოკიდებულია აქტივის კრიტიკულობაზე, წინა გამოცდილებაზე (ინციდენტებზე), ცნობილ მოწყვლადობებზე. რისკების მიახლოებითი შეფასება შეიძლება იყოს როგორც ციფრული (რაოდენობრივი), ასევე თვისობრივი (ხარისხობრივი). მიახლოებით შეფასებული რისკი წარმოადგენს ინციდენტის სცენარის და მისი უარყოფითი შედეგების ალბათობის კომბინაციას.



სურ.2. 1.ინფორმაციული უსაფრთხოების რისკების მართვა ISO სტანდარტით

შემდეგ ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით, სადაც წარმოდგენილია შემდეგი ვარიანტები:

1. რისკების შემცირებისთვის (შემსუბუქება) საჭიროა კონტროლის მექანიზმის სწორად შერჩევა. კონტროლის მექანიზმების შერჩევის და მათი დანერგვის დროს უნდა მოხდეს შეზღუდვების გათვალისწინება, როგორიცაა: ტექნიკური, სამართლებრივი, საკადრო, ფინანსური, დროითი და სხვა.
2. თუ რისკის დონე შეესაბამება რისკის მიღების კრიტერიუმებს, მაშინ არ არის აუცილებელი დამატებითი კონტროლის მექანიზმის დანერგვა და ხდება რისკის დაშვება.
3. რისკის თავიდან არიდება გამართლებულია, როდესაც რისკებთან მოპყრობის სხვა ვარიანტების განხორციელების დანახარჯები მეტია სარგებელზე და ასეთ დროს ხდება რისკის მთლიანად აღმოფხვრა.
4. რისკის გადაცემა გულისხმობს გადაწყვეტილებას გარკვეული რისკების მესამე მხარისთვის გაზიარების შესახებ. ეს შეიძლება იყოს ქვეკონტრაქტორი კომპანია ან დაზღვევა.

აღსანიშნავია, რომ ISO27001 სტანდარტით მოცემული ოთხი ვარიანტი არ არის ურთიერთგამომრიცხავი, ვინაიდან გარკვეულ შემთხვევებში გამართლებულია მათი კომბინაციაც.

როგორც ვნახეთ, სხვადასხვა სტანდარტების ანალიზის შედეგად დგინდება (PECB, 2023), რომ პირველი ეტაპი უნდა იყოს ინფორმაციული აქტივების იდენტიფიცირება. ეს აქტივები შეიძლება იყოს სერვერები, ქსელური მოწყობილობები, სისტემები, კომპიუტერული ტექნიკა და ნებისმიერი მოწყობილობა, რომელშიც ინახება, მუშავდება და გაიცვლება ინფორმაცია. აქტივი შეიძლება იყოს დოკუმენტიც, ორგანიზაციაში დასაქმებული თანამშრომლებიც.

მეორე ეტაპი არის საფრთხეების იდენტიფიცირება აქტივებთან მიმართებაში. საფრთხე არის უცნობი ინციდენტის პოტენციური მიზეზი, რომელმაც შეუძლია ზიანი მოუტანოს ორგანიზაციას. ეს შეიძლება იყოს ქურდობა, მავნე პროგრამული უზრუნველყოფა, ბუნებრივი მოვლენები, ინფორმაციის გამჟღავნება და სხვა.

მესამე ეტაპი არის მოწყვლადობების იდენტიფიცირება. ეს შეიძლება იყოს სარეზერვო ასლების არარასებობა, დაშიფვრის არარსებობა, არასაიმედო პაროლები, დაბალი კიბერცნობიერება, ქსელური დაცვის ეკრანის შეუსაბამობა, ბიზნესის უწყვეტობის გეგმის არქონა და სხვა.

მეოთხე ეტაპი არის საფრთხის ალბათობის დადგენა. ალბათობის დადგენისთვის შესაძლებელია სტატისტიკის, ანგარიშების გამოყენება. ალბათობის დონეები შეიძლება იყოს როგორც რაოდენობრივი, ასევე თვისობრივი (მაგ.: დაბალი, საშუალო, მაღალი).

მეხუთე ეტაპზე ალბათობა უნდა დავუკავშიროთ გავლენას. შესაძლოა, ალბათობა იყოს დაბალი, ხოლო საფრთხის სიმძიმე ძალიან მაღალი, ან პირიქით და ეს შემთხვევები განსხვავებულ სურათს იძლევა. სწორედ ალბათობისა და გავლენის ურთიერთშეკავშირება გვაძლევს საშუალებას შევაფასოთ რისკი. რისკის შეფასებისთვის, ასევე შეგვიძლია გამოვიყენოთ შკალა, ან შევაფასოთ ის ხარისხობრივად.

წარმოგიდგენთ რისკების შეფასების მაგალითს, სადაც ვიყენებთ რაოდენობრივ მეთოდს და ალბათობასა და გავლენას ვაფასებთ 1-დან 5 ქულამდე. ბოლო სვეტში ვიღებთ რისკის შეფასების შედეგს.

აქტივი	საფრთხე	მოწყვლადობა	რისკის მფლობელი	გავლენა (1-5)	ალბათობა (1-5)	რისკი
სერვერი (ტექნიკური უზრუნველყოფა)	კვების წყვეტა	უწყვეტი კვების წყაროს (UPS) არარსებობა	ინფორმაციული უსაფრთხოების მენეჯერი	4	2	**6**
	ხანძარი	ცეცხლმაქრის არარსებობა		5	3	**8**
ხელშეკრულება (დოკუმენტი)	წვდომის მიღება არაავტორიზებული პირის მიერ	ხელშეკრულება დატოვებულია მაგიდაზე	აღმასრულებელი დირექტორი	4	4	**8**
	ხანძარი	ხანძრისგან დამცავი სისტემის არარსებობა		4	3	**7**

სისტემის ადმინისტრატორი (ადამიანი)	ავარია	სხვამ არავინ იცის პაროლი	დეპარტამენტის უფროსი	5	3	**8**

ბოლო ეტაპზე ხდება გადაწყვეტილების მიღება რისკებთან მოპყრობასთან დაკავშირებით. სხვადასხვა სტანდარტების მიხედვით, ეს შეიძლება იყოს (Infosec, 2018): რისკის შემცირება (შემსუბუქება), რისკის თავიდან არიდება, რისკის გადაცემა, რისკის მიღება. წარმოგიდგენთ შესაბამის მაგალითს.

აქტივი	საფრთხე	მოწყვლადობა	რისკთან მოპყრობა	დანერგვის საშუალება
სერვერი	ხანძარი	ცეცხლმაქრის არარსებობა	რისკის გადაცემა	დაზღვევის პოლისის შესყიდვა
პორტატული კომპიუტერი	არაავტორიზებული პირის მიერ წვდომა	არასაიმედო პაროლი	რისკის შემცირება	პაროლების წესის შემუშავება
სისტემის ადმინინისტრატორი	სამსახურის დატოვება	შემცვლელი კადრის არარსებობა	რისკის შემცირება	სისტემის მეორე ადმინისტრატორის დასაქმება

ინფორმაციული უსაფრთხოების რისკების მართვა, ცხადია, საკმაოდ კომპლექსური პროცესია, რომელიც მოითხოვს გარკვეულ ძალისხმევას ორგანიზაციის თითოეული რგოლისგან. რისკების მართვის პროცესის ჩავარდნის მიზეზები ხშირად ხდება (Al-Ahmad & Mohammad, 2013):

- ✓ მმართველი რგოლის მხარდაჭერის არარსებობა: ინფორმაციული უსაფრთხოება იმართება მენეჯმენტის გადაწყვეტილებების საფუძველზე. მმართველი რგოლის მხარდაჭერის არარსებობა იწვევს რესურსების ფლანგვას, არასწორ შეფასებებს, რაც

საბოლოოდ რისკების შეფასების შედეგების უგულებელყოფამდე მიგვიყვანს;

- ✓ ინფორმაციული უსაფრთხოების პოლიტიკის/პროცედურების არარსებობა: შესაბამისი დოკუმენტების არარსებობა მიგვიყვანს რისკების შეფასების არასისტემურ მიდგომასთან;
- ✓ არასწორი მართვა: მიუხედავად რისკების მართვის მნიშვნელობისა, ზოგჯერ ის არ იმართება, როგორც პროექტი და არ განიხილება ოპერაციად. რისკების მართვის პროცესის გაუთვალისწინებლობა გადაწყვეტილების მიღების, დაგეგმვის და აღსრულების პროცესში იწვევს რესურსების არამიზნობრივ ხარჯვას;
- ✓ აქტივების მფლობელი დაუდგენელია: შეუძლებელია ინფორმაციული უსაფრთხოების რისკი შეფასდეს აქტივების მფლობელის ჩართულობის გარეშე. როდესაც აქტივებს არ გააჩნიათ მფლობელი, მის წინაშე მდგარი საფრთხეების და შესაბამისი მოწყვლადობების ჯეროვნად მოკვლევა და შემდეგ ინფორმაციული უსაფრთხოების რისკების მართვის პროცესში გამოყენება შეუძლებელია;
- ✓ რისკების მართვის მეთოდოლოგიის შერჩევა: ზოგიერთი ორგანიზაცია რისკების მართვისთვის იყენებს რამდენიმე მეთოდოლოგიას, რითაც მართვის პროცესი კიდევ უფრო ჩახლართული ხდება.

ასევე, მივიჩნევ, რომ ამ პროცესში გამოწვევას წარმოადგენს კადრების დეფიციტი და კვალიფიკაციის ნაკლებობა. ინფორმაციული უსაფრთხოების რისკების მართვა კომპლექსური პროცესია და მასზე პასუხისმგებელი პირი უნდა ფლობდეს შესაბამის ცოდნას. ამის მიუხედავად, საქართველოში ჯერ კიდევ მრავლად შევხვდებით კრიტიკული ინფორმაციული სისტემის სუბიექტებს, რომელთაც არ ჰყავთ ინფორმაციული უსაფრთხოების მენეჯერი ან ინფორმაციულ უსაფრთოხებაზე პასუხისმგებელი პირი.

ინფორმაციული უსაფრთხოების რისკების მართვა არ წარმოადგენს ინფორმაციული უსაფრთხოების მენეჯერის ერთპიროვნულ პასუხისმგებლობას. პირიქით, ეს არის მაღალი რგოლის მენეჯმენტის მიერ გასააზრებელი და მისაღები გადაწყვეტილება, რომელშიც

ორგანიზაციას გარკვეული ინვესტიცია დაჭირდება. თუმცა, ჩადებული რესურსი შეუძლებელია ჩაითვალოს ფუჭად, ვინაიდან რისკების შემცირებით სუბიექტი მნიშვნელოვნად ამცირებს ინფორმაციული უსაფრთხოების ინციდენტების ალბათობას, თავიდან ირიდებს რეპუტაციულ და ფინანსურ ზიანს, რაც, საბოლოო ჯამში, ხაზს უსვამს გაღებული ძალისხმევის სისწორესა და ეფექტურობას.

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონი კრიტიკული ინფორმაციული სისტემის სუბიექტებისთვის სავალდებულოდ ადგენს ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებას. თუმცა, აღნიშნული პოლიტიკა ზოგად მიმართულებებს განსაზღვრავს და არ აწესებს ისეთ შეზღუდვებს, რომელსაც საბოლოო მომხმარებლები უნდა იცავდნენ თუნდაც სამსახურებრივი ინფორმაციული ინფრასტრუქტურით სარგებლობის პროცესში. ამ მიზნით, შეგვიძლია გავითვალისწინოთ საერთაშორისო პრაქტიკა, რომელიც გულისხმობს ვიწრო მიმართულებით ინფორმაციული უსაფრთხოების პოლიტიკების შემუშავებას, რომელთა შორისაც უნდა იყოს:

- ინფორმაციული აქტივების მართვის და განადგურების პოლიტიკები;
- ინფორმაციის კლასიფიკაციის პოლიტიკა;
- ინფორმაციული უსაფრთხოების რისკების მართვის პოლიტიკა;
- სუფთა მაგიდის პოლიტიკა;
- ფიზიკური უსაფრთხოების მინიმალური მოთხოვნები და წვდომის პოლიტიკა;
- ელექტრონული ფოსტის მოხმარების პოლიტიკა;
- პაროლების უსაფრთხოების პოლიტიკა;
- სოციალური მედიის პოლიტიკა;
- ანტივირუსის გამოყენებისა და კონფიგურაციის მინიმალური მოთხოვნების პოლიტიკა;
- სამუშაო კომპიუტერის კონფიგურაციის პოლიტიკა;
- ქსელური სენსორის კონფიგურაციის პოლიტიკა;
- ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის განახლების მართვის პოლიტიკა;
- სარეზერვო ასლების მართვის პოლიტიკა;
- მოწყვლადობის სკანირების პოლიტიკა;

- კომპიუტერული ინციდენტების მართვის პოლიტიკა;
- სერვერისათვის განკუთვნილი შენობა-ნაგებობის ან/და სასერვერო ოთახის მოწყობის პოლიტიკა;
- მარშრუტიზატორის უსაფრთხოების პოლიტიკა;
- აპლიკაციის შექმნის და უსაფრთხოების პოლიტიკა;
- ვირტუალური კერძო ქსელის უსაფრთხო კონფიგურაციის და გამოყენების პოლიტიკა;
- დისტანციური წვდომის პოლიტიკა;
- ქსელური დაცვის ეკრანის უსაფრთხოების მინიმალური კონფიგურაციის პოლიტიკა.

იმისთვის, რომ რისკების მართვის პროცესთან დაკავშირებით სუბიექტი არ შეხვდეს ჩვენ მიერ განხილულ პრობლემებს, მან საწყის ეტაპზე შეიძლება გაითვალისწინოს ISO 27001 Academy-ს მიერ წარმოდგენილი რისკების მართვასთან დაკავშირებულ რჩევები (Dejan):

- სწორი მეთოდოლოგიის არჩევა - საჭიროა სწორი მეთოდოლოგიის არჩევა და საჭიროებისამებრ მისი გამარტივება;
- სწორი საშუალების არჩევა - რისკების მართვის პროცესში რეკომენდებულია პროგრამული უზრუნველყოფის გამოყენება. ზოგიერთ შემთხვევაში, ჩახლართულ პროგრამას სჯობს Microsoft Office Excel-ის ფორმის გამოყენება;
- საჭირო პერსონალის ჩართვა - საჭიროა მმართველობითი რგოლის ჩართვა ამ პროცესებში, ვინაიდან სტრუქტურული დანაყოფების უფროსებმა იციან, რის უკან იმალება პრობლემები;
- მიზანი არ არის სრულყოფილება - რისკების მართვა უწყვეტი პროცესია. პირველ ეტაპზე, შეუძლებელია ყველა საფრთხის გამოვლენა და აღწერა.

რაც შეეხება კონკრეტულ სტანდარტებს, მხოლოდ ორგანიზაციაზეა დამოკიდებული ის, თუ რომელ მიდგომას აირჩევს ინფორმაციული უსაფრთხოების რისკების მართვისთვის და ის იცვლება საქმიანობის სფეროს, მასშტაბების, ამოცანების, საჭიროებებისა და შესაძლებლობების მიხედვით. თუმცა, მნიშვნელოვანია ნაშრომში განხილული მეთოდოლოგიების გათვალისწინებაც, ვინაიდან

მოცემულმა სტანდარტებმა უკვე მრავალწლიანი აპრობაცია გაიარეს და მათი ეფექტურობის ხარისხი კითხვის ნიშნის ქვეშ კიბერუსაფრთხოების ექსპერტებს ნამდვილად არ დაუყენებიათ.

კიბერდაზღვევა

დაახლოებით 5 წლის წინ, მათ შორის საქართველოში, დამკვიდრდა ტერმინი „კიბერდაზღვევა“ და ის არის იმ ტიპის სადაზღვევო პროდუქტი, რომელიც მოიცავს კიბერშეტევისგან მიყენებული ზიანის ფინანსურ ანაზღაურებას.

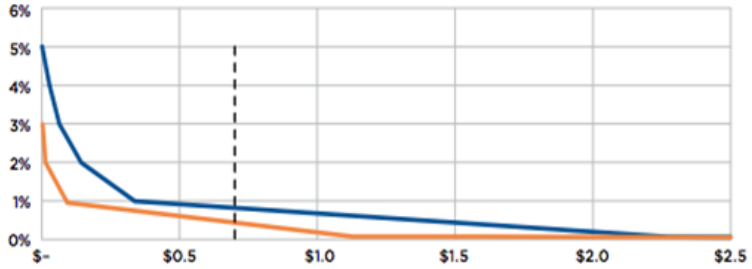
კიბერდაზღვევის პოლისი პირველად ქართულ ბაზარზე შემოიტანა კომპანია „ალდაგმა“. მისი გენერალური დირექტორის, გიორგი ბათიაშვილის განცხადებით (კაკაურიძე, 2017), კიბერდაზღვევის პოლისს ფართო დაფარვა აქვს და მოიცავს იმ ფინანსური ზარალის ანაზღაურებას, რომელიც გამოწვეულია შემდეგი გარემოებებით:

- ორგანიზაციის თანამშრომლის მხრიდან შეცდომის დაშვება, სისტემის არასწორი გამოყენება;
- კომპანიის საკომუნიკაციო არხებით იმიჯის დამაზიანებელი ან დანაშაულებრივი კორესპონდენციის წარმოება;
- თანამშრომლის მიერ არასწორი ინფორმაციის შეყვანა, ან ინფორმაციის გატანას კომპანიიდან;
- კომპიუტერული თავდასხმა.

როგორც ზემოთ აღვნიშნეთ და მსოფლიოში მომხდარი ბოლო დროის ყველაზე მძლავრი კიბერშეტევებითაც დავადასტურეთ, სამომავლოდ, კიბერშეტევის უმთავრეს ვექტორად შანტაჟის/გამოსასყიდი პროგრამული უზრუნველყოფა უნდა მივიჩნიოთ. ამ კუთხით, რასაკვირველია, შეუფასებელია ისეთი მექანიზმის არსებობის დადებითი სარგებელი, როგორიცაა კიბერდაზღვევა.

მიუხედავად იმისა, რომ მსოფლიოში, პრაქტიკულად, ჯერ-ჯერობით, ღია წყაროების საფუძველზე, არ მოიძებნება ისეთი სახელმწიფოები, რომლებიც სამთავრობო ინფრასტრუქტურისთვის კიბერდაზღვევის მომსახურებას მიმართავენ, აშშ-ს და კანადის სამთავრობო ფინანსური ოფიცრების ასოციაციამ, ციფრული მმართველობის ცენტრთან თანამშრომლობით, საჯარო და კერძო სექტორში მოღვაწე ექსპერტების ავტორობით, 2022 წელს გამოსცა პუბლიკაცია კიბერდაზღვევაზე

(Government Finance Officers Association, 2022). კვლევის შედეგად დადგინდა, რომ მაშინაც კი, თუკი სახელმწიფო დაწესებულებები დანერგავენ კონტროლის უახლეს მექანიზმებს (ნარინჯისფერი ხაზი), სტანდარტული მექანიზმებისგან განსხვავებით (ლურჯი ხაზი), მათი ფინანსური ზიანის თვითანაზღაურების (წყვეტილი ხაზი) ლიმიტი ვერ იქნება 0.5 მლნ დოლარზე მეტი, ხოლო უფრო მძლავრი კიბერშეტევის ალბათობა კვლავ შენარჩუნებული რჩება და მათი ზიანი 1 მლნ დოლარს აღემატება.



სურ.2. 2.კიბერშეტევით მიყენებული ფინანსური ზიანი კონტროლის მექანიზმების არსებობის შემთხვევაში და მათ გარეშე

ამ და სხვა პარამეტრებით, კიბერდაზღვევის ზემოხსენებულ სარგებელთან ერთად შედგენილ კვლევის ანგარიშს დადებითი შეფასება მოჰყვა აშშ-ს სამთავრობო სტრუქტურის სპეციალისტებისგან და ეროვნული კვლევითი ორგანიზაციებიდან, როგორიცაა მარკ უიზერფორდი, აშშ-ს კიბერუსაფრთხოების ეროვნული ცენტრის სტრატეგიის წამყვანი ოფიცერი და ფილ ბერტოლინი, ციფრული მმართველობის ცენტრის ვიცე-პრეზიდენტი, რომელმაც განაცხადა, რომ პუბლიკაცია მოიცავს ისეთ ინფორმაციას, რომელიც დიდ სარგებელს მოუტანს ქვეყნის სამთავრობო სტრუქტურებს (GFOA). ეს კი ნიშნავს, რომ უახლოეს მომავალში აშშ-ს სამთავრობო სტრუქტურების მხრიდან უნდა ველოდოთ კიბერდაზღვევის პოლისებით დაინტერესებას.

საქართველოში კიბერდაზღვევა ჯერ კიდევ არ წარმოადგენს დამკვიდრებულ პრაქტიკას. მივიჩნევ, რომ ინფორმაციული უსაფრთხოების აუთსორსინგისგან განსხვავებით, რომელსაც დადებითი სარგებლის გარდა, თან სდევს ეჭვები ინფორმაციის კონფიდენციალურობის დაცვასთან დაკავშირებით, კიბერდაზღვევა

სრულად უსაფრთხო და პრაქტიკულად გამოყენებადია საჯარო უწყებებისთვის. მისი პოპულარიზაციისთვის, საჭიროა კერძო სექტორის მიერ პროდუქტების რეკლამირება და მათი მორგება სამთავრობო სექტორზე, დაწყებული პოლისის შინაარსით და დამთავრებული მისი პრემიით. მიუხედავად იმისა, რომ მსგავსი მექანიზმი არ გულისხმობს ინფორმაციის კომპრომეტირებისგან თავის დაცვას, ინფრასტრუქტურის ფუნქციონირების აღდგენისთვის საჭირო ფინანსური რესურსების ამგვარად მობილიზება უდავოდ გამოსადეგი იქნება კრიზისულ ვითარებებში.

ინოვაციურ ტექნოლოგიებთან დაკავშირებული რისკები ინდუსტრია 4.0-ში

მე-4 ინდუსტრიულ რევოლუცია აერთიანებს მოწყობილობებს, ადამიანურ რესურსსა და ფიზიკურ აქტივებს ინტეგრირებულ ციფრულ ეკოსისტემაში. მისი საშუალებთ შესაძლებელია მონაცემების დამუშავება და ოპერაციების წარმოება ადამიანის ნაკლები მონაწილეობის გარეშე და ფოკუსირებულია ავტომატურ მანქანურ სწავლებაზე, ურთიერთკავშირებსა და ჭკვიანი ციფრული ტექნოლოგიების გამოყენებაზე ბიზნესში.

NIST-ის მიდგომით, ინდუსტრია 4.0-ის განხილვა საჭიროა 4 ურთეირთგადამფარავი საკითხის გათვალისწინებით (Toth, 2022). ესენია:

1. კიბერფიზიკური სისტემები და რობოტიკა

კიბერფიზიკური სისტემები აერთიანებს სენსორებს და სენსორულ ქსელებს, რომელთაც აქვთ ფიზიკური გარემოს მონიტორინგის და კონტროლის უნარი. რობოტებს აპროგრამებენ კონკრეტული ოპერაციების შესასრულებლად და ამ ნაწილში, ისინი ანაცვლებენ ადამიანურ რესურსს. ექსპერტების აზრით, მიუხედავად იმისა, რომ უსაფრთხოების ნორმები ბოლო წლებში, შედარებით, გაუმჯობესდა, რობოტების უსაფრთხოება მაინც დგას კითხვის ნიშნის ქვეშ.

2. საგნების ინტერნეტი და დიდი მონაცემები

დიდი მონაცემები გულისხმობს ინფორმაციის დიდი მასივის ეფექტურ და ეფექტიან დამუშავებას, ხოლო მისი კომბინაცია საგნების ინტერნეტთან, უკვე იძლევა ინფორმაციის მოგროვების და

დამუშავების საშუალებას, რომელიც აუმჯობესებს წარმოების სრულ პროცესს.

3. ღრუბლოვანი ტექნოლოგიები

ორგანიზაციის შიდა სისტემებში და მის გარეთ არსებული სერვისებისა და მონაცემების ერთ სივრცეში კომბინაციის საშუალებას იძლევა ღრუბლოვანი ტექნოლოგიები.

4. ავტომატიზაცია

ინდუსტრია 4.0-ის არსი სწორედ წარმოების პროცესების ეფექტიანობის გაზრდასა და ავტომატიზაციაში მდგომარეობს. ტექნიკური და პროგრამული უზრუნველყოფის გამოყენებით უნდა დამუშავდეს ინფორმაცია, ჩაერთოს მანქანური სწავლება, რომელზეც დაშენდება ხელოვნური ინტელექტის ტექნოლოგიები, ამ ტექნოლოგიებმა უნდა მიიღონ სწორი გადაწყვეტილებები და ამით უნდა შემცირდეს ადამიანის ჩარევა. აქ ვხვდებით ისეთ ციფრულ სერვისებს, როგორიცაა: ავტონომიური მართვა, ტარებადი დისპლეები, ტელედასწრების აპლიკაციები, წარმოსახვითი რეალობა, იმპლანტირებული მოწყობილობები, ტაქტილური და ინდუსტრიული ინტერნეტი და სხვა უამრავი აღმოცენებადი სერვისი.

ზემოაღნიშნული ტექნოლოგიები, ცხადია, გააუმჯობესებს და განავითარებს წარმოების ტექნოლოგიებს, და, ზოგადად, ბიზნეს-საქმიანობას, თუმცა, ისინი, ასევე, მოიცავენ რისკებს, ვინაიდან ორგანიზაციის სენსიტიური ინფორმაცია ხვდება ქსელში ჩართულ უამრავ მოწყობილობაში (IoT). რისკები და ეჭვები დგას თითოეულ ინოვაციურ ტექნოლოგიასთან დაკავშირებით. მაგალითად, არსებობს შეშფოთების საფუძველი, რომ „6G უსაფრთხოება და კონფიდენციალურობა შეიძლება იყოს უარესი, ვიდრე წინა თაობების“ (ხუროძე, შავგულიძე, & ჩხაიძე, 2022).

შემაშფოთებელ ფაქტს წარმოადგენს ის, რომ, ინდუსტრია 4.0-ის უსაფრთხოების საკითხებს, საჯარო სექტორისგან განსხვავებით, კვლევის საფუძველზე, საქართველოში მოქმედი ბიზნეს სუბიექტები ჯერ კიდევ არასათანადოდ აღიარებენ (მაისურაძე, მეტრეველი, & რევაზიშვილი, 2019).

ამ დროს, კიბერკრიმინალები ხელოვნურ ინტელექტს თავად იყენებენ საკუთარი კიბერთავდასხმითი შესაძლებლობების განვითარებისთვის და მასირებული შეტევების წარმოებისთვის.

ხელოვნურ ინტელექტს ჰაკერები იყენებენ რევერსული ინჟინერსიითვის, მოწყვლადი აპლიკაციების, მოწყობილობებისა და ქსელების აღმოჩენისთვის. ხელოვნურ ინტელექტს მარტივად შეუძლია ამოიცნოს სისუსტეები ადამიანურ ქცევაში, რომელიც აადვილებს ბოროტმოქმედების მიერ შესაძლებლობების დანახვას სენსიტიური ინფორმაციის წვდომისთვის. AI-ს იყენებენ ყალბი შინაარსის რესურსის შექმნისთვის (Deepfake). მაგალითისთვის, გერმანული კომპანიის აღმასრულებელი დირექტორის ხმისა და საუბრის ინტონაციის გაყალბებით, მისი შვილობილი ბრიტანული კომპანიის დირექტორს 220 000 ევრო გადაარიცხინეს უნგრელ მწარმოებელთან, სინამდვილეში კი კიბერკრიმინალებთან (Stupp, 2019). გარდა ამისა, ბოროტმოქმედები AI-ს საშუალებით ქმნიან მუტირებად მავნე პროგრამულ უზრუნველყოფას, რომელიც თავად ცვლის საკუთარ სტრუქტურას, რათა შეუძლებელი იყოს მისი აღმოჩენა. მავნე პროგრამული უზრუნველყოფის სავარაუდო ზიანი და სიმძიმე ჩვენ წინა თავებში განვიხილეთ.

საერთაშორისო ჟურნალში Defense and Security Studies გამოქვეყნებულ სტატიაში „Cybersecurity challenges in Industry 4.0: A state of the art review“ (Avdibasic, Toksanovna, & Durakovic, 2022) ავტორების მიერ ჩატარებული კვლევის შედეგად ინდუსტრია 4.0-ის მთავარ გამოწვევებად დასახელდა: ცნობიერების ნაკლებობა, ექსპერტების ნაკლებობა, სენსიტიური ინფორმაციის მოპარვა, DoS შეტევები, ფინანსური ზიანი, მოწყვლადი მოწყობილობების ქსელთან დაკავშირება, მარტივი პაროლების გამოყენება, ქსელის კავშირის პრობლემების შედეგად სერვისების წყვეტა.

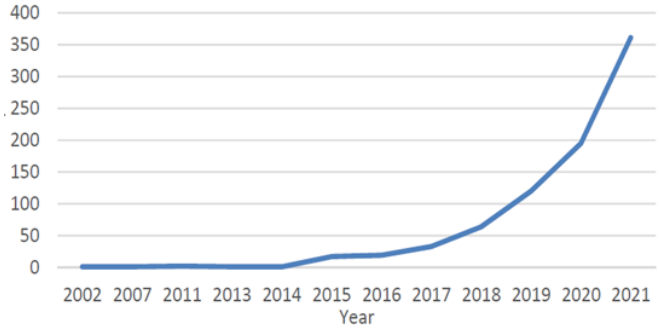
ამ ყოველივეს, თავის მხრივ, კიბერუსაფრთხოების სპეციალისტები პასუხობენ ინოვაციური ტექნოლოგიების გამოყენებით მეტი დაცულობის უზრუნველსაყოფად. ვინაიდან ხელოვნურ ინტელექტს აქვს ანომალიური ქმედებების და მოწყვლადობების იდენტიფიცირების უნარი, ის ფართოდ გამოიყენება ქსელების მონიტორინგისთვის. სპეციალისტებმა AI-ს გამოყენებით შექმნეს IDS (შეჭრის აღმოჩენის სისტემები), რომელიც ახდენს ქსელის მონიტორინგს. ასევე მას იყენებენ ინფორმაციული უსაფრთხოების

რისკების შეფასებისთვის, ოპერაციების ავტომატიზაციისთვის (Bhagat, 2022).

ხელოვნური ინტელექტის გამოყენება კიბერუსაფრთხოებაში თვალსაჩინოა ჩვენთვის საკმაოდ ცნობილ ციფრულ სერვისებში. Google-მა ML-ის (მანქანური სწავლება) გამოყენება დაიწყო დაახლოებით 20 წლის წინ ელექტრონული წერილების ფილტრაციისთვის და მას დადებითად აფასებენ კომპანიაში: „მანამდე ჩვენ ვიყავით სამყაროში, სადაც მეტი მონაცემები ნიშნავდა მეტ პრობლემას. ღრმა სწავლების დახმარებით, რაც მეტი მონაცემი გვაქვს, მით უკეთესია“ (Bursztein, 2018). კოგნიტურ სწავლებას იყენებს კომპანია IBM საფრთხეების გამოვლენისა და ცოდნის კონსოლიდაციის ამოცანებში.

ინდუსტრია 4.0-ის ინფორმაციული უსაფრთხოების საკითხების განხილვა დღითიდღე პოპულარული ხდება. წინა გვერდზე მოტანილი 2022 წელს გამოქვეყნებული კვლევის ფარგლებში, გლობალურ ქსელში სულ მოიძებნა 332 სტატია, რომელშიც ნახსენები იყოს მე-4 ინდუსტრიული რევოლუციის კიბერუსაფრთხოების საკითხი. დადებით მაჩვენებელს აქ წარმოადგენს დაინტერესების ზრდა.

ინდუსტრია 4.0-თან დაკავშირებული ტექნოლოგიების უსაფრთხოების ადმინისტრირებისას, გლობალურ ქსელში განთავსებული 332 პუბლიკაციის ანალიზის შედეგად, უნდა გავითვალისწინოთ რისკების შემცირების საშუალებები: ავტორიზაციის მექანიზმები, საფრთხეების ანალიზი, ძლიერი დაშიფვრა, ბლოკჩეინის ტექნოლოგია, საიმედო პაროლების გამოყენება, რეგულარული განახლებები და, რაც ყველაზე ხშირადაა ნახსენები ექსპერტების მიერ - ტრენინგები და განათლება, მოწყვლადი ადგილების გამოვლენა და მეტი დაცულობის უზრუნველყოფა (Avdibasic, Toksanovna, & Durakovic, 2022).



სურ.2. 3.ინდუსტრია 4.0-ის საკითხების კვლევის მაჩვენებელი

ინფორმაციული უსაფრთხოების მართვის პროცესში შეუძლებელია უგულებელვყოთ ინოვაციური ტექნოლოგიები, თუმცა მათი გათვალისწინება გვჭირდება როგორც ამ ტექნოლოგიების გამოყენებასთან დაკავშირებული საფრთხეების კუთხით, ასევე, უშუალოდ მათი საშუალებით ზოგადი უსაფრთხოების გაძლიერების ჭრილში. გამონაკლისს არ წარმოადგენს საჯარო სექტორი, სადაც, ვთვლი, რომ ხელოვნური ინტელექტის და სხვა ახალი ციფრული გარღვევების გათვალისწინება უნდა მოხდეს ეროვნული კანონმდებლობის და უსაფრთხოების სტრატეგიების შედგენის და გაახლების პროცესში.

ხელოვნურ ინტელექტზე დაფუძნებული გადაწყვეტების გამოყენება სახელმწიფოს მიერ უახლესი და დადებითი პრაქტიკაა, მათ შორის ეროვნული უსაფრთხოების კუთხით, მაგალითად, ანალიტიკური სისტემების გაძლიერებით. თუმცა, თავად სახელმწიფო სერვისებში AI-ს გამოყენებისას, საჭიროა იყოს მეტი გამჭვირვალობა. საქართველოს შინაგან საქმეთა სამინისტროს მიერ ჭკვიანი კამერების გამოყენებასთან დაკავშირებით, პრობლემის არსებობას მოიაზრებენ IDFI-ს კვლევაში „ხელოვნური ინტელექტის სისტემების გამოყენება საქართველოში“. სისუსტედ სახელდება მონაცემთა ბაზებში განხორციელებული აქტივობების აღრიცხვის სისტემის არარსებობა იმ პირობებში, როდესაც არსებობს ხელოვნური ინტელექტის სისტემების არამიზნობრივად გამოყენების რისკი, შესაბამისი პრეცედენტის მითითებით (ინფორმაციის თავისუფლების განვითარების ინსტიტუტი, 2021).

გარდა ამისა, ვინაიდან საქართველოში ამ სფეროში კვლევა ჯერ კიდევ ძალიან ადრეულ ეტაპზეა და, პრაქტიკულად, არ ვხვდებით ღრმა კვლევითი ხასიათის სამეცნიერო ნაშრომებს, სახელმწიფოს მხრიდან აუცილებლად უნდა წახალისდეს კვლევითი საქმიანობა, სხვადასხვა პროექტებისა და გრანტების უზრუნველყოფით, რაშიც უაღრესად დიდი წვლილი ექნება საქართველოს განათლებისა და მეცნიერების სამინისტროს.

თავი 3: საფრთხეები კიბერუსაფრთხოებაში, მოწყვლადობები და შეტევები

საფრთხეები, მოწყვლადობა და თავდასხმები კიბერუსაფრთხოების პროფესიონალების საქმიანობის ძირითად ფოკუს-ჯგუფს წარმოადგენს. საფრთხე არის შესაძლებლობა, რომ მავნე მოვლენა, როგორიცაა თავდასხმა, მოხდება. მოწყვლადობა არის სისუსტე, რაც შესაძლოა გახდეს თავდასხმის სამიზნე. თავდასხმა არის მიზანმიმართული გამოყენება კომპიუტერულ საინფორმაციო სისტემაში აღმოჩენილი სისუსტისა. კიბერდამნაშავეებს შეიძლება ჰქონდეთ განსხვავებული მოტივაცია თავდასხმის სამიზნის შერჩევისას. კიბერდამნაშავეები აღწევენ წარმატებას სისტემებში აშკარა მოწყვლადობის განუწყვეტლივ ძიებისა და გამოვლენის გზით. თავდასხმათა მსხვერპლთა არეალი მოიცავს განუახლებელ სისტემებს ან სისტემებს, სადაც არაა დაინსტალირებული ანტივირუსული პროგრამული უზრუნველყოფა.

3.1 მავნე კოდი

მავნე კოდი, ან მავნე პროგრამა (პროგრამული უზრუნველყოფა), ანუ Malware, არის ტერმინი, რომელიც გამოიყენება პროგრამული უზრუნველყოფის აღსაწერად, რომელიც მიზნად ისახავს მავნე ჩარევას კომპიუტერულ ოპერაციებში ან კომპიუტერულ სისტემებზე წვდომას, მომხმარებლის შეტყობინებისა ან/და ნებართვის გარეშე. Malware გახდა ტერმინი, რომელიც გამოიყენება ყველა მტრული ან შეღწევითი პროგრამული უზრუნველყოფის აღსაწერად. ტერმინი Malware მოიცავს კომპიუტერულ ვირუსებს, ჭიას, ტროიანებს, გამომძალველ პროგრამებს, ჯაშუშ პროგრამებს, მავნე პროგრამული უზრუნველყოფის გამავრცელებელ პროგრამებს და სხვა ბოროტგანზრახულ პროგრამებს. Malware შეიძლება იყოს აშკარა და მარტივად იდენტიფიცირებადი ან შეიძლება იყოს ძალიან რთულად გამოსავლენი.

ვირუსი, ჭია და ტროიანი

კიბერდამნაშავეები სამიზნეში იღებენ მომხმარებლის მოწყობილობებს ზიანის მომტანი პროგრამული პროდუქტის ინსტალაციის შედეგად.

ვირუსი - არის ზიანის მომტანი შესრულებადი კოდი, რომელიც, როგორც წესი, ერთვის სხვა შესრულებად ფაილს, როგორიცაა ავთენტური პროგრამა. ყველაზე გავრცელებული ვირუსები მოითხოვენ საბოლოო მომხმარებლის მიერ გაშვებას ან შეუძლიათ გააქტიურდნენ კონკრეტულ დროს ან თარიღზე. კომპიუტერული ვირუსები, როგორც წესი, ვრცელდებიან სამი გზით: მედია მატარებლები, ჩამოტვირთვები ინტერნეტიდან და ელექტრონულ ფოსტაზე მიმაგრებული ფაილები. ვირუსები შეიძლება იყვნენ უვნებელნი ან შეიძლება იყვნენ გამანადგურებლები და შეცვალონ ან წაშალონ მონაცემები. გამოვლენის თავიდან აცილების მიზნით, ვირუსებს გააჩნიათ მუტაციის უნარი. ფაილის გახსნის მარტივმა მოქმედებამ შეიძლება გამოიწვიოს ვირუსის გააქტიურება. ჩატვირთვის სექტორის ან ფაილური სისტემის ვირუსი, აინფიცირებს USB მეხსიერების ბარათებს და შეიძლება გავრცელდეს სისტემის მყარ დისკზეც. მას შემდეგ, რაც ვირუსი აქტიურია, ის, როგორც წესი, აინფიცირებს სხვა პროგრამებს კომპიუტერზე ან სხვა კომპიუტერებზე ქსელში. Melissa ვირუსი იყო მსოფლიოში მაგალითი ელექტრონული ფოსტით გავრცელებული ვირუსისა. Melissa-მ დააზარალა ათობით ათასი მომხმარებელი და გამოიწვია სავარაუდო $1.2 მილიარდის ზარალი.

ჭია (Worm) - წარმოადგენს ზიანის მომტან კოდს, რომელიც დამოუკიდებლად ვრცელდება ქსელების მოწყვლადი ადგილების გამოყენებით. ამ ტიპის პროგრამები, როგორც წესი, ანელებენ ტრაფიკის სიჩქარეს ქსელში. განსხვავებით ვირუსებისაგან, რომლებიც მოითხოვენ კომპიუტერს ვირუსული პროგრამის გასაშვებად, ჭიები არსებობენ და ვრცელდებიან დამოუკიდებლად. თავდაპირველი გავრცელების შემდეგ პროგრამა აღარ მოითხოვს მომხმარებლის მონაწილეობას. მას შემდეგ, რაც ჭია დააინფიცირებს ჰოსტს, მას შეუძლია ძალიან სწრაფად გავრცელდეს ქსელში. სხვადასხვა ჭიას ქმედებები ჰგვანან ერთმანერს. ისინი იყენებენ მოწყვლადობას, აქვთ თვითგავრცელების უნარი და გამოიყურებიან, როგორც სასარგებლო პროდუქტი.

ვორმები პასუხისმგებელნი არიან ზოგიერთ ყველაზე დამანგრეველ თავდასხმაზე ინტერნეტში. მაგალითად, 2001 წელს, კოდის წითელმა ვორმმა დააინფიცირა 658 სერვერი. 19 საათის განმავლობაში, ვორმმა მოახდინა 300,000-ზე მეტი სერვერის ინფიცირება.

Trojan horse (ტროას ცხენი) - წარმოადგენს მავნე კოდს, რომელიც ახორციელებს დამაზიანებელ ოპერაციებს სასურველი ოპერაციის საფარქვეშ, როგორიცაა ონლაინ თამაში. ეს ზიანის მომტანი კოდი იყენებს მომხმარებლისათვის მინიჭებულ პრივილეგიებს. ტროიანი განსხვავდება ვირუსისგან, რადგან იგი ებმება არაშესრულებად ფაილებს, როგორიცაა ე.წ.“იმიჯის“ ფაილები, აუდიო ფაილები ან თამაშები.

ლოგიკური ბომბი - არის მავნე პროგრამა, რომელიც იყენებს ამ კოდის გაღვიძების მექანიზმს. მაგალითად, მისი გაღვიძების მიზეზი შეიძლება იყოს თარიღები, სხვა პროგრამების გაშვება ან მომხმარებლის ანგარიშის წაშლა. ლოგიკური ბომბი უმოქმედო რჩება მანამ, სანამ რაიმე მისი გამომწვევი მოვლენა არ მოხდება. ერთხელ გააქტიურებული, ლოგიკური ბომბი ახორციელებს ზიანის მომტან კოდს, რომელიც აინფიცირებს კომპიუტერს. ლოგიკურმა ბომბმა შეიძლება დააზიანოს მონაცემთა ბაზის ჩანაწერები, წაშალოს ფაილები და საფრთხე შეუქმნას ოპერაციულ სისტემას ან სხვა პროგრამებს. კიბერუსაფრთხოების სპეციალისტებმა ცოტა ხნის წინ აღმოაჩინეს ლოგიკური ბომბები, რომლებიც თავს ესხმიან და ანადგურებენ აპარატურულ კომპონენტებს სამუშაო სადგურზე ან სერვერზე, მათ შორის გაგრილების სისტემებს, ცენტრალურ პროცესორს, მეხსიერებას, მყარ დისკებს და დენის წყაროებს. ლოგიკური ბომბები იწვევენ ამ მოწყობილობების გადატვირთვას, რის შედეგადაც ისინი გადახურდებიან და გამოდიან მწყობრიდან.

გამომძალველი პროგრამები (Ransomware) - ეუფლებიან კომპიუტერულ სისტემას ან მონაცემებს, რომელთაც ის შეიცავს და არ აძლევენ მას ფუნქციონირების შესაძლებლობას, სანამ არ მოხდება სისტემის "გამოსყიდვა". გამომძალველი პროგრამები ჩვეულებრივ მუშაობენ კომპიუტერის მონაცემების დაშიფვრის გზით მომხმარებლისთვის უცნობი გასაღების გამოყენებით. მომხმარებელმა უნდა გადაუხადოს გამოსასყიდი დამნაშავეებს, რათა მოეხსნას შეზღუდვა.

გამომძალველი პროგრამის ზოგიერთ სხვა ვერსიას შეუძლია ისარგებლოს კონკრეტული სისტემის მოწყვლადობით და "ჩაკეტოს" სისტემა. გამომძალველი პროგრამები ვრცელდებიან, როგორც ტროიანები გადმოწერილი ფაილის ან ზოგიერთი პროგრამული სისუსტის გამოყენებით.

სისტემის "გამოსყიდვა" უპრეცედენტო გადახდის სისტემის მეშვეობით წარმოადგენს კრიმინალთა მიზანს. მსხვერპლის მიერ გადახდის შემდეგ, ზოგიერთ შემთხვევაში, კრიმინალი უზრუნველყოფს მას გაშიფვრის პროგრამით ან უგზავნის კოდს.

ბექდორები (Backdoors) და რუთკიტები (Rootkits) - ბექდორი წარმოადგენს პროგრამას ან კოდს, შექმნილს კრიმინალის მიერ, რომელიც ახდენს სისტემის კომპრომეტირებას. ბექდორი გვერდს უვლის ნორმალურ ავტორიზაციას, რომელიც გამოიყენება სისტემაში წვდომისთვის. ძირითადი backdoor პროგრამები, როგორებიცაა Netbus და Back Orifice, წარმოადგენენ საშუალებას არასანქცირებული დისტანციური წვდომის განხორციელებისათვის. ბექდორ პროგრამის მიზანი არის კიბერკრიმინალებისათვის სისტემაზე ხელმისაწვდომობის მინიჭება იმ შემთხვევაშიც კი, თუ ორგანიზაცია აფიქსირებს სისტემის შეტევისთვის გამოყენებულ თავდაპირველ მოწყვლადობას. როგორც წესი, დამნაშავეები აიძულებენ მომხმარებლებს მათგან დამოუკიდებლად ტროიანის ინსტალაციას სისტემაში ბექდორ პროგრამის გასაშვებად.

რუთკიტი (Rootkit) ახდენს ოპერაციული სისტემის მოდიფიცირებას ბექდორ პროგრამის შესაქმნელად. თავდამსხმელები ამის შემდეგ იყენებენ ბექდორ პროგრამას კომპიუტერთან დისტანციური წვდომის მოსაპოვებლად. უმრავლესი რუთკიტები სარგებლობენ სისტემის მოწყვლადობით, მოიპოვებენ პრივილეგიებს და ცვლიან სისტემურ ფაილებს. პრივილეგიების ესკალაცია ახდენს პროგრამული შეცდომების გამოვლენას და მოიპოვებს წვდომას ქსელურ რესურსებსა და მონაცემებზე. ასევე რუთკიტები ცვლიან სისტემური მონიტორინგის ინსტრუმენტებს, რის შედეგადაც მეტად ძნელდება მათი გამოვლენა. ხშირად, მომხმარებელი იძულებულია წაშალოს და თავიდან დააინსტალიროს ოპერაციული სისტემა კომპიუტერზე, რომელიც ინფიცირებულია რუთკიტ პროგრამის მიერ.

დაცვა ზიანის მომტანი პროგრამების წინააღმდეგ

რამდენიმე მარტივი ნაბიჯი დაგეხმარებათ დაიცვათ თქვენი სისტემა ყველა ფორმის ზიანის მომტანი პროგრამებისაგან.

- ანტივირუსული პროგრამა - ანტივირუსულ პროგრამათა უმრავლესობას შეუძლია გაანეიტრალოს ყველაზე გავრცელებული ზიანის მომტანი პროგრამები. თუმცა, კიბერდამნაშავეები ყოველდღიურად ვითარდებიან და ახალ საფრთხეებს ქმნიან. აქედან გამომდინარე, ეფექტური ანტივირუსული გადაწყვეტის გამოსავალი არის სისტემის მუდმივი განახლება. ხელმოწერა თითის ანაბეჭდის მსგავსია. იგი განსაზღვრავს ზიანის მომტანი კოდის მახასიათებლებს.
- უახლესი პროგრამული უზრუნველყოფა - მავნე პროგრამების მრავალი ფორმა მიზნად ისახავს პროგრამული უზრუნველყოფის მოწყვლადობის ექსპლუატაციას, როგორც ოპერაციულ სისტემაში, ასევე პროგრამებში. მიუხედავად იმისა, რომ ოპერაციული სისტემის მოწყვლადობა პრობლემების ძირითადი წყარო იყო, დღევანდელი აპლიკაციათა დონის მოწყვლადობა ყველაზე დიდ რისკებს ქმნის. სამწუხაროდ, მიუხედავად იმისა, რომ ოპერაციული სისტემის შემქმნელები მეტად პასუხისმგებლიანები ხდებიან განახლებების მიმართ, ამას ვერ ვიტყვით აპლიკაციათა შემქმნელებზე.

სპამი (Spam)

ელ-ფოსტა უნივერსალური მომსახურებაა, რომელსაც მილიარდობით ადამიანი იყენებს მსოფლიოში. როგორც ერთ-ერთი ყველაზე პოპულარული სერვისი, ელ-ფოსტა წარმოადგენს მომხმარებლებისა და ორგანიზაციების მნიშვნელოვან მოწყვლადობის სექტორს. სპამი, ასევე ცნობილი როგორც უსარგებლო (junk) ელექტრონული შეტყობინება, არის არასასურველი ელ-შეტყობინება. უმრავლეს შემთხვევებში სპამი წარმოგვიდგება, როგორც სარეკლამო გზავნილი. თუმცა სპამს შეუძლია გამოგზავნოს ზიანის მომტანი ბმული, საზიანო კოდი ან ტყუილის შემცველი კონტენტი. მისი საბოლოო მიზანია ისეთი სენსიტიური ინფორმაციის მოპოვება, როგორებიცაა პირადი ნომერი ან საბანკო ანგარიშის მონაცემები. სპამის უმრავლესობა იგზავნება ქსელში ჩართული მრავალი კომპიუტერიდან ვირუსის ან ვორმის მეშვეობით. ეს დაინფიცირებული კომპიუტერები აგზავნიან რაც შეიძლება დიდი რაოდენობის ელექტრონულ შეტყობინებას.

უსაფრთხოების ზომების მიღების მიუხედავად, ზოგიერთმა სპამ წერილმა შესაძლოა მიაღწიოს მიზანს. ჩამოთვლილია სპამის ზოგიერთი ყველაზე გავრცელებული მაჩვენებელი:

- ✓ ელექტრონულ შეტყობინებას არ აქვს სათაური;
- ✓ შეტყობინება ითხოვს ანგარიშის განახლებას;
- ✓ ელ-ფოსტის ტექსტში არის გამოტოვებული სიტყვები ან არასწორი პუნქტუაცია;
- ✓ შეტყობინებაში არსებული ბმული დიდია ან/და დაშიფრული;
- ✓ ელექტრონულ;ი გზავნილი გამოიყურება, როგორც კორესპონდენცია ავტენტური ბიზნესიდან;
- ✓ ელექტრონული გზავნილი მოითხოვს მიმაგრებული ფაილის გახსნას.

თუ მომხმარებელი იღებს ელ-ფოსტას, რომელიც შეიცავს ამ ინდიკატორებს, მან არ უნდა გახსნას ელ-ფოსტა ან ნებისმიერი მიმაგრებული ფაილი. თითქმის ყველა ელ-ფოსტის სერვისი ახდენს სპამის ფილტრაციას. სამწუხაროდ, სპამი კვლავ მოიხმარს ტრაფიკს და მიმღების სერვერს უწევს გზავნილის მონაცემთა დამუშავება.

Spyware, Adware და Scareware

ჯაშუში პროგრამა (Spyware) არის პროგრამული უზრუნველყოფა, რომელიც საშუალებას აძლევს კრიმინალს მიიღოს ინფორმაცია მომხმარებლის კომპიუტერული აქტივობის შესახებ. Spyware ხშირად მოიცავს აქტივობის თვალყურის მადევნებელ ფუნქციას, კლავიშების კომპონაციის შეგროვებას და მონაცემთა მოპარვას. უსაფრთხოების ზომების გადალახვის მცდელობისას, spyware ხშირად ცვლის უსაფრთხოების პარამეტრებს. Spyware ხშირად ებმება ავთენტურ პროგრამულ უზრუნველყოფას ან ტროიანებს. ბევრი ვებგვერდი, რომელზეც განთავსებულია უფასო პროგრამული პროდუქტი, სავსეა spyware პროგრამებით.

Adware, როგორც წესი, ვებსაიტებზე ხსნის გამაღიზიანებელ pop-up ფანჯრებს. მავნე კოდის გამავრცელებელმა პროგრამამ შეიძლება გააანალიზოს მომხმარებლის ინტერესები მისი თვალთვალით საიტებზე, რომლებზეც მომხმარებელს ჰქონდა წვდომა. მას შემდეგ შეუძლია გააგზავნოს pop-up სარეკლამო გზავნილები შესაბამისად იმ საიტებზე. პროგრამული უზრუნველყოფის ზოგიერთი ვერსია ავტომატურად აინსტალირებს Adware-ს. ზოგიერთი adware მხოლოდ რეკლამას მოიცავს, მაგრამ, როგორც წესი, adware მოდის spyware-თან ერთად.

Scareware არწმუნებს მომხმარებელს, განახორციელოს კონკრეტული ქმედება შიშის საფუძველზე. Scareware გამოსახავს ყალბ pop-up ფანჯრებს, რომელიც ჰგავს ოპერაციული სისტემის დიალოგურ ფანჯრებს. ეს ფანჯრები ყალბი შეტყობინებებია, რომლებიც იტყობინებიან, რომ სისტემა რისკის ქვეშ იმყოფება ან საჭიროებს კონკრეტული პროგრამის შესრულებას ნორმალურ ოპერაციაში დაბრუნების მიზნით. სინამდვილეში, პრობლემები არ არსებობს და თუ მომხმარებელი ეთანხმება და საშუალებას აძლევს აღნიშნული პროგრამის შესრულებას, მავნე კოდი აინფიცირებს მის სისტემას.

Phishing (ფიშინგი)

მატყუარა წერილები (ფიშინგი) თაღლითობის ერთ-ერთი ფორმაა. კიბერდამნაშავეები იყენებენ ელ-ფოსტას, მოკლეტექსტურ შეტყობინებებს ან სხვა სოციალური მედიის რესურსებს, რათა შეეცადონ ისეთი ინფორმაციის შეგროვებას, როგორიცაა ფინანსური და ავტორიზაციის მონაცემები, წარუდგენენ რა თავის თავს მომხმარებელს, როგორც რეპუტაციის მქონე პირს ან ორგანიზაციას. ფიშინგი ხორციელდება ელექტრონული ფოსტით გაგზავნილი ყალბი და მავნე კოდის შემცველი გზავნილის მეშვეობით ისე, თითქოს ის გამოგზავნილი იყოს სანდო წყაროდან. გზავნილი გათვლილია მომხმარებლის მიერ მის მოწყობილობაზე მავნე კოდის პროგრამის ინსტალირებაზე, რის შედეგადაც შესაძლებელი გახდება მისი პერსონალური მონაცემების გაზიარება არასასურველი პირებისათვის. ფიშინგის მაგალითი არის ელექტრონული ფოსტის გზავნილი, რომელიც აუწყებს მომხმარებელს მოგებული ჯილდოს შესახებ და მოითხოვს მისგან მითითებულ ბმულზე გადასვლას. ბმულზე გადასვლის შემდეგ შესაძლებელია მოთხოვნილ იქნას პირადი მონაცემების შეყვანა ან მავნე პროგრამის დაინსტალირება.

Spear ფიშინგი უაღრესად მიზანმიმართული ფიშინგის შეტევაა. მიუხედავად იმისა, რომ ფიშინგი და Spear ფიშინგი ორივე იყენებს ელ-ფოსტას მსხვერპლთან წვდომისათვის, Spear ფიშინგი აგზავნის მორგებულ ელ-ფოსტას კონკრეტულ პირზე. კრიმინალი პოტენციური მსხვერპლის ინტერესებს ელ-ფოსტის გაგზავნამდე იკვლევს. მაგალითად, კრიმინალი შეისწავლის, რომ სამიზნე დაინტერესებულია მანქანებით და ეძებს ავტომობილის კონკრეტული მოდელის შეძენას. კრიმინალი უერთდება იმავე მანქანის დისკუსიის ფორუმს, სადაც პოტენციური მსხვერპლია გაწევრიანებული, აქვეყნებს ავტომანქანის

გაყიდვის შეთავაზებას და უგზავნის ელ-ფოსტას მსხვერპლს. ელექტრონული ფოსტის გზავნილი შეიცავს ბმულს მანქანის სურათებით. როდესაც სამიზნე დააჭერს ბმულს, ის თავისდაუნებურად აინსტალირებს მავნე კოდს თავის კომპიუტერში.

Vishing, Smishing, Pharming და Whaling

Vishing არის ფიშინგის ფორმა, რომელიც წარმოადგენს ხმის გამოყენებით საკომუნიკაციო ტექნოლოგიას. კრიმინალებს შეუძლიათ განახორციელონ spoof ზარები ლეგიტიმური წყაროებიდან VoIP ტექნოლოგიის გამოყენებით. დაზარალებულებმა შესაძლოა მიიღონ ჩაწერილი ხმოვანი შეტყობინება, რომელიც, ერთი შეხედვით, ავთენტური წყაროდანაა მიღებული. კრიმინალებს სურთ მიიღონ საკრედიტო ბარათის ნომრები ან სხვა ინფორმაცია დაზარალებულის იდენტობის მოპარვის მიზნით. Vishing კრიმინალი სარგებლობს იმით, რომ ხალხი ენდობა სატელეფონო ქსელს.

Smishing (შემოკლებული შეტყობინების ფიშინგი) — წარმოადგენს ფიშინგს მობილურ ტელეფონებზე ტექსტური შეტყობინებების გამოყენებით. დამნაშავეები იყენებენ ავთენტურ წყაროს მსხვერპლის ნდობის მოპოვების მცდელობის მიზნით. მაგალითად, smishing შეტევის შედეგად შესაძლოა მსხვერპლს ვებგვერდის ბმული გაეგზავნოს. როდესაც მსხვერპლი ეწვევა შეთავაზებულ ვებსაიტს, malware კოდი დაინსტალირდება მის მობილურ ტელეფონზე.

Pharming არის ლეგიტიმური საიტის განსახიერება მომხმარებლის მოტყუების მიზნით, რათა მან შეიყვანოს თავისი ანგარიშის ავტორიზაციის მონაცემები. Pharming-ს შეცდომაში შეჰყავს მომხმარებლები ყალბი ვებსაიტებით, რომელნიც, ერთი შეხედვით, ავთენტური ჩანან. მსხვერპლი, რომელსაც შეჰყავს პირადი ინფორმაცია, ფიქრობს, რომ ის დაკავშირებულია რეალურ საიტთან.

Pharming წარმოადგენს ფიშინგის შეტევის ნაირსახეობას, რომელიც მიზნად ისახავს მაღალი რგოლის მენეჯმენტის დაინფიცირებას ორგანიზაციის ფარგლებში, როგორიცაა დირექტორები. დამატებითი სამიზნეები მოიცავენ პოლიტიკოსებს ან ცნობილ სახეებს.

ბრაუზერის მოდულები და ბრაუზერის მოწამვლა (Poisoning)

უსაფრთხოების მოწყვლადობებმა შეიძლება გავლენა იქონიონ ვებბრაუზერებზე pop-up რეკლამის ჩვენებით, ინფორმაციის

შეგროვებით ან adware-ის, ვირუსების ან spyware-ის ინსტალაციით. კრიმინალს შეუძლია გატეხოს ბრაუზერის პროგრამული ფაილი, ბრაუზერის კომპონენტები ან მისი დანამატები.

პლაგინები (Plugins) - Flash-ისა და Shockwave პლაგინები Adobe-დან საშუალებას იძლევა, მივიღოთ საინტერესო გრაფიკული და მულტიპლიკაციური ანიმაციები, რაც მნიშვნელოვნად აუმჯობესებს ვებგვერდის დიზაინს. პლაგინები გამოსახავენ შესაბამისი პროგრამული უზრუნველყოფის გამოყენებით შემუშავებულ კონტენტს.

ბოლო დრომდე, პლაგინები წარმოადგენდნენ შესანიშნავ უსაფრთხო ჩანაწერებს. მას შემდეგ, რაც Flash-ზე დაფუძნებული კონტენტი განვითარდა და უფრო პოპულარული გახდა, დამნაშავეებმა შეისწავლეს Flash პლაგინები და მისი პროგრამული უზრუნველყოფა, გამოიკვლიეს მისი მოწყვლადი ადგილები და დაიწყეს Flash Player-ის თავისი მიზნებისათვის გამოყენება. წარმატებულმა ექსპლუატაციამ შეიძლება გამოიწვიოს სისტემის შეფერხება ან დაუშვას კრიმინალის მიერ დაზარალებული სისტემის კონტროლი. მოსალოდნელია გაზრდილი მონაცემების დანაკარგები, რადგან დამნაშავეები კვლავაც განაგრძობენ პოპულარული პლაგინებისა და პროტოკოლების გამოკვლევას მისი მოწყვლადი ადგილების მოძიების მიზნით.

SEO Poisoning (საძიებო სისტემის ძრავის დაინფიცირება) - საძიებო ძრავები, როგორიცაა Google მუშაობენ გვერდების რანჟირების მიხედვით და შესაბამისი შედეგების წარდგენით მომხმარებელთათვის საძიებო შეკითხვებზე დაყრდნობით. ვებგვერდის შინაარსიდან გამომდინარე, იგი შეიძლება აღმოჩნდეს უფრო მაღლა ან დაბლა ძიების შედეგების სიაში. SEO წარმოადგენს ტექნიკურ საშუალებათა კრებულს, რომელიც გამოიყენება საძიებო ძრავში ვებსაიტთა რანჟირების გასაუმჯობესებლად. მიუხედავად იმისა, რომ ბევრი ლეგიტიმური კომპანია სპეციალიზდება ვებსაიტების ოპტიმიზაციაში, რათა უკეთესად პოზიციონირდეს, SEO მოწამვლა იყენებს ალგორითმს, რათა მავნე ვებსაიტი უფრო მაღალ პოზიციაზე აღმოჩნდეს ძიების შედეგ

SEO-ს მოწამვლის ყველაზე გავრცელებული მიზანი არის მავნე საიტების ტრაფიკის გაზრდა, რომლებსაც შეუძლიათ მავნე პროგრამების განთავსება ან სოციალური ინჟინერიის განხორციელება.

იმისათვის, რომ მავნე კოდის შემცველი საიტი გამოისახოს უფრო მაღლა ძიების შედეგებში, თავდამსხმელები სარგებლობენ პოპულარული საძიებო ტერმინებით.

ბრაუზერის გამტაცებელი (Hijacker) - ბრაუზერის გამტაცებელი არის მავნე კოდი, რომელიც ცვლის კომპიუტერის ბრაუზერის პარამეტრებს, რათა მომხმარებელი გადამისამართდეს კიბერკრიმინალის სასურველ საიტზე. ბრაუზერის გამტაცებელი, როგორც წესი, ინსტალირდება მომხმარებლის ნებართვის გარეშე და ეშვება დისკზე რაიმეს ჩამოტვირთვის შედეგად. Drive by download არის პროგრამა, რომელიც ავტომატურად ჩამოტვირთავს კონტენტს კომპიუტერში, როდესაც მომხმარებელი სტუმრობს ვებგვერდს ან ხსნის ელფოსტის შეტყობინებას. პროგრამების ჩამოტვირთვის დროს ყოველთვის ყურადღებით წაიკითხეთ ტექსტი, რათა არ გახდეთ ზიანის მომტანი კოდის მსხვერპლი.

დაცვა ელ-ფოსტისა და ბრაუზერზე თავდასხმებისგან

სპამთან დაკავშირებული მეთოდები მოიცავს ელ-ფოსტის ფილტრაციას, მომხმარებლის ყურადღებას უცნობი ელ-ფოსტის მიმართ და სერვერული ფილტების გამოყენების აუცილებლობას.

სპამის სრულად შეჩერება ძნელია, მაგრამ არსებობს საშუალებები მისი მინიმუმამდე დაყვანისათვის. მაგალითისთვის, ზოგიერთი ინტერნეტ პროვაიდერი კომპანია ფილტრავს სპამს, სანამ ისინი მიაღწევენ მომხმარებლის შემოსულ წერილებში (inbox). მრავალი ანტივირუსული და ელ-ფოსტის პროგრამა ავტომატურად ფილტრავს სპამს, სანამ ის მიაღწევდეს მომხმარებლამდე. ეს ნიშნავს, რომ მათ აღმოაჩინეს და წაშალეს სპამ შეტყობინებები ელ-ფოსტის შემოსული წერილებიდან.

ორგანიზაციებმა უნდა აუხსნან თავიანთ თანამშრომლებს, რომ მიბმული ფაილის გახსნა შესაძლოა სახიფათო იყოს, რადგან ის შეიძლება შეიცავდეს ვირუსს ან ქსელურ ჭიას (worm), ან რომელიმე სხვა მავნე პროგრამას. დარწმუნდით, რომ შემოსული ელ-ფოსტის წერილები არ შეიცავენ სპამს, იმ შემთხვევაშიც კი, თუ მათი გამომგზავნი სანდო კონტაქტია. ვირუსი შეიძლება გავრცელდეს გამომგზავნის კომპიუტერის გამოყენებით. ყოველთვის შეამოწმეთ ფოსტის მიბმული ფაილები, სანამ გახსნით მათ.

ანტი-ფიშინგის სამუშაო ჯგუფი (APWG) წარმოადგენს ინდუსტრიის ასოციაციას, რომელიც ორიენტირებულია პიროვნების ქურდობისა და კიბერთაღლითობის აღმოფხვრაზე, რომელთაც ფიშინგი და ელ-ფოსტის გაყალბება იწვევს.

მუდმივი პროგრამული განახლება და უახლესი ვერსიების ინსტალირება უზრუნველყოფს სისტემის მდგარდობას და უსაფრთხოებას ცნობილი მოყვლადი ადგილების მიმართ.

3.2 მოტყუების ხელოვნება. სოციალური ინჟინერიაში გამოყენებული სხვადასხვა მეთოდები

Social Engineering (სოციალური ინჟინერია)

სოციალური ინჟინერია წარმოადგენს სრულიად არატექნიკურ საშუალებას კრიმინალისთვის ინფორმაციის შეგროვების მიზნით. სოციალური ინჟინერია არის თავდასხმა, რომელიც ცდილობს დაარწმუნოს ინდივიდები ქმედებების შესრულებაში ან კონფიდენციალური ინფორმაციის გამჟღავნებაში.

სოციალური ინჟინერიის გამოყენებით თაღლითები ხშირად ეყრდნობიან ხალხის სურვილს, რომ იყვნენ სასარგებლონი, თუმცა ასევე აგებენ თავიანთ გეგმებს ადამიანების სისუსტეებზე დაყრდნობით. მაგალითად, თავდამსხმელს შეუძლია დაურეკოს უფლებამოსილ თანამშრომელს და შესჩივლოს მას გადაუდებელი პრობლემის შესახებ, რომელიც მოითხოვს ქსელზე დაუყოვნებლივ ხელმისაწვდომობას. თავდამსხმელს შეუძლია ისარგებლოს ასევე დასაქმებულის პატივმოყვარეობით ან სიხარბით და გამოსტყუოს მას საჭირო ინფორმაცია.

ქვემოთ ჩამოთვლილია გარკვეული სახის სოციალური საინჟინრო თავდასხმები:

Pretexting - როდესაც თავდამსხმელი უკავშირდება ინდივიდს და ატყუებს მას პრივილეგირებულ მონაცემებზე წვდომის მიზნით. მაგალითში მოყვანილია შემთხვევა, როდესაც ბოროტგანმზრახველი თავს აჩვენებს, თითქოს ესაჭიროება პერსონალური ან ფინანსური მონაცემები მიმღების იდენტობის დასაფიქსირებლად.

Something for Something (Quid pro quo) - ესაა შემთხვევა, როდესაც თავდამსხმელი ითხოვს პერსონალური მონაცემების რაიმეში, მაგალითად, საჩუქარში, გაცვლას.

სოციალური ინჟინერიით მოსაგებლე კრიმინალები რამდენიმე ტაქტიკას ეყრდნობიან. სოციალური საინჟინრო ტაქტიკა მოიცავს:

- უფლებამოსილება — ხალხი უფრო მეტად ენდობა „უფროსების“ ინსტრუქციებს;
- ზეწოლა - დამნაშავეები პოტენციურ მსხვერპლს აშინებენ გარკვეული ქმედების განხორციელების მუქარით;
- კონსენსუსი/სოციალური მტკიცებულება - ადამიანები იმოქმედებენ, თუ გადაწყვეტენ, რომ სხვა ადამიანები მოიწონებენ ამ ქმედებას;
- უნარის სიმწირე - ადამიანები იმოქმედებენ, თუ გადაწყვეტენ, რომ ამ ქმედების განსახორციელებლად აქვთ შეზღუდული შესაძლებლობა;
- გადაუდებელი აუცილებლობა — ადამიანები იმოქმედებენ, თუ გადაწყვეტენ, რომ ამ ქმედების განსახორციელებლად აქვთ მცირე დრო;
- გაცნობა/სიამოვნება - კრიმინალები მსხვერპლთან ურთიერთობის დამყარების მიზნით ამყარებენ მასთან ახლო ურთიერთობას;
- ნდობა - დამნაშავეები ქმნიან ნდობით ურთიერთობას დაზარალებულთან, რასაც შეიძლება უფრო მეტი დრო დასჭირდეს.

წარმოგიდგენთ ტაქტიკის მაგალითებს:

- ავტორიტეტი - მომხმარებელი ხსნის ინფიცირებულ PDF-ს, რომელიც გამოიყურება, როგორც ოფიციალური სასამართლო უწყება;
- დაშინება - მდივანი იღებს ზარს, რომელშიც ნათქვამია, რომ მისი უფროსი აპირებს მნიშვნელოვანი პრეზენტაციის გამოქვეყნებას, მაგრამ მისი ფაილები დაზიანებულია. კიბერკრიმინალი ითხოვს ფაილების დაუყოვნებლივ გაგზავნას;

- კონსენსუსი - კრიმინალები ქმნიან ვებგვერდებს ყალბი ჩვენებებით, რომლებიც ხელს უწყობენ პროდუქტის რეალიზებას და უთითებენ, რომ ის არის უსაფრთხო;
- დეფიციტი - კრიმინალები გთავაზობენ შეზღუდულ დროს შეთავაზებისთვის, რომელიც არ გრძელდება დიდ ხანს იმ იმედით, რომ დაზარალებული სწრაფად იმოქმედებს;
- გადაუდებელი - დამნაშავეები ადგენენ ბოლო ვადას ქმედების გასაყალბებლად და ადგენენ გარკვეულ ფასს;
- ცოდნა - ხალხი დიდი ალბათობით აკეთებს იმას, რასაც სხვა ადამიანი სთხოვს, თუ მათ აქვთ ამ ადამიანის ნდობა;
- ნდობა - „უსაფრთხოების ექპერტი“ ურეკავს დაზარალებულს. სთავაზობს რჩევებს და იღებს მისგან ინფორმაციას ავტორიზაციის მონაცემების შესახებ. დაზარალებულის დახმარების პროცესში, კრიმინალი აღმოაჩენს „სერიოზულ შეცდომას“, რომელიც დაუყოვნებლივ ყურადღებას საჭიროებს. შედეგად კრიმინალი მოიპოვებს გარკვეულ შესაძლებლობებს.

კიბერუსაფრთხოების პროფესიონალები პასუხისმგებელნი არიან ორგანიზაციაში პერსონალის განათლებაზე სოციალური ინჟინრების ტაქტიკების შესახებ.

Shoulder Surfing და Dumpster Diving

Shoulder surfing-ით კრიმინალები ცდილობენ მოიპოვონ PIN კოდები, წვდომის კოდები და საკრედიტო ბარათის ნომრები. თავდამსხმელი შეიძლება იყოს მისი სავარაუდო მსხვერპლის სიახლოვეს ან თავდამსხმელს შეუძლია გამოიყენოს ბინოკლები ან დახურული მიკროსქემის კამერები shoulder surfing-ის განსახორციელებლად. საპასუხოდ, ტექნოლოგიები ისე დაინერგა, რომ ადამიანს შეუძლია ბანკომატის ეკრანის დანახვა მხოლოდ გარკვეული კუთხით. ამ ტიპის დაცვები surfing-ის განხორციელებას ბევრად უფრო ართულებს.

„ერთი კაცის ნაგავი სხვისი საგანძურია“ - ეს ფრაზა შეიძლება განსაკუთრებით შეესაბამებოდეს dumpster diving-ის სამყაროს, რომელიც გულისხმობს ბოროტგანმზრახველის მცდელობას, შეაღწიოს ორგანიზაციის „სანაგვე ურნებში“, რათა გაიგოს, რა მონაცემებთან მუშაობდა ეს ორგანიზაცია. განვიხილოთ ამ „ნაგვის“ დაცვის უზრუნველყოფა. ნებისმიერი სენსიტიური ინფორმაცია უნდა იყოს

სათანადოდ განკარგული ან განადგურებული მას შემდეგ, რაც აღარაა მისი გამოყენების საჭიროება. კონტეინერი, რომელიც ფლობს საიდუმლო ან მგრძნობიარე დოკუმენტებს, უნდა იქნეს დამწვარი.

პერსონაცია და მოტყუებები (Hoaxes)

ვინმედ თავის გასაღება (Impersonation) არის ქმედება ქმედება, როდესაც ადამიანი წარადგენს თავის თავს, როგორც სხვა პერსონას. მაგალითად, მან შესაძლოა თავი წარადგინოს, როგორც სატელეფონო scam-ის მიზნობრივმა გადამხდელმა. ზოგჯერ კრიმინალი წარადგენს თავს, როგორც ხაზინის თანამშრომელი, და აცხადებს, რომ პოტენციურ მსხვერპლს მართებს ბიუჯეტის ვალი. მსხვერპლს ევალება დაუყოვნებლივ დაფაროს ვალი გადარიცხვით. თაღლითი იმუქრება, რომ გადაუხდელობის შემთხვევა გამოიწვევს მსხვერპლის დაპატიმრებას. დამნაშავეები ასევე იყენებენ პერსონაციას სხვებზე თავდასხმის მიზნით. მათ შეუძლიათ ძირი გამოუთხარონ ინდივიდების სანდოობას ვებგვერდის ან სოციალური მედიის გამოყენებით.

მოტყუება (hoax) წარმოადგენს აქტს, რომელიც მიზნად ისახავს სავარაუდო მსხვერპლის შეცდომაში შეყვანას. Hoax-მა შესაძლოა გამოიწვიოს ისეთივე დაზიანება, როგორც სხვა ზიანის მომტანმა ქმედებებმა. Hoax იწვევს მომხმარებლის რეაქციას. ამ რეაქციას შეუძლია გამოიწვიოს ზედმეტი შიში და ირაციონალური ქცევა. მომხმარებელი განიცდის Hoaxes-ის გავლენას ელექტრონული ფოსტით და სოციალური მედიის საშუალებით.

Piggybacking და Tailgating

Piggybacking ხდება მაშინ, როდესაც კრიმინალი ახერხებს უფლებამოსილ პირთან ერთად მოიპოვოს წვდომა დაცულ ლოკაციაზე ან შეზღუდულ არეაზე. დამნაშავეები იყენებენ piggyback-ის რამდენიმე მეთოდს :

- ისინი ქმნიან შთაბეჭდილებას, რომ წარმოადგენენ უფლებამოსილი პირის ესკორტს;
- ისინი უერთდებიან ორგანიზაციის წევრთა დიდ ჯგუფს, აჩვენებენ რა თავს, რომ ისინიც ამ ჯგუფის წევრები არიან;
- ისინი მიზანში იღებენ თანამშრომელს, რომელიც უყურადღებოდ ექცევა დაწესებულების წესებს.

Tailgating არის კიდევ ერთი ტერმინი, რომელიც აღწერს იგივე პრაქტიკას.

Piggybacking- თან გამკლავება შესაძლებელია სპეციფიური ხაფანგის (ორი კარების პრინციპი) გამოყენებით. მას შემდეგ, რაც პირები შედიან გარე კარებში, ის უნდა დაიხუროს შიდა კარში შესვლამდე.

დაცვა თაღლითობის წინააღმდეგ

ორგანიზაციებმა უნდა უზრუნველყონ სოციალური ინჟინერიის ტაქტიკის ცნობიერების ამაღლება და თანამშრომლების სათანადო განათლება პრევენციული ღონისძიებების შესახებ, როგორიცაა:

- არასოდეს გასცეს კონფიდენციალური ინფორმაცია ან ანგარიშის ავტორიზაციის მონაცემები ელექტრონული ფოსტით, ჩატით, პერსონალურად ან ტელეფონით უცნობებთან შეხვედრებზე;
- დაძლიეთ სურვილი დააჭიროთ უცნობ ბმულებს ან ელ.ფოსტით მიღებულ გზავნილს;
- ყურადღება მიაქციეთ არაინიცირებულ ან ავტომატურ ჩამოტვირთვებს;
- შექმენით მყარი პოლიტიკა და მიაწოდეთ ინფორმაცია თანამშრომლებს მის შესახებ;
- როდესაც საქმე უსაფრთხოებას ეხება, გააღვიძეთ თანამშრომლებში პირადი პასუხისმგებლობის გრძნობა;
- არ დაჰყვეთ ზეწოლას უცნობი პირებისგან.

3.3 კიბერთავდასხმის სახეები. უსადენო და მობილურ მოწყობილობებზე თავდასხმები

სერვისზე წვდომის შეზღუდვა (Denial of Service)

სერვისზე წვდომის შეზღუდვის (Denial-of-Service (DoS)) თავდასხმა წარმოადგენს ქსელზე თავდასხმის ტიპს. DoS თავდასხმა იწვევს ქსელის სერვისების გარკვეულ შეფერხებას მომხმარებლებისთვის, მოწყობილობებისთვის ან აპლიკაციებისთვის. არსებობს DOS თავდასხმების ორი ძირითადი ტიპი:

- ტრაფიკის აბსოლუტური დაკავება - თავდამსხმელი აგზავნის მონაცემთა უზარმაზარ რაოდენობას, რომელსაც ქსელი, ჰოსტი

ან აპლიკაცია ვერ უმკლავდება. ეს იწვევს გადაცემის ან რეაგირების შეფერხებას, ან მოწყობილობის ან მომსახურების დაზიანებას.

- ბოროტგანზრახულად (Maliciously) ფორმატირებული პაკეტები - თავდამსხმელი აგზავნის ბოროტგანზრახულად ფორმატირებულ პაკეტებს ქსელში, რომლის დამუშავებასაც ჰოსტი ან აპლიკაცია ვერ უმკლავდება. მაგალითად, აპლიკაციას არ შეუძლია შეცდომების შემცველი პაკეტების იდენტიფიცირება ან თავდამსხმელის მიერ გადაგზავნილი არასწორად ფორმატირებული პაკეტების დამუშავება. ეს იწვევს მიმღებ მოწყობილობის მიერ პაკეტთა გადაცემის შენელებას ან სრულად შეწყვეტას.

DoS თავდასხმები წარმოადგენენ ძირითადი რისკებს, რადგან მათ შეუძლიათ ადვილად ჩაშალონ კომუნიკაცია და გამოიწვიონ დროისა და ფინანსური რესურსების მნიშვნელოვანი დანაკარგი. ეს თავდასხმები შედარებით მარტივია და მისი განხორციელება შეუძლია თუნდაც არაკვალიფიციურ ჰაკერს.

წვდომის შეზღუდვის მიზანია ჩაშალოს ავტორიზებული მომხმარებლების წვდომა ქსელთან (გახსოვდეთ უსაფრთხოების სამი ძირითადი პრინციპი: კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა).

განაწილებული DoS თავდასხმა (DDoS) მსგავსია DoS თავდასხმისა, მაგრამ იგი წარმოიშობა მრავალი, კოორდინირებული წყაროებიდან. მაგალითად, DDoS თავდასხმა შეიძლება განხორციელდეს შემდეგნაირად:

თავდამსხმელი ქმნის ინფიცირებულ კვანძთა ქსელს, რომელსაც ეწოდება ბოტნეტი და რომელიც შედგება ზომბი (zombie) ჰოსტებისაგან. ზომბები წარმოადგენენ ინფიცირებულ ჰოსტებს. თავდამსხმელი იყენებს სპეციფიურ დამმუშავებელ სისტემებს, რომლებიც აკონტროლებენ ზომბ ჰოსტებს. ზომბი კომპიუტერები ახდენენ ჰოსტების სკანირებასა და ინფიცირებას, ქმნიან რა ამ ქმედებებით მეტ ზომბებს. მზადყოფნის მიღწევისას, ჰაკერი ავალებს დამმუშავებელ სისტემას, რომ ზომბმა ბოტნეტმა განახორციელოს DDoS თავდასხმა.

სნიფინგი (Sniffing) - მსგავსია ვინმეს მიყურადების პროცესისა. ეს ხდება მაშინ, როდესაც თავდამსხმელები შეისწავლიან იმ ქსელების ტრაფიკს, რომლებიც გადიან მათი ქსელის ადაპტერის გავლით, მიუხედავად იმისა, ეკუთვნით მათ ეს მონაცემები თუ არა. დამნაშავეები განახორციელებენ ქსელის sniffing-ს სპეციალური პროგრამული უზრუნველყოფის, აპარატურის ან ორივეს კომბინაციით. sniffing-ით შესაძლებელია ყველა ქსელის ტრაფიკის ან პროტოკოლის, სერვისის ან თუნდაც ისეთი სტრიქონების გამორჩევა, როგორიცაა მომხმარებლის სახელები და პაროლები. ზოგიერთი ქსელის sniffers-ს შეუძლია გამოარჩიოს ყველა ქსელის ტრაფიკი და შეცვალოს მათი ტრაფიკი სურვილისამებრ.

Sniffing-ს ასევე გააჩნია თავისი სარგებელი. ქსელის ადმინისტრატორებს ასევე შეუძლიათ გამოიყენონ სნიფერები ქსელური ტრაფიკის გასაანალიზებლად, გამტარუნარიანობის საკითხების იდენტიფიცირებისა და სხვა ქსელური საკითხების მოგვარების მიზნით.

ფიზიკური უსაფრთხოების უზრუნველყოფა მნიშვნელოვანია შიდა ქსელში sniffer-ის ბოროტად გამოყენების თავიდან ასაცილებლად.

სპუფინგი (Spoofing) - არის თავდასხმის სახეობა, რომელიც იყენებს სანდო ურთიერთობას ორ სისტემას შორის. თუ ორი სისტემა შეათანხმებს ერთმანეთის მიმართ განხორციელებულ ავთენტიფიკაციას, ერთ სისტემაზე შესულმა ინდივიდმა შესაძლოა, სხვა სისტემასთან წვდომისთვის კვლავ ვერ გაიაროს ავტორიზაციის პროცესი. თავდამსხმელს შეუძლია ისარგებლოს ამ შეთანხმებით და გაგზავნოს პაკეტი ერთი სისტემიდან, რომელიც, ერთი შეხედვით, სანდო სისტემაა. სანდო ურთიერთობის დამყარების შემდეგ მიზანში ამოღებულმა სისტემამ შეიძლება დაამუშაოს მიღებული მოთხოვნები შემდგომი ავთენტიფიკაციის გარეშე.

არსებობს მრავალი სახის spoofing თავდასხმა.

- MAC მისამართის spoofing ხდება მაშინ, როდესაც ერთი კომპიუტერი იღებს მონაცემთა პაკეტებს სხვა კომპიუტერის MAC მისამართის საფუძველზე;
- IP spoofing აგზავნის IP პაკეტებს უკვე დაზიანებული წყაროდან მისამართის შენიღბვის მიზნით;

- მისამართის რეზოლუციის პროტოკოლი (ARP) წარმოადგენს პროტოკოლს, რომელიც გარდაქმნის IP მისამართებს MAC მისამართებში მონაცემთა გადაცემისთვის. ARP spoofing აგზავნის დაზიანებულ ARP შეტყობინებებს მთელი ქსელის მასშტაბით, რათა დაუკავშიროს ყალბი MAC მისამართი ქსელის ლეგალური წევრის IP მისამართს;
- დომენური სახელის სისტემა (DNS) გარდაქმნის დომენურ სახელებს IP მისამართებში. DNS სერვერის spoofing აიძულებს DNS სერვერს კონკრეტული დომენის სახელის გარდაქმნას ყალბ IP მისამართში, რომელსაც მართავს ბოროტგანმზრახველი.

შუამავლის თღლითობა (Man-in-the-middle) - ბოროტგანმზრახველი ახორციელებს შუამავლის (MitM) შეტევას, ერევა რა ორ კომპიუტერს შორის გადაცემის პროცესში და იპარავს ინფორმაციას, რომელიც გადაიცემა ქსელში. ბოროტგანმზრახველს ასევე შეუძლია მოახდინოს მანიპულაცია გზავნილებზე და გადასცეს ყალბი ინფორმაცია კვანძებს შორის, სანამ გაირკვევა ამ მონაცემთა სიყალბე. MitM საშუალებას აძლევს კრიმინალს აკონტროლოს მოწყობილობა ისე, რომ მომხმარებელმა ამის შესახებ არაფერი იცოდეს.

MitMo აკონტროლებს მობილურ მოწყობილობებს. ინფიცირებული მობილური მოწყობილობა თავდამსხმელებს უგზავნის მომხმარებლის სენსიტიურ ინფორმაციას. ZeUs წარმოადგენს MitMo-ს შესაძლებლობების გამოყენების მაგალითს, რომელიც საშუალებას აძლევს შემტევს, მიიღოს მომხმარებლის მიერ გაგზავნილი SMS გზავნილის 2-ეტაპიანი ავტორიზაციის ინფორმაცია. მაგალითად, როდესაც მომხმარებელი ქმნის Apple ID-ის, მან უნდა მიიღოს დროებითი დამოწმების კოდი ტექსტური შეტყობინების მეშვეობით მომხმარებლის ვინაობის დასამტკიცებლად. Malware ჯაშუშები "იჭერენ" ამ ტიპის კომუნიკაციას და გადასცემენ ინფორმაციას დამნაშავეებს.

Replay თავდასხმა ხდება მაშინ, როდესაც თავდამსხმელი იღებს კომუნიკაციის ნაწილს ორ მხარეს შორის და ახდენს "დაჭერილი" გზავნილის გადაგზავნას მოგვიანებით. Replay თავდასხმები ხორციელდება ავტორიზაციის მექანიზმების გვერდის ავლით.

Zero-Day შეტევები - Zero-Day შეტევა, ზოგჯერ მოხსენიებული როგორც ნულოვანი-დღის საფრთხე, არის კომპიუტერული შეტევა, რომელიც ცდილობს პროგრამული უზრუნველყოფის იმ დაუცველი ადგილების გამოყენებას, რომლებიც არ არის ცნობილი ან გასაიდუმლოებულია პროგრამის მწარმოებლის მიერ. ტერმინი ნულოვანი-დღის საათი აღწერს მომენტს, როდესაც ვინმე აღმოაჩენს ქმედებას. იმ დროის განმავლობაში, რაც აუცილებელია მწარმოებლის პროგრამული უზრუნველყოფის განახლების შემუშავებასა და გამოშვებისთვის, ქსელი დაუცველია ასეთი ექსპლოიტებისაგან. ასეთი სწრაფად მოძრავი შეტევებისგან დაცვა მოითხოვს ქსელის უსაფრთხოების პროფესიონალებისაგან, გამოიყენონ უფრო რთული ტიპის არქიტექტურა. უკვე აღარაა შესაძლებელი რამდენიმე შემოჭრის არსებობა ქსელში.

კლავიატურის მიყურადება - კლავიატურის მიყურადება (Keylogging) წარმოადგენს პროგრამული პროდუქტს, რომელიც ახდენს ჟურნალირებას ან ჩაიწერს სისტემის მომხმარებლის კლავიშების გამოყენების თანმიმდევრობას. კრიმინალებს შეუძლიათ განახორციელონ კლავიატურის ჟურნალირება სპეციალური პროგრამით ან მსხვერპლის კომპიუტერთან ფიზიკურად მიერთებული სპეციფიური აპარატურის მეშვეობით. კრიმინალი აკონფიგურირებს კლავიატურის ჟურნალირების პროგრამულ უზრუნველყოფას ისე, რომ ლოგფაილი გაიგზავნება ელ.ფოსტაზე. შედეგად "დაჭერილი" ლოგფაილი შესაძლოა შეიცავდეს მსხვერპლის სახელებს, პაროლებს, ვებსაიტებს, რომლებზეც განხორციელდა ვიზიტი და სხვა სენსიტიურ ინფორმაციას.

კლავიატურის ჟურნალირების პროგრამა შეიძლება წარმოადგენდეს ლეგიტიმურ, კომერციულ პროგრამულ უზრუნველყოფას. მშობლები ხშირად ყიდულობენ ამ პროგრამულ უზრუნველყოფას, რათა თვალყური ადევნონ ბავშვების მიერ ინტერნეტში განხორციელებულ ვიზიტებს სხვადასხვა საიტებზე. ბევრ ანტივირუსულ პროგრამას შეუძლია აღმოაჩინოს და წაშალოს არაავტორიზებული ჟურნალირების პროგრამა. მიუხედავად იმისა, რომ ზოგჯერ keylogging პროგრამული უზრუნველყოფა კანონიერია, დამნაშავეები მას ხშირად იყენებენ უკანონო მიზნებისათვის.

თავდასხმებისგან დაცვა

ორგანიზაციას შეუძლია გადადგას მთელი რიგი ნაბიჯები სხვადასხვა თავდასხმისგან თავის დასაცავად. მაგ.:ქსელური დაცვის ეკრანის გამართვა ისე, რომ მან უკუაგდოს ის პაკეტები ქსელის გარედან, რომელთა მისამართები აჩვენებენ, რომ მათი გენერირება მოხდა ქსელს შიგნით. ეს სიტუაცია ჩვეულებრივ არ ხდება და ეს მიუთითებს იმაზე, რომ ხდება კიბერკრიმინალური მცდელობა, კერძოდ spoofing თავდასხმა.

DoS და DDoS თავდასხმების თავიდან აცილების მიზნით, დარწმუნდით, რომ განახლებები არის განხორციელებული და მოახდინეთ ICMP პაკეტთა ბლოკირება ქსელის საზღვარზე. ქსელური მოწყობილობები იყენებენ ICMP პაკეტებს ყალბი შეტყობინებების გასაგზავნად. მაგალითად, ping ბრძანება იყენებს ICMP პაკეტებს, რათა გადამოწმდეს, ხორციელდება თუ არა წარმატებული კავშირი ორ ჰოსტს შორის.

Replay შეტევების თავიდან ასაცილებლად კომპანიებს შეუძლიათ დაშიფრონ ტრაფიკი, უზრუნველყონ კრიპტოგრაფიული ავტორიზაცია და დროის მონიშვნა (time stamp) გზავნილთა ყოველ პორციას შორის.

სმარტფონების პოპულარობის ზრდასთან ერთად, Grayware გადაიქცა საკმაოდ სერიოზულ პრობლემად. Grayware მოიცავს პროგრამებს, რომლებიც მოქმედებენ საფრთხის შემცველი ან არასასურველი გზით. Grayware შეიძლება არ იყოს ხილული ცნობად malware კოდის დაფარული ფარგლებში, მაგრამ შეიძლება მაინც საფრთხეს უქმნიდეს მომხმარებელს. მაგალითად, Graywar-ს შეუძლია აკონტროლოს მომხმარებლის ადგილმდებარეობა. Grayware-ის შემქმნელები ცდილობენ წარმოაჩინონ მათ მიერ წარმოდგენილი პროდუქტი, როგორც ავთენტური, შეაქვთ რა ის აპლიკაციის შესაძლებლობათა სალიცენზიო შეთანხმებაში. მომხმარებელი ბევრ მობილურ აპლიკაციას აინსტალირებს მათი შესაძლებლობების განხილვის გარეშე.

Smishing წარმოადგენს SMS ფიშინგის მოკლე ვარიანტს. იგი იყენებს მოკლე შეტყობინების სერვისს (SMS) ყალბი ტექსტური შეტყობინებების გასაგზავნად. დამნაშავეები სთავაზობენ მომხმარებელს ვებსაიტის მონახულებას ან მითითებულ ტელეფონის

ნომერზე დარეკვას. მსვერპლმა, რომელიც არაფერს არ ეჭვობს, შესაძლოა გასცეს ისეთი სენსიტიური ინფორმაცია, როგორიცაა საკრედიტო ბარათის მონაცემები. ვებსაიტის მონახულებამ შეიძლება გამოიწვიოს მომხმარებლის მიერ მავნე კოდის შემცველი კონტენტის ჩამოტვირთვა, რომელიც დააინფიცირებს მოწყობილობას.

Rogue წვდომის წერტილი არის უსადენო წვდომის წერტილი, კონფიგურირებული უსაფრთხო ქსელში აშკარა ავტორიზაციის გარეშე. Rogue წვდომის წერტილი შეიძლება შეიქმნას ორი გზით. პირველ შემთხვევაში კარგი განზრახვის მქონე თანამშრომელი ცდილობს სასარგებლო ქმედება ჩაიდინოს მობილური მოწყობილობების სათანადოდ დასაკავშირებლად. მეორე შემთხვევაში ბოროტგანმზრახველი თაღლითურად ფიზიკურად აღწევს ორგანიზაციაში და თვითონ ახდენს უსადენო წვდომის წერტილის კონფიგურირებას. გამომდინარე იქედან, რომ ორივე ქმედება არასანქცირებულია, ისინი საფრთხეს უქმნიან ორგანიზაციას.

Rogue წვდომის წერტილი ასევე ეხება კრიმინალის წვდომის წერტილს. ამ შემთხვევაში, კრიმინალი ქმნის წვდომის წერტილს, როგორც MitM მოწყობილობას, რათა მიიღოს მომხმარებლის სახელი და პაროლი.

Evil Twin შეტევა იყენებს ბოროტგანმზრახველის წვდომის წერტილის უფრო მძლავრ ანტენასა და სიმძლავრეებს, რათა მომხმარებელს თაღლითური მიზნით შეთავაზოს შედარებით უკეთესი დაკავშირების პირობები. მას შემდეგ, რაც კლიენტები უერთდებიან ბოროტგანმზრახველის წდომის წერტილს, მას საშუალება ეძლევა გამოიკვლიოს ტრაფიკი და განახორციელოს MitM შეტევა.

უსადენო ქსელის სიგნალები მგრძნობიარეა ელექტრომაგნიტური ინტერფერენციის (EMI), რადიოსიხშირული ჩარევის (RFI) მიმართ და ასევე შეიძლება იყოს მგრძნობიარე ელვის ან ფლუორესცენტური განათების მიმართაც. უსადენო სიგნალები ასევე მგრძნობიარეა წინასწარგანზრახული ჯემირების მიმართაც. რადიოსიხშირული (RF) ჯემირება აზიანებს რადიო ან სატელიტური სადგურის გადაცემას ისე, რომ სიგნალი ვერ აღწევს მიმღებ სადგურამდე.

RF ჯემერის სიხშირე, მოდულაცია და ძალა უნდა იყოს ერთნაირი იმ მოწყობილობებზე, რომელთა წვდომაც სურს კრიმინალს უსადენო სიგნალის წარმატებული ჯემირების მიზნით.

Bluetooth არის მოკლე სპექტრის, დაბალი სიმძლავრის პროტოკოლი. Bluetooth აგზავნის მონაცემებს პერსონალურ ქსელში ან PAN-ში, და შეიძლება მოიცავდეს მოწყობილობებს, როგორიცაა მობილური ტელეფონები, ლეპტოპები და პრინტერები. Bluetooth-მა გაიარა რელიზების რამდენიმე ვერსია. Bluetooth- ის ერთ-ერთი დამახასიათებელი მისი მარტივი კონფიგურირებაა, ამიტომ არაა საჭიროება ქსელის დამისამართებისა. Bluetooth იყენებს დაწყვილების პრინციპს, რათა დაამყაროს ურთიერთობა მოწყობილობებს შორის. დაწყვილების დამყარებისას ორივე მოწყობილობა იყენებს იგივე საპაროლე სიტყვას (passkey).

Bluetooth-ის მოწყვლადობა თვალნათელია, მაგრამ რადგანაც Bluetooth-ს გააჩნია მოქმედების შეზღუდული არეალი, მსხვერპლიც და თავდამსხმელიც საერთო გაზიარების ფარგლებში უნდა იყვნენ.

- Bluejacking არის ტერმინი, რომელიც გამოიყენება სხვა Bluetooth მოწყობილობისთვის არაავტორიზებული შეტყობინებების გაგზავნისთვის. ამის ვარიაციაა სხვა მოწყობილობისთვის შოკისმომგვრელი გამოსახულების გაგზავნა.
- Bluesnarfing ხდება მაშინ, როდესაც თავდამსხმელი ასრულებს დაზარალებულის ინფორმაციის კოპირებას მისი მოწყობილობიდან. ეს ინფორმაცია შეიძლება შეიცავდეს წერილებს და საკონტაქტო სიებს.

WEP და WPA თავდასხმები

სადენიანი ექვივალენტური კონფიდენციალურობა (WEP) არის უსაფრთხოების პროტოკოლი, რომელიც ცდილობს უსადენო ლოკალური ქსელის (WLAN) უზრუნველყოფას იმავე დონის უსაფრთხოებით, როგორც სადენიანი LAN-ისა. მაშინ, როდესაც ფიზიკური უსაფრთხოების ზომები უზრუნველყოფს სადენიანი LAN-ის დაცვას, WEP ცდილობს უზრუნველყოს WLAN- ზე გადაცემული მონაცემების მსგავსი დაცვა დაშიფვრის საშუალებით.

WEP იყენებს დაშიფვრის გასაღებს. WEP-თან საკვანძო მენეჯმენტის უზრუნველყოფა არ არსებობს, ამიტომ გასაღების გამზიარების ადამიანების რიცხვი მუდმივად იზრდება. მას შემდეგ, რაც ყველა იყენებს ერთსა და იმავე გასაღებს, კრიმინალს უჩნდება წვდომის

შესაძლებლობა დიდი მოცულობის ტრაფიკზე ანალიტიკური თავდასხმებისთვის.

WEP-ს ასევე აქვს რამდენიმე პრობლემა მისი ინიციალიზაციის ვექტორთან (IV), რომელიც კრიპტოგრაფიული სისტემის ერთ-ერთი კომპონენტია:

- ეს არის 24 ბიტიანი ველი, რაც ძალიან მცირეა;
- ის გადაიცემა ღია ტექსტით, რაც იმას ნიშნავს, რომ არის ადვილად წაკითხვადი;
- ის არის სტატიკური, შესაბამისად იდენტური გასაღების ნაკადები მეორდება ქსელში.

Wi-Fi დაცული წვდომა (WPA) და შემდეგ WPA2 შემუშავდა, როგორც გაუმჯობესებული ვერსიები, რომელთაც შეცვალეს WEP. WPA2- ს არ გააჩნია დაშიფვრის იგივე პრობლემები, რადგან თავდამსხმელს არ შეუძლია გასაღების აღდგენა ტრაფიკის გამოკვლევით. WPA2 სენსიტიურია თავდასხმთა მიმართ, რადგან კიბერდამნაშავეებს შეუძლიათ გაანალიზონ პაკეტები წვდომის წერტილსა და ლეგიტიმურ მომხმარებელს შორის. კიბერდამნაშავეები იყენებენ პაკეტების სნიფერს (sniffer) და შემდეგ ახორციელებენ offline თავდასხმებს ოფლაინ პაროლის გასაღებით.

უსადენო და მობილური მოწყობილობის თავდასხმებისგან დაცვა

არსებობს რამდენიმე ნაბიჯი იმისათვის, რომ დავიცვათ უსადენო და მობილური მოწყობილობები თავდასხმებისაგან. უმრავლესი WLAN პროდუქტები იყენებენ სტანდარტულ პარამეტრებს. ისარგებლეთ ძირითადი უსადენო უსაფრთხოების მახასიათებლებით, როგორიცაა ავტორიზაციის და დაშიფვრის ნაგულისხმევი კონფიგურაციის პარამეტრების შეცვლა.

შეზღუდეთ წვდომის წერტილის განთავსება ქსელური დაცვის ეკრანის ფარგლებს მიღმა ან დემილიტარიზებულ ზონაში (DMZ), რომელიც შეიცავს სხვა არასანდო მოწყობილობებს, როგორიცაა ელ-ფოსტისა და ვებსერვერები.

WLAN ინსტრუმენტებს, როგორიცაა NetStumbler, შეუძლიათ აღმოაჩინოთ rogue წვდომის წერტილები ან არაავტორიზებული სამუშაო სადგურები. შეიმუშავეთ სტუმრის პოლიტიკა იმ შემთხვევაში, როდესაც სტუმრები საჭიროებენ ინტერნეტთან

დაკავშირებას. ავტორიზებული თანამშრომლებისთვის WLAN-ის წვდომისთვის გამართეთ დისტანციური წვდომის ვირტუალური კერძო ქსელი (VPN).

Cross-site სკრიპტინგი

Cross-site Scripting (XSS) წარმოადგენს დაუცველობებს, ნაპოვნს ვებაპლიკაციებში. XSS საშუალებას აძლევს დამნაშავეებს, მოახდინონ სკრიპტების ინექცია მომხმარებლების მიერ ნანახ ვებ-გვერდებზე. ეს სკრიპტი შეიძლება შეიცავდეს ზიანის მომტან კოდს.

არსებობს Cross-site სკრიპტინგის სამი მონაწილე: კრიმინალი, მსხვერპლი და ვებსაიტი. კიბერკრიმინალი მსხვერპლს არ იღებს მიზანში უშუალოდ. ბოროტგანმზრახველი იყენებს მოწყვლადობას ვებსაიტზე ან ვებაპლიკაციაში. კიბერკრიმინალები ახდენენ კლიენტის-მხრის სკრიპტის ინექციას ვებსაიტზე, რომელსაც ეწვია კლიენტი. ზიანის შემცველი სკრიპტი მომხმარებლისაგან დამოუკიდებლად ებმება მის ბრაუზერს. ამ ტიპის მავნე სკრიპტს შეუძლია წვდომა ნებისმიერი cookie-ფაილებზე, სესიის სიმბოლოებზე ან სხვა სენსიტიურ ინფორმაციზე. თუ დამნაშავეები დაზარალებულის სესიის cookie-ფაილს მიიღებენ, მათ შეუძლიათ ამ მომხმარებლის სახელით მოქმედება.

ვებ-გვერდის მონაცემების შენახვის ერთ-ერთი გზაა მონაცემთა ბაზის გამოყენება. არსებობს რამდენიმე სხვადასხვა ტიპის მონაცემთა ბაზა, როგორიცაა სტრუქტურირებული მოთხოვნის ენა (SQL) მონაცემთა ბაზა ან გაფართოებული მარკირების ენის (XML) მონაცემთა ბაზა. როგორც XML, ასევე SQL საინექციო შეტევები იყენებენ სისუსტეებს პროგრამაში, როგორიცაა მონაცემთა ბაზის მოთხოვნათა არასწორი ვალიდაცია.

XML ინექცია - XML მონაცემთა ბაზის გამოყენებისას XML ინექცია წარმოადგენს თავდასხმას, რომელსაც შეუძლია მონაცემების დაზიანება. მას შემდეგ, რაც მომხმარებელი უზრუნველყოფს მონაცემთა შეტანას, სისტემა ახდენს წვდომას ბაზასთან შესაბამისი მოთხოვნის საფუძველზე. პრობლემა ჩნდება მაშინ, როდესაც სისტემა ვერ ახერხებს სათანადოდ დაამუშაოს მომხმარებლის მიერ მოწოდებული მოთხოვნა. კრიმინალებს შეუძლიათ მოთხოვნის მანიპულირება პროგრამირების გზით ისე, რომ მოარგონ ის თავის საჭიროებას და მოიპოვონ ინფორმაცია მონაცემთა ბაზიდან.

მონაცემთა ბაზაში შენახული მგრძნობიარე მონაცემები ხელმისაწვდომი ხდება დამნაშავეებისთვის და მათ შეუძლიათ ნებისმიერი რაოდენობის ცვლილებების შეტანა ვებგვერდზე. XML საინექციო თავდასხმა საფრთხეს უქმნის ვებ-გვერდის უსაფრთხოებას.

SQL ინექცია - კიბერკრიმინალი იყენებს მოწყვლადობას ზიანის მომტანი SQL განცხადის შეტანით ბაზის ველში. კიდევ ერთხელ, სისტემა არ ახდენს მომხმარებლის მიერ შეტანილი სიმბოლოების ფილტრაციას SQL განაცხადში. კიბერკრიმინალები იყენებენ SQL ინექციას ვებსაიტებზე ან SQL მონაცემთა ბაზაში.

დამნაშავეებმა შეიძლება მოახდინონ იდენტობის სპუფინგი (spoof), შეცვალონ ან გაანადგურონ არსებული მონაცემები, ან მოიპოვონ ადმინისტრატორის უფლებები მონაცემთა ბაზის სერვერზე.

ბუფერის გადავსება (Buffer Overflow) - ხდება, როდესაც მონაცემები სცილდება ბუფერის საზღვრებს..ბუფერები არიან მეხსიერების საზღვრები რომლებიც გამოყოფილია აპლიკაციებისათვის. ბუფერის საზღვრების მიღმა მონაცემების შეცვლით, აპლიკაცია მოითხოვს წვდომას სხვა პროცესებისთვის გამოყოფილ მეხსიერებაზე. ამ პროცესმა შეიძლება გამოიწვიოს სისტემის შეფერხება, მონაცემთა კომპრომიტირება, ან პრივილეგიების ესკალაცია.

კარნეგი მელონის უნივერსიტეტის CERT/CC აფასებს, რომ კომპიუტერული პროგრამების მოწყვლადობათა თითქმის ნახევარი ისტორიულად ბუფერული გადავსების ზოგიერთი ფორმითაა გამოწვეული. ზოგადი კლასიფიკაცია ბუფერული გადავსებისა მოიცავს მრავალ ვარიანტს, როგორიცაა სტატიკური ბუფერული გადავსება, ინდექსირების შეცდომები, ფორმატის სტრიქონთა შეცდომები, უნიკოდი და ANSI ბუფერული ზომის შეუსაბამობა, და სხვა მრავალი.

მოწყვლადობა საშუალებას აძლევს კიბერკრიმინალს შეასრულოს ზიანის მომტანი კოდი და გააკონტროლოს სისტემა მომხმარებლის პრივილეგიებით, რომლითაც ის უშვებს აპლიკაციას. დისტანციური კოდის აღსრულება საშუალებას აძლევს კრიმინალს შეასრულოს ნებისმიერი ბრძანება სამიზნე მანქანაზე.

მიიღეთ, მაგალითად, მეტასპლოიტი (Metasploit). Metasploit არის ინსტრუმენტი, რომელიც აღასრულებს კოდს დისტანციურ სამიზნეზე.

Meterpreter არის ექსპლოიტის მოდული Metasploit-ის ფარგლებში, რომელსაც გააჩნია გაფართოებული მახასიათებლები. კიბერკრიმინალები ატვირთავენ და ახდენენ ფაილის ინექციას გაშვებულ პროცესში სამიზნე ობიექტზე. Meterpreter იტვირთება და ახორციელებს თავის ქმედებებს ოპერატიულ მეხსიერებაში, ამიტომ ისინი არ მოითხოვენ კონტაქტს მყარ დისკზე. ეს ასევე ნიშნავს, რომ ეს ფაილები შეუმჩნეველი რჩება ანტივირუსული პროგრამებისათვის. Meterpreter-ს აქვს მოდული, რომელსაც შეუძლია დისტანციურად განახორციელოს ვებკამერის მართვა. მას შემდეგ, რაც კრიმინალი აყენებს მეტერპრეტერს პოტენციური მსხვერპლის სისტემაზე , მას შეუძლია ნახოს და გადაიღოს სურათები მისი ვებკამერიდან.

ზოგიერთი ვებსაიტი არ მუშაობს სათანადოდ, თუ სისტემაში არ არის ინსტალირებული ActiveX მართვა. ActiveX მართვა უზრუნველყოფს ინტერნეტ ექსპლორერის პლაგინების (plugin) შესაძლებლობებს. ActiveX მართვა წარმოადგენს მომხმარებლების მიერ რეალიზებული პროგრამული უზრუნველყოფას, რომელიც უზრუნველყოფს გაფართოებულ შესაძლებლობებს. ActiveX მართვა შესაძლოა დაწერილი იყოს მესამე მხრის მიერ და ის შესაძლოა შეიცავდეს ზიანის მომტან კოდს. მათ შეუძლიათ მოახდინონ ვებ საიტთა მონიტორინგი, დააინსტალირონ malware, ან შექმნან keystrokes ლოგები. ActiveX მართვა ასევე მუშაობს Microsoft-ის სხვა პროგრამებშიც.

Java ოპერირებს ინტერპრეტატორის მეშვეობით - Java-ს ვირტუალური მანქანა (JVM). JVM საშუალებას იძლევა Java პროგრამის ფუნქციონირებისა. JVM განთავსებულია სენდბოქსში ან ახდენს არასანდო კოდის იზოლაციას დანარჩენი ოპერაციული სისტემისგან. არსებობს მოწყვლადობა, რომელიც საშუალებას აძლევს არასანდო კოდს, შეაღწიოს სენდბოქსის მიერ დაწესებულ შეზღუდვებში. ასევე არსებობს ხარვეზები ჯავას კლასის ბიბლიოთეკაში, რომლის აპლიკაციაც გამოიყენება უსაფრთხოების უზრუნველსაყოფად. Java წარმოადგენს მეორე ყველაზე დიდ მოწყვლადობას Adobe Flash მოდულის შემდეგ.

აპლიკაციის თავდასხმებისგან დაცვა

აპლიკაციის თავდასხმებისგან დაცვის პირველი ნაბიჯია ძლიერი კოდის დაწერა. მიუხედავად გამოყენებული ენისა, ან გარე შეტანის წყაროსა, გონივრული პროგრამირების პრაქტიკაა ყოველი გარედან

შეტანილი მონაცემი განხილულ იქნას, როგორც მავნე. უნდა მოხდეს ყოველი შეტანილი მონაცემის ვალიდაცია, თითქოს ის იყოს მავნე.

განაახლეთ პროგრამული უზრუნველყოფა, მათ შორის ოპერაციული სისტემები და პროგრამები და არასდროს დააიგნოროთ განახლების მოთხოვნა. ყველა პროგრამა ავტომატურად არ განახლდება. სულ მცირე, აირჩიეთ გეგმური განახლების ვარიანტი. გეგმური განახლებები საშუალებას აძლევს მომხმარებლებს თვალი ადევნონ, ზუსტად რა განახლებები ხდება სისტემაში.

თავი 4. საიდუმლოების დაცვის ხელოვნება. ტექნოლოგიები, პროდუქტები და პროცედურები კონფიდენციალობის დასაცავად

4.1 კრიპტოგრაფია. კონფიდენციალურობის დაცვა შიფრაციის ტექნიკის გამოყენებით

კრიპტოლოგია არის მეცნიერება საიდუმლო კოდების შექმნისა და გატეხვის შესახებ, რომელიც გამოიყენება მონაცემების დასაცავად. კრიპტოგრაფიის მიზანია მონაცემთა კონფიდენციალურობის, მთლიანობისა და ავთენტურობის უზრუნველყოფა.

კრიპტოგრაფია მოიცავს სხვადასხვა ტექნიკას, მათ შორის დაშიფვრას, რომელიც გარდაქმნის უბრალო ტექსტს დაშიფრულ ტექსტად, რათა ის წაუკითხავი გახდეს შესაბამისი გაშიფვრის გასაღების გარეშე. ის ასევე მოიცავს ისეთ ტექნიკას, როგორიცაა ციფრული ხელმოწერა, ჰეშირება და ავთენტიფიკაციის პროტოკოლები, რათა უზრუნველყოს მონაცემთა მთლიანობა და გადაამოწმოს კომუნიკაციის მხარეთა ვინაობა.

კრიპტოგრაფია მნიშვნელოვან როლს ასრულებს მგრძნობიარე ინფორმაციის დაცვაში სხვადასხვა სფეროში, როგორიცაა საკომუნიკაციო სისტემები, ელექტრონული კომერცია, საბანკო და ციფრული კონფიდენციალურობა. ის ქმნის კიბერუსაფრთხოების საფუძველს და აუცილებელია ციფრული ურთიერთქმედების ნდობისა და უსაფრთხოების შესანარჩუნებლად.

ისტორიულად, მხარეები იყენებდნენ დაშიფვრის სხვადასხვა ალგორითმებს და მეთოდებს. ამბობენ, რომ იულიუს კეისარი იცავდა შეტყობინებებს ანბანის ორი ნაკრების გვერდიგვერდ დაყენებით და შემდეგ ერთი მათგანის გარკვეული რაოდენობის ადგილით გადაადგილებით. ანბანში გადანაცვლებული ადგილების რაოდენობა წარმოადგენს მთავარ ფაქტორს (ამ შემთხვევაში შიფრაციის/დეშიფრაციის გასაღებს). ამ გასაღებით იულიუს კეისარს ჩვეულებრივი ტექსტი გადაჰყავდა დაშიფრულ ტექსტად და მხოლოდ მისმა გენერლებმა, რომლებსაც ჰქონდათ გასაღები, იცოდნენ როგორ გაეშიფრათ შეტყობინებები. ამ მეთოდი ცნობილია როგორც “კეისრის შიფრი”.

საუკუნეების განმავლობაში ხდებოდა სხვადასხვა დაშიფვრის მეთოდების და ფიზიკური მოწყობილობების გამოყენება ინფორმაციის დასაშიფრად (მაგ. ვიჯინერის ცხრილი, ენიგმა მანქანა და სხვა).

დაშიფვრის თითოეული მეთოდი იყენებს სპეციფიკურ ალგორითმს, რომელსაც ეწოდება შიფრი, შეტყობინებების დაშიფვრისა და გაშიფვრის. შიფრი არის კარგად განსაზღვრული ნაბიჯების თანმიმდევრობა, რომელიც გამოიყენება შეტყობინებების დაშიფვრისა და დეშიფრაციისთვის.

დაშიფვრის ძველი ალგორითმები, როგორიცაა კეისრის შიფრი ან ენიგმა მანქანა, კონფიდენციალურობის მისაღწევად დამოკიდებული იყო ალგორითმის საიდუმლოებაზე. თანამედროვე ტექნოლოგიებში, მხარეები იყენებენ საჯარო დომენის ალგორითმებს. თანამედროვე ალგორითმებით, წარმატებული გაშიფვრა მოითხოვს შესაბამისი კრიპტოგრაფიული გასაღებების ცოდნას. ეს ნიშნავს, რომ დაშიფვრის უსაფრთხოება მდგომარეობს გასაღებების საიდუმლოებაში და არა ალგორითმში.

გასაღების მართვა კრიპტოსისტემის ყველაზე რთული ნაწილია. ყველა თანამედროვე კრიპტოგრაფიული ალგორითმი მოითხოვს გასაღების მართვის პროცედურებს. პრაქტიკაში, კრიპტოგრაფიულ სისტემებზე თავდასხმების უმეტესობა მოიცავს თავდასხმას გასაღების მართვის სისტემაზე და არა თავად კრიპტოგრაფიულ ალგორითმზე.

ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდები საინფორმაციო უსაფრთხოების საფუძველს წარმოადგენს. კრიპტოგრაფიული მეთოდები დაფუძნებულია ინფორმაციის კრიპტოგრაფიულ გარდაქმნებზე, რომლებიც ცვლიან საწყის ინფორმაციას ისე, რომ გამორიცხული იქნეს ამ ინფორმაციის არა სანქცირებული წაკითხვა და მოდიფიკაცია.

არსებობს ინფორნმაციის შემდეგი სახის კრიპტოგრაფიული გარდაქმნები:

- დაშიფრვა - ღია გზავნილების კრიპტოგრაფიული გარდაქმნა დახურულ გზავნილებად.
- გაშიფრვა - დახურული გზავნილების კრიპტოგრაფიული გარდაქმნა ღია გზავნილებად.

- კრიპტოანალიზი - დახურული გზავნილიდან ღია გზავნილის მიღება იმ დროს, როცა უცნობია კრიპტოგრაფიული გარდაქმნა.

ჩვეულებრივ დაშიფრვის და გაშიფრვის პროცესი წარმოებს სპეციალური გასაღებების და კრიპტოგრაფიული ალგორითმების გამოყენებით. დაშიფრვის ალგორითმები შემდეგნაირად კლასიფიცირდება:

- სიმეტრიული: ა. ბლოკური; ბ. ნაკადური
- ასიმეტრიული

სიმეტრიული ალგორითმები ხასიათდება დაშიფრვის და გაშიფრვის ერთი გასაღებით, რომელიც საიდუმლოდ ინახება და გადაიცემა ჩვეულებრივ უსაფრთხო კავშირის გამოყენებით.

ბლოკური შიფრვის ალგორითმები გარდაქმნებს გზავნილის თითოეულ ბლოკზე ცალცალკე ახდენენ. ეს ალგორითმები ძირითადად ცალკე აღებული მთლიანი გზავნილის, რომელიც წარმოდგენილია მაგალითად ფაილის სახით, დაშიფრვის დროს გამოიყენება. ნაკადური ალგორითმები გზავნილის თითოეულ სიმბოლოს ცალკე-ცალკე შიფრავენ. ასეთი ალგორითმები გამოიყენება მაგალითად გასაიდუმლოებული სატელეფონო კავშირის დროს.

ასიმეტრიული ალგორითმები ხასიათდება ორი, ღია და დახურული გასაღებით. პირველი მათგანი გამოიყენება დაშიფრვის, ხოლო მეორე გაშიფრვის დროს. ეს ალგორითმები იძლევა საშუალებას გადავცეთ ღია გასაღებები კავშირის ღია არხებით. შვეულებრივ გასაღებების გენერაციას ახდენს მიმღები მხარე და უგზავნის ღია გასაღებს გადამცემ მხარეს. ხოლო დახურულ გასაღებს ინახავს საიდუმლოდ.

სიმეტრიული დაშიფრვის ალგორითმები

არსებობს შემდეგი სახის სიმეტრიული შიფრვის ალგორითმები:

მარტივი ჩანაცვლების ანუ ელექტრონული კოდური წიგნის ალგორითმი - მარტივი ჩანაცვლების ანუ ელექტრონული კოდური წიგნის ალგორითმით დაშიფრვის დროს ხდება ღია გზავნილის თითო ბლოკის შეცვლა დახურული გზავნილის თითო ბლოკით. მთავარი იდეა არის ტექსტის დაყოფა N ბიტის ბლოკებად (დამოკიდებულია

შეყვანილი მონაცემების ბლოკის ზომაზე, დაშიფვრის ალგორითმზე) და შემდეგ ტექსტის თითოეული ბლოკის დაშიფვრა (გაშიფვრა) ერთადერთი გასაღების გამოყენებით. დაშიფრვა შეიძლება აღვწეროთ ფორმულით:

Ci=F(Pi), i=1÷N

სადაც Ci და Pi შესაბამისად დაშიფრული და გაშიფრული ტექსტის ბლოკებია, ხოლო F კრიპტოგრაფიული გარდაქმნა. ეს მეთოდი ყველაზე ნაკლებად საიმედოა შიფრაციის სხვა მეთოდებს შორის.

შიფრაცია შეცვლით - ყველაზე მარტივი შიფრაციის მეთოდი. დასაშიფრი ტექსტის სიმბოლოები იცვლებიან სხვა ერთი ანბანიდან აღებული სიმბოლოებით (ერთანბანიანი შეცვლა) ან რამოდენიმე ანბანიდან (მრავალანბანიანი შეცვლა).

ერთანბანიანი შეცვლის მეთოდი - დასაშიფრი ტექსტის სიმბოლოების შეცვლა ამავე, ან სხვა ანბანის სიმბოლოებით. მაგალითი:

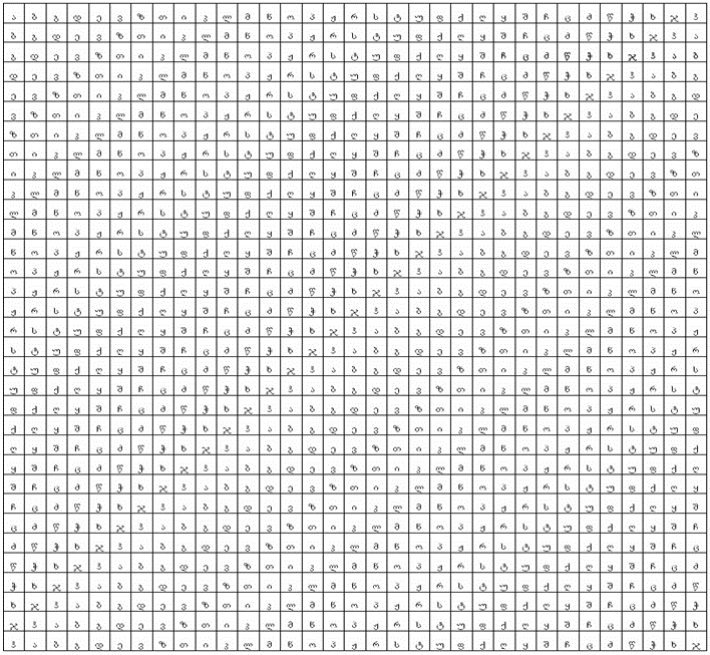
ა ბ გ დ ე ვ ზ თ ი კ ლ მ ნ ო პ ჟ რ . .

ჰ მ ნ წ ჯ კ ლ ო ქ დ ა ბ ც ყ უ შ თ . .

ერთანბანიანი მარტივი შეცვლის მეთოდის მდგრადობა ძალიან დაბალია, დაშიფრული ტექსტის სიმბოლოებს გააჩნია იგივე სტატისტიკური მახასიათებლები როგორც საწყის ტექსტს, სიმბოლოების სტანდარტული შეხვედრის სიხშირის ცოდნით იმ ენაში, რომელზეც დაწერილია შეტყობინება და სიმბოლოების სტატისტიკური შეხვედრის სიხშირესთან შედარებით დაშიფრულ ტექსტში, შეიძლება აღდგენილი იყოს შიფრაციის ცხრილი. ამისათვის საკმარისია დაშიფრული ტექსტის საკმარისი მოცულობა, იმისათვის რომ მივიღოთ სიმბოლოების სიხშირის შეფასება. ამიტომ ერთანბანიანი მარტივი შეცვლის მეთოდს გამოიყენებენ იმ შემთხვევაში, როცა დასაშიფრი ტექსტი პატარაა. მეთოდის მდგრადობა დაბალია, სირთულე განისაზღვრება სიმბოლოს მოძებნით შეცვლის ცხრილში.

მრავალანბანიანი შეცვლის მეთოდი - სიმბოლოების შესაცვლელად გამოიყენება რამოდენიმე ანბანი. ანბანი ამოირჩევა გასაღები სიტყვის ასოების შესაბამისად ისე, რომ სიტყვის ყოველი ასო შეესაბამებოდეს ანბანის პირველ ასოს. ანბანის შეცვლა ხორციელდება თანმიმდევრობით და ციკლურად: პირველი სიმბოლო იცვლება

შესაბამისი სიმბოლოთი პირველი ანბანიდან, მეორე სიმბოლო - შესაბამისი სიმბოლოთი მეორე ანბანიდან და ასე შემდეგ, სანამ არ გამოილევა ყველა ანბანი. განვიხილოთ შიფრაცია ვიჯინერის ცხრილის მიხედვით - კვადრატული მატრიცის n*2 ელემენტით, სადაც n, გამოყენებული ანბანის სიმბოლოების რაოდენობა. პირველ სტრიქონში არის საწყისი ანბანი, ყოველი შემდეგი მიიღება საწყისი ანბანის ერთი სიმბოლოების წანაცვლებით მარცხნივ ერთი სიმბოლოთი.



სურ. 4.1. ვიჯინერის ცხრილი

შიფრაციისთვის აუცილებელია გასაღები სიტყვის განსაზღვრა – სიტყვა, რომელშიც ასოები არ მეორდება. შეცვლის ცხრილი მიიღება შემდეგნაირად: დასაშიფრი ტექსტის სიმბოლოებს იღებენ პორველი სტრიქონიდან, ხოლო შეცვლის სტრიქონებს ადგენენ იმ სტრიქონებისგან, რომლის პირველი ასოები ემთხვევა გასაღები სიტყვის შესაბამის ასოს. შიფრაციის და დეშიფრაციის დროს არ არის აუცილებელი წინასწარ შევინახოთ მეხსიერებაში მთელი ვიჯინერის ცხრილი, რადგან ციკლური ჩანაცვლებით შეგვიძლია მივიღოთ ნებისმიერი სტრიქონი მისი ნომრის მიხედვით. მეთოდის მდგრადობა

უდრის მარტივი შეცვლის მეთოდის მდგრადობას გამრავლებულს L-ზე , სადაც L არის გასაღები სიტყვის სიგრძე. ალგებრულად ვიჯინერის ცხრილი შემდეგნაირად ჩაიწერება:

დაშიფვრა: Ei = (Pi + Ki) mod 26; გაშიფვრა: Di = (Ei - Ki) mod 26

სადაც, E არის დაშიფრული ტექსტი, P არის დასაშიფრი ტექსტი, K - გასაღები.

შიფრაცია გადაადგილებით - გადაადგილების მეთოდით შიფრაციის დროს დასაშიფრი ტექსტის სიმბოლოები გადადგილდებიან გარკვეული წესების მიხედვით. მარტივი გადაადგილების მეთოდი - ირჩევა შიფრაციის ბლოკი, რომელიც შედგება n სვეტებისგან და m სტრიქონებისგან და გასაღები რიცხვების თანმიმდევრობა, რომელიც ამოირჩევა ნატურალური რიცხვებიდან შემთხვევითი გადაადგილებით. შიფრაცია ხდება შემდეგი თანმიმდევრობით:

1. დასაშიფრი ტექსტი იწერება სტრიქონებად გასაღები რიცხვების თანმიმდევრობის ქვეშ და წარმოქმნიან დასაშიფრ ბლოკს n*m-ზე
2. დასაშიფრი ტექსტი ამოიწერება სვეტებად, სვეტების მიხედვით, მზარდი გასაღები რიცხვების თანმიმდევრობის მიხედვით.

დეშიფრაცია ხდება შემდეგნაირად:

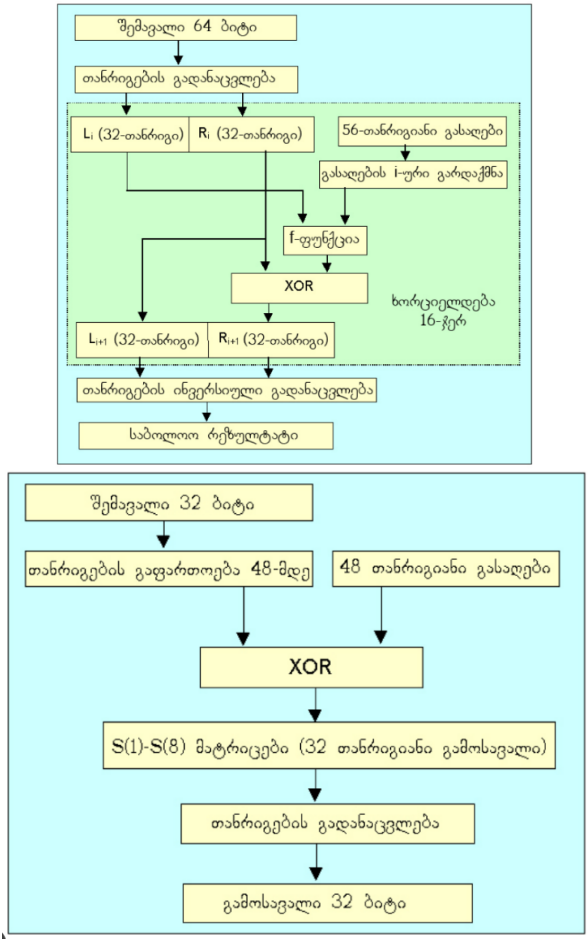
1. დაშიფრილი ტექსტიდან გამოიყოფა ბლოკი n*m-ზე;
2. ბლოკი იყობა n ჯგუფებზე, რომლებშიც არის m სიმბოლო;
3. სტრიქონები ჩაიწერება შეცვლის ცხრილის შესაბამის სვეტებში;
4. გაშიფრული ტექსტი იკითხება სტრიქონების მიხედვით.

ალგორითმი DES - რომელიც შეიქმნა აშშ-ს სტანდარტების ეროვნული ბიუროს მიერ 1977 წელს, როგორც სახელმწიფო სტრუქტურებში ასევე კომერციულ ორგანიზაციებში რეკომენდირებული დაშიფრვის ალგორითმი Data Encryprion Standard (DES). მისი მოდიფიკაცია გრძელდება და იქმნება მის საფუძველზე უფრო რთული და საიმედო ალგორითმები. DES ბლოკური დაშიფვრის ალგორითმია, რომელიც შემდეგნაირად აღიწერება:

დაშიფვრის შემთხვევაში: $C = E(K_i, P)$

გაშიფვრის შემთხვევაში: $P = D(Ki, P)$

მასში გამოყენებულია როგორც შეცვლის, ასევე გადასმის მეთოდები. ბლოკის სიგრძე 64 ბიტია, ხოლო გასაღების 56 ბიტი. ალგორითმი შემდეგნაირად სრულდება:



სურ.4.2. DES სიმერტიული ალგორითმის და f ფუნქციის სქემა

1. თავდაპირველად ხდება ბლოკის ბიტების არევა. ბიტები ლაგდება გარკვეული თანმიმდევრობით

2. შემდეგ 16-ჯერ მეორდება: გასაღების გარდაქმნა; ითვლება ბლოკის მარჯვენა ნახევარი Ri+1= Ri⊕f(Li,Ki); ბლოკის მარცხენა ნახევარში იწერება მარჯვენა ნახევარი Li+1=Ri; ბოლოს ხდება თანრიგების ინვერსული გადანაცვლება გარკვეული თანმიმდევრობით:

f ფუნქციას ვითვლით შემდეგნაირად: ფუნქციის პირველი არგუმენტი ფართოვდება 32 თანრიგიდან 48 თანრიგამდე ზოგიერთი თანრიგის გამეორებით; შემდეგ ის იკრიბება მოდულით 2 (mod2) 48 თანრიგიან გასაღებთან და გარდაიქმნება სპეციალური S მატრიცების გამოყენებით 32 თანრიგიან ბლოკად, რომლის თანრიგები კიდევ გადანაცვლდება. მიღებული 32 თანრიგიანი ბლოკი წარმოადგენს f ფუნქციის მნიშვნელობას.

S მატრიცები წარმოადგენენ ცხრილებს 4 სტრიქონით და 16 სვეტით. S მატრიცების შემავალი 48 თანრიგი იყოფა რვა 6 თანრიგიან მონაცემად. პირველი 2 თანრიგი განსაზღვრავს სტრიქონის ნომერს, ხოლო დანარჩენი 4 თანრიგი მატრიცის სვეტის ნომერს. მატრიცის საშუალებით გარდაქმნის რეზულტატი სწორედ ამ უჯრედის მნიშვნელობაა.

გასაღების გარდაქმნა, რომელიც f ფუნქციის შემავალ 48 თანრიგიან გასაღებს იძლევა შემდეგი სქემით ხორციელდება: 56 თანრიგიანი გასაღები საწყისი გადანაცვლების შემდეგ იყოფა ორ 28 თანრიგიან სიტყვად. თითოეულ რაუნდში (სულ 16 რაუნდი) ორივე რეგისტრი ციკლურად იძვრის მარცხნივ შემდეგი პრინციპით:

- I, II, IX და XVI რაუნდებში ერთი თანრიგით;

- დანარჩენ ღაუნდებში ორი თანრიგით.

ყოველ რაუნდში ორი 28 თანრიგიანი სიტყვის გაერთიანებით მიღებული 56 თანრიგიან გასაღებს ემატება თითო თანრიგი ყოველი 7 თანრიგის საკონტროლო ჯამის (ჯამი მოდულით 2) სახით. მიღებული 64 თანრიგიდან ხდება 48 თანრიგის ამორჩევა მოცემული ცხრილის მიხედვით.

DES ალგორითმის გაშიფრვა ანალოგიურად ხდება. განსხვავება მხოლოდ გასაღებების ამორჩევის თანმიმდევრობაა რაუნდებში.

3DES (Triple DES): ციფრული დაშიფვრის სტანდარტი (DES) არის სიმეტრიული ბლოკის შიფრი 64-ბიტიანი ბლოკის ზომით, რომელიც იყენებს 56-ბიტიან გასაღებს. ის ყოველთვის მუშაობს თანაბარი ზომის ბლოკებზე და იყენებს როგორც გადანაცვლებას, ასევე ჩანაცვლებებს ალგორითმში.

Triple DES დაშიფვრავს მონაცემებს სამჯერ და იყენებს განსხვავებულ გასაღებს სამივე გადასასვლელიდან მინიმუმ ერთისთვის, რაც აძლევს მას 112-168 ბიტის კუმულაციური გასაღების ზომას. 3DES მდგრადია შეტევის მიმართ, მაგრამ ის გაცილებით ნელია ვიდრე DES. 3DES დაშიფვრის ციკლი შემდეგია:

1. მონაცემები დაშიფრულია პირველი DES-ით

2. მონაცემები გაშიფრულია მეორე DES-ით

3. მონაცემები ხელახლა დაშიფრულია მესამე DES-ის მიერ

საპირისპირო პროცესი გაშიფრავს დაშიფრულ ტექსტს. მისი ალგებრული აღწერა შემდეგნაირად ჩაიწერება:

$$\textit{დაშიფვრის შემთხვევაში: } C = E\left(K_3, D\left(K_2, E(K_1, P)\right)\right)$$
$$\textit{გაშიფვრის შემთხვევაში: } P = D\left(K_1, E\left(K_2, D(K_3, C)\right)\right)$$

სადაც, K არის გასაღები, D - დეშიფრაციის ალგორითმი, E - შიფრაციის ალგორითმი, P – დასაშიფრი ტექსტი.

IDEA(International Data Encryption Algorithm): მონაცემთა დაშიფვრის საერთაშორისო ალგორითმი (IDEA) იყენებს 64-ბიტიან ბლოკებს და 128-ბიტიან გასაღებებს. IDEA ახორციელებს ტრანსფორმაციის რვა რაუნდს 16 ბლოკიდან თითოეულზე, რაც ხდება თითოეული 64-ბიტიანი ბლოკის გაყოფის შედეგად. IDEA იყო DES-ის ჩანაცვლება და ახლა მას იყენებს PGP (Pretty Good Privacy - პროგრამა, რომელიც უზრუნველყოფს კონფიდენციალურობას და ავთენტიფიკაციას მონაცემთა კომუნიკაციისთვის).

AES (Advanced Encryption Standard): დაშიფვრის გაფართოებული სტანდარტი (AES), რომელიც შეიქმნა აშშ-ს სტანდარტებისა და ტექნოლოგიების ეროვნული ინსტიტუტის (NIST) მიერ 2001 წელს. AES ფართოდ გამოიყენება დღეს, რადგან ის ბევრად უფრო ძლიერია ვიდრე DES და 3DES, მიუხედავად იმისა, რომ უფრო რთულია.

AES არის ბლოკის შიფრი. მისი გასაღების ზომა შეიძლება იყოს 128/192/256 ბიტი. შიფრავს მონაცემებს თითოეული 128 ბიტიანი ბლოკებით. ეს ნიშნავს, რომ მას იღებს 128 ბიტი, როგორც შეყვანა და გამოაქვს 128 ბიტიანი დაშიფრული ტექსტი. AES ეყრდნობა ჩანაცვლება-პერმუტაციის (გადანაცვლების) პრინციპს. AES ფართოდ გამოიყენება მრავალ აპლიკაციაში, რომლებიც საჭიროებენ მონაცემთა უსაფრთხო შენახვას და გადაცემას:

- უსადენო უსაფრთხოება: AES გამოიყენება უკაბელო ქსელების დასაცავად, როგორიცაა Wi-Fi ქსელები, მონაცემთა კონფიდენციალურობის უზრუნველსაყოფად და არაავტორიზებული წვდომის თავიდან ასაცილებლად.
- მონაცემთა ბაზის დაშიფვრა: AES შეიძლება გამოყენებულ იქნას მონაცემთა ბაზებში შენახული მგრძნობიარე მონაცემების დასაშიფრად. ეს ხელს უწყობს პირადი ინფორმაციის, ფინანსური ჩანაწერების და სხვა კონფიდენციალური მონაცემების დაცვას არაავტორიზებული წვდომისგან მონაცემთა დარღვევის შემთხვევაში.
- უსაფრთხო კომუნიკაციები: AES ფართოდ გამოიყენება პროტოკოლებში, როგორიცაა ინტერნეტ კომუნიკაციები, ელფოსტა, მყისიერი შეტყობინებები და ხმოვანი/ვიდეო ზარები. ეს უზრუნველყოფს მონაცემების კონფიდენციალურობას.
- მონაცემთა შენახვა: AES გამოიყენება მყარ დისკებზე, USB დისკებზე და სხვა საცავის მედიაზე შენახული მგრძნობიარე მონაცემების დასაშიფრად, დაკარგვის ან ქურდობის შემთხვევაში არაავტორიზებული წვდომისგან დასაცავად.
- ვირტუალური პირადი ქსელები (VPN): AES ჩვეულებრივ გამოიყენება VPN პროტოკოლებში მომხმარებლის მოწყობილობასა და დისტანციურ სერვერს შორის კომუნიკაციის უზრუნველსაყოფად. ის უზრუნველყოფს, რომ VPN-ით გაგზავნილი და მიღებული მონაცემები დარჩეს კონფიდენციალური და არ შეიძლება მისი გაშიფვრა მომსმენების მიერ.
- პაროლების უსაფრთხო შენახვა: AES დაშიფვრა ჩვეულებრივ გამოიყენება პაროლების უსაფრთხოდ შესანახად. ჩვეულებრივი ტექსტის პაროლების შენახვის ნაცვლად, დაშიფრული ვერსია ინახება. ეს ამატებს უსაფრთხოების

დამატებით ფენას და იცავს მომხმარებლის სერთიფიკატებს საცავში არაავტორიზებული წვდომის შემთხვევაში.

- ფაილების და დისკის დაშიფვრა: AES გამოიყენება კომპიუტერებზე, გარე შენახვის მოწყობილობებზე და ღრუბლოვან საცავებზე ფაილების და საქაღალდეების დასაშიფრად. ის იცავს მოწყობილობებზე შენახულ მგრძნობიარე მონაცემებს ან მონაცემთა გადაცემის დროს, რათა თავიდან აიცილოს არაავტორიზებული წვდომა.

დაშიფრვის ასიმეტრიული ალგორითმები

ასიმეტრიული ალგორითმების გავრცელება გამოიწვია ორი გასაღების: ღია - დაშიფრვისთვის, და დახურული - გაშიფრვისთვის ქონის აუცილებლობამ. ღია, ანუ ისეთი გასაღების შემოტანა, რომელიც პოტენციურად ყველასათვის ცნობილია, საშუალებას გვაძლევს თავი ავარიდოთ საიდუმლო გასაღებების გაცვლის რთულ ამოცანას.

ასიმეტრიული ალგორითმები იყენებენ ფორმულებს, რომლებთა მოძიებაც ყველას შეუძლია. ამ ალგორითმების უსაფრთხოებას ქმნის ორი, ერთმანეთისაგან დამოუკიდებლად შექმნილი გასაღები.

RSA (Rivest-Shamir-Adleman) - იყენებს ორ, ერთი სიგრძის მქონე ძალიან დიდი მნიშვნელობის მარტივ რიცხვს p-ს და q-ს. თავდაპირველად ვიგებთ:

$n=p*q;$ n გამოიყენება როგორც ღია, ისე დახურული გასაღებების მოდული.

$\varphi(n) = (p-1) * (q-1)$; ვირჩევთ დიდ შემთხვევით რიცხვს d-ს ისეთს, რომ ის იყოს ურთიერთ მარტივი $\varphi(n)$-თან (ანუ არ ჰქონდეს არცერთი მთელი საერთო გამყოფი გარდა 1-ისა).

ვსაზღვრავთ ისეთ მთელ რიცხვს e-ს, რომლისთვისაც ჭეშმარიტია შემდეგი ტოლობა: $(e*d) \bmod \varphi(n)=1$. ღია გასაღებია (e,n), ხოლო დახურული (d,n).

საკუთრივ დაშიფრვა. დასაშიფრი გზავნილი იყოფა ბლოკებად Mi ისე, რომ მისი ზომა k აკმაყოფილებდეს შემდეგ პირობას $10k-1<n<10k$; დაშიფრული გზავნილის შესაბამისი ბლოკის მნიშვნელობაა: $Ci=M_i^e \bmod (n)$.

გზავნილის გაშიფრვისათვის ვიყენებთ დახურულ გასაღებს *(d,n)* და ვითვლით გაშიფრული გზავნილის ბლოკის მნიშვნელობას შემდეგი ფორმულით: $Mi=C_i^d mod(n)$.

Diffie-Hellman - უზრუნველყოფს ელექტრონული გაცვლის მეთოდს საიდუმლო გასაღების გასაზიარებლად. უსაფრთხო პროტოკოლები, როგორიცაა უსაფრთხო სოკეტების ფენა (SSL), სატრანსპორტო შრის უსაფრთხოება (TLS), უსაფრთხო გარსი (SSH) და ინტერნეტ პროტოკოლის უსაფრთხოება (IPSec), გამოიყენებენ დიფი-ჰელმანის პროტოკოლს.

ვაიტფილდ დიფფიმ (Whitfield Diffie) და მარტინ ჰელმანმა (Martin Hellman) 1976 წელს გამოიგონა Diffie-Hellman (DH) ალგორითმი. DH ალგორითმი წარმოადგენს უმრავლესობა თანამედროვე, გასაღებების ავტომატური გაცვლის მეთოდების საფუძველს და ის ასევე არის დღეს ქსელში გამოყენებული პროტოკოლებიდან ერთ-ერთ ყველაზე გავრცელებული პროტოკოლი. Diffie-Hellman არ არის შიფრაციის მექანიზმი და ის როგორც წესი არ გამოიყენება მონაცემთა დასაშიფრად. ის არის მეთოდი, რომელიც გამოიყენება მონაცემთა დაშიფვრისთვის საჭირო გასაღებების უსაფრთხოდ გასაცვლელად.

DH-ის უსაფრთხოება დაფუძნებულია იმ ფაქტზე, რომ ის თავის გამოთვლებში იყენებს წარმოუდგენლად დიდ რიცხვებს. მაგალითად, DH-ის 1024-ბიტიანი რიცხვი, უხეშად რომ ვთქვათ, უდრის 309 ციფრიან ათობით რიცხვს. იმის გათვალისწინებით, რომ მილიარდი წარმოადგენს 10 ათობით ციფრს (1,000,000,000), ადვილად შეგვიძლია წარმოვიდგინოთ მუშაობის სირთულე არა ერთ, არამედ 309 ციფრიან ათობით რიცხვებთან.

სამწუხაროდ, ასიმეტრიული გასაღების სისტემები მეტისმეტად ნელია ნებისმიერი სახის მოცულობის შიფრაციისთვის. ამიტომაცაა, რომ ტრაფიკის მოცულობას უფრო ხშირად შიფრავენ სიმეტრიული ალგორითმებით, როგორიცაა 3DES ან AES და DH ალგორითმს იყენებენ გასაღებების შესაქმნელად, რომელიც იქნება გამოყენებული შიფრაციის ალგორითმის მიერ.

Elgamal - იყენებს ამერიკის მთავრობის სტანდარტს ციფრული ხელმოწერებისთვის. ეს ალგორითმი უფასოა, რადგან არავის გააჩნია პატენტი.

ელიფსური მრუდის კრიპტოგრაფია (ECC) - ალგორითმის ნაწილად იყენებს ელიფსურ მრუდებს. აშშ-ში ეროვნული უსაფრთხოების სააგენტო იყენებს ECC-ს ციფრული ხელმოწერის გენერაციისა და გასაღებთა გაცვლისთვის.

გასაღების მართვა. გასაღების მართვა მოიცავს შიფრაციის ალგორითმში გამოყენებული გასაღების გენერირებას, გაცვლას, შენახვას, გამოყენებას და ჩანაცვლებას. იგი კრიპტოსისტემის დაპროექტების ყველაზე რთული ნაწილია. მრავალი კრიპტოსისტემის განვითარება ვერ მოხერხდა მათი გასაღების მართვის პროცედურების შეცდომების გამო. პრაქტიკაში კრიპტოგრაფიულ სისტემებზე თავდასხმების უმრავლესობა მიზნად ისახავს შეტევას გასაღების მართვის დონეზე, და არა თავად კრიპტოგრაფიულ ალგორითმზე. გასაღების აღსაწერად გამოყენებული ორი ტერმინია:

გასაღების სიგრძე - ასევე უწოდებენ გასაღების ზომას, იზომება ბიტების რაოდენობით.

Keyspace - ეს არის რიგი შესაძლებლობები, რომლებიც გამოიყენება კონკრეტული გასაღების სიგრძის გენერირებისათვის.

გასაღების სიგრძის ზრდასთან ერთად გასაღების სივრცეც (Keyspace) ექსპონენციალურად იზრდება. ალგორითმის გასაღების სივრცე არის ყველა შესაძლო გასაღების მნიშვნელობის კრებული. გრძელი გასაღებები უფრო უსაფრთხოა; თუმცა, ისინი მოითხოვენ უფრო მეტ გამოთვლით რესურსს. თითქმის ყველა ალგორითმს გააჩნია გარკვეული სუსტი გასაღებები თავის საკვანძო სივრცეში, რომელიც საშუალებას აძლევს კრიმინალს დაარღვიოს დაშიფვრა.

4.2. წვდომის მართვა. მონაცემთა კონფიდენციალურობის დაცვა წვდომის მართვის მეთოდების გამოყენებით. იდენტიფიკაცია/ავთენტიფიკაცია/ავტორიზაცია

მონაცემებზე არავტორიზებული წვდომისაგან დაცვა პირველი ნიშნავს, ფიზიკური წვდომის შეუძლებლობას კომპიუტერულ ქსელში, სერვერებთან, ვებ სცენარებთან, ქსელურ კაბელებთან/მოწყობილობებთან და სხვა რესურსებთან.

როგორ ბრიყვულადაც არ უნდა ჟღერდეს, ხშირად არასნქცირებული წვდომისგან გვიცავს უბრალო კარის საკეტი. სერვერები რომლებზეც ინახება მნიშვნელოვანი ინფორმაცია არ უნდა იდგნენ ღიად მაგიდაზე ან დაუკეტავ ოთახში, სადაც ნებისმიერს შეუძლია შევიდეს. ანალოგიური გზით უნდა იყოს დაცული სხვა მოწყობილობებიც. თუ რომელიმე თანამშრომელი მუშაობს მთელი დღე და ღამე მაშინ ამ ოთახის დაკეტვა არ არის აუცილებელი- მხოლოდ იმ შემთხვევაში თუ პერსონალი არ მორიგეობს მარტო. იდელურ შემთხვევაში ასეთ ოთახში შესვლა უნდა კონტროლირდებოდეს.

როდესაც ქსელური კავშირები გადის თქვენი დაქვემდებარების ზონიდან, მაშინ რა თქმა უნდა იკარგება ქსელის ფიზიკური კონტროლის ასპექტები და საჭიროა დავეყრდნოთ სხვა დაცვით მექნიზმებს.

ფიზიკური წვდომის მართვა წარმოადგენს ფაქტობრივ ბარიერს, რომელიც განთავსებულია სისტემებთან უშუალო კონტაქტის თავიდან ასაცილებლად. მოცემული მართვის მიზანია, თავიდან იქნას აცილებული არასანქცირებული მომხმარებლების ფიზიკური წვდომა ობიექტებზე, აპარატურასა და სხვა ორგანიზაციულ აქტივებზე. ფიზიკური წვდომის მართვა განსაზღვრავს ვინ, სად და როდის შეიძლება შევიდეს (ან გავიდეს) დაცულ ობიექტზე.

ლოგიკური წვდომის მართვა არის აპარატურისა და პროგრამული უზრუნველყოფის გადაწყვეტილებები, რომლებიც გამოიყენება რესურსებსა და სისტემებზე ხელმისაწვდომობის განსაზღვრისათვის. ამ ტექნოლოგიებზე დაფუძნებული გადაწყვეტილებები მოიცავს ინსტრუმენტებსა და ოქმებს, რომლებიც კომპიუტერულ სისტემებს იყენებენ იდენტიფიკაციის, ავთენტიფიკაციის, ავტორიზაციისა და სააღრიცხვო ანგარიშვალდებულების მიზნით.

ადმინისტრაციული დაშვების მართვა წარმოადგენს ორგანიზაციების მიერ განსაზღვრულ პოლიტიკასა და პროცედურებს, რომლებიც განახორციელებენ და აღასრულებენ არასანქცირებული წვდომის მართვის ყველა ასპექტს. ადმინისტრაციული მართვა ფოკუსირებულია პერსონალსა და ბიზნეს პრაქტიკაზე.

სავალდებულო წვდომის მართვა (MAC) ზღუდავს იმ ქმედებებს, რომლებიც სუბიექტს შეუძლია განახორციელოს ობიექტზე. სუბიექტს შეიძლება წარმოადგენდეს მომხმარებელი ან პროცესი. ობიექტი

შეიძლება იყოს ფაილი, პორტი, ან შეტანის/გამოტანის მოწყობილობა. ავტორიზაციის წესი განსაზღვრავს, აქვს თუ არა სუბიექტს ობიექტზე წვდომის უფლება. ორგანიზაციები იყენებენ MAC-ს, სადაც არსებობს უსაფრთხოების კლასიფიკაციის განსხვავებული დონე. ყველა ობიექტს გააჩნია თავისი ეტიკეტი და ყველა სუბიექტს აქვს თავისი ნებართვა. MAC სისტემა ზღუდავს სუბიექტს ობიექტის უსაფრთხოების კლასიფიკაციისა და მომხმარებლისთვის თანდართული ეტიკეტის საფუძველზე.

მაგალითად, სამხედრო უსაფრთხოების კლასიფიკაციით განისაზღვრება საიდუმლო და მკაცრად საიდუმლო ობიექტები. თუ ფაილი (ობიექტი) ითვლება საიდუმლოდ, იგი კლასიფიცირდება (ფასდება) მკაცრად საიდუმლოდ. ერთადერთი პერსონა (სუბიექტი), რომელსაც შეუძლია იხილოს ფაილი (ობიექტი) არის ის, ვისაც ყველაზე მაღალი დონის ნებართვა გააჩნია. ეს არის წვდომის მართვის მექანიზმი, რომელიც უზრუნველყოფს პროცესს ისე, რომ ინდივიდი (სუბიექტი), რომელსაც გააჩნია მხოლოდ უბრალო ნებართვა, ვერასოდეს მოიპოვებს ფაილს, რომელიც შეფასებულია, როგორც მკაცრად საიდუმლო. ანალოგიურად, მკაცრად საიდუმლო წვდომის მქონე მომხმარებელი (სუბიექტი) ვერ შეცვლის ფაილის (ობიექტის) კლასიფიკაციას, რომელიც განისაზღვრება, როგორც ორმაგად მკაცრად საიდუმლო. გარდა ამისა, მკაცრად გასაიდუმლოებული მომხმარებელი ვერ შეძლებს გაგზავნოს მკაცრად საიდუმლო ფაილი მომხმარებლისთვის, რომელსაც აქვს მხოლოდ საიდუმლო ინფორმაციის მიღების ნებართვა.

ობიექტის მფლობელი განსაზღვრავს ობიექტის ხელმისაწვდომობის *დისკრეციული დაშვების მართვის* (DAC) დონეს. DAC-ის მეშვეობით ობიექტის მფლობელი განსაზღვრავს ობიექტის ხელმისაწვდომობას სხვა სუბიექტთათვის. მართვა დისკრეციულია, რადგან ობიექტის მფლობელს გარკვეული დაშვების ნებართვებით შეუძლია ამ ნებართვების სხვა სუბიექტზე გავრცელება.

სისტემებში, რომლებიც იყენებენ დისკრეციულ წვდომის მართვას, ობიექტის მფლობელს შეუძლია გადაწყვიტოს, რომელ სუბიექტებს შეუძლიათ მიიღონ ეს ობიექტი და რა კონკრეტული წვდომის უფლებით. ერთი საერთო მეთოდი ამ მიზნის მისაღწევად არის სპეციფიური ნებართვების გაცემა. დოკუმენტის მფლობელს შეუძლია

განსაზღვროს, თუ რა ნებართვები (წაკითხვის/ჩაწერა/შესრულება) შეუძლიათ მიიღონ სხვა მომხმარებლებმა.

როლზე დაფუძნებული დაშვების მართვა (RBAC) დამოკიდებულია სუბიექტის როლზე. როლები წარმოადგენენ ორგანიზაციის ფარგლებში სამუშაო ფუნქციებს. სპეციფიური როლები მოითხოვენ გარკვეული ოპერაციების განხორციელებას.. მომხმარებელი იღებს ნებართვას მისი როლის გათვალისწინებით. RBAC-ს შეუძლია ფუნქციონირება DAC ან MAC-თან ერთად კომბინაციაში მათ მიერ დაწესებული ნებართვების გამკაცრებით. RBAC აუმჯობესებს უსაფრთხოების ადმინისტრირების რეალიზებას მსხვილ ორგანიზაციებში, სადაც დასაქმებულია ასობით მომხმარებელი და გაცემულია ათასობით შესაძლო ნებართვა. ორგანიზაციები ფართოდ იყენებენ RBAC-ს სისტემებში/აპლიკაციებში კომპიუტერული ნებართვების მართვის მიზნით.

წესებზე დაფუძნებული წვდომის მართვა იყენებს წვდომის მართვის სიებს (ACLs), რათა განსაზღვროს ობიექტზე წვდომის წესები. ACL შეიცავს სპეციფიურ წესთა თანმიმდევრობას. წვდომის მინიჭებისა და აკრძალვის განსაზღვრა დამოკიდებულია ამ წესებზე.

იდენტიფიკაცია, ავთენტიფიკაცია, ავტორიზაცია

იდენტიფიკაცია აუმჯობესებს ავტორიზაციის პოლიტიკით დადგენილ წესებს. სუბიექტი ითხოვს სისტემის რესურსზე წვდომის უფლებას. ყოველთვის, როდესაც სუბიექტი ითხოვს რესურსზე წვდომას, წვდომის მართვა განსაზღვრავს, დაერთოს მას ნება თუ უარი ეთქვას. ავტორიზაციის პოლიტიკა განსაზღვრავს, რა სახის აქტივობის განხორციელების უფლება უნდა მიეცეს სუბიექტს. უნიკალური იდენტიფიკატორი უზრუნველყოფს სათანადო ასოციაციას დაშვებულ საქმიანობასა და სუბიექტს შორის. მომხმარებლის სახელი არის ყველაზე გავრცელებული მეთოდი, რომელიც გამოიყენება მომხმარებლის იდენტიფიცირებისთვის. მომხმარებლის სახელი შეიძლება იყოს ალფანუმერული კომბინაცია, პირადი საიდენტიფიკაციო ნომერი (PIN), ჭკვიანი ბარათი ან ბიომეტრიული, როგორიცაა თითის ანაბეჭდი, ბადურის სკანირება ან ხმის ამოცნობა.

უნიკალური იდენტიფიკატორი უზრუნველყოფს სისტემის მიერ თითოეული მომხმარებლის ინდივიდუალურ იდენტიფიკაციას: შესაბამისად, ის საშუალებას აძლევს უფლებამოსილ მომხმარებელს განახორციელოს შესაბამისი ქმედებები კონკრეტულ რესურსზე.

კიბერ უსაფრთხოების პოლიტიკა განსაზღვრავს, თუ რომელი საიდენტიფიკაციო მართვა უნდა იქნას გამოყენებული. ინფორმაციული და საინფორმაციო სისტემების მგრძნობელობა განსაზღვრავს რამდენად მკაცრი უნდა იყოს მართვა. მონაცემთა დაცვის მნიშვნელობის ზრდამ მრავალი ორგანიზაცია აიძულა მათი საიდენტიფიკაციო მართვის გაძლიერების გადაწყვეტილება მიეღო. მაგალითად, ამერიკის შეერთებულ შტატებში საკრედიტო ბარათის ინდუსტრია მოითხოვს ყველა ვენდორისაგან, გადაიყვანონ საიდენტიფიკაციო სისტემები ჭკვიან ბარათებზე.

პაროლები, პასპორტები, ან PIN წარმოადგენენ მაგალითებს, რომლებიც მომხმარებელმა იცის. პაროლები ყველაზე პოპულარული მეთოდია, რომელიც გამოიყენება ავთენტიფიკაციისთვის. პაროლი არის სიმბოლოებისაგან შემდგარი სტრიქონი, რომელიც გამოიყენება მომხმარებლის ვინაობის დასამტკიცებლად. თუ სიმბოლოთა ეს სტრიქონი უკავშირდება მომხმარებელს (როგორიცაა სახელი, დაბადება ან მისამართი), კიბერ დამნაშავეებს უფრო გაუადვილდებათ მომხმარებლის პაროლის გამოცნობა.

სმარტ ბარათი წარმოადგენს კრედიტ ბარათის ზომების მქონე ბარათს მასში ინტეგრირებული მიკროჩიპით. ჩიპი არის ინტელექტუალური მონაცემთა გადამტანი, რომელსაც შეუძლია დაამუშაოს, შეინახოს და დაიცვას მონაცემები. „ჭკვიანი“ ბარათები ინახავენ პირად ინფორმაციას, როგორიცაა საბანკო ანგარიშის ნომრები, პირადი საიდენტიფიკაციო მონაცემი, სამედიცინო ჩანაწერები და ციფრული ხელმოწერები. „ჭკვიანი“ ბარათები მონაცემთა უსაფრთხოების დასაცავად უზრუნველყოფენ ავთენტიფიკაციას და შიფრაციას.

უნიკალურ ფიზიკურ მახასიათებელს, როგორიცაა თითის ანაბეჭდი, ბადურა ან ხმა, რომელიც განსაზღვრავს კონკრეტულ მომხმარებელს, ეწოდება ბიომეტრიკა. ბიომეტრიული უსაფრთხოება ადარებს მომხმარებლის ფიზიკურ მონაცემებს, მისი შენახული პროფილის ავთენტიფიკაციის განსახორციელებლად. პროფილი არის მონაცემთა ფაილი, რომელიც შეიცავს ფიზიკური პირის ცნობილ მახასიათებლებს.

სისტემა დაუშვებს მომხმარებლის წვდომას, თუ მისი მახასიათებლები ემთხვევა შენახულ პარამეტრებს. თითის ანაბეჭდის წამკითხავი (Fingerprint reader) არის ყველაზე გავრცელებული ბიომეტრული მოწყობილობა. ბიომეტრიკა სულ უფრო პოპულარული ხდება საზოგადოებრივი უსაფრთხოების სისტემებში, სამომხმარებლო ელექტრონიკისა და სავაჭრო აპლიკაციებში. ბიომეტრიკის განხორციელება იყენებს სპეციალურ წამკითხველს ან სკანირების მოწყობილობას, პროგრამულ უზრუნველყოფას, რომელიც სკანირებულ ინფორმაციას ციფრულ ფორმაში გარდაქმნის და მონაცემთა ბაზას, რომელიც შედარებისთვის ბიომეტრიულ მონაცემებს ინახავს.

<u>მრავალფაქტორიანი ავთენტიფიკაცია</u>

მრავალ ფაქტორიანი ავთენტიფიკაცია იყენებს გადამოწმების მინიმუმ ორ მეთოდს. მრავალფაქტორიან ავტორიზაციას შეუძლია შეამციროს სიხშირე ონლაინ იდენტობის ქურდობისა, რადგან მხოლოდ პაროლის ცოდნა არ მისცემს კიბერ კრიმინალებს სისტემაში წვდომის საშუალებას. აუტენტიფიკაციის ძლიერი საშუალებები წარმოადგენენ მნიშვნელოვან ხერხს, პაკეტების სნიფინგის წინააღმდეგ. ”ძლიერი” საშუალებების ქვეშ იგულისხმება ისეთი მეთოდები, რომლისთვის გვერდის ავლა ძნელად შესაძლებელია.

მაგალითად, ისეთი აუტენტიფიკაციისა არის ერთჯერადი პაროლები (One Time Passwords, OTP) OTP- ეს არის აუტენტიფიკაციის ორფაქტორიანი ტექნოლოგია, რომლის დროსაც ხდება გათვალისწინება იმისა, რაც თქვენ გაქვთ და იმასა რაც თქვენ იცით, ტიპიური მაგალითია ორფაქტორიანი აუტენტიფიკაცისა წარმოადგენს ბანკომატი, რომელიც ამოგიცნობთ თქვენ, ჯერ ერთი თქვენი პლასტიკური ბარათით და მეორე თქვენი პინ კოდით. აუტენტიფიკაციისათვის OTP სისტემაში აგრეთვე მოითხოვება პინ კოდი და თქვენი პირადი ბარათი. ”ბარათის” ქვეშ იგულისხმება აპარატურული ან პროგრამული საშუალება, რომელიც აგენირირებს უნიკალურ (შემთხვევითი შერჩევის პრინციპით) ერთმომენტიან, ერთჯერად პაროლს. თუ ჰაკერი გაიგებს მოცემულ პაროლს სნიფერის საშუალებით, მისთვის ეს ინფორმაცია იქნება გამოუსადეგარი, რადგანაც ეს პაროლი უკვე იქნება გამოყენებული და უვარგისი

შემდგომი გამოყენებისთვის. ავღნიშნოთ, რომ ეს ხერხი სნიფინგის საწინააღმდეგოდ საბრძოლველად ეფექტურია მხოლოდ პაროლის დაჭერის შემთხვევაში, სნიფერი, რომელიც დაიჭერს სხვა ინფორმაციას (მაგ. ელ ფოსტის ინფორმაციას) არ კარგავს თავის ეფექტურობას.

აუტენტიფიკაცია ამოწმებს კომუნიკაციის დროს პირის უტყუარობას. დაშორებული პროცესის უტყუარობის შემოწმება ითხოვს რთულ პროტოკოლებს, დამყარებულს კრიპტოგრაფიაზე.

აღსანიშნავია, რომ ხშირად ერთმანეთში ურევენ ავთენტიფიკაციას და ავტორიზაციას. აუტენტიფიკაცია დაკავებულია მოსაუბრის უტყუარობის შემოწმებით, ავტორიზაციას კი საქმე აქვს ნებართვებთან. მაგ., პროგრამა კლიენტი მიმართავს ფაილურ სერვერს და ეუბნება: "მე ვარ პროცესი A და მინდა test.doc ფაილის წაშლა". ფაილურმა სერვერმა უნდა გადაწყვიტოს:

პირველი - არის თუ არა სინამდვილში ეს პროცესი A? (აუტენტიფიკაცია).

მეორე - აქვს თუ არა A-ს test.doc ფაილის წაშლის უფლება? (ავტორიზაცია).

მხოლოდ იმის შემდეგ, რაც ორივე კითხვაზე იქნება არაორაზროვანი პასუხი გაცემული, შესაძლებელია განხორციელდეს მოთხოვნილი მოქმედება. მნიშვნელოვანია პირველი კითხვა. მას შემდეგ, რაც სერვერმა იცის თუ ვის ელაპარაკება, უფლების შესამოწმებლად საჭიროა მხოლოდ ცხრილების ლოკალურად შემოწმება. ყველა აუტენტიფიკაციის პროტოკოლის მიერ გამოყენებული საერთო სქემა შემდეგნაირია:

მომხმარებელს (პროცესს) A-ს, სურს დაამყაროს დაცული კავშირი მეორე მომხმარებელთან, B-სთან. B ბანკირია და A-ს უნდა მასთან საქმიანი გარიგება. A იწყებს იმით, რომ უგზავნის B-ს შეტყობინებას, ან ნდობით აღჭურვილ გასაღებების გამავრცელებელ ცენტრს (KDC – Key Distribution Center). შემდეგ მრავალი მიმართულებით აგზავნის კიდევ რამოდენიმე შეტყობინებას. ამის შემდეგ ბოროტმიქმედმა შეიძლება დაიჭიროს, შეცვალოს და ხელახლა შექმნას ეს შეტყობინება იმისათვის, რომ მოატყუოს A და B ან უბრალოდ ჩაშალოს გარიგება. ასე თუ ისე, როდესაც პროტოკოლი ამთავრებს თავის მუშაობას, A უნდა იყოს დარწმუნებული, რომ ელაპარაკება B-ს, ხოლო B — კი A-ს. ბევრ

პროტოკოლში მოსაუბრეები ქმნიან სეანსის საიდუმლო გასაღებს, რომლითაც მომხმარებლები გაცვლიან შემდგომ ინფორმაციას.

პრაქტიკაში მონაცემთა ყველა გაცვლა იშიფრება სიმეტრიული ალგორითმის გამოყენებით, რადგან სიმეტრიული ალგორითმის მწარმოებლურობა გაცილებით მაღალია გარდა ასიმეტრიული ალგორითმების. მიუხედავად ამისა, ასიმეტრიული ალგორითმები, ფართოდ გამოიყენება აუტენტიფიკაციის პროტოკოლებში სეანსის გასაღების შესაქმნელად. სეანსის გასაღები იქმნება კავშირის ყოველ კონკრეტულ სეანსზე და იძლევა საშუალებას უზრუნველვყოთ ინფორმაციის მეტი დაცვა. თუ ბოროტმოქმედმა დაიჭირა ერთ სეანსზე გადაცემული ინფორმაცია და მოახერხა მისი დაშიფრვის გასაღების გამოთვლა, მას ეს გასაღები აღარ გამოადგება შემდეგ სეანსზე.

განვიხილოთ აუტენტიფიკაციის პროტოკოლი საერთო საიდუმლო გასაღებით. A-ს და B-ს აქვთ საერთო საიდუმლო გასაღები KAB. ამ საიდუმლო გასაღების შეთანხმება შესაძლებელია პირადი შეხვედრისას, ან ტელეფონით, მაგრამ არა დაუცველი ქსელის საშუალებით.

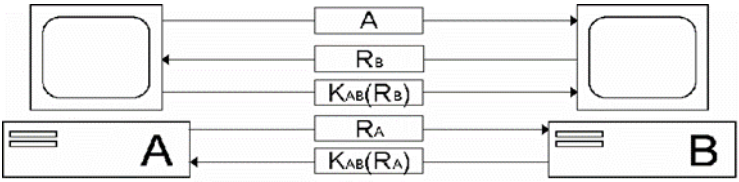
ამ პროტოკოლს საფუძვლად უდევს პრინციპი, გამოყენებული მრავალ აუტენტიფიკაციის პროტოკოლში: ერთი მხარე უგზავნის მეორეს შემთხვევით რიცხვს, რომელსაც მეორე მხარე გარდაქმნის განსაკუთრებული მეთოდით და აბრუნებს შედეგს:

R_i — პასუხი, სადაც ინდექსი აღნიშნავს მის გამგზავნს.

K_i — გასაღები, სადაც ინდექსი აღნიშნავს გასაღების მფლობელს.

K_s –სეანსი გასაღები.

აუტენტიფიკაციის პროტოკოლის შეტყობინებების თანმიმდევრობა ნაჩვენებია სურ. 4.3-ზე. თავიდან A უგზავნის თავის პირადობის მოწმობას B-ს იმ სახით, რომელიც გასაგებია B-სთვის. B-მ რა თქმა უნდა არ იცის მოვიდა თუ არა ეს შეტყობინება A-სგან, თუ ბოროტმოქმედისაგან. ამიტომ ის ირჩევს დიდ შემთხვევით რიცხვს RB-ს და უგზავნის პასუხად A-ს.



სურ. 4.3. აუტენტიფიკაციის პროტოკოლის შეტყობინებების თანმიმდევრობა

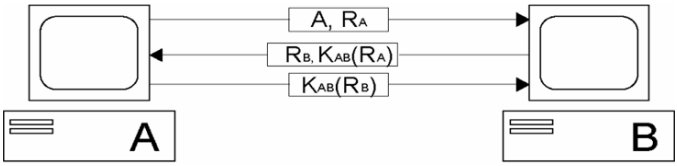
შემდეგ A დახურული გასაღებით შიფრავს ამ შეტყობინებას და მიღებულ რეზულტატს KAB(RB)-ს უგზავნის B-ს. როდესაც B მიიღებს ამ შეტყობინებას, ის იგებს, რომ ეს შეტყობინება მოვიდა A-სგან, რადგანაც ბოროტმოქმედს არ შეეძლო ქონოდა გასაღები KAB და ამიტომ არ შეეძლო შეექმნა ეს შეტყობინება. უფრო მეტიც, პასუხი RB აირჩა შემთხვევით დიდი რიცხვების ჯგუფიდან (მაგ. 128 ბიტიანი შემთხვევითი რიცხვებიდან) და ნაკლებად სავარაუდოა, რომ ბოროტმოქმედმა შეძლო წინა სეანსებში პასუხის ნახვა და ძველი პასუხის გამოყენება. ამ მომენტისთვის B დარწმუნებულია, რომ ლაპარაკობს A-სთან, მაგრამ A ჯერ კიდევ არ არის დარწმუნებული არაფერში.

ბოროტმოქმედს შეეძლო დაეჭირა პირველი შეტყობინება და გამოეგზავნა უკან პასუხი RB. შესაძლებელია B საერთოდ არ არსებობს. შემდეგ პროტოკოლი მუშაობს სიმეტრიულად:

A აგზავნის RA-ს და B პასუხობს მას. უკვე ორივე მხარე დარწმუნებულია, რომ ლაპარაკობენ ზუსტად ისინი, რადაც თავი მოქონდათ. ამის შემდეგ მათ შეუძლიათ შექმნან სეანსის გასაღები KS, რომელიც შეიძლება გადაუგზავნონ ერთმანეთს კოდირებული იგივე საერთო KAB გასაღებით.

ამ პროტოკოლებში შეტყობინების რაოდენობა შეიძლება შემცირდეს სურ. 4.4-ზე მოცემული სქემის მიხედვით. ეს პროტოკოლი წინაზე კარგია იმით, რომ ის უფრო მოკლეა. მაგრამ ამ პროტოკოლით სარგებლობა არაა რეკომენდირებული. ზოგიერთ შემთხვევაში ბოროტმოქმედმა შეიძლება განახორციელოს თავდასხმა ამ პროტოკოლზე, რომელიც ცნობილია სახელით "სარკისებური შეტევა". კერძოდ, ბოროტმოქმედს შეუძლია პროტოკოლის გატეხვა, თუ მას

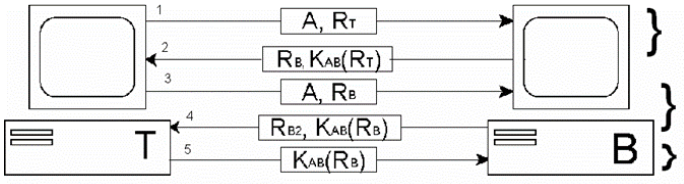
ეძლევა შესაძლებლობა B-სთან გახსნას რამდენიმე სეანსი ერთდროულად. რაც სრულებით შესაძლებელია, თუ B ბანკია და რომლისთვისაც ნებადართულია ერთდროულად რამდენიმე კავშირი ბანკომატთან.



სურ. 4.4. პროტოკოლებში შეტყობინების რაოდენობის შემცირების სქემა

სარკისებური შეტევის სქემა ნაჩვენებია სურ. 4.5-ზე. ის იწყება იმით, რომ ბოროტმოქმედს (T) თავი მოაქვს A-დ და უგზავნის პასუხს RT B-ს. B უბრუნებს პასუხის პასუხს RB. რის შემდეგ თითქოს ბოროტმოქმედი უნდა აღმოჩნდეს ჩიხში. რა ქნას როდესაც არ იცის როგორ გამოითვალოს KAB(RB)?

ბოროტმოქმედს შეუძლია გახსნას მეორე სესია და გაუგზავნოს B-ს პასუხად ისევ B-ს პასუხი RB, რომელიც მან აიღო B-სთან პირველი სესიის გახსნისას. B მშვიდად შიფრავს მას და უგზავნის მას უკან KAB(RB). ბოროტმოქმედს უკვე აქვს აუცილებელი ინფორმაცია, ამიტომ ის წყვეტს მეორე სესიას და ასრულებს პირველ სესიას. B უკვე დარწმუნებულია, რომ ბოროტმოქმედი არის — A, ამიტომ ის ბოროტმოქმედს ამლევს A-ს საბანკო ანგარიშებზე წვდომას და ნებას რთავს გადარიცხოს თანხა მიმდინარე ანგარიშიდან ბოროტმოქმედის საიდუმლო ანგარიშზე ყოველგვარი ყოყმანის გარეშე.



სურ. 4.5. სარკისებური შეტევის სქემა

არსებობს სამი საერთო წესი, რომლის გამოყენებაც ხშირად სასარგებლოა:

1. სეანსის ინიციატორმა უნდა დაამოწმოს საკუთარი თავი მოპასუხე მხარეზე ადრე. ამ შემთხვევაში ბოროტმოქმედი ვერ შეძლებს მიიღოს ღირებული ინფორმაცია მანამ, სანამ ის არ დაადასტურებს საკუთარ პიროვნებას.

2. საჭიროა გამოვიყენოთ ორი გასაღები KAB და K'AB, ერთი ინიციატორისთვის მეორე კი მოპასუხისათვის.

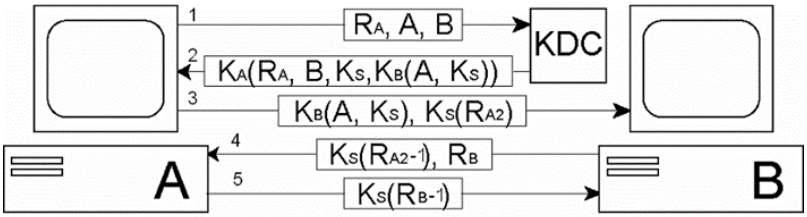
3. ინიციატორმა და მოპასუხემ უნდა აირჩიოს პასუხები განსხვავებული არამკვეთი რიცხვების სიმრავლიდან. მაგალითად თუ ინიციატორი აირჩევს წყვილ რიცხვებს და მოპასუხე მხარე კენტ რიცხვებს.

წინა მაგალითზე ყველა ეს პირობა იყო დარღვეული, რამაც მიგვიყვანა უარყოფით შედეგებამდე. ნიდჰემ-შროდერის აუტენტიფიკაციის პროტოკოლი უფრო რთული აუტენტიფიკაციის მეთოდია და გულისხმობს მრავალ გამოძახება-პასუხის მრავალმხრივ გამოყენებას.

ნიდჰემ-შროდერის პროტოკოლი. პროტოკოლის მუშაობა იწყება იმით, რომ A ატყობინებს ნდობით აღჭურვილ გასაღებების გამავრცელებელ ცენტრს (KDC), რომ მას უნდა საუბარი B-სთან. ეს შეტყობინება შეიცავს A-ს და B-ს იდენტიფიკატორებს და დიდ შემთხვევით რიცხვს RA-ს.

KDC უგზავნის A-ს პასუხს, რომელიც დაშიფრულია KA გასაღებით და შეიცავს A-ს გაგზავნი შემთხვევით რიცხვს RA და სეანსის გასაღებს KS, რომელსაც უწოდებან აგრეთვე ბილეთს და რომელიც მან შეუძლია გაუგზავნოს B-ს. მთავარი მიზანი შემთხვევითი რიცხვის გაგზავნისა არის ის, რომ A-ს შეტყობინება ახალია, ანუ მიმდინარე, და არა განმეორებული. გარდა ამის მეორე შეტყობინებაში თავსდება B-ს იდენთიფიკატორი. აგრეთვე სეანსის გასაღები და A-ს იდენტიფიკატორი დაშიფრული B-ს გასაღებით KB(A, KS). თუ ბოროტმოქმედი შეცვლის B-ს იდენტიფიკატორს საკუთარი იდენტიფიკატორით პირველ შეტყობინებაში, მაშინ KDC ცენტრი დაშიფრავს ბილეთს მეორე შეტყობინების ბოლოში გასაღებით KT, ნაცვლად გასაღებისა KB. ბილეთი დაშიფრული გასაღებით KB თავსდება დაშიფრული შეტყობინების შიგნით იმისათვის, რომ ბოროტმოქმედმა ვერ შეძლოს შეცვალოს ის სხვა გასაღებით მანამ, სანამ

მეორე შეტყობინება არ მიაღწევს A-მდე. ამის შემდეგ მესამე შეტყობინებაში A უგზავნის ბილეთს KB(A, KS) B-ს ახალ შემთხვევით რიცხვთან RA2-თან ერთად, რომელიც დაშიფრულია სეანსის გასაღებით. მეოთხე შეტყობინებაში B უგზავნის უკან A-ს KS(RA2–1), იმისათვის რომ A დარწმუნდეს, რომ ის ელაპარაკება B-ს. უკან გადაგზავნა მხოლოდ KS(RA2) არ შეიძლება, იმიტომ რომ ეს რიცხვი შესაძლებელია ყოფილიყო მოპარული მესამე შეტყობინებიდან ბოროტმოქმედების მიერ.



სურ. 4.6. ნიდჰემ-შროდერის პროტოკოლი.

მეოთხე შეტყობინების მიღების შემდეგ A რწმუნდება, რომ ლაპარაკობს B-სთან, მაგრამ B ჯერ კიდევ არ არის დარწმუნებული, რომ საუბრობს A-სთან. მეორე შემთხვევითი რიცხვის RA2 გაგზავნისა და KS(RA2-1) პასუხის მიღებას შორის გადის ძალიან ცოტა დრო. მეხუთე შეტყობინების მიზანია B-ს დარწმუნება იმაში, რომ საუბრობს A-სთან. მიუხედავად ასეთი სოლიდური ალგორითმისა, მასაც აქვს სუსტი წერტილი. თუ ბოროტმოქმედს მიეცა შესაძლებლობა მიიღოს ძველი სეანსის გასაღები KS, მას შეუძლია ინიცირება გაუკეთოს ახალ სეანს B-სთან, თავიდან წარმოქმნას მესამე შეტყობინება კომპრომენტირებული სეანსის გასაღებით, და თავი გაასაღოს A-დ. ამ შემთხვევაში ბოროტმოქმედს შეუძლია მოპაროს თანხა A-ს.

ავტორიზაციის წესების განსაზღვრა არის პირველი ნაბიჯი წვდომის მართვის პროცესში. ავტორიზაციის პოლიტიკა ადგენს ამ წესებს. ჯგუფის წევრობის პოლიტიკა განსაზღვრავს ავტორიზაციის საფუძველზე წევრობას კონკრეტულ ჯგუფში. მაგალითად, ორგანიზაციის ყველა თანამშრომელს აქვს გასატარებელი (swipe) ბარათი, რომელიც უზრუნველყოფს ობიექტის ხელმისაწვდომობას. თუ დასაქმებულის სამუშაო არ მოითხოვს მის სერვერის ოთახზე

წვდომას, მისი უსაფრთხოების ბარათი არ მისცემს მას ოთახში შესვლის საშუალებას.

ავტორიტეტული დონის პოლიტიკა განსაზღვრავს ორგანიზაციის ფარგლებში დასაქმებულის დაშვების ნებართვას. მაგალითად, IT დეპარტამენტში მხოლოდ ამ დეპარტამენტის უფროსი დონის თანამშრომლებს შეუძლიათ მიიღონ წვდომა სერვერის ოთახზე.

4.3 გაურკვეველი მონაცემები. მონაცემთა შენიღბვა

მონაცემთა შენიღბვის ტექნოლოგია უზრუნველყოფს მგრძნობიარე ინფორმაციის შეცვლას მისი არამგრძნობიარე ვერსიის ინფორმაციით. არამგრძნობიარე ვერსია გამოიყურება და მოქმედებს, როგორც ორიგინალი. ეს იმას ნიშნავს, რომ ბიზნეს პროცესს შეუძლია გამოიყენოს არამგრძნობიარე მონაცემები და არ დადგეს აპლიკაციების ან მონაცემთა საცავების შესაძლებლობების მხარდაჭერის წინაშე. ყველაზე გავრცელებულ შემთხვევებში, ნიღაბი ზღუდავს მგრძნობიარე მონაცემების გავრცელებას IT სისტემებში ტესტირებისა და ანალიზისთვის შემცვლელი მონაცემების გავრცელების გზით. ინფორმაცია შეიძლება იქნას დინამიურად შენიღბული, თუ სისტემა ან აპლიკაცია განსაზღვრავს, რომ მომხმარებლის მიერ მგრძნობიარე ინფორმაციის მოთხოვნა სარისკოა.

მონაცემთა შენიღბვას შეუძლია შეცვალოს მგრძნობიარე მონაცემები არასაწარმოო გარემოში ძირითადი ინფორმაციის დაცვის მიზნით. არსებობს რამდენიმე შენიღბვის ტექნიკა, რომელიც უზრუნველყოფს მონაცემთა შეცვლას, მაგრამ უზრუნველყოფს მის აზრობრივ მთლიანობას.

- ჩანაცვლება ცვლის მონაცემების აუთენტურ სახეს, რათა უზრუნველყოს მისი ანონიმურობა მონაცემთა ჩანაწერებზე;
- Shuffling იღებს ჩანაცვლებათა კრებულს მონაცემთა იმავე სვეტიდან, რომლის შენიღბვაც სურს მომხმარებელს. ეს ტექნიკა კარგად მუშაობს ფინანსური ინფორმაციის სატესტო მონაცემთა ბაზაში, მაგალითად;
- კონკრეტული ველის განულებისათვის გამოიყენება ნულოვანი მნიშვნელობა, რაც ტექსტს გარდაქმნის სრულიად უხილავად.

სტეგანოგრაფია (საიდუმლო დამწერლობა) - ინფორმაციის ფარული გადაცემის ხერხია, რომლის დროსაც შეტყობინებას დაშიფვრის ნაცვლად მალავენ ჩვეულებრივ ტექსტურ ან მულტიმედიურ ფაილში. მისი მიზანია, უცხო თვალისთვის შეუმჩნეველი გახადოს ინფორმაცია.

თანამედროვე სტეგანოგრაფია ითვალისწინებს მიკროფოტოების, წყლის ნიშნებისა და საავტორო უფლებების დამცავი ჰოლოგრამების გამოყენებას. ჯერ კიდევ II მსოფლიო ომის დროს შეძლეს ფოტოების დაპატარავება წერტილის ზომამდე. ადრესატი წერტილს ადიდებდა და ისე კითხულობდა ინფორმაციას.

ვინაიდან სტეგანოგრაფიის გამოყენებით ინფორმაცია კარგად არის შენიღბული, ინფორმაციის გადაცემა და მიღება ეჭვს არავის აღუძრავს. მაგრამ შენიღბული ინფორმაციის აღმოჩენის შემთხვევაში, შესაძლებელია მისი წაკითხვა, თუ ის ამავე დროს დაშიფრული არ არის. კრიპტოგრაფიასთან შედარებით სტეგანოგრაფიას აქვს ის უპირატესობა, რომ საიდუმლო შეტყობინება არ იქცევს რაიმე განსაკუთრებულ ყურადღებას. ფაილის ელექტრონულად ან ნაბეჭდი სახით დათვალიერებისას, ვერავინ ვერასდროს გაიგებს, რომ სურათი შეიცავდა საიდუმლო შეტყობინებას.

მონაცემების დამალვაში რამდენიმე კომპონენტია ჩართული. პირველი, არსებობს მიბმული მონაცემები, რომელიც საიდუმლო გზავნილს წარმოადგენენ. დაფარული ტექსტი (გამოსახულება ან აუდიო) მალავს მიბმულ მონაცემებს, აწარმოებს რა ტექსტის (გამოსახულების ან აუდიოს) სტეგანოგრაფიას. სტეგანოგრაფიის გასაღები მართავს დამალვის პროცესს.

მონაცემების საფარ-გამოსახულებაში მიბმისთვის გამოყენებულ მიდგომას წარმოადგენს ნაკლებად მნიშვნელოვანი ბიტების (Least Significant Bits – LSB) გამოყენება. ეს მეთოდი იყენებს გამოსახულებაში არსებულ თითოეული პიქსელის ბიტებს. პიქსელი, კომპიუტერულ გამოსახულებაში, წარმოადგენს პროგრამირებადი ფერის ბაზისურ ერთეულს. პიქსელის კონკრეტული ფერი წარმოადგენს სამი ფერის ნაზავს. ეს ფერებია წითელი, მწვანე. ლურჯი (RGB). მონაცემთა სამი ბაიტი განსაზღვრავს პიქსელის ფერს (ერთი ბიტი თითო ფერისთვის). რვა ბიტი ქმნის ერთ ბაიტს. 24-ბიტიანი ფერთა სისტემა იყენებს სამივე ბაიტს. LSB იყენებს წითელ, მწვანე და ლურჯ ფერთა კომპონენტის თითოეულ ბიტს.. თითოეულ პიქსელს შეუძლის 3 ბიტის შენახვა.

საშუალოდ, საიდუმლო გზავნილის ეფექტურად დამალვისათვის გამოსახულების ნახევარზე მეტი არ უნდა შეიცვალოს.

სოციალური სტეგანოგრაფია მალავს ინფორმაციას ისე, რომ მისი უშუალო ხილვა შეუძლებელია და ქმნის შეტყობინებას, რომელიც იკითხება გარკვეული წესით ამ შეტყობინების მიმღების მიერ. სხვები ნორმალურ რეჟიმში ვერ ხედავენ შეტყობინებას. მოზარდები სოციალური მედიაში ამ ტაქტიკას იყენებენ თავიანთ უახლოეს მეგობრებთან კომუნიკაციისთვის, რათა სხვა ადამიანებმა, მაგალითად, მშობლებმა, ვერ შეიტყონ ამ შეტყობინების შინაარსი.

იმ ქვეყნებში, რომლებშიც ცენზორი ახდენს მედიის მონიტორინგს, ასევე იყენებენ სოციალურ სტეგანოგრაფიას, რათა მათი შეტყობინებების შინაარსი არ გახდეს ცნობილი ხელისუფლებისათვის. ფაქტობრივად, ისინი ერთდროულად სხვადასხვა აუდიტორიასთან ახდენენ კომუნიკაციას.

სტეგანოანალიზი არის აღმოჩენა იმ ფაქტისა, რომ ფარული ინფორმაცია არსებობს. სტეგანოანალიზის მიზანია ფარული ინფორმაციის აღმოჩენა. ორიგინალური გამოსახულების სტეგო-სურათთან შედარებით, ანალიტიკოსს შეუძლია ვიზუალურად შეარჩიოს განმეორებადი ნიმუშები.

კიბერ უსაფრთხოების და კიბერ დაზვერვის პროფესიაში მონაცემების ნიღბისა და სტეგანოგრაფიის ტექნიკის გამოყენება და პრაქტიკა ხორციელდება მონაცემთა შენიღბვით. მონაცემთა შენიღბვა არის ხელოვნება გაუგებარი, ორაზროვანი ან რთულად გასაგები ინფორმაციის გადაცემის ან მიღებისა. სისტემა შეიძლება მიზანმიმართულად ნიღბავდეს შეტყობინებებს მგრძნობიარე ინფორმაციაზე არასანქცირებული წვდომის თავიდან ასაცილებლად.

თავი 5. მთლიანობის უზრუნველყოფა. ტექნოლოგიების, პროდუქტების და პროცედურების გამოყენება მთლიანობის უზრუნველსაყოფად

5.1 მონაცემთა მთლიანობის მართვის სახეები

მონაცემთა მთლიანობა ფუნდამენტურად გულისხმობს მონაცემთა საიმედოობისა და ავთენტურობის გარანტიას მისი სასიცოცხლო ციკლის განმავლობაში. ეს ასევე ეხება მონაცემთა სისრულეს, სიზუსტეს და თანმიმდევრულობას. ის შეიძლება ჩაითვალოს მონაცემთა სანდოობად მთელი მისი სასიცოცხლო ციკლის განმავლობაში, დაწყებული მისი გენერირების მომენტიდან. მონაცემთა მთლიანობის კონტროლი არის კონტროლი, რომელიც ხორციელდება მონაცემთა მთლიანობის უზრუნველსაყოფად. ეს კონტროლი მოიცავს, მაგრამ არ შემოიფარგლება მხოლოდ არაავტორიზებული მონაცემების შეყვანის/გამოტანის თავიდან აცილებას, არასწორი მონაცემების შეყვანის უარყოფას და მონაცემთა და პროგრამების დაცვას შემთხვევითი ან მავნე ხელყოფისგან. ცუდმა და არასანდო მონაცემებმა შეიძლება გამოიწვიოს კომპანიებში მილიონობით დოლარის შემოსავლის დაკარგვა და რეპუტაციის შელახვა. კვლევითი ორგანიზაციის Gartner-ის მიერ ჩატარებული გამოკითხვის თანახმად, კორპორაციების შეფასებით, მონაცემთა ცუდი მთლიანობა არის საშუალოდ 15 მილიონი დოლარის ყოველწლიური ფინანსური ზარალის მიზეზი. მონაცემთა მთლიანობა გადამწყვეტია ინდუსტრიის ლიდერებისთვის, კორპორაციებისთვის, ბიზნესისთვის და მთავრობებისთვის. მონაცემთა მთლიანობის განსახორციელებლად, ინსტიტუტები ჩვეულებრივ დაშიფვრავენ თავიანთ მონაცემებს, ახორციელებენ მონაცემთა ხშირი სარეზერვო ასლებს, აწარმოებენ აუდიტს, რათა თვალყური ადევნონ ნებისმიერი მონაცემთა მანიპულაციის წყაროებს და რაც მთავარია, დანერგონ წვდომის კონტროლი. მონაცემთა მთლიანობა მოითხოვს, რომ მონაცემები იყოს სანდო, ავთენტური, მიკუთვნებული, თანმიმდევრული და მართებული. ის ასევე მოითხოვს, რომ მონაცემები იყოს სრული და ზუსტი. უნდა აღინიშნოს, რომ მონაცემთა მთლიანობა არ არის მონაცემთა უსაფრთხოების სინონიმი, თუმცა ორივე, როგორც წესი, თანმიმდევრულია.

ყოველდღიურად, ორგანიზაციები მთელს მსოფლიოში ქმნიან, აგროვებენ და იყენებენ უფრო მეტ მონაცემს კრიტიკული ბიზნეს გადაწყვეტილებების მისაღებად. მონაცემები არის კრიტიკული დიფერენციატორი კომპანიებისთვის, რადგან უფრო და უფრო მეტი მონაცემი იქმნება, გამოიყენება, ზიარდება და ინახება. შეცდომების ალბათობა იზრდება მონაცემთა მოცულობის მატებასთან ერთად. ასეთი შეცდომების შედეგებმა შეიძლება დიდი გავლენა მოახდინოს მომხმარებლებზე.

მონაცემთა მთლიანობა უზრუნველყოფს კონფიდენციალურობასაც, სადაც ეს საჭიროა. მაგალითად, კომპანიებმა შეიძლება შეაგროვონ თავიანთი კლიენტების საკრედიტო ბარათის ინფორმაცია ან სოციალური დაცვის ნომრები, რომლებიც შეიძლება გამოყენებულ იქნას ფიზიკური პირებისთვის სპეციფიკური ფინანსური ტრანზაქციების დასამუშავებლად. თუმცა, ნებისმიერმა შემთხვევითმა ან მავნე მანიპულაციამ შეიძლება გამოიწვიოს არა მხოლოდ მომხმარებლის ინფორმაციის დამახინჯება, არამედ გამოიწვიოს პირადობის მოპარვა, მომხმარებლის ნდობის დაკარგვა და ფინანსური ზარალი. პირადობის ქურდობასთან დაკავშირებული რისკები და ხარჯები მაღალია და შეიძლება სერიოზულად იმოქმედოს ბიზნესსა და მომხმარებლებზე.

მონაცემთა მთლიანობა შეიძლება დაირღვეს სხვადასხვა მიზეზის გამო. ადამიანური შეცდომა ასევე შეიძლება იყოს ერთ-ერთი ასეთი მიზეზი. მონაცემთა მთლიანობა შეიძლება დაირღვეს, თუ დაინტერესებული მხარეები ან თანამშრომლები არ შეასრულებენ პროცედურებს, პოლიტიკას ან სახელმძღვანელო მითითებებს, რომლებიც შექმნილია მათ უზრუნველსაყოფად. ტექნოლოგიასთან დაკავშირებული წარუმატებლობის მაგალითის მოყვანისთვის, მონაცემთა გადაცემის შეცდომებმა ასევე შეიძლება გამოიწვიოს მონაცემთა მთლიანობის დარღვევა, თუ მონაცემები არ იყო ზუსტად და ეფექტურად გადაცემული წყაროდან დანიშნულების ადგილზე. რელაციურ მონაცემთა ბაზებში, მონაცემთა მთლიანობის ასეთი დარღვევა შეიძლება მოხდეს, როდესაც არსებობს მონაცემთა შეუსაბამობა სამიზნე და წყაროს ცხრილებს შორის, წყაროსა და სამიზნე მონაცემთა ელემენტებს შორის არაადეკვატური კორელაციის გამო.

შეცდომებს, ვირუსებს და მავნე პროგრამებს ასევე შეუძლიათ ხელი შეუწყონ მონაცემთა დარღვევას, რადგან მათ შეუძლიათ ხელი შეუწყონ მონაცემთა არაავტორიზებული წვდომას, მანიპულირებას და ღირებული მონაცემების ქურდობას.

მომხმარებელმა ყოველთვის უნდა იცოდეს, რომ მისი მონაცემები უცვლელი რჩება შენახვის ან გადაცემის პროცესში. ჰეშირება (Hashing) არის ინსტრუმენტი, რომელიც უზრუნველყოფს მონაცემთა მთლიანობას, იღებს რა ოროობით კოდს (გზავნილს) და აწარმოებს მისგან ფიქსირებული სიგრძის ჰეშ-კოდს,

ჰეშირების ინსტრუმენტი იყენებს კრიპტოგრაფიულ ჰეშ- ფუნქციას მონაცემთა მთლიანობის გადამოწმებისა და უზრუნველყოფის მიზნით. მას ასევე შეუძლია დაამოწმოს აუთენტიფიკაცია. ჰეშ ფუნქციები ანცვლებენ ღია ტექსტის პაროლებს ან დაშიფრულ გასაღებებს, რადგან ისინი წარმოადგენენ შეუქცევად (ერთი გზის) ფუნქციებს. ეს იმას ნიშნავს, რომ თუ პაროლი ჰეშირებულია კონკრეტული ჰეშირების ალგორითმის მეშვეობით, ყოველი მომდევნო ჰეშირებისას გენერირებულ იქნება იგივე შედეგი ანუ ჰეშ-დაიჯესტი, ჰეშირების ფუნქცია განიხილება შეუქცევადად, რადგან პრაქტიკულად შეუძლებელია ორი სხვადასხვა მონაცემის ჰეშირებისას მივიღოთ ერთი და იგივე შედეგი.

ყოველთვის, როდესაც მონაცემები იცვლება, იცვლება ასევე ჰეშ-დაიჯესტიც. ამის გამო კრიპტოგრაფიულ ჰეშ-დაიჯესტებს ხშირად უწოდებენ ციფრულ თითის ანაბეჭდებს. მათ შეუძლიათ აღმოაჩინონ დუბლიკატი მონაცემთა ფაილები, ფაილის ვერსიის ცვლილებები და მსგავსი პროგრამები. ეს დაიჯესტები იცავენ მონაცემების შემთხვევითი ან განზრახ ცვლილებასა და შემთხვევით მონაცემთა დაზიანებას. ერთი და იგივე ჰეშ-ფუნქციის გამოყენებისას, დიდი ფაილი ან მთელი დისკის კონტენტი იძლევა ერთი და იგივე ზომის დაიჯესტს.

ჰეშ ალგორითმის მათემატიკური მოდელი

1. ორიგინალი მონაცემი - *M*, რომლის ჰეშირებაც უნდა მოხდეს. იგი შეიძლება იყოს ნებისმიერი სიგრძის;
2. ჰეშირების ჰუნქცია - *H*(*M*), ჰეშის ფუნქცია *H* იღებს *M* შეტყობინებას შეყვანის სახით და აწარმოებს ფიქსირებული

ზომის გამომავალს, რომელსაც ეწოდება ჰეშის მნიშვნელობა ან დაიჯესტი.

3. გამომავალი ჰეშის მნიშვნელობა - *h*, არის ფიქსირებული ზომის სტრიქონი, რომელიც ჩვეულებრივ წარმოდგენილია ბიტების ან თექვსმეტობითი სტრიქონის სახით.

ჰეშ ალგორითმის კომპონენტებია:

- შეტყობინებაზე მონაცემთა დამატება, როგორც წესი, მოიცავს "1" ბიტს, რასაც მოჰყვება საკმარისი "0" ბიტები სასურველი სიგრძის მისაღწევად. ℓ სიგრძის *M შეტყობინებისთვის გვექნება* :

$$M'=M\|1\|0^k\|\ell$$

სადაც, *M'*- არის დანამატი შეტყობინებაზე, *k* არის '0' ბიტების რაოდენობა, რომელიც ემატება იმისათვის, რომ სიგრძე შეესაბამებოდეს *B*-ს ჯერადს გამოკლებული ℓ კოდირებისთვის საჭირო ზომის მნიშვნელობა.

- ჰეშ მნიშვნელობის ინიციალიზაცია რომელსაც უმეტესად შემდეგნაირად აღნიშნავენ *H0,H1,…,Hn.*

- შეტყობინების დამუშავება ბლოკებში. ხდება *M* შეტყობინების დაყოფა *B* ფიქსირებული ზომის ბლოკებად: *M'=M1,M2,…,Mt.*

- შეკუმშვის ფუნქცია *C* ამუშავებს თითოეულ ბლოკს მიმდინარე ჰეშის მნიშვნელობასთან ერთად. იგი იღებს ორ მნიშვნელობას: მიმდინარე ბლოკს M_i და მიმდინარე ჰეშ მნიშვნელობას H_i, და აწარმოებს ახალ ჰეშ მნიშვნელობას H_{i+1}:

$$H_{i+1}=C(H_i,M_i)$$

- გამეორება ხდება ყველა ბლოკისთვის. საწყისი ჰეშ მნიშვნელობა H_0

და შეტყობინების ბლოკების $M_1,M_2,\ldots,M_t$ განმეორებით მუშავდება:

$H_1=C(H_0,M_1)$

$H_2=C(H_1,M_2)$

$\vdots$

$H_t=C(H_{t-1},M_t)$

შეტყობინებების ყველა ბლოკის დამუშავების შემდეგ გამომავალი ჰეშის მნიშვნელობა h არის საბოლოო ჰეშის მნიშვნელობა H_t.

თანამედროვე ჰაშირების ალგორითმები

დღეს ფართოდ გამოიყენება მრავალი თანამედროვე ჰაშირების ალგორითმი. მათაგან ყველაზე პოპულარულებია MD5 და SHA.

გზავნილის დაიჯესტის 5 (MD5) ალგორითმი რონ რივესტმა შეიმუშავა და რამდენიმე ინტერნეტ აპლიკაცია მას დღესაც იყენებს. MD5 არის შეუქცევადი ფუნქცია, რომელიც ახდენს შეტანილი ინფორმაციის მარტივ კონვერტაციას ჰეშ-დაიჯესტში, მაგრამ უკუქმედების განხორციელება ძალიან რთულია.

MD5 აწარმოებს 128 ბიტიან ჰეშ-დაიჯესტს. ფლეიმის მავნე კოდმა 2012 წელს განახორციელა MD5-ის უსაფრთხოების კომპრომეტირება. ფლეიმის მავნე კოდის ავტორებმა გამოიყენეს MD5-ის კოლიზია Windows-ის კოდის ხელმოწერის სერტიფიკატის გაყალბების მიზნით.

აშშ-ის სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST) შეიმუშავა ალგორითმი SHA, რომელიც მითითებულია უსაფრთხო ჰეშის სტანდარტში (SHS). NIS-მა 1994 წელს გამოსცა SHA-1. SHA-2 შეცვალა SHA-1 ოთხი დამატებითი ჰეშის ფუნქციით და შექმნა მთელი SHA "ოჯახი".

- SHA-224 (224 ბიტი)
- SHA-256 (256 ბიტი)
- SHA-384 (384 ბიტი)
- SHA-512 (512 ბიტი)

SHA-2 არის ძლიერი ალგორითმი და ის ანაცვლებს MD5-ს. SHA-256, SHA-384 და SHA-512 წარმოადგენენ შემდეგი თაობის ალგორითმებს.

SHA-512 ალგორითმის მიმდვრობა:

- შეტყობინებაზე მონაცემების დამატება/შევსება. ხდება ორიგინალი შეტყობინების გაფართოება ისე, რომ მისი მთლიანი სიგრძე იყოს 1024 ბიტის (128 ბაიტი) ჯერადი. შეტყობინებას ემატება ერთი "1" ბიტი, და

"0" ბიტები, სანამ შეტყობინების სიგრძე არ გახდება 896 ბიტი მოდულით 1024.

შეფუთულ შეტყობინებას ემატება 128-ბიტიანი (16-ბაიტი) ორიგინალური შეტყობინების სიგრძის გამოსახულება ბიტებში.

- ხორციელდება რვა 64-ბიტიანი (8-ბაიტი) ჰეშის მნიშვნელობის ინიციალიზაცია, *H* კონკრეტული მუდმივი მნიშვნელობებით:

$H_0=0x6a09e667f3bcc908,$
$H_1=0xbb67ae8584caa73b,$
$H_2=0x3c6ef372fe94f82b,$
$H_3=0xa54ff53a5f1d36f1,$
$H_4=0x510e527fade682d1,$
$H_5=0x9b05688c2b3e6c1f,$
$H_6=0x1f83d9abfb41bd6b,$
$H_7=0x5be0cd19137e2179.$

- ხდება მონაცემის დაყოფა 1024 ბიტიან (128 ბაიტი) ბლოკებად.

- იქმნება შეტყობინების განრიგის მასივი *W, ოთხმოცი 64-ბიტიანი სიტყვისგან.* პირველი 16 სიტყვა *W[0],W[1],…,W[15],* პირდაპირ აღებულია მიმდინარე ბლოკიდან. დანარჩენი 64 სიტყვა *W[16],W[17],…,W[79]* გენერირდება შემდეგი ფორმულის საფუძველზე:

$$W[t]=\sigma_1(W[t-2])+W[t-7]+\sigma_0(W[t-15])+W[t-16]$$

სადაც:

$\sigma_0(x)=(x\gg 1)\oplus(x\gg 8)\oplus(x\gg 7)$

$\sigma_1(x)=(x\gg 19)\oplus(x\gg 61)\oplus(x\gg 6)$

- ხორციელდება რვა სამუშაო ცვლადის ინიციალიზაცია a,b,c,d,e,f,g,h მიმდინარე ჰეშის მნიშვნელობებით:

$a=H_0$, $b=H_1$, $c=H_2$, $d=H_3$, $e=H_4$, $f=H_5$, $g=H_6$, $h=H_7$.

- ძირითადი შეკუმშვის ციკლი შემდეგნაირია *t=0*-დან *79*-მდე:

$T_1=h+\Sigma_1(e)+Ch(e,f,g)+K[t]+W[t],$
$T_2=\Sigma_0(a)+Maj(a,b,c),$
$h=g,$
$g=f,$

$f=e,$
$e=d+T_1,$
$d=c,$
$c=b,$
$b=a,$
$a=T_1+T_2.$

სადაც,

$\Sigma_0(x)=(x\gg 28)\oplus(x\gg 34)\oplus(x\gg 39)$
$\Sigma_1(x)=(x\gg 14)\oplus(x\gg 18)\oplus(x\gg 41)$
$Ch(x,y,z)=(x\wedge y)\oplus(\neg x\wedge z)$
$M_{aj}(x,y,z)=(x\wedge y)\oplus(x\wedge z)\oplus(y\wedge z)$

K[t] არის მუდმივები, რომლებიც მიღებულია პირველი 80 მარტივი რიცხვიდან.

- ჰეშის მნიშვნელობები განახლდება შეკუმშვის ციკლის შედეგებით:

$H_0=H_0+a,$
$H_1=H_1+b,$
$H_2=H_2+c,$
$H_3=H_3+d,$
$H_4=H_4+e,$
$H_5=H_5+f,$
$H_6=H_6+g,$
$H_7=H_7+h.$

ყველა ბლოკის დამუშავების შემდეგ მიიღება საბოლოო ჰეშის მნიშვნელობა: $H_0,H_1,H_2,H_3,H_4,H_5,H_6,H_7$.

მთლიანობა უზრუნველყოფს მონაცემებისა და ინფორმაციის სისრულესა და შეუცვლელობას მისი მიღების დროს. ეს მეტად მნიშვნელოვანია, როდესაც მომხმარებელი ახდენს ფაილების ჩამოტვირთვას ინტერნეტიდან ან სასამართლო ექსპერტი მოიძიებს დამამტკიცებელ საბუთებს ციფრულ მედიაში. ჰეშირების ალგორითმები ასევე გარდაქმნიან ნებისმიერი რაოდენობის მონაცემებს ფიქსირებული სიგრძის თითის ანაბეჭდად ან ციფრულ ჰეშ-დაიჯესტად.

ჰეშ-დაიჯესტის "გატეხვის" მიზნით, თავდამსხმელმა უნდა გამოიცნოს პაროლი. არსებობს ორი ყველაზე ცნობილი თავდასხმა, რომლებიც

გამოიყენება პაროლების გამოსაცნობად: ლექსიკონის (dictionary) და უხეში ძალის (brute-force) თავდასხმები.

ლექსიკონის თავდასხმა იყენებს საერთო სიტყვების, ფრაზებისა და პაროლების შემცველ ფაილს. ფაილში ჩაწერილია გამოთვლილი ჰეშები. თავდასხმა ადარებს ფაილში ჩაწერილ ჰეშებს პაროლის ჰეშს. მათი დამთხვევის შემთხვევაში, თავდამსხმელმა იცის ჯგუფის პაროლები.

უხეში ძალის (brute-force) თავდასხმა ცდილობს გამოთვალოს სიმბოლოთა ყველა შესაძლო კომბინაცია მოცემულ სიგრძეზე. უხეში ძალის შეტევა დიდ პროცესორულ რესურსს მოითხოვს, მაგრამ ეს დრო იხარჯება მხოლოდ პაროლის აღმოსაჩენად. პაროლები უნდა იყოს საკმარისად გრძელი იმისათვის, რომ უხეში ძალის თავდასხმას დასჭირდეს იმდენად დიდი დრო, რომ მისი გამოყენება გახდეს უაზრო.

5.2. ციფრული ხელმოწერა

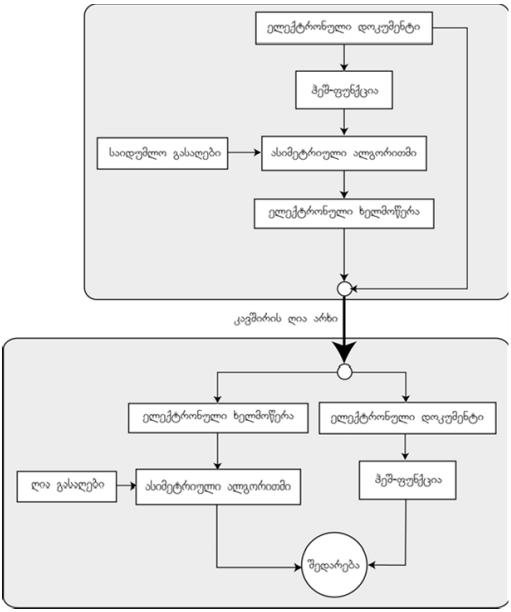
დაუცველი ციფრული დოკუმენტების შეცვლა ძალიან ადვილია. ციფრულ ხელმოწერას შეუძლია განსაზღვროს, მოხდა თუ არა დოკუმენტის რედაქტირება მომხმარებლის მიერ ხელის მოწერის შემდეგ. ციფრული ხელმოწერა არის მათემატიკური მეთოდი, რომელიც გამოიყენება შეტყობინების, ციფრული დოკუმენტის ან პროგრამული უზრუნველყოფის ნამდვილობისა და მთლიანობის შესამოწმებლად.

ბევრ ქვეყანაში ციფრულ ხელმოწერებს აქვთ იგივე სამართლებრივი მნიშვნელობა, როგორც ხელით ხელმოწერილ დოკუმენტებს. ხელმოწერები განმამტკიცებელია კონტრაქტების, მოლაპარაკებების ან ნებისმიერი სხვა დოკუმენტისთვის, რომელიც მოითხოვს ხელნაწერ ხელმოწერას. ხელმოწერის რეალიზაცია ხორციელდება დაშიფრვის ასიმეტრიული ალგორითმით, ოღონდ ამ შემთხვევაში ღიაა ის გასაღები, რომლითაც ხდება გაშიფრვა, ხოლო დახურულია დაშიფრვის გასაღები. იმისათვის, რომ ხელმოწერა მიბმული იყოს დოკუმენტზე, გამოიყენება დოკუმენტის ჰეშ-კოდი.

ელექტრონული დოკუმენტიდან ჰეშ-ფუნქციის გამოყენებით გენერირდება ჰეშ-კოდი, რომელიც საიდუმლო გასაღების

გამოყენებით დაშიფრვის ასიმეტრიული ალგორითმით იშიფრება და მიიღება ელექტრონული ხელმოწერა, რომელიც ებმება დოკუმენტს და იგზავნება ღია არხით ადრესატთან.

ციფრული ხელმოწერა შემდეგი სქემით ხორციელდება:



სურ. 5.1. ციფრული ხელმოწერის სქემა

ადრესატი გამოყოფს ციფრულ ხელმოწერას, ახდენს მის გაშიფრვას ღია გასაღების გამოყენებით და ადარებს დოკუმენტის ჰეშ კოდს. თუ ისინი არ დაემთხვა, ე.ი. დოკუმენტი ან გაყალბებულია, ან შეცდომებით გადმოიცა კავშირის არხის საშუალებით.

სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST) შეიმუშავა ციფრული ხელმოწერის სტანდარტი (DSS), რომელიც მოიცავს რამდენიმე განსხვავებულ ალგორითმს ციფრული ხელმოწერების გენერირებისა და გადამოწმებისთვის. NIST DSS დაფუძნებულია საჯარო გასაღების კრიპტოგრაფიის არქიტექტურაზე და იძლევა მითითებებს ალგორითმის პარამეტრების, გასაღების სიგრძისა და ციფრული ხელმოწერის პროცესის სხვა მნიშვნელოვანი

ასპექტების არჩევისთვის. NIST-ის მიერ შემუშავებული სამი ყველაზე ხშირად გამოყენებული ციფრული ხელმოწერის ალგორითმი არის RSA (Rivest-Shamir-Adleman), DSA (ციფრული ხელმოწერის ალგორითმი) და ECDSA (ელიპტური მრუდის ციფრული ხელმოწერის ალგორითმი). თითოეულ ალგორითმს აქვს თავისი ძლიერი და სუსტი მხარეები და NIST DSS იძლევა რეკომენდაციებს მათი სათანადო გამოყენებისთვის სხვადასხვა სცენარებში. ციფრული ხელმოწერების გამოყენება არა მხოლოდ უზრუნველყოფს ელექტრონული დოკუმენტების უსაფრთხოებას, არამედ უზრუნველყოფს უსაფრთხო კომუნიკაციას და ტრანზაქციებს სხვადასხვა სფეროში, მათ შორის ელექტრონული კომერცია, ფინანსები და სამთავრობო კავშირები. ციფრული ხელმოწერები მოითხოვს ორ ოპერაციას:

1. გასაღების გენერირება

2. გასაღების დამოწმება

ორივე ოპერაცია მოითხოვს გასაღების დაშიფვრასა და დეშიფრაციას.

DSA იყენებს დიდი რიცხვების ფაქტორიზაციას. მთავრობები იყენებენ DSA მეთოდს ციფრული ხელმოწერების შესაქმნელად. DSA არ სცილდება გზავნილის ციფრულ ხელმოწერის პროცესს.

RSA არის ყველაზე გავრცელებული საჯარო გასაღების კრიპტოგრაფიის ალგორითმი, რომელიც დღეისათვის გამოიყენება. RSA ატარებს ის პირების სახელებს, რომლებმაც ის 1977 წელს შექმნეს: რონ რივესტი, ადი შამირი და ლეონარდ ადლემანი. RSA მოიცავს ხელმოწერას და ასევე შიფრავს გზავნილის შინაარსს.

DSA უფრო სწრაფად ქმნის ხელმოწერის მომსახურების ციფრულ დოკუმენტს, ვიდრე RSA. RSA არის საუკეთესო იმ აპლიკაციებისათვის, რომლებიც მოითხოვენ ციფრულ ხელმოწერასა და გადამოწმებას ელექტრონული დოკუმენტების და გზავნილთა დაშიფვრისათვის.

კრიპტოგრაფიის უმეტესი სფეროების მსგავსად, RSA ალგორითმი ეფუძნება ორ მათემატიკურ პრინციპს: მოდულსა და მარტივ რიცხვთა ფაქტორიზაციას.

ECDSA არის უახლესი ციფრული ხელმოწერის ალგორითმი, რომელიც თანდათან ცვლის RSA-ს. უპირატესობა ამ ახალი ალგორითმისა არის ის, რომ მას შეუძლია გამოიყენოს ბევრად უფრო მცირე ზომის გასაღები

და უზრუნველყოს იგივე დონის უსაფრთხოება, ამასთან ის მოითხოვს ნაკლებ გამოთვლებს, ვიდრე RSA.

განვიხილოთ ელექტრონული ხელმოწერის სტანდარტი DSA. გასაღებების გენერაცია შემდეგნაირად ხორციელდება.

1. ვირევთ მარტივ რიცხვს q-ს, ისეთს, რომ $2159<q<2160$

2. ვირჩევთ t-ს ისეთს, რომ $0\le t\le 8$, და ვირჩევთ მარტივ რიცხვს

p-ს, ისეთს, რომ $2^{511+64t}<p<2^{512+64t}$, ამასთან q უნდა ყოფდეს $(p-1)$-ს

3. ვითვლით $g=h^{p-1/q} \bmod p$, სადაც h ნებისმიერი მთელი რიცხვია ისე, რომ $0<h<p$ და რომელიც აკმაყოფილებს პირობას $h^{p-1/q} \bmod p>1$.

საიდუმლო გასაღები x აირჩევა შუალედიდან $[1,q]$, ხოლო ღია გასაღები $y=g^x \bmod p$. ყველა მომხმარებლისათვის ქვეყნდება p, q, g და y.

ციფრული ხელმოწერის გენერირება ხდება შემდეგნაირად:

1. ვითვლით დოკუმენტის ჰეშ-კოდს $h=H(m)$

2. შუალედიდან $[1, q]$ შემთხვევით ვირჩევთ k-ს და ვითვლით

$$r=(g^k \bmod p) \bmod q.$$

3. ვითვლით $s=(k^{-1}(h+x*r)) \bmod q$, სადაც ელექტრონულ ხელმოწერას წარმოადგენს r და s.

მიღებული m დოკუმენტის და (r,s) ხელმოწერის შემოწმებისათვის:

1. ვამოწმებთ პირობას $0<r<q$ და $0<s<q$, და თუ ერთი მათგანი მაინც არ სრულდება ხელმოწერა ყალბია.

2. ვითვლით:

$$w=s1^{-1} \bmod q;\ u1=(H(m)*w) \bmod q;\ u2=((r/w) \bmod q;$$

$$v=((g^{u1}y^{u2}) \bmod p) \bmod q.$$

3. მოწმდება ტოლობა $v=r$. თუ ტოლობა სრულდება ელექტრონული ხელმოწერა მისაღებია.

მოცემულ ალგორითმში რეკომენდირებულია p-ს სიგრძე იყოს არა ნაკლებ 768 ბიტი. მაქსიმალური საიმედოობისათვის სასურველია 1024 ბიტის გამოყენება.

5.3 ციფრული სერტიფიკატები

დღევანდელ ციფრულ ეპოქაში უმთავრესია ინტერნეტის საშუალებით უსაფრთხო და ავთენტიფიცირებული კომუნიკაციის უზრუნველყოფა. ამ უსაფრთხოების მიღწევის ერთ-ერთი ფუნდამენტური ელემენტია ციფრული სერთიფიკატი.

ციფრული სერთიფიკატი არის კრიპტოგრაფიული დოკუმენტი, რომელიც ამოწმებს ერთეულის ავთენტურობას, როგორიცაა პირი, ორგანიზაცია ან მოწყობილობა, და ხელს უწყობს უსაფრთხო კომუნიკაციას. ისევე როგორც პასპორტი ამოწმებს პირის ვინაობას საერთაშორისო მოგზაურობისას, ციფრული სერთიფიკატი ადასტურებს ერთეულის ვინაობას ციფრულ სამყაროში.

ციფრული სერთიფიკატი შეიცავს რამდენიმე ძირითად ინფორმაციას:

- საჯარო გასაღები: ეს არის ერთეულის გასაღების წყვილის (საჯარო და პირადი გასაღები) საჯარო ნაწილი. იგი გამოიყენება დაშიფვრისა და ციფრული ხელმოწერებისთვის.

- სერთიფიკატის მფლობელის ინფორმაცია: დეტალები სუბიექტის შესახებ, ვისთვისაც გაიცემა სერტიფიკატი, როგორიცაა მათი სახელი, ორგანიზაცია და დომენის სახელი.

- სერტიფიკატის გამცემი ორგანოს (Certificate Authority) ინფორმაცია: დეტალები CA-ს შესახებ, რომელმაც გასცა სერთიფიკატი, ციფრული ხელმოწერის ჩათვლით.

- მოქმედების პერიოდი: ვადა, რომლის განმავლობაშიც სერტიფიკატი ითვლება ძალაში. ეს მოიცავს დაწყების თარიღს და ვადის გასვლის თარიღს.

- სერიული ნომერი: უნიკალური იდენტიფიკატორი, რომელიც მინიჭებულია CA-ს მიერ თითოეულ სერტიფიკატზე.

- ციფრული ხელმოწერა: CA-ს ციფრული ხელმოწერა, რომელიც აკავშირებს CA-ს იდენტურობას სერტიფიკატის მფლობელის საჯარო გასაღებთან, რაც უზრუნველყოფს სერტიფიკატის მთლიანობას და ავთენტურობას.

გაცემის პროცესში თავდაპირველად ხდება გასაღების წყვილის გენერაცია. ერთეული, რომელიც ითხოვს სერთიფიკატს, ქმნის გასაღების წყვილს, რომელიც შედგება საჯარო გასაღებისა და პირადი

გასაღებისგან. შემდეგ იგი ითხოვს სერტიფიკატის ხელმოწერას (CSR): ერთეული ქმნის CSR-ს, რომელიც მოიცავს მის საჯარო გასაღებს და საიდენტიფიკაციო ინფორმაციას და აგზავნის ამ მოთხოვნას CA-სთან. CA ამოწმებს მომთხოვნის ვინაობას. ეს შეიძლება მოიცავდეს ერთეულის დომენის საკუთრების, ორგანიზაციის დეტალების და სხვა შესაბამისი ინფორმაციის შემოწმებას. თუ დადასტურება წარმატებით დასრულდა, CA ხელს აწერს სერტიფიკატს მისი პირადი გასაღებით.

შემოწმების პროცესის შემთხვევაში (მაგ., ვებსაიტის უსაფრთხო კავშირის დროს), სერტიფიკატი ეგზავნება მხარეს, რომელსაც ესაჭიროება შემოწმება (მაგ., ვებ ბრაუზერი). მიმღები იყენებს CA-ს საჯარო გასაღებს სერტიფიკატზე CA-ს ციფრული ხელმოწერის გასაშიფრად და დასადასტურებლად. თუ გაშიფრული ხელმოწერა ემთხვევა მოსალოდნელ მნიშვნელობას და სერტიფიკატი მოქმედების პერიოდშია, სერტიფიკატი ჩაითვლება როგორც მოქმედი და სანდო.

არსებობს ციფრული სერთიფიკატების რამდენიმე ტიპი, რომელთაგან თითოეული ემსახურება კონკრეტულ მიზანს:

SSL/TLS სერთიფიკატები: გამოიყენება ვებ ბრაუზერსა და ვებ სერვერს შორის კომუნიკაციის უზრუნველსაყოფად, რაც უზრუნველყოფს მონაცემთა კონფიდენციალურობას და მთლიანობას. ისინი გამოდიან სამი ვალიდაციის დონეზე:

- ✓ DV (დომენის დადასტურება): ადასტურებს დომენზე კონტროლს.
- ✓ OV (ორგანიზაციის ვალიდაცია): მოიცავს დამატებით ორგანიზაციული იდენტურობის შემოწმებას.
- ✓ EV (გაფართოებული ვალიდაცია): გთავაზობთ ვალიდაციის უმაღლეს დონეს, უზრუნველყოფს ვიზუალური ნდობის ინდიკატორებს, როგორიცაა მწვანე მისამართის ზოლი ბრაუზერებში.

კოდის ხელმოწერის სერთიფიკატები: საშუალებას აძლევს პროგრამული უზრუნველყოფის შემქმნელებს ხელი მოაწერონ თავიანთ კოდს და პროგრამულ უზრუნველყოფას, რაც უზრუნველყოფს მის ავთენტურობას და მთლიანობას მომხმარებლებისთვის.

ელ.ფოსტის სერთიფიკატები (S/MIME სერთიფიკატები): ელ.ფოსტის დაცვა, რაც საშუალებას აძლევს მომხმარებლებს დაშიფრონ და ციფრულად მოაწერონ ხელი მათ ელექტრონულ წერილებს.

კლიენტის სერთიფიკატები: კლიენტების (მომხმარებლების ან მოწყობილობების) ავთენტიფიკაცია სერვერებზე, სერვისებსა და რესურსებზე უსაფრთხო წვდომის უზრუნველსაყოფად.

ციფრული სერთიფიკატები მომხმარებლებს სთავაზობს უამრავ სარგებელს. უსაფრთხოება - ისინი ხელს უწყობენ მონაცემთა დაშიფვრას, იცავენ არაავტორიზებული წვდომისგან და უზრუნველყოფენ კონფიდენციალურობას. ავთენტიფიკაცია - ისინი ამოწმებენ კომუნიკაციაში ჩართული პირების იდენტურობას, ხელს უშლიან მსგავსებას და თაღლითობას. მონაცემთა მთლიანობა - ისინი უზრუნველყოფენ, რომ მონაცემები არ შეცვლილა გადაცემის დროს. ნდობა - სანდო CA-ების მიერ გაცემული სერთიფიკატები აღიარებულია ბრაუზერებისა და ოპერაციული სისტემების მიერ, რაც ქმნის ნდობის ჯაჭვს.

ციფრული სერთიფიკატების ერთ-ერთი ყველაზე გავრცელებული პროგრამაა HTTPS-ის საშუალებით ვებ ტრაფიკის დაცვა. როდესაც მომხმარებელი ეწვევა HTTPS-ზე ჩართული ვებსაიტს, მისი ბრაუზერი დაიბრუნებს საიტის SSL/TLS სერთიფიკატს. შემდეგ ბრაუზერი ამოწმებს ამ სერტიფიკატს CA-ს საჯარო გასაღების გამოყენებით. წარმატებული გადამოწმების შემდეგ იქმნება დაშიფრული კავშირი, რომელიც უზრუნველყოფს უსაფრთხო კომუნიკაციას ბრაუზერსა და ვებ სერვერს შორის.

ციფრული სერთიფიკატები თანამედროვე ციფრული უსაფრთხოების ინფრასტრუქტურის ფუნდამენტური ელემენტებია. ისინი უზრუნველყოფენ საიმედო მექანიზმს ნდობის დასამყარებლად და უსაფრთხო კომუნიკაციის უზრუნველსაყოფად მზარდ ციფრულ სამყაროში. საჯარო გასაღების ინფრასტრუქტურის (PKI) და სერტიფიკატის ორგანოებისადმი ნდობის გამოყენებით, ციფრული სერთიფიკატები იძლევა უსაფრთხო ონლაინ აქტივობების ფართო სპექტრს, ვებსაიტების დათვალიერებიდან და ელფოსტის გაგზავნიდან პროგრამული უზრუნველყოფის ჩამოტვირთვამდე და უსაფრთხო ქსელებზე წვდომამდე.

სერტიფიკატის მართვა და გაუქმება

ციფრული სერტიფიკატის სიცოცხლის ციკლი მოიცავს მის გაცემას, მართვას და პოტენციურ გაუქმებას. ამ პროცესების გაგება გადამწყვეტია ციფრული კომუნიკაციებისა და ტრანზაქციების უსაფრთხოებისა და მთლიანობის შესანარჩუნებლად.

ციფრული სერთიფიკატების სათანადო მართვა აუცილებელია მათი მუდმივი მოქმედების და უსაფრთხოების უზრუნველსაყოფად მათი სიცოცხლის ციკლის განმავლობაში. გაცემის შემდეგ, ციფრული სერთიფიკატი უნდა იყოს დაინსტალირებული ერთეულის სერვერებზე, მოწყობილობებზე ან აპლიკაციებზე. სათანადო კონფიგურაცია უზრუნველყოფს სერტიფიკატის სწორად გამოყენებას უსაფრთხო კომუნიკაციისთვის.

ციფრულ სერთიფიკატებს აქვთ განსაზღვრული მოქმედების ვადა. სუბიექტებმა უნდა განაახლონ თავიანთი სერთიფიკატები ვადის გასვლამდე, რათა თავიდან აიცილონ შეფერხებები უსაფრთხო კომუნიკაციებში. განახლების პროცესი, როგორც წესი, მოიცავს ახალი CSR-ის გენერირებას და ხელახლა შემოწმებას.

ციფრულ სერტიფიკატთან დაკავშირებული პირადი გასაღები უსაფრთხოდ უნდა იყოს შენახული და მართული. თუ პირადი გასაღები დაზიანებულია, სერთიფიკატის უსაფრთხოებაც ირღვევა. ძირითადი მართვის პრაქტიკა მოიცავს ტექნიკის უსაფრთხოების მოდულების (HSM) გამოყენებას და გასაღების როტაციის პოლიტიკის განხორციელებას.

სერთიფიკატის გაუქმება არის ციფრული სერტიფიკატის ბათილობის პროცესი მისი ვადის გასვლამდე. ეს შეიძლება მოხდეს რამდენიმე მიზეზის გამო, მათ შორის ძირითადი კომპრომისის, საკუთრების ცვლილების ან ასოცირებული სერვისის შეწყვეტის გამო. გაუქმების მიზეზი შეიძლება გახდეს:

- თუ პირადი გასაღები გატეხილია, სერთიფიკატი უნდა გაუქმდეს არაავტორიზებული გამოყენების თავიდან ასაცილებლად.

- თუ სერტიფიკატში არსებული ინფორმაცია (მაგ. დომენის სახელი, ორგანიზაციის დეტალები) იცვლება, სერტიფიკატი უნდა გაუქმდეს და ხელახლა გაიცეს განახლებული ინფორმაციით.

- თუ სერტიფიკატთან დაკავშირებული სერვისი აღარ არის ხელმისაწვდომი, სერთიფიკატი უნდა გაუქმდეს.

- გაუქმებულია სერთიფიკატების სია CRL, რომელიც გამოქვეყნებულია CA-ს მიერ. სუბიექტებს შეუძლიათ შეამოწმონ ეს სია, რათა დადგინდეს, გაუქმდა თუ არა სერტიფიკატი. ონლაინ სერტიფიკატის სტატუსის პროტოკოლი (OCSP), რომელიც გამოიყენება სერტიფიკატის გაუქმების სტატუსის მისაღებად. ის საშუალებას აძლევს ერთეულებს რეალურ დროში მიმართონ CA-ს, რათა შეამოწმონ სერტიფიკატის მოქმედების ვადა.

ციფრული სერთიფიკატების უსაფრთხოება ეყრდნობა საჯარო გასაღების კრიპტოგრაფიას, ციფრულ ხელმოწერებს და ჰეშის ფუნქციებს.

გასაღების გენერაცია ხორციელდება შემდეგი ფორმულის საშუალებით:

$$(K_{pub},K_{priv})=KeyGen(1^n)$$

სადაც, n არის უსაფრთხოების პარამეტრი, რომელიც მიუთითებს გასაღების ზომას.

ციფრული ხელმოწერის სქემები უზრუნველყოფს შეტყობინების ავთენტურობას და მთლიანობას. იგი შედგება სამი ალგორითმისგან: გასაღების გენერაცია, ხელმოწერა და გადამოწმება.

ხელმოწერა - σ=Sign(K_{priv},M), სადაც σ არის ხელმოწერა და M - შეტყობინება.

ვალიდაცია - $Verify(K_{pub},M,\sigma)\rightarrow\{true,false\}$, ალგორითმი იღებს ჭეშმარიტ მნიშვნელობას, თუ ხელმოწერა სწორია და მცდარს სხვა შემთხვევაში.

ხემნოწერა ციფრულ სერტიფიკატზე, შემდეგნაირად ჩაიწერება:

$$Cert=(V,S,K_{pub},CA,sig_{CA})$$

სადაც, V - ვალიდაციის პერიოდია (T_{start},T_{end}), S - ინფორმაცია სუბიექტის შესახებ (სახელი, ორგანიზაცია და სხვა), K_{pub} - სუბიექტის საჯარო გასაღები, CA - სერტიფიკატის გამცემი ორგანო (Certificate Authority).

5.4 მონაცემთა ბაზის მთლიანობა

მონაცემთა ბაზები უზრუნველყოფენ მონაცემთა შენახვის, მოძიებისა და ანალიზის ეფექტურ საშუალებას. მონაცემთა შეგროვებასა და ზრდასთან ერთად ისინი უფრო მგრძნობიარენი ხდებიან თავდასხმის მიმართ, ამიტომ კიბერუსაფრთხოების სპეციალისტებისთვის მეტად მნიშვნელოვან ფუნქციას იძენს მონაცემთა ბაზების მზარდი რაოდენობის დაცვა. მონაცემთა მთლიანობა მოიცავს მონაცემთა ბაზაში შენახული მონაცემების სიზუსტეს, თანმიმდევრულობასა და საიმედოობას. პასუხისმგებლობა მონაცემთა მთლიანობაზე ეკისრებათ მონაცემთა ბაზის დიზაინერებს, დეველოპერებს და ორგანიზაციის მართვის გუნდს.

არსებობს მონაცემთა მთლიანობის ოთხი წესი ან შეზღუდვა:

- ობიექტის მთლიანობა: ყველა რიგს უნდა გააჩნდეს უნიკალური იდენტიფიკატორი, რომელსაც ეწოდება პირველადი გასაღები.
- დომენის მთლიანობა: სვეტში შენახული ყველა მონაცემი უნდა ემორჩილებოდეს ერთსა და იმავე ფორმატს.
- ბმულის მთლიანობა: ცხრილის ურთიერთობები უნდა დარჩეს თანმიმდევრული. აქედან გამომდინარე, მომხმარებელს არ შეუძლია ცხრილში წაშალოს ჩანაწერი, რომელიც დაკავშირებულია მეორე ცხრილთან.
- მომხმარებლის მიერ განსაზღვრული მთლიანობა: მომხმარებლის მიერ განსაზღვრული წესების კომპლექტი, რომელიც არ მიეკუთვნება რომელიმე სხვა კატეგორიას. მაგალითად, მომხმარებელი განათავსებს ცხრილში ახალ შეკვეთას, იგი თავდაპირველად ამოწმებს, არის თუ ეს ახალი კლიენტი. თუ ახალია, მომხმარებელი ამატებს ახალ კლიენტს კლიენტთა ცხრილში.

მონაცემთა შეტანა მოიცავს სისტემაში გარკვეული ტიპის ინფორმაციის შეტანას. მართვა უზრუნველყოფს მომხმარებელთა მიერ სწორი მონაცემების შეტანას. მონაცემთა მთლიანობის მიღწევის ერთ-ერთი მთავარი მეთოდი არის ვალიდაციის წესების დანერგვა. ვალიდაციის წესი ამოწმებს, რომ მონაცემები განეკუთვნება მონაცემთა ბაზის დიზაინერის მიერ განსაზღვრულ პარამეტრებს. ვალიდაციის

წესი ხელს უწყობს მონაცემების სისრულის, სიზუსტისა და თანმიმდევრულობის დაცვას. კრიტერიუმები, რომლებიც გამოიყენება ვალიდაციის წესებისთვის, მოიცავენ შემდეგს:

- ზომა — ამოწმებს სიმბოლოების რაოდენობას მონაცემებში;
- ფორმატი — ამოწმებს შეტანილი მონაცემების შესაბამისობას მითითებულ ფორმატთან;
- თანმიმდევრულობა — ამოწმებს კოდების თანმიმდევრულობას დაკავშირებულ მონაცემთა ელემენტებში;
- დიაპაზონი — ამოწმებს, რომ მონაცემები შეტანილია დაშვებული მინიმალური და მაქსიმალური მნიშვნელობით;
- ციფრების შემოწმება - ითვალისწინებს დამატებით გაანგარიშებას შეცდომის გამოვლენისთვის შემოწმების ციფრის გენერირებისათვის;

მონაცემთა ტიპის დადასტურება არის მარტივი მონაცემების დადასტურება და ამოწმებს, რომ მომხმარებლის მიერ შეტანილი მონაცემები შეესაბამება მოსალოდნელი სიმბოლოების ტიპს. მაგალითად, ტელეფონის ნომერი არ უნდა შეიცავდეს ალფა სიმბოლოებს.

მონაცემთა ბაზის მთლიანობის მართვის ერთ-ერთი ყველაზე დაუცველი ასპექტია მონაცემთა შეტანის პროცესის მართვა. მრავალი ცნობილი თავდასხმა აწარმოებს მონაცემთა ბაზის წინააღმდეგ ქმედებას, არასწორი ინფორმაციის შეტანით. თავდამსხმელს შეუძლია დააზიანოს, აურიოს ან გამოამჟღავნოს აპლიკაცია დიდი რაოდენობის ინფორმაციის შეტანით. თავდამსხმელები იყენებენ ავტომატური შეტანის შეტევებს. მაგ., მომხმარებლები ავსებენ ფორმას ვებ აპლიკაციის საშუალებით, რათა გამოიწეროთ საინფორმაციო ბიულეტენი. მონაცემთა ბაზის აპლიკაცია ავტომატურად ქმნის და აგზავნის ელ. ფოსტის დადასტურებას. როდესაც მომხმარებლები მიიღებენ ელ. ფოსტის დადასტურებას URL-ის ბმულით, რათა დაადასტურონ მათი გამოწერა, თავდამსხმელები ცვლიან ამ URL ბმულს. ეს ცვლილებები მოიცავს მომხმარებლის სახელის, ელექტრონული ფოსტის მისამართის ან გამოწერის სტატუსის შეცვლას. ელ. ფოსტა ბრუნდება სერვერზე, რომელზეც განთავსებულია

აპლიკაცია. თუ სერვერზე არ გადამოწმდა, რომ ელექტრონული ფოსტის მისამართი ან სხვა ანგარიშის ინფორმაცია შეესაბამება ხელმოწერილ ინფორმაციას, სერვერი მიიღებს ყალბ ინფორმაციას. ჰაკერებს შეუძლიათ თავდასხმათა ავტომატიზირება საინფორმაციო ბიულეტენების ბაზაში ათასობით ვებ განაცხადის გაგზავნით.

მონაცემების ნიმუშების იდენტიფიცირებას, რომლებიც არ შეესაბამება მოსალოდნელ ქცევას ანომალიის გამოვლენას უწოდებენ. ეს შეუსაბამო ნიმუშები წარმოადგენენ ანომალიებს, გამონაკლისებს, გადახრებს, ან სხვა ტიპის არასასურველ მონაცემებს. ანომალიის გამოვლენა და შემოწმება წარმოადგენს მეტად მნიშვნელოვან კონტროლონისძიებას ან დაცვას თაღლითობის გამოვლენის პროცესში. ანომალიის შემოწმება მოითხოვს მონაცემთა გადამოწმებას ან ცვლილებებს, როდესაც სისტემა აღმოაჩენს და ჩათვლის უჩვეულოდ.

მონაცემთა ბაზა წარმოადგენს ელექტრონული შეტანის სისტემას. სათანადო შეტანის მხარდაჭერა კრიტიკულად მნიშვნელოვანია მონაცემთა ბაზაში არსებული მონაცემების სანდოობისა და სარგებლობის შენარჩუნებაში. ცხრილები, ჩანაწერები, ველები და მონაცემები თითოეულ ველში ქმნიან მონაცემთა ბაზას. მონაცემთა ბაზის შეტანის სისტემის მთლიანობის შენარჩუნების მიზნით, მომხმარებლებმა უნდა დაიცვან გარკვეული წესები. ობიექტის მთლიანობა არის მთლიანობის წესი, რომელშიც ნათქვამია, რომ ყველა ცხრილს უნდა ჰქონდეს პირველადი გასაღები და რომ ძირითადი გასაღების არჩეული სვეტი ან სვეტები უნდა იყვნენ უნიკალურები და არ შეიცავდნენ “Null” მნიშვნელობის. “Null” მონაცემთა ბაზაში ნიშნავს დაკარგულ ან უცნობ ღირებულებებს.

ყველა ელემენტი სვეტში უნდა აკმაყოფილებდეს განსაზღვრულ ვალიდურ წესებს. თითოეულ სვეტს გააჩნია განსაზღვრული ღირებულებების კომპლექტი, როგორიცაა საკრედიტო ბარათის ნომრები, სოციალური დაცვის ნომრები ან ელექტრონული ფოსტის მისამართები. ამ სვეტის მაგალითზე მინიჭებული ღირებულების მკაცრი დაცვა (ატრიბუტი) აღასრულებს დომენის მთლიანობას. დომენის მთლიანობის აღსრულება შეიძლება ისეთივე მარტივი იყოს, როგორც სვეტის სწორი მონაცემების ტიპის, სიგრძისა და ფორმატის არჩევა.

თავი 6. ხუთი ცხრიანის კონცეფცია

6.1 მაღალი ხელმისაწვდომობა

ხუთი ცხრა, ასევე ცნობილი როგორც მაღალი ხელმისაწვდომობა, ეხება სტანდარტს გამოთვლითი სისტემებისა და ქსელების ოპერაციული მუშაობისთვის, სადაც ხელმისაწვდომობა იზომება 99,999%-ით. ხუთი ცხრიანი ნიშნავს, რომ სისტემები და მომსახურება ხელმისაწვდომია 99.999% დროის განმავლობაში, რაც ნიშნავს მაქსიმალურ შეფერხებას წელიწადში დაახლოებით 5,26 წუთის განმავლობაში. მაღალი ხელმისაწვდომობა ეხება სისტემას ან კომპონენტს, რომელიც მუდმივად ფუნქციონირებს მოცემული დროის განმავლობაში და მის უზრუნველსაყოფად საჭიროა: ერთეული მტყუნებების აღმოფხვრა; საიმედოობის გეგმის შემუშავება; მტყუნებათა სწრაფი გამოვლენა მათი მოხდენის შემთხვევაში. სისტემის ხელმისაწვდომობა გამოითვლება შემდეგი ფორმულით:

$$\textit{ხელმისაწვდომობა} = \left(\frac{\textit{მთლიანი მუშაობის დრო}}{\textit{მთლ. მუშაობის დრო} + \textit{მთლ. შეფერხების დრო}}\right) \times 100$$

ხუთი ცხრისთვის:

$$\textit{ხელმისაწვდომობა} = 99.999\%$$

შესაბამისად მთლიანი შეფერხების დრო წელიწადში ტოლია:

$$\textit{მთლ. შეფერხების დრო} \approx \frac{0{,}001}{100} \times 365 \times 24 \times 60 \approx 5{,}26 \textit{წთ.}$$

მიუხედავად იმისა, რომ მაღალი ხელმისაწვდომობის შენარჩუნების ღირებულება შეიძლება ძალიან ძვირი იყოს ზოგიერთი ინდუსტრიისთვის, უმნიშვნელოვანესია მან შეინარჩუნოს მაღალი ხელმისაწვდომობა მომხმარებელთა ნდობისთვის, რადგან საზოგადოება მოელის, რომ საინფორმაციო მედია ინდუსტრია მიაწვდის მას ინფორმაციას მოვლენების შესახებ დაუყოვნებლივ, მისი მოხდენისთანავე 24/7-ზე.

მაღალი ხელმისაწვდომობა აერთიანებს სამ ძირითად პრინციპს მონაცემებისა და მომსახურების უწყვეტი ხელმისაწვდომობის მიზნის მისაღწევად:

1. მარცხის ერთჯერადი წერტილების აღმოფხვრა ან შემცირება

2. სისტემის მდგრადობა

3. მტყუნებების მიმართ მედეგობა

მნიშვნელოვანია იმის გააზრება, თუ როგორ უნდა აღმოიფხვრას მარცხის ცალკეული წერტილები. წარუმატებლობის რომელიმე ერთეული წერტილი შეიძლება მოიცავდეს ცენტრალურ მარშრუტიზატორებს ან კონცენტრატორებს, ქსელის მომსახურებას და მაღალკვალიფიციურ IT პერსონალს. მთავარი ის არის, რომ სისტემის, პროცესის, ან პერსონის მტყუნებამ შეიძლება დამანგრეველი გავლენა იქონიოს მთელ სისტემაზე. მთავარია მოხდეს პროცესების, რესურსებისა და კომპონენტების მართვა ისეთნაირად, რომ მაქსიმალურად იქნას შემცირებული მარცხის ალბათობა ცალკეულ წერტილებზე. მაღალი ხელმისაწვდომობის კლასტერები არის ერთ-ერთი გზა ამის უზრუნველსაყოფად. ეს კლასტერი წარმოადგენს კომპიუტერების ჯგუფს, რომლებსაც აქვთ წვდომა იმავე საზიარო საცავში და აქვთ იდენტური ქსელის კონფიგურაციები. ყველა სერვერი ერთდროულად მონაწილეობს მომსახურების დამუშავებაში. გარედან ისე ჩანს, რომ, სერვერთა ჯგუფი ფუნქციონირებს, როგორც ერთი მოწყობილობა. თუ კლასტერში მწყობრიდან გამოვა რომელიმე სერვერი, სხვა სერვერები განაგრძობენ იმავე სერვისის დამუშავებას, შეუმჩნევლად შეცვლიან რა დაზიანებულ მოწყობილობას.

სისტემების მდგრადობა ეხება მონაცემთა ხელმისაწვდომობისა და ოპერატიული დამუშავების შესაძლებლობას თავდასხმების ან რაიმე მოვლენის დარღვევის მიუხედავად. ზოგადად, ეს მოითხოვს ჭარბ სისტემებს, რაც ნიშნავს, რომ ერთი სისტემის მტყუნების შემთხვევაში მეორე სისტემა დაუყოვნებლად იწყებს მის მიერ შესასრულებელი სამუშაოს განხორციელებას. სისტემის მდგრადობა უფრო მეტია, ვიდრე უბრალოდ მოწყობილობების გაძლიერება; ის მოითხოვს, რომ როგორც მონაცემები, ასევე მომსახურება ხელმისაწვდომი იყოს მაშინაც კი, როდესაც სისტემა განიცდის თავდასხმას.

მტყუნებამედეგობა საშუალებას აძლევს სისტემას განაგრძოს ფუნქციონირება მაშინაც კი, თუ ერთი ან მეტი კომპონენტი გამოდის მწყობრიდან. მონაცემთა „სარკისებური ანარეკლი“ (mirroring) არის მტყუნებამედეგობის ერთ-ერთი მაგალითი. თუ „მტყუნება“ მოხდება, რაც გამოიწვევს მოწყობილობის დაზიანებას, სარკისებური სისტემა

უზრუნველყოფს მოთხოვნილი მონაცემების დამუშავებას, რაც დარჩება შეუმჩნეველი მომხმარებლისათვის.

6.2. ზომები ხელმისაწვდომობის გასაუმჯობესებლად. აქტივების მართვა

ორგანიზაციას ესაჭიროება იცოდეს, რა აპარატურა და პროგრამული უზრუნველყოფა წარმოადგენს წინაპირობას იმის შესახებ, თუ რა კონფიგურაციის პარამეტრები უნდა იყოს გათვალისწინებული. აქტივების მართვა მოიცავს აპარატურისა და პროგრამული უზრუნველყოფის სრულ ინვენტარიზაციას. ეს ნიშნავს, რომ ორგანიზაციამ უნდა იცოდეს თითოეული კომპონენტი, რომელიც შეიძლება დაექვემდებაროს უსაფრთხოების რისკებს, მათ შორის:

- ყველა აპარატურა და აპარატურული სისტემა
- ყველა ოპერაციული სისტემა
- ყველა აპარატურული ქსელის მოწყობილობა და მათი ოპერაციული სისტემა
- ყველა პროგრამული უზრუნველყოფა
- ყველა პირადი ბიბლიოთეკა

ორგანიზაციას შეუძლია აირჩიოს ავტომატური გადაწყვეტები აქტივების მონიტორინგისათვის. აქტივების კლასიფიკაცია ენიჭება ორგანიზაციის ყველა რესურს ჯგუფს, რომელიც დაფუძნებულია საერთო მახასიათებლებზე. ორგანიზაციამ აქტივების კლასიფიკაციის სისტემა შეიძლება გამოიყენოს დოკუმენტებთან, მონაცემთა ჩანაწერებთან, მონაცემთა ფაილებთან და დისკებთან. ყველაზე კრიტიკულ ინფორმაციას უნდა ჰქონდეს დაცვის უმაღლესი დონე და ასევე შეიძლება მოითხოვდეს სპეციალურ დამუშავებას.

ორგანიზაციამ შეიძლება გამოიყენოს მარკირების სისტემა იმისდა მიხედვით, თუ როგორი ფასეულია, როგორი მგრძნობიარეა და რამდენად კრიტიკულია ინფორმაცია. ცხრილი 6.1-ში ნაჩვენებია დეტალურ ინფორმაცია ორგანიზაციის აქტივების იდენტიფიკაციისა და კლასიფიკაციისთვის.

ცხრილი 6.1.

I ეტაპი: აქტივის იდენტიფიცირება	**II ეტაპი: აქტივის ანგარიშვალდებულება**
ინფორმაციული აქტივები; *პროგრამული აქტივები;* *ფიზიკური აქტივები;* *სერვისები.*	*ყველა ინფორმაციული აქტივის მფლობელის განსაზღვრა;* *ყველა პროგრამული აპლიკაციის მფლობელის განსაზღვრა.*
III ეტაპი: კლასიფიკაციის სქემის კრიტერიუმები	**IV ეტაპი: კლასიფიკაციის სქემა**
კონფიდენციალურობა; *მნიშვნელობა;* *დრო;* *წვდომის კონტროლი;* *განადგურება.*	*ერთიანი დაცვის უზრუნველყოფისთვის ინფორმაციის იდენტიფიკაციის ერთიანი მეთოდის მიღება.*

აქტივების მართვა მონიტორინგს უწევს ტექნოლოგიური აქტივების ციკლსა და ინვენტარს, მოწყობილობებისა და პროგრამული უზრუნველყოფის ჩათვლით. როგორც IT აქტივების მართვის სისტემის ნაწილი, ორგანიზაცია განსაზღვრავს მისაღებ IT აქტივებს, რომლებიც აკმაყოფილებენ მის მიზნებს. ეს პრაქტიკა ეფექტურად ამცირებს სხვადასხვა აქტივების ტიპებს. მაგ., ორგანიზაცია აინსტალირებს მხოლოდ იმ აპლიკაციებს, რომლებიც აკმაყოფილებენ მის მითითებებს. როდესაც ადმინისტრატორები შლიან პროგრამებს, რომლებიც არ აკმაყოფილებენ სახელმძღვანელო პრინციპებს, შედეგად ეფექტურად იზრდება უსაფრთხოების დონე.

აქტივების სტანდარტები განსაზღვრავენ სპეციფიურ აპარატურულ და პროგრამულ პროდუქტებს, რომლებსაც ორგანიზაცია იყენებს და ახდენს მათ მხარდაჭერას. მტყუნების მოხდენისას, სწრაფი ქმედება ხელს უწყობს როგორც ხელმისაწვდომობის შენარჩუნებას, ასევე უსაფრთხოებას. თუ ორგანიზაცია არ ახდენს ტექნიკის შერჩევის სტანდარტიზაციას, პერსონალმა შესაძლოა ზუსტად ვერ მოიძიოს ჩასანაცვლებელი კომპონენტი. არასტანდარტული გარემო მოითხოვს უფრო მეტ ექსპერტულ ცოდნას, რაც ზრდის მომსახურების კონტრაქტებისა და ინვენტარის ღირებულებას. ორგანიზაციამ უნდა გაავრცელოს აქტივების კლასიფიკაციის სისტემა დოკუმენტებზე, მონაცემთა ჩანაწერებზე, მონაცემთა ფაილებსა და დისკებზე. ყველაზე კრიტიკულად მნიშვნელოვანმა ინფორმაციამ უნდა მიიღოს უმაღლესი დონის დაცვა და ასევე შესაძლოა მოთხოვნილ იქნას სპეციალური დამუშავება. ორგანიზაციას შეუძლია მიიღოს ეტიკეტირების სისტემა

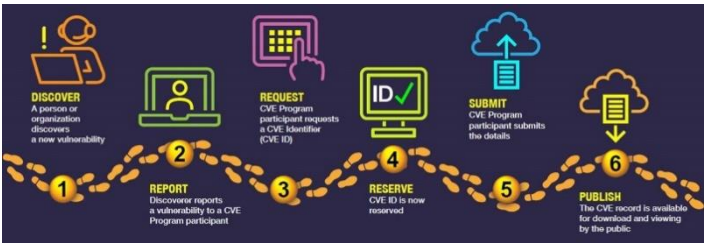
იმის მიხედვით, თუ რამდენად ღირებული, რამდენად მგრძნობიარეა და რამდენად კრიტიკულად მნიშვნელოვანია ინფორმაცია. მაგ., აშშ-ის მთავრობა ახდენს მონაცემების სენსიტიურობის კლასიფიცირებას შემდეგნაირად: ზესაიდუმლო; საიდუმლო; კონფიდენციალური; საზოგადოების ნდობა; და არაკლასიფიცირებული.

საერთო დაუცველობები და ექსპოზიციები (CVE - Common Vulnerabilities and Exposures) არის ცნობილი უსაფრთხოების დაუცველობის კატალოგი პროგრამულ და აპარატურულ სისტემებში. CVE სისტემა უზრუნველყოფს სტანდარტიზებულ მეთოდს მოწყვლადობის იდენტიფიცირებისა და განხილვისთვის, ეხმარება ორგანიზაციებს პრიორიტეტების განსაზღვრაში და უსაფრთხოების რისკების მოგვარებაში. CVE სისტემა ანიჭებს უნიკალურ იდენტიფიკატორებს საჯაროდ ცნობილ უსაფრთხოების ხარვეზებს. მისი CVE-ის ძირითადი კომპონენტებია:
- CVE იდენტიფიკატორი: უნიკალური ალფანუმერული სტრიქონი, რომელიც მინიჭებულია კონკრეტულ დაუცველობაზე. ფორმატი შემდეგნაირად არის წარმოდგენილი CVE-[Year]-[Number], მაგ., CVE-2024-34527.

- CVE აღწერა: დაუცველობის მოკლე მიმოხილვა, მისი ბუნებისა და პოტენციური ზემოქმედების ჩათვლით.

- მითითებები: დამატებითი ინფორმაციის ბმულები, როგორიცაა უსაფრთხოების რჩევები, დაუცველობის მონაცემთა ბაზები და სხვა.

CVE სიაში თითოეული დაუცველობისთვის არის ერთი CVE ჩანაწერი. თავდაპირველად ხდება დაუცველობის აღმოჩენა და შემდეგ ის ეცნობება CVE პროგრამას. მომხსენებელი ითხოვს CVE ID-ს, რომელიც შემდეგ დარეგისტრირდება აღნიშნული დაუცველობისთვის. როგორც კი მოხსენებული დაუცველობა დადასტურდება CVE ჩანაწერისთვის მინიმალური საჭირო მონაცემთა ელემენტების განსაზღვრით, ჩანაწერი გამოქვეყნდება CVE სიაში, და მოიცავს ისეთ დეტალებს, როგორიცაა დაზარალებული ან დაფიქსირებული პროდუქტის ვერსიები; დაუცველობის ტიპი, ძირეული მიზეზი ან გავლენა და სხვა. ბოლოს CVE ჩანაწერები გამოქვეყნდება CVE პროგრამის პარტნიორების მიერ მთელს მსოფლიოში. ეს პროცესი აღწერილია სურ. 6.1-ზე მოცემულია აღნიშნული პროცესის სასიცოცხლო ციკლი.



სურ. 6.1. CVE ჩანაწერის სიცოცხლის ციკლი

<u>რისკების ანალიზი</u>

რისკების ანალიზი წარმოადგენს ორგანიზაციის აქტივების მიმართ ბუნებრივი და ადამიანის მიერ გამოწვეული მოვლენების საფრთხეების ანალიზის პროცესს. მომხმარებელი ასრულებს აქტივის იდენტიფიკაციას დასაცავი აქტივების განსასაზღვრად. რისკების ანალიზს აქვს ოთხი მიზანი:

- აქტივების იდენტიფიცირება და მათი ღირებულება;

- მოწყვლადობისა და საფრთხეების იდენტიფიცირება;

- გამოვლენილი საფრთხეების ალბათობისა და გავლენის განსაზღვრა;

- გავლენის საფრთხის ღირებულებისა და კონტრზომების დაბალანსება.

არსებობს რისკის ანალიზის ორი მიდგომა. რაოდენობრივი რისკების ანალიზი, რომელიც ანიჭებს ნომრებს რისკის ანალიზის პროცესში და ხარისხობრივი რისკის ანალიზი, რომელიც იყენებს მოსაზრებებს და სცენარებს (გათვლებს).

რისკის ანალიზი	
ხარისხობრივი	რაოდენობრივი
რისკის რეგისტრაცია; რისკის კატეგორიზაცია; ექსპერტის გადაწყვეტილება; ალბათობის ზემოქმედების (PI-Probability-Impact) მატრიცა.	სენსიტიურობის ანალიზი გადაწყვეტილების ხის ანალიზი; სცენარის ანალიზი; სიმულაცია.

გუნდი აფასებს თითოეულ აქტივის საფრთხეს, გაწერს მათ ცხრილში და შედეგებს იყენებს როგორც გარკვეულ სახელმძღვანელოს.

მრავალი სახის ტექნიკური კონტროლი, მათ შორის ავტორიზაციის სისტემები, ფაილური ნებართვები და დამცავი ეკრანები, ამცირებს რისკს. რისკის შერბილება გულისხმობს დანაკარგის სიმძიმის ან დანაკარგის მოხდენის ალბათობის შემცირებას.

ორგანიზაციის და უსაფრთხოების პროფესიონალებმა უნდა გაიაზრონ, რომ რისკის შემარბილებელ ქმედებას შეიძლება ჰქონდეს როგორც დადებითი, ასევე უარყოფითი ზეგავლენა ორგანიზაციაზე. რისკის შემსუბუქების სათანადო მიდგომაა, იპოვოს ბალანსი კონტრზომებსა და მის მიერ გამოწვეულ უარყოფით ზემოქმედებას და რისკის შემცირების სარგებელს შორის. არსებობს რისკის შემცირების/შერბილების ოთხი ძირითადი გზა:

1. რისკის მიღება და მისი პერიოდულად ხელახლა შეფასება;
2. რისკის შემცირება კონტროლის განხორციელების გზით;
3. რისკის სრულად თავიდან აცილება მიდგომების ტოტალური შეცვლით;
4. რისკის გადატანა მესამე მხარისთვის.

მოკლევადიანი სტრატეგიაა რისკის მიღება გაუთვალისწინებელი გარემოებების წინააღმდეგ გეგმის შემუშავებით. ადამიანებმა და ორგანიზაციებმა ყოველდღიურად უნდა მიიღონ რისკი. თანამედროვე მეთოდოლოგიები რისკის შემცირებას ახდენენ პროგრამული უზრუნველყოფის თანდათანობით განვითარებით და რეგულარული განახლებების უზრუნველყოფით სისტემების მოწყვლადობისა და არასწორი კონფიგურაციების მოსაგვარებლად.

აუთსორსინგის (Outsourcing) მომსახურება, დაზღვევის ან მხარდაჭერის კონტრაქტების შეძენა წარმოადგენენ რისკის გადაცემის მაგალითს. სპეციალისტების დაქირავება, რომლებიც შეასრულებენ სპეციფიურ სამუშაოებს და განახორციელებენ კრიტიკულ ამოცანებს რისკის შესამცირებლად, შეიძლება იყოს კარგი გადაწყვეტილება. რისკის შემარბილებელი გეგმა შეიძლება ასევე შეიცავდეს ორ ან მეტ სტრატეგიას.

სიღრმისეული თავდაცვა არ უზრუნველყოფს გაუვალ კიბერ ფარს, ამიტომ ორგანიზაციამ უნდა შექმნას დაცვის რამდენიმე სხვადასხვა

შრე. მსგავსი მრავალშრიანი მიდგომა უზრუნველყოფს ყველაზე ყოვლისმომცველ დაცვას. თუ კიბერ დამნაშავეები გადალახავენ ერთ შრეს, მათ კვლავ უნდა დახვდეთ რამდენიმე შრე, რომელთა გადალახვაც უფრო რთული იქნება, ვიდრე წინა ფენისა.

შრეებად დაყოფა (Layering) ქმნის ბარიერს მრავალი თავდაცვითი ზღუდით, რომლებიც კოორდინირებენ თავდასხმების თავიდან ასაცილებლად. მაგალითად, ორგანიზაციამ შეიძლება შეინახოს თავისი საიდუმლო დოკუმენტები სერვერზე ელექტრონული ღობით გარშემორტყმულ შენობაში.

მნიშვნელოვანია ასევე მონაცემებსა და ინფორმაციაზე ხელმისაწვდომობის **შეზღუდვა**, რომელიც ამცირებს საფრთხის შესაძლებლობას. ორგანიზაციამ უნდა შეზღუდოს ხელმისაწვდომობა ისე, რომ მომხმარებლებს გააჩნდეთ წვდომის მხოლოდ ის დონე, რომელიც საჭიროა მათი სამუშაოსათვის. მაგალითად, მარკეტინგის დეპარტამენტში დასაქმებულ ადამიანებს არ სჭირდებათ სახელფასო ჩანაწერებთან წვდომა თავიანთი მოვალეობების შესასრულებლად. ორგანიზაციამ ასევე უნდა განახორციელოს პროცედურული ღონისძიებები. პროცედურა უნდა იყოს განხორციელებული ისე, რომ თანამშრომელს არ უნდა მიეცეს მგრძნობიარე დოკუმენტების შენობიდან გატანის უფლება.

თუ ყველა დაცული ფენა ერთგავროვანია, კიბერ დამნაშავეებს არ გაუჭირდებათ წარმატებული თავდასხმის ჩატარება. ამიტომ, შრეები უნდა იყოს განსხვავებული. ორგანიზაციამ შეიძლება გამოიყენოს სხვადასხვა დაშიფვრის ალგორითმი ან აუთენტიფიკაციის სისტემა სხვადასხვა სტატუსის მქონე მონაცემების დასაცავად. **მრავალფეროვნების** მიზნის მისაღწევად ორგანიზაციებს შეუძლიათ გამოიყენონ სხვადასხვა კომპანიების მიერ წარმოებული უსაფრთხოების პროდუქტები მრავალფაქტორიანი აუთენტიფიკაციის განხორციელების მიზნით. მაგალითად, სერვერი, რომელიც შეიცავს საიდუმლო დოკუმენტებს, ჩაკეტილია ოთახში, რომელიც მოითხოვს ერთი კომპანიის მიერ დამზადებულ გასატარებელ ბარათს (swipe card) და სხვა კომპანიის მიერ მოწოდებულ ბიომეტრიულ აუთენტიფიკაციას.

შეუმჩნეველ ინფორმაციას ასევე შეუძლია დაიცვას მონაცემები და ინფორმაცია. ორგანიზაციამ არ უნდა გაამჟღავნოს ისეთი სახის

ინფორმაცია, რომელიც წარმოდგენას შეუქმნის კიბერკრიმინალებს, რომელი ოპერაციული სისტემაა ინსტალირებული სერვერზე და რა სახის აპარატურაა გამოყენებული.

სირთულე არ აიძლევა აუცილებელი უსაფრთხოების გარანტიას. თუ ორგანიზაცია ახდენს კომპლექსური სისტემების რეალიზებას, რომლებიც ძნელია გასარკვევად და მასში შექმნილ პრობლემათა გადასაჭრელად, ამან შესაძლოა გამოიწვიოს უკუეფექტი. თუ თანამშრომლებს არ ესმით, თუ როგორ უნდა მოახდინონ კომპლექსურ გადაწყვეტათა კონფიგურაცია სწორად, ამ ფაქტმა შეიძლება გაუმარტივოს კიბერ კრიმინალებს სისტემის მოწყვლადი ადგილების მოძიება. ხელმისაწვდომობის შენარჩუნების მიზნით, უსაფრთხოების ორგანიზება უნდა იყოს **მარტივი** შიგნიდან, მაგრამ რთული დასაძლევი გარედან.

N+1 სიჭარბე არის საერთო სტრატეგია საინჟინრო და IT სისტემებში საიმედოობისა და ხელმისაწვდომობის უზრუნველსაყოფად. ეს მიდგომა ვარაუდობს, რომ არსებობს N ძირითადი კომპონენტი, რომელიც საჭიროა სისტემის დატვირთვის მოსაგვარებლად, პლუს ერთი დამატებითი (სარეზერვო) კომპონენტი. სარეზერვო კომპონენტს შეუძლია აიღოს კონტროლი, თუ რომელიმე ძირითადი კომპონენტი გამოდის მწყობრიდან ან ვერ უმკლავდება დატვირთვას.

(N) წარმოადგენს კომპონენტების რაოდენობას, რომლებიც საჭიროა ოპერატიული დატვირთვის გასატარებლად. (+1) მიუთითებს დამატებით კომპონენტზე, რომელიც სარეზერვო ფუნქციას ასრულებს.

N+1 სიჭარბის მთავარი მიზანია, თავიდან აიცილოს შეფერხება და უზრუნველყოს უწყვეტი მუშაობა კომპონენტის გაუმართაობის შემთხვევაშიც კი. ეს ძალიან მნიშვნელოვანია სისტემებისთვის, სადაც ხელმისაწვდომობა კრიტიკულია, როგორიცაა მონაცემთა ცენტრები, ტელეკომუნიკაციები, ელექტრო ქსელები და წარმოება. მაგ., N+1 მონაცემთა ცენტრში არის დენის გენერატორი, რომელიც ირთვება ავტომატურად, როდესაც ძირითადი კვების წყარო ზიანდება.

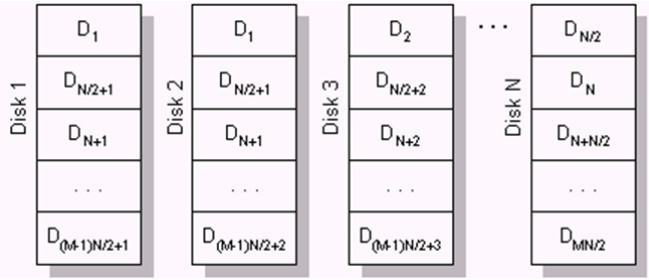
RAID (დამოუკიდებელი დისკების ჭარბი მასივი) ახდენს მრავალი ფიზიკური დისკის კომბინირებას ერთ ლოგიკურ ერთეულში მაღალი მწარმოებლობისა და მონაცემთა დუბლირების უზრუნველყოფის მიზნით. RAID იღებს მონაცემებს, რომლებიც ჩვეულებრივ ინახება ერთ დისკზე და ავრცელებს მას რამდენიმე დისკზე. თუ რომელიმე

დისკი მწყობრიდან გამოვა, მომხმარებელს შეუძლია მონაცემების აღდგენა სხვა დისკებიდან, სადაც მონაცემები დუბლირებულია.

RAID-ს ასევე შეუძლია გაზარდოს მონაცემთა აღდგენის სიჩქარე. მრავალჯერადი დისკების გამოყენება უფრო სწრაფად აღადგენს მოთხოვნილ მონაცემებს, ვიდრე მხოლოდ ერთ დისკზე დაყრდნობა.

RAID გადაწყვეტა შეიძლება იყოს აპარატურული ან პროგრამული. აპარატურაზე დაფუძნებული გადაწყვეტა მოითხოვს სპეციალიზებულ კონტროლერთა არსებობას სისტემაში, რომელიც შეიცავს RAID დისკებს. არსებობს RAID-ის რამოდენიმე სახეობა. განვიხილოთ ყველაზე გავრცელებული RAID-1, RAID-2, RAID-3 და RAID-5.

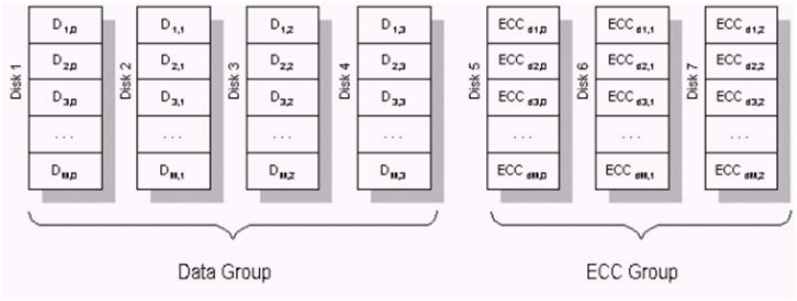
RAID-1 - დისკური მასივი დუბლირებით ანუ სარკე. დიკური მასივი დუბლირებით გულისხმობს, რომ ინფორმაცია დუბლირდება ჩაწერის პროცესში და იწერება ორ დისკზე პარალელურად. ერთი დისკის მწყობრიდან გამოსვლის შემთხვევაში ჩვენ გვრჩება მეორე კოპია და სისტემა ინფორმაციის მთელი მასივის კოპიას აღადგენს დაზიანებული დისკის გამოცვლის შემდეგ.



სურ. 6.1. RAID 1

RAID-1-ის უპირატესობაა სიმარტივე და სისწრაფე, ნაკლი კი მისი ძვირადღირებულება.

RAID-2 - დისკური მასივი ჰემინგის კოდის გამოყენებით. ჭარბი კოდირება, რომელიც გამოიყენება RAID-2-ში ატარებს ჰემინგის კოდის სახელს. ეს კოდირება იძლევა ერთმაგი ან ორმაგი შეცდომების გასწორების საშუალებას.



სურ.6.2.RAID 2

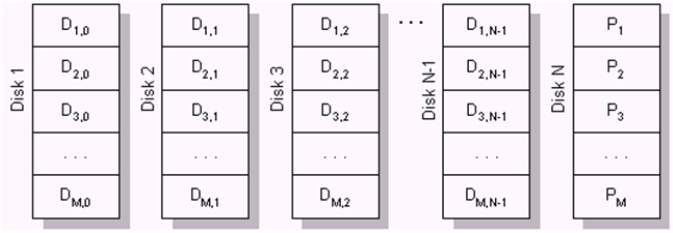
7 დისკის შემთხვევაში 4-ზე იწერება მონაცემები, ხოლო 3-ზე ე.წ. ECC კოდი, რომელიც იძლევა ინფორმაციის აღდგენის საშუალებას იმ შემთხვევაში, თუ ერთი ან ორი დისკი გამოვიდა მწყობრიდან. ეს სისტემა მოსახერხებელია დიდი რაოდენობის დისკების გამოყენების შემთხვევაში და იძლევა ინფორმაციის სწრაფად გასწორების შესაძლებლობას.

RAID-3 სისტემაში გამოიყენება ე.წ. საკონტროლო ჯამი. ინფორმაციის თითო-თითო ბიტი იწერება N დისკზე, ხოლო ერთ დისკზე იწერება ამ ბიტების ჯამი მოდულით ორი:

$$P_i = D_{1,i} \oplus D_{2,i} \oplus \dots D_{N,i}$$

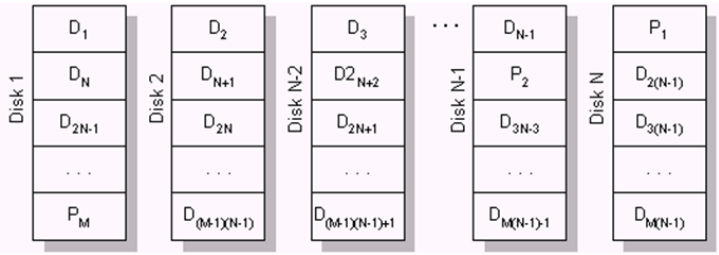
ერთი დისკის მწყობრიდან გამოსვლის შემთხვევაში შესაძლებელია მისი აღდგენა დანარჩენი ინფორმაციით:

$$D_{x,i} = D_{1,i} \oplus D_{2,i} \oplus \dots \oplus D_{x-1,i} \oplus D_{x+1,i} \oplus \dots \oplus D_{N,i} \oplus P_i$$



სურ.6.3. RAID 3

RAID-5 გამოირჩევა საკონტროლო ჯამის ყველა დისკზე განაწილებით, რაც ამაღლებს დისკების წარმადობას მცირე მოცულობის ინფორმაციის ბლოკების ჩაწერისას.



სურ.6.4. RAID 5

სიჭარბის რეალიზება (Redundancy) ზრდის ინფრასტრუქტურის ხელმისაწვდომობას, იცავს რა ქსელს, მტყუნების ერთეული წერტილის ზემოქმედებისაგან. მაგ., დაზიანებული ან არასათანადოდ შეერთებული კაბელი. Spanning Tree პროტოკოლი (STP) მიმართულია ამ საკითხების გადასაწყვეტად. STP-ის ძირითადი ფუნქციაა ქსელში მარყუჟების თავიდან აცილება, როდესაც კომუტატორები უკავშირდებიან ერთმანეთს მრავალი გზით. იგი უზრუნველყოფს მხოლოდ ერთი ლოგიკური მარშრუტის არსებობას გამგზავნსა და მიმღებს შორის ქსელში. STP განზრახ ბლოკავს დუბლირებულ გზებს, რომელთაც შეუძლიათ გამოიწვიონ მარყუჟი.

დუბლირებული გზების ბლოკირება კრიტიკულად მნიშვნელოვანია ქსელის მარყუჟების თავიდან ასაცილებლად. ფიზიკური გზები ჯერ კიდევ არსებობს, რათა უზრუნველყოფილ იქნას დუბლირება, მაგრამ STP გამორთავს ამ გზებს მარყუჟის წარმოქმნის თავიდან ასაცილებლად. თუ ქსელის კაბელი ან კომუტატორი გამოვიდა მწყობრიდან, STP გადათვლის გზებს და ახდენს საჭირო პორტების განბლოკვას, რათა დუბლირებული გზა გახდეს აქტიური.

სისტემის ან ქსელის მტყუნების მედეგობის უზრუნველსაყოფად გამოიყენება მდგრადობა. ქსელში შეიძლება არსებობდეს დუბლირებული კავშირები (STP უზრუნველყოფს ალტერნატიულ მარშრუტს ქსელში არსებული შეერთების მწყობრიდან გამოსვლის

შემთხვევაში), მაგრამ მიუხედავად ამისა გადართვა შეიძლება არ მოხდეს დაუყოვნებლივ, თუ კონფიგურაცია არ არის ოპტიმალურად გამართული.

მარშრუტიზაციის პროტოკოლები ასევე უზრუნველყოფენ მდგრადობას, მაგრამ ქსელის სათანადოდ გამართვამ შეიძლება უზრუნველყოს კომუტატორთა გადართვა ისე, რომ მომხმარებლებმა ეს საერთოს ვერ შეამჩნიონ. ქსელის მდგრადი დიზაინი უფრო მეტია, ვიდრე უბრალოდ დუბლირების განხორციელება. კრიტიკულად მნიშვნელოვანია ბიზნეს საჭიროებების გააზრება, შემდეგ კი მდგრადი ქსელის შექმნა.

აპლიკაციის მდგრადობა არის მისი უნარი რეაგირება მოახდინოს პრობლემაზე, თუ მისი ერთ-ერთ კომპონენტი ჯერ კიდევ ფუნქციონირებს. სამუშაო დროის გაცდენა გამოწვეულია აპლიკაციათა შეცდომებითა და ინფრასტრუქტურული მტყუნებებით. ადმინისტრატორმა საბოლოოდ უნდა გამორიცხოს აპლიკაციათა შეცდომები ვერსიის განახლებების, ახალი მახასიათებლების რეალიზებით. სამუშაო დროის გაცდენა ასევე შეიძლება იყოს მონაცემთა დაზიანების, აპარატურული მტყუნებების, აპლიკაციის შეცდომებისა და ადამიანური ფაქტორების შედეგი.

მრავალი ორგანიზაცია ცდილობს დააბალანსოს აპლიკაციათა ინფრასტრუქტურის მდგრადობის მისაღწევად გაწეული ფასი მომხმარებელთა ან ბიზნესის დაკარგვის ხარჯთან, რომელიც გამოწვეულია აპლიკაციათა შეცდომების გამო.

საკომუნიკაციო ქსელს აქვს უნარი დინამიურად მოახდინოს აღდგენა მოწყობილობის მტყუნების შემთხვევაში, ამისთვის იყენებენ ე.წ. **დუბლირებას**. ქვემოთ ჩამოთვლილია იმ პროტოკოლების სია, რომლებიც გამოიყენება მარშრუტიზატორის დუბლირებისთვის:

"ცხელი" ლოდინის მარშრუტიზატორის პროტოკოლი (HSRP) - HSRP უზრუნველყოფს მაღალი დონის ქსელის ხელმისაწვდომობას პირველი ჰოპის მარშრუტიზაციის დუბლირების უზრუნველყოფის გზით. მარშრუტიზატორების ჯგუფი იყენებს HSRP-ს აქტიური მოწყობილობისა და სარეზერვო მოწყობილობის შესარჩევად. მოწყობილობის ინტერფეისების ჯგუფში აქტიური მოწყობილობა არის მოწყობილობა, რომელიც ახდენს პაკეტების მარშრუტირებას; სარეზერვო მოწყობილობა არის მოწყობილობა, რომელიც იღებს

აქტიური მოწყობილობის როლს ძირითადი მარშრუტიზატორის მწყობრიდან გამოსვლის შემთხვევაში. HSRP სარეზერვო როუტერის ფუნქციაა HSRP ჯგუფის საოპერაციო სტატუსის მონიტორინგი და სწრაფი მოქმედება პაკეტთა მარშრუტიზაციისათვის, თუ ძირითადი მარშრუტიზატორი მწყობრიდან გამოვა.

ვირტუალური Router Redundancy პროტოკოლი (VRRP) - VRRP როუტერი აამოქმედებს VRP პროტოკოლს ერთი ან მეტი სხვა მარშრუტიზატორისათვის, რომლებიც შეერთებულნი არიან LAN-თან. VRRP კონფიგურაციაში, არჩეული როუტერი წარმოადგენს ოსტატ ვირტუალურ როუტერს, ხოლო სხვა მარშრუტიზატორები მოქმედებენ, როგორც სარეზერვო როუტერები, იმ შემთხვევაში, თუ ოსტატი ვირტუალური როუტერი შეწყვეტს ფუნქციონირებას.

კარიბჭის დატვირთვის ბალანსირების ოქმი (GLBP) - GLBP იცავს მონაცემთა ტრაფიკს მწყობრიდან გამოსული მარშრუტიზატორის ან მარყუჟის წარმოქმნის შემთხვევაში, როგორიცაა HSRP და VRP, ასევე უზრუნველყოფს დატვირთვის დაბალანსებას (დატვირთვის გაზიარება) დუბლირებულ მარშრუტიზატორთა ჯგუფებს შორის.

ორგანიზაციამ ასევე შეიძლება მოითხოვოს ლოკაციის დუბლირება თავისი საჭიროებების მიხედვით. არსებობს დუბლირების სამი ფორმა.

სინქრონული - ახდენს ორივე ლოკაციის სინქრონიზირებას რეალურ დროში; მოითხოვს მაღალ გამტარუნარიანობას; ლოკაციები განლაგებული უნდა იყოს ახლოს ერთმანეთთან, რათა შემცირდეს დაყოვნება.

ასინქრონული - არ არის სინქრონიზებული რეალურ დროში; მოითხოვს ნაკლებ გამტარუნარიანობას; საიტები შეიძლება იყოს უფრო შორს, რადგან დაყოვნება ნაკლებია.

Point-in-time - განაახლებს სარეზერვო მონაცემების ადგილმდებარეობას პერიოდულად; უზრუნველყოფს ყველაზე მაღალ გამტარუნარიანობას, რადგან არ საჭიროებს მუდმივ კავშირს;

6.3 ინციდენტებზე რეაგირება - ეტაპები და ტექნოლოგიები

ინციდენტებზე რეაგირება წარმოადგენს პროცედურებს, რომლებსაც ასრულებს ორგანიზაცია მას შემდეგ, რაც მოვლენები ცდებიან დადგენილ წესებს. მონაცემთა გაჟონვა ავრცელებს ინფორმაციას არასანდო გარემოში. იგი შეიძლება მოხდეს შემთხვევითი ან წინასწარ განზრახული აქტის შედეგად. მონაცემთა გაჟონვა შესაძლოა მოხდეს ნებისმიერ დროს, როდესაც არაავტორიზებული პირი ასრულებს, გადასცემს, კითხულობს, იპარავს, ან იღებს წვდომას მგრძნობიარე ინფორმაციაზე.

ორგანიზაციამ უნდა იცოდეს, როგორ უპასუხოს არასასურველ ინციდენტს. ორგანიზაციამ უნდა შეიმუშაოს ინციდენტებზე რეაგირების გეგმა და შეკრიბოს კომპიუტერული უსაფრთხოების ინციდენტებზე რეაგირების გუნდი (CSRT- Computer Security Incident Response Team), რათა მოახდინოს რეაგირება. აღნიშნული გუნდი ასრულებს შემდეგ ქმედებებს:

- მხარს უჭერს ინციდენტზე რეაგირების გეგმას;
- რწმუნდება, რომ მისი წევრები არიან გათვითცნობიერებულნი გეგმის შესახებ;
- ამოწმებს გეგმას;
- იღებს მენეჯმენტისგან გეგმის დამტკიცების თანხმობას.

გუნდი მიჰყვება წინასწარ განსაზღვრულ ნაბიჯებს, რათა დარწმუნდეს, რომ მათი მიდგომა ერთგვაროვანია და რომ ისინი არ გამოტოვებენ რაიმე ნაბიჯს.

ინციდენტის **გამოვლენა** იწყება, როდესაც ვინმე აღმოაჩენს ინციდენტს. ორგანიზაციებს შეუძლიათ შეიძინონ ყველაზე დახვეწილი გამოვლენის სისტემები. სათანადო გამოვლენა მოიცავს, თუ როგორ მოხდა ინციდენტი, რა მონაცემებს და სისტემებს ეხებოდა. დარღვევის შესახებ შეტყობინება ეგზავნება მენეჯერებს, რომლებიც პასუხისმგებელნი არიან მონაცემებსა და სისტემებზე. გამოვლენა და ანალიზი მოიცავს:

- გაფრთხილებებს და შეტყობინებებს;

- მონიტორინგს და შემდგომ ქმედებებს.

ინციდენტების ანალიზი ხელს უწყობს მონაცემთა დარღვევის წყაროს, მასშტაბის, გავლენის და დეტალების იდენტიფიცირებას. ორგანიზაციას შეიძლება ესაჭიროებოდეს გადაწყვიტოს, დასჭირდება თუ არა ექსპერტთა ჯგუფის მოწვევა სასამართლო ექსპერტიზის ჩასატარებლად.

შეკავების ძალისხმევა მოიცავს მყისიერ ქმედებებს, როგორიცაა ქსელის სისტემის გათიშვა ინფორმაციის გაჟონვის შესაჩერებლად. დარღვევის იდენტიფიცირების შემდეგ ორგანიზაციამ უნდა შეაკავოს და აღმოფხვრას იგი. ამ ქმედებებმა შესაძლოა მოითხოვოს სისტემის სამუშაო დროის დამატებითი დანაკარგი. აღდგენის ეტაპი მოიცავს იმ ქმედებებს, რომლებიც ორგანიზაციამ უნდა მიიღოს, რათა აღმოფხვრას დარღვევა და აღადგინოს სისტემა. პრობლემის გამოსწორების შემდეგ ორგანიზაციამ უნდა აღადგინოს ყველა სისტემა დარღვევამდე არსებულ ორიგინალ მდგომარეობამდე.

ინციდენტის შემდგომ, ნორმალურ მდგომარეობაში ყველა ოპერაციის აღდგენის შემდეგ, ორგანიზაციამ უნდა შეისწავლოს ინციდენტის მიზეზი და დასვას შემდეგ კითხვები:

- ✓ რა ქმედებები შეუშლის ხელს ინციდენტის მოხდენას?
- ✓ რა პრევენციული ზომები საჭიროებს გაძლიერებას?
- ✓ როგორ შეიძლება გაუმჯობესდეს სისტემის მონიტორინგი?
- ✓ როგორ შეიძლება შემცირდეს სამუშაო დროის დანაკარგი შეკავების, აღმოფხვრისა და აღდგენის ფაზის მსვლელობის დროს?
- ✓ როგორ შეუძლია მენეჯმენტს, მინიმუმამდე შეამციროს გავლენა ბიზნესზე?

მიღებული გამოცდილება და სწორად გამოტანილი დასკვნები ეხმარება ორგანიზაციას უკეთესად მოემზადოს დანაკარგების თავიდან ასაცილებლად ინციდენტებზე რეაგირების გეგმის გაუმჯობესების გზით.

შეჭრის გამოვლენა არის კომპიუტერულ სისტემაში ან ქსელში მომხდარი მოვლენების მონიტორინგის პროცესი და მათი ანალიზი. ინციდენტებს აქვთ მრავალი მიზეზი, როგორიცაა მავნე პროგრამები (მაგ., ჭიები, ვირუსები), თავდამსხმელები (მაგ. ინტერნეტიდან სისტემებზე უნებართვო წვდომის მოთხოვნისას) და სისტემების ავტორიზებული მომხმარებლები, რომლებიც ბოროტად იყენებენ

თავიანთ პრივილეგიებს. მიუხედავად იმისა, რომ ბევრი ინციდენტი გამიზნულად ხორციელდება, ზოგი მათგანი შეიძლება, რომ მოხდეს შემთხვევითად. მაგალითად, ადამიანმა შეიძლება არასწორად აკრიფოს კომპიუტერის მისამართი და შემთხვევით შეეცადოს სხვა სისტემასთან დაკავშირებას ავტორიზაციის გარეშე.

შეღწევის აღმომჩენი სისტემები (IDS) და შეღწევის პრევენციის სისტემები (IPS) ძირითადად გამოიყენება შესაძლო საფრთხეების იდენტიფიცირებისთვის, მათ შესახებ ინფორმაციის ჩასაწერად, მათი შეჩერების მცდელობისა და ინფორმაციის უსაფრთხოების ადმინისტრატორებისთვის შესატყობინებლად. ბევრ სისტემას შეუძლია უპასუხოს აღმოჩენილ საფრთხეს და შეეცადოს ხელი შეუშალოს მის წარმატებას. IDPS-ს შეუძლია შეაჩეროს თავდასხმა, შეცვალოს უსაფრთხოების გარემო ან შეცვალოს თავდასხმის ხასიათი. IDS ტექნოლოგიებთან შედარებით, IDPS ტექნოლოგიები არა მხოლოდ აღმოაჩენს საეჭვო აქტივობას, არამედ ცდილობს ხელი შეუშალოს მის წარმატებას ავტომატური რეაგირებით. IDPS ტექნოლოგიები გამოირჩევა მოვლენების ტიპებით, რომლებიც გამოიყენება ინციდენტების იდენტიფიცირებისთვის. ყველა ტიპის IDPS ტექნოლოგიას შეუძლია შეასრულოს შემდეგი სამი ფუნქცია:

- ✓ აღმოჩენილ მოვლენებთან დაკავშირებული ინფორმაციის ჩაწერა - ინფორმაცია მოვლენების შესახებ იწერება ლოკალურად, შემდგომში შეიძლება გაიგზავნოს სხვა სისტემებში, მაგ. ჟურნალის სერვერები;
- ✓ უსაფრთხოების ადმინისტრატორის შეტყობინება აღმოჩენილი კრიტიკული მოვლენების შესახებ – IDPS იყენებს რამდენიმე მეთოდს ადმინისტრატორთან შეტყობინებების გასაგზავნად, როგორიცაა ელ. ფოსტა, შეტყობინებები IDPS მომხმარებლის ინტერფეისზე, syslog შეტყობინებები და მომხმარებლის მიერ განსაზღვრული პროგრამები ან სკრიპტები. შეტყობინება მოვლენის შესახებ შეიცავს მხოლოდ ძირითად ინფორმაციას. ადმინისტრატორს სჭირდება წვდომა IDPS-ში დამატებითი ინფორმაციისთვის;
- ✓ ანგარიშების მომზადება. ანგარიშები აჯამებს მონიტორინგის მოვლენებს ან შეიცავს დეტალებს კონკრეტულ მოვლენებზე.

IDPS-ში გამოიყენება რეაგირების რამდენიმე ტექნიკა: 1. სესიის შეწყვეტა - წყვეტს ქსელურ კავშირს ან მომხმარებლის სესიას ასევე შეუძლია დაბლოკოს წვდომა დანიშნულების ადგილზე ან დაბლოკოს მთელი კომუნიკაცია დანიშნულების ჰოსტთან, სერვისთან, აპლიკაციასთან ან სხვა რესურსთან. 2. დინამიური რეკონფიგურაცია - IDPS-ს შეუძლია შეცვალოს კონფიგურაცია შეტევის ჩაშლის მიზნით. მოახდინოს ქსელური მოწყობილობის ხელახალი კონფიგურაცია, როგორიცაა firewall ან გადამრთველი თავდამსხმელიდან ან დანიშნულების ადგილამდე წვდომის დასაბლოკად. 3. IDPS-ის ზოგიერთ სისტემას შეუძლია თავდასხმის ინფიცირებული ან საეჭვო ნაწილების ამოღება პაკეტიდან და ამით იგი უვნებელს ხდის კომუნიკაციას, მაგ. IDPS-ს შეუძლია ამოიღოს ინფიცირებული მიმაგრებული ფაილი ელფოსტიდან და შემდეგ გაუგზავნოს სუფთა ელ.წერილი მის მიმღებს.

შეჭრის აღმოჩენის სისტემა (IDS) არის კიბერუსაფრთხოების გადაწყვეტა, რომელიც აკონტროლებს ქსელის ტრაფიკს და საეჭვო ქცევის მოვლენებს. IDS უსაფრთხოების სისტემები მიზნად ისახავს შეჭრისა და უსაფრთხოების დარღვევების აღმოჩენას, რათა ორგანიზაციებმა შეძლონ სწრაფად რეაგირება პოტენციურ საფრთხეებზე. IDS-ის ტიპები მოიცავს:

ქსელზე დაფუძნებული: ქსელზე დაფუძნებული IDS (NIDS) განლაგებულია კომპიუტერული ქსელის სტრატეგიულ წერტილებზე, რომელიც შეისწავლის შემომავალ და გამავალ ტრაფიკს. ის ფოკუსირებულია ქსელის პროტოკოლების, ტრაფიკის შაბლონებისა და პაკეტის სათაურების მონიტორინგზე.

ჰოსტზე დაფუძნებული: ჰოსტზე დაფუძნებული IDS (HIDS) დაინსტალირებულია ცალკეულ მანქანებზე ან სერვერებზე IT გარემოში. ის ყურადღებას ამახვილებს სისტემის ჟურნალების და ფაილების მონიტორინგზე, რათა აღმოაჩინოს ისეთი მოვლენები, როგორიცაა არაავტორიზებული წვდომის მცდელობები და სისტემაში არანორმალური ცვლილებები.

ჰიბრიდი: ჰიბრიდული IDS აერთიანებს როგორც ქსელზე დაფუძნებულ, ისე ჰოსტზე დაფუძნებულ მიდგომებს. ამ ტიპის IDS უზრუნველყოფს უფრო სრულ ხედვას IT ეკოსისტემაში მოვლენებზე.

IDS მუშაობს ქსელის პაკეტების ანალიზით და ახორციელებს მათ შედარებას ცნობილ თავდასხმის ხელმოწერებთან ან ქცევის შაბლონებთან. თუ IDS თვლის, რომ მან აღმოაჩინა თავდამსხმელი, ის აგზავნის გაფრთხილებას სისტემის ადმინისტრატორებს ან უსაფრთხოების ჯგუფებს. ეს გაფრთხილებები იძლევა დეტალურ ინფორმაციას აღმოჩენილი აქტივობის შესახებ, რაც თანამშრომლებს საშუალებას აძლევს სწრაფად გამოიძიონ და უპასუხონ. IDS მნიშვნელოვან როლს ასრულებს კომპიუტერული ქსელებისა და სისტემების უსაფრთხოებისა და მთლიანობის შენარჩუნებაში. IDS-ის უპირატესობებია:

საფრთხის ადრეული გამოვლენა: IDS ინსტრუმენტებს შეუძლიათ პროაქტიულად დაიცვან კიბერთავდასხმები შეჭრის ადრეულ ეტაპზე პოტენციური საფრთხეების გამოვლენით.

მეტი ხილვადობა: IDS გადაწყვეტილებები ზრდის ორგანიზაციების ხილვადობას მათ IT გარემოში, ეხმარება უსაფრთხოების გუნდებს უპასუხონ თავდასხმებს უფრო სწრაფად და ეფექტურად.

IDS ინსტრუმენტები არ არის სრულყოფილი; მათ შეუძლიათ წარმოქმნან როგორც ცრუ პოზიტივი (უსაფრთხო მოვლენების საფრთხედ მონიშვნა) და ცრუ ნეგატივები (როცა რეალური საფრთხეების გამოვლენა ვერ ხერხდება). IDS გადაწყვეტილებებს შეუძლიათ თავდასხმების წარმოქმნისთანავე აღმოაჩინონ, მაგრამ მათ არ შეუძლიათ თავიდან აიცილონ ისინი.

შეჭრის პრევენციის სისტემა (IPS) არის კიბერუსაფრთხოების გადაწყვეტა, რომელიც ეფუძნება IDS-ის შესაძლებლობებს. IPS კიბერუსაფრთხოების ინსტრუმენტები არა მხოლოდ აღმოაჩენს პოტენციურ შეჭრას, არამედ აქტიურად აფერხებს და ამსუბუქებს მათ. IDS-ის მსგავსად, IPS-ის ტიპები მოიცავს:

ქსელზე დაფუძნებული: ქსელის IPS (NIPS) განლაგებულია კომპიუტერული ქსელის სტრატეგიულ წერტილებზე, ხშირად ქსელის კარიბჭეებზე. მას შეუძლია დაიცვას ორგანიზაციის მთელი ქსელი, მათ შორის მრავალი დაკავშირებული ჰოსტი და მოწყობილობა.

ჰოსტზე დაფუძნებული: ჰოსტზე დაფუძნებული IPS (HIPS) განლაგებულია კონკრეტულ კომპიუტერზე ან სერვერზე, რომელიც უზრუნველყოფს დაცვას ერთი ჰოსტისთვის. ის აკონტროლებს

სისტემის აქტივობას და შეუძლია მიიღოს ზომები სისტემის რესურსებზე წვდომის დაბლოკვის ან შეზღუდვის მიზნით.

ჰიბრიდი: ჰიბრიდული IPS აერთიანებს როგორც ქსელზე დაფუძნებულ, ისე ჰოსტზე დაფუძნებულ მიდგომებს. მაგალითად, ჰიბრიდული IPS შეიძლება იყოს ძირითადად ქსელზე დაფუძნებული, მაგრამ ასევე მოიცავს ჰოსტის სპეციფიკურ უსაფრთხოების შესაძლებლობებს.

IPS-ის უპირატესობებში შედის:

რეალურ დროში საფრთხის პრევენცია: IPS-ს შეუძლია დაბლოკოს ან შეამსუბუქოს იდენტიფიცირებული საფრთხეები რეალურ დროში, რაც უზრუნველყოფს 24/7 ავტომატიზირებულ დაცვას თქვენი IT გარემოსთვის.

გაუმჯობესებული ქსელის უსაფრთხოება. IDS ინსტრუმენტებისგან განსხვავებით, IPS სისტემებს შეუძლიათ არა მხოლოდ აღმოაჩინონ საფრთხეები, არამედ მიიღონ ზომები მათგან დასაცავად მავნე და საეჭვო ტრაფიკის დაბლოკვით.

IPS ინსტრუმენტებმა უნდა შეამოწმოს ყველა შემომავალი და გამავალი ტრაფიკი, რამაც შეიძლება გამოიწვიოს შეფერხება და ქსელის მუშაობის შემცირება. მაქსიმალური ეფექტურობის მისაღწევად, IPS გადაწყვეტა რეგულარულად უნდა განახლდეს უახლესი საფრთხის ხელმოწერის ინფორმაციით, რაც შეიძლება მოითხოვდეს დროისა და ექსპერტიზის მნიშვნელოვან ინვესტიციას.

მთავარი განსხვავება IDS-სა და IPS-ს შორის ისაა, რომ მიუხედავად იმისა, რომ IDS ინსტრუმენტებს შეუძლიათ მხოლოდ შეჭრის გამოვლენა, IPS ინსტრუმენტებს ასევე შეუძლიათ მათი აქტიური პრევენცია. ამ ძირითად განსხვავებას აქვს რამდენიმე მნიშვნელოვანი გავლენა:

ფუნქციონალობა: IDS ინსტრუმენტები შემოიფარგლება საფრთხის აღმოჩენით, ხოლო IPS ინსტრუმენტებს შეუძლიათ მათი აღმოჩენა და თავიდან აცილება.

პასუხი: IDS ინსტრუმენტები აგზავნის გაფრთხილებებს საფრთხის აღმოჩენისას და IPS ხელსაწყოებს შეუძლიათ ავტომატურად დაბლოკონ საფრთხეები წინასწარ განსაზღვრული პოლიტიკის ან უსაფრთხოების წესების საფუძველზე.

სამუშაო პროცესი: IDS ინსტრუმენტები პასიურად აკონტროლებენ მონაცემთა ნაკადს, ხოლო IPS ხელსაწყოები აქტიურად ამოწმებს ქსელის პაკეტებს და იღებენ ზომებს საფრთხეების თავიდან ასაცილებლად ან შესამცირებლად.

IDS/IPS ტექნოლოგია მნიშვნელოვნად შეიცვალა დაარსების დღიდან. დღესდღეობით, IDS/IPS ინსტრუმენტებს შეუძლიათ გამოიყენონ მანქანათმცოდნეობა და ხელოვნური ინტელექტი მათი აღმოჩენის შესაძლებლობების გასაუმჯობესებლად ისტორიული კიბერ საფრთხეების მონაცემების შესწავლით. მათ შეუძლიათ გამოიყენონ ტექნიკა, რომელიც ცნობილია როგორც ქცევითი ანალიზი: ქსელის ტრაფიკის ან მომხმარებლის ქცევის შედარება საწყისთან, რათა დაეხმაროს ანომალიების ან გადახრების იდენტიფიცირებას. ამასთან, ღრუბლოვანი გამოთვლის მზარდი პოპულარობით, მრავალი IDS/IPS ხელსაწყო ახლა შეიძლება განთავსდეს ღრუბლოვან IT გარემოში, რათა უფრო მოქნილი და მასშტაბური გახდეს.

მონაცემთა კონფიდენციალურობისა და უსაფრთხოების მრავალი რეგულაცია ცალსახად ან ირიბად მოითხოვს ორგანიზაციებისგან IDS და IPS ინსტრუმენტების დანერგვას. მაგალითად, PCI DSS არის უსაფრთხოების სტანდარტი ბიზნესისთვის, რომელიც ამუშავებს გადახდის ბარათის ინფორმაციას. PCI DSS მოთხოვნის 11.4 პუნქტის შესაბამისად, კომპანიებმა უნდა „გამოიყენონ ქსელში შეჭრის გამოვლენის და/ან შეჭრის პრევენციის ტექნიკა ქსელში შეჭრის აღმოსაჩენად და/ან თავიდან ასაცილებლად“. GDPR (ზოგადი მონაცემთა დაცვის რეგულაცია) არის კიდევ ერთი რეგულაცია, რომელიც შეიძლება მოითხოვდეს IDS/IPS გადაწყვეტილებებს. GDPR არის ევროკავშირის კანონი, რომელიც იცავს მოქალაქეთა პერსონალური მონაცემების კონფიდენციალურობას. GDPR-ის თანახმად, ბიზნესებმა უნდა მიიღონ „შესაბამისი ტექნიკური და ორგანიზაციული ზომები“, რათა დაიცვან ეს მონაცემები დარღვევისა და არაავტორიზებული წვდომისგან, რაც შეიძლება მოიცავდეს IDS/IPS-ის გამოყენებას.

6.4 ბიზნეს უწყვეტობის მნიშვნელობა

ბიზნესის უწყვეტობა კომპიუტერული უსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი კონცეფციაა. მიუხედავად იმისა, რომ

კომპანიები მაქსიმუმ ძალისხმევას გასწევენ კატასტროფებისა და მონაცემების დაკარგვის თავიდან ასაცილებლად, ყველა შესაძლო სცენარის პროგნოზირება შეუძლებელია. მნიშვნელოვანია, რომ კომპანიებს ჰქონდეთ გეგმები, რომლებიც უზრუნველყოფენ ბიზნესის უწყვეტობას, მიუხედავად იმისა, თუ რა შეიძლება მოხდეს. ბიზნესის უწყვეტობის გეგმა მოიცავს კრიტიკული სისტემების მიღებას სხვა ლოკაციაზე მაშინ, როდესაც მიმდინარეობს ორიგინალური ობიექტის გაუმართაობის აღმოფხვრა. პერსონალი განაგრძობს ყველა ბიზნეს პროცესის ალტერნატიულ რეჟიმში შესრულებას, სანამ ნორმალური პროცესი არ განახლდება.

ხელმისაწვდომობა უზრუნველყოფს იმას, რომ ორგანიზაციის ფუნქციონირებისათვის საჭირო რესურსები კვლავაც ხელმისაწვდომი იქნება პერსონალისა და სისტემებისთვის.

ბიზნესის უწყვეტობის მართვა გულისხმობს არა მხოლოდ მონაცემთა სარეზერვო ასლების შექმნას და დუბლირებული აპარატურის უზრუნველყოფას. ორგანიზაციებს სჭირდებათ კვალიფიციური თანამშრომლები სისტემების სწორად კონფიგურირებისა და ფუნქციონირებისათვის. ორგანიზაციამ, ბიზნესის უწყვეტობისთვის უნდა უზრუნველყოს შემდეგი:

- მიიღოს კვალიფიციური პერსონალი;
- მოახდინოს კონფიგურაციათა დოკუმენტირება;
- ჩამოაყალიბოს ალტერნატიული საკომუნიკაციო არხები როგორც ხმის, ასევე მონაცემებისთვის;
- უზრუნველყოს ელექტრომომარაგება;
- უზრუნველყოს აპლიკაციებისა და პროცესების ყველანაირი დამოკიდებულების იდენტიფიცირება, რათა ისინი სწორად იქნან გაგებულნი;
- გაიაზროს, თუ როგორ უნდა განხორციელდეს ავტომატური ამოცანები ხელით.

სტანდარტებისა და ტექნოლოგიების ეროვნულმა ინსტიტუტმა (NIST) შეიმუშავა შემდეგი საუკეთესო პრაქტიკა:

1. უნდა მოხდეს პოლიტიკის შექმნა, რომელიც ითვალისწინებს ბიზნესის უწყვეტობის გეგმის შემუშავებას და ანაწილებს როლებს ამოცანების შესასრულებლად.

2. მოხდეს კრიტიკული სისტემებისა და პროცესების იდენტიფიცირება და მათი პრიორიტეტების განსაზღვრა აუცილებლობის საფუძველზე.

3. მოხდეს მოწყვლადობის, საფრთხეების იდენტიფიცირება და რისკების გამოთვლა.

4. რისკის შესამცირებლად კონტროლისა და კონტრზომების იდენტიფიცირება და განხორციელება.

5. შემუშავდეს მეთოდები კრიტიკულად მნიშვნელოვანი სისტემების სწრაფად აღსადგენად.

6. შეიქმნას პროცედურები ქაოტურ მდგომარეობაში მოქმედი ორგანიზაციის შესანარჩუნებლად.

8. რეგულარულად ხორციელდებოდეს გეგმის შემოწმება და განახლება.

მდგრადი სისტემის დიზაინი უნდა მოიცავდეს ღონისძიებებს, რომლებიც უზრუნველყოფენ აპარატურის დუბლირებას და მდგრადობას ისე, რომ ორგანიზაციას შეეძლოს სისტემის სწრაფად აღდგენა და ოპერირების გაგრძელება.

თავი 7. ტექნოლოგიების, პროცესებისა და პროცედურების გამოყენება ქსელის კომპონენტის დასაცავად

დომენის დაცვა არის მუდმივად მიმდინარე პროცესი, რომელიც უზრუნველყოფს ორგანიზაციის ქსელური ინფრასტრუქტურის სათანადო ფუნქციონირებას. ის მოითხოვს, რომ ინდივიდები მუდმივად ფხიზლად იყვნენ საფრთხეების მიმართ და მიიღონ ზომები სისტემის ნებისმიერი კომპრომეტირების თავიდან ასაცილებლად. უსაფრთხო ქსელი იმდენად ძლიერია, რამდენადაც ძლიერია მისი ყველაზე სუსტი ბმული. მნიშვნელოვანია, რომ უზრუნველყოფილი იყოს საბოლოო მოწყობილობების დაცვა, რომლებიც გაერთიანებულნი არიან ქსელში.

7.1 დამცავი სისტემები და მოწყობილობები

ოპერაციული სისტემა კრიტიკულ როლს ასრულებს კომპიუტერული სისტემის ფუნქციონირებაში და წარმოადგენს მრავალი თავდასხმის სამიზნეს. ოპერაციული სისტემის უსაფრთხოებას გააჩნია კასკადური ეფექტი კომპიუტერული სისტემის საერთო უსაფრთხოებაზე.

ადმინისტრატორი აძლიერებს ოპერაციულ სისტემას ნაგულისხმევი კონფიგურაციის შეცვლით, რათა ის უფრო უსაფრთხო იყოს გარე საფრთხეების მიმართ. ეს პროცესი მოიცავს არააუცილებელი პროგრამებისა და სერვისების წაშლას. კიდევ ერთი კრიტიკული მოთხოვნა ოპერაციული სისტემების გაძლიერებისა არის უსაფრთხოების პატჩებისა და განახლებების გამოყენება. უსაფრთხოების პატჩები და განახლებები წარმოადგენენ ერთგვარ პროგრამულ დანამატებს, რომელთაც შეიმუშავებენ კომპანიები, რათა შეამცირონ თავიანთი პროდუქტების მოწყვლადობა და გახადონ ისინი უფრო მეტად მედეგნი საფრთხის მიმართ.

ორგანიზაციას უნდა ჰქონდეს სისტემური მიდგომა სისტემის განახლებების მისამართით. უნდა შეიმუშაოს უსაფრთხოებასთან

დაკავშირებული ინფორმაციის მონიტორინგის პროცედურები და შეაფასოს და დაგეგმოს აპლიკაციისთვის განახლებები.

განახლებების ინსტალაცია დოკუმენტირებული გეგმის გამოყენებით

ოპერაციული სისტემების უზრუნველყოფის კიდევ ერთი კრიტიკულად მნიშვნელოვანი მოთხოვნაა პოტენციური მოწყვლადობის იდენტიფიცირება. ეს შეიძლება განხორციელდეს საბაზისო დაფუძნების გზით. საბაზისო დაფუძნების შემუშავება საშუალებას აძლევს ადმინისტრატორს გააკეთოს შედარება, თუ როგორ ფუნქციონირებს სისტემა მისი საბაზისო მოლოდინების წინააღმდეგ.

Microsoft Baseline Security ანალიზატორი (MBSA) აფასებს დაუინსტალირებელ უსაფრთხოების განახლებებს და არასწორად კონფიგურირებულ უსაფრთხოების პარამეტრებს Microsoft Windows სიტემაში. MBSA ამოწმებს ცარიელ, მარტივ ან არარსებულ პაროლებს, დამცავი ეკრანის პარამეტრებს, სააღრიცხვო ანგარიშის სტატუსებს, ადმინისტრატორის ანგარიშის დეტალებს, უსაფრთხოების ღონისძიების აუდიტს, არასაჭირო მომსახურებას, ქსელურ გაზიარებებსა და რეესტრის პარამეტრებს. ოპერაციული სისტემის გაძლიერების შემდეგ ადმინისტრატორი ქმნის პოლიტიკებსა და პროცედურებს უსაფრთხოების მაღალი დონის შესანარჩუნებლად.

საზიანო პროგრამა შეიცავს ვირუსებს, ქსელურ ჭიებს, ტროიანებს, კლავიატურის შპიონებს (ქეილოგერები), ჯაშუშურ პროგრამებს და სარეკლამო ვირუსებს. ისინი არღვევენ პრივატულობას, იპარავენ ინფორმაციას, აზიანებენ სისტემას ან შლიან მონაცემებს.

ამიტომ, მეტად მნიშვნელოვანია კომპიუტერებისა და მობილური მოწყობილობების დაცვა სათანადო ანტივირუსული პროგრამული პროდუქტის გამოყენებით:

ანტივირუსული დაცვა - პროგრამები მუდმივად ახდენენ ვირუსების მონიტორინგს. ვირუსის აღმოჩენის შემთხვევაში ანტივირუსული პროგრამა იძლევა ამის შესახებ შეტყობინებას და ცდილობს, წაშალოს ან კარანტინში მოაქციოს ის.

სარეკლამო შეტყობინებებიდან დაცვა – პროგრამა მუდმივად ახდენს რეკლამის შემცველი შეტყობინებების აღმოჩენას სისტემაში.

ფიშინგისაგან დაცვა – პროგრამა ბლოკავს ცნობილი ფიშინგური ვებ საიტების IP მისამართებს და აფრთხილებს მომხმარებელს საეჭვო საიტების შესახებ.

"შპიონებისაგან" დაცვა – პროგრამა ახდენს სხვადასხვა "შპიონი" პროგრამის სკანირებას.

სანდო/არასანდო წყაროები - პროგრამა აფრთხილებს მომხმარებელს სახიფათო პროგრამების შესახებ, რომლებიც ცდილობენ დააინსტალირონ ან შექმნან საფრთხე ვებ საიტებზე მანამ, სანამ მომხმარებელი ესტუმრება მათ.

შესაძლოა საჭირო გახდეს რამდენიმე სხვადასხვა პროგრამის გამოყენება და მრავალჯერადი სკანირების ჩატარება იმისათვის, რომ ზიანის მომტანი პროგრამული პროდუქტი სრულად იქნეს წაშლილი სისტემიდან. რამოდენიმე მაღალი რეპუტაციის მქონე უსაფრთხოების ორგანიზაცია, როგორებიცაა McAfee, Symantec, და Kaspersky გვთავაზობენ all-inclusive პროგრამულ პროდუქტს კომპიუტერებისა და მობილური მოწყობილობების დასაცავად.

სიფრთხილეა საჭირო საზიანო ყალბ ანტივირუსულ პროგრამებთან, რომლებიც შეიძლება გამოჩნდნენ ინტერნეტში ნავიგაციის დროს. ამ ყალბი ანტივირუსული პროდუქტების უმეტესობას გამოაქვს განცხადება ან პოპ-აპი, რომლებიც გამოიყურება ისე, როგორც სტანდარტული Windows-ის გამაფრთხილებელი ფანჯარა, აცხადებენ, რომ კომპიუტერი არის ინფიცირებული და მოითხოვენ მომხმარებელისაგან მის გაწმენდას. გამოტანილი ფანჯრის რომელიმე ადგილას მაუსის ღილაკის დაჭერით შეიძლება დაიწყოს ზიანის მომტანი კოდის ჩამოტვირთვა და ინსტალაცია.

არასასურველი და არასათანადო პროგრამა არ არის მხოლოდ პროგრამა, რომელსაც მომხმარებელი უნებლიედ აინსტალირებს სისტემაში. ის ასევე შეიძლება მოდიოდეს მომხმარებლებიდან, რომლებიც ნიშნავს, რომ უნდა მოხდეს მისი ინსტალაცია. ის შეიძლება არ იყოს საზიანო, მაგრამ შესაძლოა არღვევდეს უსაფრთხოების

პოლიტიკას. ასეთი ტიპის შეუსაბამო სისტემამ შეიძლება ხელი შეუშალოს კომპანიის პროგრამულ უზრუნველყოფას ან ქსელურ სერვისებს. მომხმარებელმა უნდა წაშალოს არასასურველი პროგრამა დაუყოვნებლივ.

პატჩები არის კოდის განახლებები, რომელსაც მწარმოებელი გვაწვდის ახლად აღმოჩენილი ვირუსების ან ვორმებისგან დასაცავად, რათა არ განხორციელდეს წარმატებული შეტევა. დროდადრო მწარმოებლები აერთიანებენ პატჩებს და განახლებებს აპლიკაციის კომპლექსურ განახლებაში, რომელსაც სერვის პაკს ვუწოდებთ. ბევრ დამანგრეველ ვირუსულ შეტევას შეიძლება ჰქონდეს ნაკლები ეფექტი, თუ მომხმარებლებმა გადმოწერეს და დააინსტალირეს სერვის პაკის ბოლო ვერსია.

Windows-ი გამუდმებით ამოწმებს Windows-ის განახლების ცენტრის ვებ გვერდს მაღალი პრიორიტეტის განახლებებისთვის, რაც კომპიუტერს იცავს ახალი საფრთხეებისაგან. ეს განახლებები მოიცავს უსაფრთხოების განახლებებს, კრიტიკულ განახლებებს და მომსახურების პაკეტებს. გამომდინარე კონფიგურირებული პარამეტრებიდან, ვინდოუსის ოპერაციული სისტემა ავტომატურად ჩამოწერს და აინსტალირებს მაღალი პრიორიტეტის მქონე განახლებებს ან ატყობინებს მომხმარებელს, რომ ეს განახლებები ხელმისაწვდომია.

ზოგიერთმა ორგანიზაციამ შეიძლება მოითხოვოს პატჩის ტესტირება ორგანიზაციაში მის გავრცელებამდე. ორგანიზაცია გამოიყენებს სერვისს, რათა მართოს პატჩები ადგილობრივად, ნაცვლად იმისა, რომ გამოიყენოს მწარმოებლის (ვენდორის) ონლაინ განახლების სერვისი. ავტომატური პატჩის ან განახლების სერვისის გამოყენების სარგებელი მოიცავს შემდეგს:

- ✓ ადმინისტრატორებს შეუძლიათ მიიღონ ან უარყონ განახლებები;
- ✓ ადმინისტრატორებს შეუძლიათ მოახდინონ სისტემის განახლება კონკრეტული თარიღისთვის;

- ✓ ადმინისტრატორებს შეუძლიათ მიიღონ ანგარიშები თითოეული სისტემის მიერ მოთხოვნილი განახლების შესახებ;
- ✓ არაა აუცილებელი, თითოეული კომპიუტერი დაუკავშირდეს ვენდორის სერვისს, რათა ჩამოტვირთოთ პატჩები; სისტემა იღებს განახლებას ადგილობრივი სერვერიდან;
- ✓ მომხმარებელს არ შეუძლია განახლებების გამორთვა ან მისგან თავის არიდება.

ავტომატური პატჩის სერვისი უზრუნველყოფს ადმინისტრატორებს უფრო კონტროლირებადი პარამეტრებით.

ჰოსტზე დაფუძნებული დამცავი ეკრანები

ჰოსტზე დაფუძნებული გადაწყვეტა არის პროგრამული აპლიკაცია, რომელიც ოპერირებს ლოკალურ ჰოსტზე მისი დაცვის მიზნით. პროგრამული უზრუნველყოფა მუშაობს ოპერაციულ სისტემასთან ერთად, რათა თავიდან იქნას აცილებული თავდასხმები.

პროგრამული დამცავი ეკრანი წარმოადგენს პროგრამას, რომელიც გაშვებულია კომპიუტერში და ახდენს ტრაფიკის დაშვებას ან უარყოფას სხვა კომპიუტერებიდან, რომლებიც შეერთებულნი არიან ქსელში. პროგრამული ფაიერვოლი იყენებს წესების ნაკრებს მონაცემთა გადასაცემად მონაცემთა პაკეტების შემოწმებისა და ფილტრაციის მეშვეობით. ვინდოუსის დამცავი ეკრანი წარმოადგენს პროგრამული დამცავი ეკრანის მაგალითს. ვინდოუსის ოპერაციული სისტემა ინსტალაციის დროს ავტომატურად აინსტალირებს დამცავ ეკრანსაც.

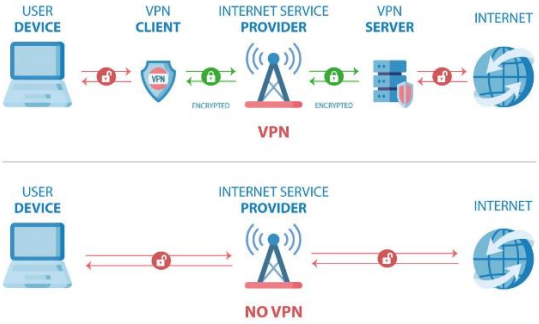
მომხმარებელს შეუძლია მართოს კომპიუტერიდან გაგზავნილი მონაცემთა ტიპები და შერჩეული პორტების გახსნა ან დაბლოკვა. ფაიერვოლები ბლოკავს შემომავალ და გამავალ ქსელურ შეერთებებს, თუ არაა განსაზღვრული გამონაკლისები, რომლებიც გახსნის ან დახურავს პროგრამის მიერ მოთხოვნილ პორტებს.

ჰოსტის შეღწევის გამოვლენის სისტემა (HIDS) არის პროგრამული უზრუნველყოფა, რომელიც გაეშვება ჰოსტ კომპიუტერზე და მონიტორინგს უწევს საეჭვო აქტივობას. თითოეული სერვერზე ან დესკტოპის სისტემაზე, რომელიც მოითხოვს დაცვას, საჭიროა

პროგრამული უზრუნველყოფის ინსტალირება. HIDS მონიტორინგს უწევს სისტემურ ზარებს და ფაილურ სისტემას, რათა დარწმუნდეს, რომ მოთხოვნები არ წარმოადგენენ მავნე აქტივობის შედეგს. მას ასევე შეუძლია მონიტორინგი გაუწიოს სისტემის რეესტრის პარამეტრებს. რეესტრი ახდენს კონფიგურაციის ინფორმაციის მხარდაჭერას კომპიუტერის შესახებ.

HIDS ინახავს ყველა ჟურნალის მონაცემს ლოკალურად. მას ასევე შეუძლია გავლენა მოახდინოს სისტემის ფუნქციონირებაზე. ჰოსტის შეღწევის გამოვლენის სისტემა ვერ აკონტროლებს ნებისმიერ ქსელურ ტრაფიკს, რომელიც ჰოსტის სისტემაში არ შეაღწევს, მაგრამ იგი ახორციელებს ოპერაციული სისტემის და ამ ჰოსტის სპეციფიური კრიტიკული სისტემური პროცესების მონიტორინგს.

ლოკალურ ქსელთან შეერთებისა და ფაილების გაზიარების შემდეგ კომპიუტერთა შორის კავშირი არ სცდება ლოკალური ქსელის ფარგლებს. მონაცემები რჩებიან უსაფრთხოდ, ვინაიდან ისინი არ ტოვებენ ქსელს და არ არიან კავშირში სხვა ქსელებთან ან ინტერნეტთან. სხვა ქსელებთან ურთიერთობისა და ფაილთა გაზიარებისათვის გამოიყენება ვირტუალური კერძო ქსელი (VPN – Virtual Private Network).



სურ.7.1. VPN-ის მუშაობის სქემა

VPN არის კერძო ქსელი, რომელიც აკავშირებს დაშორებულ საიტებს ან მომხმარებლებს ერთმანეთთან საჯარო ქსელის - ინტერნეტის

მეშვეობით. VPN-თა ძირითადი ტიპები ახდენენ წვდომას კორპორატიულ კერძო ქსელებთან. VPN იყენებს, კორპორატიული კერძო ქსელიდან დაშორებული მომხმარებლისკენ, ინტერნეტში მარშრუტიზირებულ გამოყოფილ უსაფრთხო კავშირებს. კორპორატიულ კერძო ქსელებთან შეერთებისას მომხმარებლები ხდებიან ამ ქსელის ნაწილი ისე, თითქოს მათ ჰქონდეთ ფიზიკური კავშირი კორპორატიული LAN-ის სერვერებთან და რესურსებთან.

დაშორებული წვდომის მომხმარებლებს უნდა ჰქონდეთ ინსტალირებული VPN-კლიენტი თავიანთ კომპიუტერებზე, რათა შეძლონ დაამყარონ უსაფრთხო კავშირი კორპორატიულ კერძო ქსელთან. VPN კლიენტის პროგრამული უზრუნველყოფა დაშიფრავს მონაცემებს, მათი კორპორატიული კერძო ქსელის VPN კარიბჭეზე გაგზავნის წინ, მანამ სანამ ისინი გაიგზავნება ინტერნეტის გავლით. VPN კარიბჭეები (VPN gateways), რომლებიც ამყარებენ, მართავენ და აკონტროლებენ VPN კავშირებს, ასევე ცნობილია როგორც VPN გვირაბები (VPN tunnels).

ოპერაციული სისტემები მოიცავენ VPN კლიენტს, რომელსაც მომხმარებელი გამართავს VPN კავშირისთვის. VPN-ის უპირატესობებია:

- VPN-ის გამოყენებისას შეგიძლიათ IP-ის შეცვლა.
- ინტერნეტი უსაფრთხოა და დაშიფრული.
- ფაილის გაზიარება არის პირადი და უსაფრთხო.
- თქვენი კონფიდენციალურობა დაცულია ინტერნეტით სარგებლობისას.
- აღარ არსებობს გამტარუნარიანობის შეზღუდვები.
- ეს დაზოგავს ხარჯებს.

თანამედროვე კომპიუტერული ტექნიკის ერთ-ერთი ყველაზე მნიშვნელოვანი კომპონენტია მობილური მოწყობილობები. დღევანდელ ქსელებში გაერთიანებული მოწყობილობების უმრავლესობა ლაპტოპები, ტაბლეტები, სმარტფონები და სხვა უსადენო მოწყობილობებია. მობილური მოწყობილობები გადასცემენ მონაცემებს რადიო სიგნალების გამოყენებით, რომელთაც ნებისმიერი მოწყობილობა თავსებადი ანტენით მიიღებს. ამ მიზეზით

კომპიუტერულმა ინდუსტრიამ შეიმუშავა უსადენო ან მობილური უსაფრთხოების სტანდარტების, პროდუქტებისა და მოწყობილობების კომპლექტი. ეს სტანდარტები ახდენენ მობილური მოწყობილობებით ჰაერში გადაცემული ინფორმაციის დაშიფვრას.

WEP (Wired Equivalent Privacy)

სადენიანი ექვივალენტური კონფიდენციალურობა (WEP) არის ერთ-ერთი პირველი და ფართოდ გამოყენებადი Wi-Fi უსაფრთხოების სტანდარტი. WEP სტანდარტი უზრუნველყოფს აუთენტიფიკაციას და დაშიფვრის დაცვას. WEP სტანდარტები მოძველებულია, მაგრამ ბევრი მოწყობილობას კვლავ გააჩნია WEP-ის თავსებადობის მხარდაჭერა. WEP სტანდარტი გახდა Wi-Fi უსაფრთხოების სტანდარტი 1999 წელს, როდესაც უსადენო კომუნიკაცია მხოლოდ იწყებდა გავრცელებას. მიუხედავად სტანდარტის რევიზიისა და გასაღების გაზრდილი ზომისა, WEP-ს გააჩნდა მრავალი უსაფრთხოების სისუსტე. კიბერ დამნაშავეებს შეუძლიათ WEP პაროლების გატეხვა წუთებში თავისუფლად ხელმისაწვდომი პროგრამული უზრუნველყოფის გამოყენებით. გაუმჯობესების მიუხედავად, WEP რჩება უაღრესად დაუცველი და მომხმარებლებს სჭირდებათ სისტემების მუდმივი განახლება, რომლებიც ეყრდნობიან WEP-ს.

WPA/WPA2 (Wi-Fi Protected Access)

უსადენო უსაფრთხოების შემდეგი ძირითად გაუმჯობესებას წარმოადგენდა WPA და WPA2-ის რეალიზაცია. Wi-Fi დაცული წვდომა (WPA) იყო კომპიუტერული ინდუსტრიის პასუხი WEP სტანდარტის სისუსტეზე. ყველაზე გავრცელებულ WPA კონფიგურაციას წარმოადგენს WPA-PSK (წინასწარ გაზიარებული გასაღები). WPA- ს მიერ გამოყენებული გასაღებები 256 ბიტიანია, WEP სისტემაში გამოყენებულია 64-ბიტიანი და 128 ბიტიანი კგასაღებების ზომის მნიშვნელოვანი ზრდა.

WPA სტანდარტი უზრუნველყოფდა რამდენიმე უსაფრთხოების პარამეტრის გაუმჯობესებას. უპირველეს ყოვლისა, WPA უზრუნველყოფს გზავნილის მთლიანობის შემოწმებას (MIC), რომელმაც შეიძლება აღმოაჩინოს, შეძლო თუ არა თავდამსხმელმა

"დაეჭირა" და შეეცვალა მონაცემები, რომლებიც გადაცემულ იქნა უსადენო დაშვების წერტილსა და უსადენო კლიენტს შორის. კიდევ ერთი ძირითადი უსაფრთხოების გაფართოება იყო დროებითი გასაღების მთლიანობის პროტოკოლი (TKIP)-ს შემუშავება. TKIP სტანდარტი უზრუნველყოფს უნარს, უკეთ გაუმკლავდეს, დაიცვას და შეცვალოს დაშიფვრის გასაღებები. Advanced Encryption Standard (AES) შეიცვალა TKIP სტანდარტით უკეთესი გასაღების მართვისა და დაშიფვრის დაცვის უზრუნველყოფის მიზნით.

WPA, ისევე როგორც მისი წინამორბედი WEP, შეიცავს რამდენიმე ფართოდ აღიარებულ მოწყვლადობას. შედეგად, 2006 წელს მოხდა Wi-Fi დაცული წვდომის II (WPA2) სტანდარტის შემუშავება. WPA-დან WPA2-ზე გადასვლისას უსაფრთხოების ერთ-ერთი ყველაზე მნიშვნელოვანი გაუმჯობესება იყო AES ალგორითმების სავალდებულო გამოყენება და ანტი-ბლოკჩეინის დაშიფვრის რეჟიმის დანერგვა.

უკაბელო ქსელების ერთ-ერთი ყველაზე სერიოზული დაუცველობაა არაავტორიზებული წვდომის წერტილების გამოყენება. წვდომის წერტილები არის მოწყობილობები, რომლებიც ურთიერთობენ უსადენო მოწყობილობებთან და აკავშირებენ მათ სადენიან ქსელთან. ნებისმიერ მოწყობილობას, რომელსაც აქვს უკაბელო გადამცემი და სადენიანი ინტერფეისი ქსელთან დასაკავშირებლად, შეიძლება პოტენციურად იმოქმედოს როგორც თაღლითური ან ბოროტი წვდომის წერტილი. თვითმარქვიას შეუძლია ავტორიზებული წვდომის წერტილის იმიტაცია. შედეგად, უკაბელო მოწყობილობები უკავშირდებიან მას, ავტორიზებული წვდომის წერტილის ნაცვლად.

თვითმარქვია წვდომის წერტილს შეუძლია მიიღოს მოთხოვნები შეერთებაზე, დააკოპიროს მონაცემები ამ მოთხოვნაში და შემდეგ გადააგზავნოს მონაცემები ავტორიზებულ ქსელის წვდომის წერტილზე. ამ ტიპის “კაცი შუაში” (man-in-the-middle) თავდასხმა ძალიან რთული გამოსავლენია და მას შეუძლია გამოიწვიოს სააღრიცხვო მონაცემებისა და სხვა გადაცემული მონაცემების დაკარგვა. ამის თავიდან ასაცილებლად, კომპიუტერულმა ინდუსტრიამ განავითარა ურთიერთშორისი აუთენტიფიკაცია.

ურთიერთშორისი აუთენტიფიკაცია, რომელსაც ასევე ეწოდება ორი გზის აუთენტიფიკაცია, არის პროცესი ან ტექნოლოგია, რომელშიც ორივე სუბიექტი კომუნიკაციის პროცესში ახდენს ერთმანეთის აუთენტიფიკაციას. უსადენო ქსელის გარემოში, კლიენტი ახდენს აუთენტიფიკაციას წვდომის წერტილზე და წვდომის წერტილი ახდენს კლიენტის დამოწმებას. ეს გაუმჯობესება საშუალებას აძლევს კლიენტებს, აღმოაჩინონ თვითმარქვია წვდომის წერტილი მანამ, სანამ დაუკავშირდებოდნენ არასანქცირებულ მოწყობილობას.

ნებართვები წარმოადგენენ წესებს, რომლებიც განსაზღვრავენ ფაილებსა და საქაღალდეებზე წვდომის ნებართვებს ინდივიდულაური მომხმარებლისა და მომხმარებელთა ჯგუფებისათვის. მომხმარებლებს უნდა გააჩნდეთ წვდომა მხოლოდ იმ რესურსებზე, რომელთა საჭიროებასაც ისინი განიცდიან. მაგალითად, მათ არ უნდა ჰქონდეთ წვდომის საშუალება სერვერის ყველა ფაილთან, თუ მათ სჭირდებათ მხოლოდ ერთი საქაღალდე. უფრო მარტივია, გაცემულ იქნას ნებართვა მთელი დისკის წვდომაზე, მაგრამ უფრო უსაფრთხოა წვდომის შეზღუდვა ერთ ან რამდენიმე საქაღალდეზე, რომლებიც აუცილებელია მომხმარებლისათვის თავისი სამუშაოს შესასრულებლად. ეს წარმოადგენს მინიმალური პრივილეგიების პრინციპს. რესურსებთან წვდომის შეზღუდვა ასევე უკრძალავს საზიანო პროგრამებს ჰქონდეთ წვდომა ამ რესურსებთან თუ მომხმარებლის კომპიუტერი დაინფიცირდება ვირუსით.

თუ ადმინისტრატორი კრძალავს წვდომას ქსელის გაზიარებაზე ინდივიდის ან ინდივიდთა ჯგუფისათვის, ეს აკრძალვა გადაფარავს ყველა დაშვების პარამეტრს. მაგალითად, თუ ადმინისტრატორი უკრძალავს მომხმარებელს წვდომას ქსელის გაზიარებაზე, ამ მომხმარებელს ეკრძალება წვდომა ამ გაზიარებაზე იმ შემთხვევაშიც კი, თუ იგი წარმოადგენს ადმინისტრატორს ან არის წევრი ადმინისტრატორთა ჯგუფისა. ლოკალური უსაფრთხოების პოლიტიკამ უნდა გამოკვეთოს, რომელი რესურსები და რა ტიპის წვდომაა დაშვებული თითოეული მომხმარებლისა და ჯგუფისათვის.

როდესაც მომხმარებელი ცვლის ნებართვას საქაღალდეზე, ეს შეცვლა ვრცელდება ამ საქაღალდეში არსებულ ყველა ქვე-საქაღალდეზე. ამას

ეწოდება ნებართვის გავრცელება. ნებართვების გავრცელება არის ადვილი გზა უფლებების გაცემისა ბევრ ფაილსა და საქაღალდეზე სწრაფი წვდომის მისაღწევად. მას შემდეგ, რაც გაწერილია მშობელი საქაღალდის ნებართვა, მასში შექმნილი ყველა ფაილი და საქაღალდე მემკვიდრეობით მიიღებს მშობელ საქაღალდეზე გაწერილ ნებართვებს.

დაშიფვრა არის ინსტრუმენტი, რომელიც გამოიყენება მონაცემთა დასაცავად. დაშიფვრა ახდენს მონაცემთა ტრანსფორმირებას რთული ალგორითმის გამოყენებით ისე, რომ შეუძლებელი ხდება მათი წაკითხვა. სპეციალური გასაღების მეშვეობით შესაძლებელი ხდება ტრანსფორმირებული მონაცემების გარდაქმნა ისევ წაკითხვადად. სპეციალური პროგრამული პროდუქტი ახდენს ფაილთა, საქაღალდეთა და მთლიანი დისკის დაშიფვრას.

Encrypting File System (EFS) შიფრაციის ფაილური სისტემა არის Windows-ის კომპონენტი, რომელსაც შეუძლია მონაცემთა დაშიფვრა. EFS Windows-ის განხორციელება უშუალოდ კონკრეტული მომხმარებლის ანგარიშს უკავშირდება. მხოლოდ იმ მომხმარებელს, რომელმაც დაშიფრა მონაცემები, ექნება წვდომა დაშიფრულ ფაილებთან ან საქაღალდეებთან. მომხმარებელს ასევე შეუძლია დაშიფროს მთლიანი დისკი BitLocker-ის გამოყენებით.

BitLocker-ის გამოყენებამდე მომხმარებელმა უნდა ჩართოს TPM (Trusted Platform Module) ფუნქცია ბიოსში. TPM არის სპეციალიზირებული ჩიპი, რომელიც ინსტალირებულია დედა დაფაზე. TPM ინახავს კონკრეტული ჰოსტ სისტემის ინფორმაციას, როგორიცაა შიფრაციის გასაღებები, ციფრული სერტიფიკატები და პაროლები. BitLocker-ის მსგავს აპლიკაციებს, რომლებიც იყენებენ შიფრაციას, შეუძლიათ გამოიყენონ TPM ჩიპი.

იმ შემთხვევებში, თუ კიბერ დამნაშავეები ახდენენ თავდასხმას, ორგანიზაციას შეუძლია დაკარგოს მონაცემები. ხდება აპარატურის მტყუნება ან რაიმე სახის კატასტროფა. ამ შემთხვევებისათვის, მეტად მნიშვნელოვანია მონაცემთა სარეზერვო ასლების შექმნა რეგულარულად.

მონაცემთა სარეზერვო ასლები ახდენენ მონაცემთა ასლების შენახვას კომპიუტერიდან მოსახსნელ მედიაზე. ოპერატორი ინახავს სარეზერვო მედიას უსაფრთხო ადგილას. მონაცემთა სარეზერვო ასლის შექმნა ერთ ერთი ეფექტური გზაა მონაცემების დაკარგვისგან დასაცავად. კომპიუტერული აპარატურის მწყობრიდან გამოსვლის შემთხვევაში მომხმარებელს შეუძლია მონაცემთა აღდგენა სარეზერვო ასლიდან მას შემდეგ, რაც აპარატურის ფუნქციონალობა გაგრძელდება.

ორგანიზაციის უსაფრთხოების პოლიტიკა უნდა შეიცავდეს მონაცემთა სარეზერვო ასლების შექმნას. მომხმარებელი რეგულარულად უნდა ასრულებდეს მონაცემთა სარეზერვო შენახვას. მონაცემთა სარეზერვო ასლები, როგორც წესი, ინახება გარეთ, რათა დაცული იყოს სარეზერვო ასლის მედია საშუალება იმ შემთხვევაში, თუ რაიმე მოხდა მთავარი ობიექტის შიგნით. მონაცემთა სარეზერვო ასლების ძირითადი მახასიათებლებია:

სიხშირე - სარეზერვო ასლების შექმნამ შესაძლოა წაიღოს საკმაოდ დიდი დრო. ზოგჯერ უფრო ადვილია სრული სარეზერვო ასლის გაკეთება ყოველთვიურად ან ყოველკვირეულად, და შემდეგ იმ მონაცემების ნაწილობრივი სარეზერვო ასლების ხშირი შექმნა, რომლებმაც განიცადეს ცვლილება ბოლო სრული სარეზერვო ასლის შექმნის შემდეგ. თუმცა, ბევრი დანაწევრებული სარეზერვო ასლის ქონა ზრდის მონაცემთა აღდგენისთვის საჭირო დროს.

შენახვა - უკიდურესი უსაფრთხოების განსახორციელებლად უნდა განხორციელდეს სარეზერვო ასლების გადატანა საიტს მიღმა არსებულ ლოკაციაზე ყოველდღიურად, ყოველკვირეულად ან ყოველთვიურად, გამომდინარე კომპანიის უსაფრთხოების პოლიტიკიდან.

უსაფრთხოება — დაცული უნდა იყოს სარეზერვო პაროლები.

ვალიდაცია - ყოველთვის უნდა განხორციელდეს ვალიდაცია მონაცემთა სარეზერვო ასლების აღდგენამდე, რათა დარწმუნდეთ მონაცემთა მთლიანობაში.

კონტენტის მართვის პროგრამული უზრუნველყოფა ზღუდავს იმ შინაარსს, რომელზე წვდომაც მომხმარებელს შეუძლია ინტერნეტის

საშუალებით, ვებ-ბრაუზერის გამოყენებით. კონტენტის მართვის პროგრამამ შეიძლება დაბლოკოს ისეთი საიტები, რომლებიც შეიცავენ გარკვეულ მასალას, როგორიცაა პორნოგრაფია ან საკამათო რელიგიური ან პოლიტიკური ტექსტი. მშობელს შეუძლია მოახდინოს კონტენტის კონტროლის პროგრამული უზრუნველყოფის რეალიზება კომპიუტერში, რომელსაც იყენებს არასრულწლოვანი. ბიბლიოთეკები და სკოლები ასევე ახდენენ ამ პროგრამული უზრუნველყოფის რეალიზებას, რათა თავიდან იქნას აცილებული არასასურველი კონტენტის ხელმისაწვდომობა. აღნიშნულის განსახორციელებლად, ადმინისტრატორს შეუძლია განახორციელოს შემდეგი სახის ფილტრები:

- ბრაუზერზე დაფუძნებული ფილტრები;
- ელ. ფოსტის ფილტრები კლიენტზე ან სერვერზე დაფუძნებული ფილტრების განხორციელებით;
- კლიენტის მხარის ფილტრები, დაინსტალირებული კონკრეტულ კომპიუტერზე;
- მარშრუტიზატორზე დაფუძნებული კონტენტის ფილტრები, რომლებიც ბლოკავენ ტრაფიკს ქსელში შესვლისას;
- მოწყობილობაზე დაფუძნებული კონტენტის ფილტრაცია, რომელიც მოქმედებს მარშრუტიზატორზე დაფუძნებულის ფილტრაციის მსგავსად;
- Cloud-ზე დაფუძნებული კონტენტის ფილტრაცია.

საძიებო სისტემები, როგორიცაა Google, გვთავაზობენ უსაფრთხოების ფილტრის ჩართვის ვარიანტს ძიების შედეგებისგან შეუსაბამო კავშირების გამორიცხვის მიზნით.

დისკის კლონირება ასრულებს კომპიუტერის მყარ დისკზე არსებულ მონაცემთა კოპირებას იმიჯის ფაილში. მაგალითად, ადმინისტრატორი ქმნის საჭირო დანაყოფებს სისტემაში, აფორმატებს დანაყოფს და შემდეგ აინსტალირებს ოპერაციულ სისტემას. იგი აინსტალირებს ყველა საჭირო პროგრამულ პროგრამას და ახდენს აპარატურის კონფიგურირებას. ადმინისტრატორი შემდეგ იყენებს დისკის კლონირების პროგრამას, რათა შექმნას იმიჯის ფაილი.

Deep Freeze „ყინავს“ მყარი დისკის დანაყოფს. როდესაც მომხმარებელი გადატვირთვას სისტემას, სისტემა დააბრუნებს ამ "გაყინულ"

კონფიგურაციას. სისტემა არ შეინახავს რაიმე ცვლილებას, რომელიც მომხმარებელი ახდენს, ამიტომ ნებისმიერი დაინსტალირებული პროგრამა ან შენახული ფაილი იკარგება სისტემის გადატვირთვის შემდეგ.

თუ ადმინისტრატორს სისტემის კონფიგურაციის შეცვლა სჭირდება, მან ჯერ უნდა "გაალღოს" დაცული დანაყოფი Deep Freesi-ის გამორთვით. ცვლილებების შეტანის შემდეგ, მან უნდა ხელახლა ჩართოს პროგრამა. ადმინისტრატორს შეუძლია მოახდინოს Deep Freeze-ის კონფიგურირება ისე, რომ სისტემა გადაიტვირთოს მომხმარებლის სისტემიდან გასვლის შემდეგ, გამოირთოს გარკვეული არაქტიური დროის შემდეგ ან მითითებულ დროს.

არსებობს კომპიუტერული ტექნიკის ფიზიკური დაცვის რამოდენიმე მეთოდი. მათ შორის ერთ-ერთია ე.წ. „ჩამკეტი კაბელი“. მრავალ პორტატულ მოწყობილობას და ძვირადღირებულ კომპიუტერის მონიტორებს აქვთ სპეციალური ფოლადის კრონშტეინის უსაფრთხოების სლოტი, რომელიც ჩაშენებულია კაბელების ჩამკეტთან ერთად.

კარის ჩამკეტის ყველაზე გავრცელებული ტიპია სტანდარტული გასაღებიანი კარების ჩამკეტი. ის ავტომატურად არ იბლოკება, როდესაც კარი იხურება. გარდა ამისა, ინდივიდს შეუძლია გამოიყენოს თხელი პლასტიკური ბარათი, როგორიცაა საკრედიტო ბარათი, გააცუროს ის საკეტსა და კარების გარსაცმებს შორის და გააღოს იგი. კარის ჩამკეტები კომერციულ შენობებში განსხვავდება საცხოვრებელი კარის საკეტებისაგან. დამატებითი უსაფრთხოების უზრუნველსაყოფად, deadbolt უზრუნველყოფს დამატებით უსაფრთხოებას. ნებისმიერი ჩაკეტვა, რომელიც მოითხოვს გასაღებს, ქმნის მოწყვლადობას, თუ გასაღებები დაიკარგა, მოიპარეს ან შექმნეს მისი დუბლიკატი.

ციფრული ჩამკეტი იყენებს ღილაკებს, რომლის ღილაკებზე ძესაბამისი კოდის აკრეფის შემდეგ კარები იღება. შესაძლებელია ციფრული საკეტის დაპროგრამება. ეს იმას ნიშნავს, რომ მომხმარებლის კოდი შეიძლება მუშაობდეს მხოლოდ რამდენიმე დღის ან გარკვეული დროის განმავლობაში. მაგალითად, ციფრულ საკეტს შეუძლია დაუშვას მხოლოდ ერთი ადამიანი სასერვერო ოთახში დილის 7 საათიდან საღამოს 6 საათამდე ორშაბათიდან პარასკევის ჩათვლით. ციფრულ საკეტებს ასევე შეუძლია შეინახონ ჩანაწერი, თუ როდის მოხდა კარის გაღება და რომელი კოდის გამოყენებით.

სისტემიდან გამოსვლის ტაიმერები ასევე წარმოადგენს პერსონალური კომპიუტერის დაცვის მნიშვნელოვან ფინქციას. თანამშრომელი ტოვებს თავის კომპიუტერს შესვენებაზე გასვლისას. თუ თანამშრომელი არ ატარებს რაიმე ქმედებას მისი სამუშაო სადგურის უსაფრთხოების უზრუნველსაყოფად, მისი სისტემის შესახებ ნებისმიერი ინფორმაცია დაუცველია არაავტორიზებული მომხმარებლისთვის. ორგანიზაციამ უნდა უზრუნველყოს შესაბამისი ზომები, რათა ხელი შეუშალონ არაავტორიზებულ წვდომას. მაგ., განსაზღვროს დაყოვნების დრო, რათა მოხდეს ეკრანის დაბლოკვა.

სამუშაო ადგილის დატოვებისას მომხმარებელს შეუძლია გამოვიდეს ან არ გამოვიდეს სისტემიდან. შესაბამისად, უსაფრთხოების საუკეთესო პრაქტიკა ითვალისწინებს დაყოვნების დროის დაყენებას, რის შემდეგაც გარკვეული დროის გასვლის შემდეგ სისტემა ავტომატურად დახურავს სესიას და მოახდენს ეკრანის ბლოკირებას. მომხმარებელი უკან უნდა შევიდეს სისტემაში ეკრანის დაბლოკვის მოსახსნელად პაროლის გამოყენებით.

ზოგიერთ შემთხვევაში, ორგანიზაციამ შეიძლება მოითხოვოს, რომ თანამშრომლები შევიდნენ სისტემაში კონკრეტული პერიოდის განმავლობაში, მაგალითად, დილის 7 საათიდან საღამოს 6 საათამდე, შესაბამისად, სისტემა ბლოკავს სისტემაში შესვლის მცდელობებს სხვა დროის პერიოდში.

გლობალური პოზიციონირების სისტემა (GPS) იყენებს თანამგზავრებსა და კომპიუტერებს, რათა დადგინდეს მოწყობილობის მდებარეობა. GPS ტექნოლოგია არის სტანდარტული ფუნქცია სმარტფონებზე, რომლებიც უზრუნველყოფენ რეალურ დროში ადგილმდებარეობის მოძიებას. GPS თვალთვალით შეიძლება დადგინდეს ადგილმდებარეობა 100 მეტრის ფარგლებში. ეს ტექნოლოგია ხელმისაწვდომია ბავშვების, უფროსი მოქალაქეების, შინაური ცხოველების და სატრანსპორტო საშუალებების გასაკონტროლებლად. GPS-ის გამოყენება მობილური ტელეფონის განთავსების მოსაძიებლად მომხმარებლის ნებართვის გარეშე წარმოადგენს კონფიდენციალურობის დარღვევას და ეს უკანონო ქმედებაა.

მრავალი მობილური ტელეფონის აპლიკაცია იყენებს GPS თვალთვალს ტელეფონის ადგილმდებარეობის გასაკონტროლებლად. მაგალითად, Facebook საშუალებას აძლევს მომხმარებლებს დაადგინონ მდებარეობა, რომელიც შემდეგ აისახება სხვა ადამიანთა სოციალურ ქსელებში.

რადიოსიხშირული იდენტიფიკაცია (RFID) იყენებს რადიოტალღებს ობიექტების იდენტიფიცირებისა და თვალთვალის მიზნით. RFID ინვენტარის სისტემები იყენებენ ტეგებს, მიმაგრებულს ყველა იმ ელემენტზე, რომელთა თვალთვალიც სურს ორგანიზაციას. ტეგები შეიცავენ ინტეგრირებულ მიკროსქემასს, რომელიც დაკავშირებულია ანტენასთან. RFID ტეგი მცირე ზომისაა და მოითხოვს ძალიან მცირე ენერგიას, ამიტომ მათ არ სჭირდებათ ბატარეა ინფორმაციის შესანახად ან მისი წამკითხველთან მიმოცვლისათვის. RFID-ს შეუძლია მოახდინოს აქტივების მოკვლევა ან ელექტრონული მოწყობილობების ჩაკეტვა, გახსნა და სხვა სახის კონფიგურირება.

RFID სისტემები ფუნქციონირებენ სხვადასხვა სიხშირეებზე. დაბალი სიხშირის სისტემებს გააჩნიათ მოკლე დიაპაზონზე წაკითხვის უნარი დაბალი სიჩქარით, მაგრამ არ არიან მგრძნობიარენი რადიო სიხშირეთა ინტერფერენციის მიმართ, რომელთაც იწვევენ ამ სისტემებში არსებული მეტალი და სითხეები. შედარებით მაღალი სიხშირეებით

მონაცემების გადაცემის სიჩქარეც უფრო მაღალია, მაგრამ ის უფრო მგრძნობიარეა რადიო სიხშირეთა ინტერფერენციის მიმართ.

7.2 სერვერების უსაფრთხო მართვა ქსელში

დაშორებული წვდომა ეხება აპარატურისა და პროგრამული უზრუნველყოფის ნებისმიერ კომბინაციას, რომელიც საშუალებას აძლევს მომხმარებლებს, მიიღონ ადგილობრივი შიდა ქსელზე წვდომა დისტანციურად.

ვინდოუსის ოპერაციულ სისტემაში ტექნიკოსებს შეუძლიათ გამოიყენონ დაშორებული სამუშაო მაგიდა (Remote Desktop) ან დაშორებული ასისტენტი (Remote Assistance) კომპიუტერთა აღსადგენად ან გასაახლებლად. დაშორებული სამუშაო მაგიდა საშუალებას აძლევს ტექნიკოსებს, თვალყური ადევნონ და მართონ კომპიუტერი დაშორებული ლოკაციიდან. დისტანციური დახმარება (Remote Assistance), აძლევს საშუალებას ტექნიკოსებს დაშორებული ადგილმდებარეობიდან დაეხმაროს კლიენტებს პრობლემების გადაჭრაში. დაშორებული ასისტენტი (Remote Assistance) ასევე საშუალებას აძლევს ტექნიკოსებს, აღადგინონ ან განაახლონ კომპიუტერი ეკრანზე.

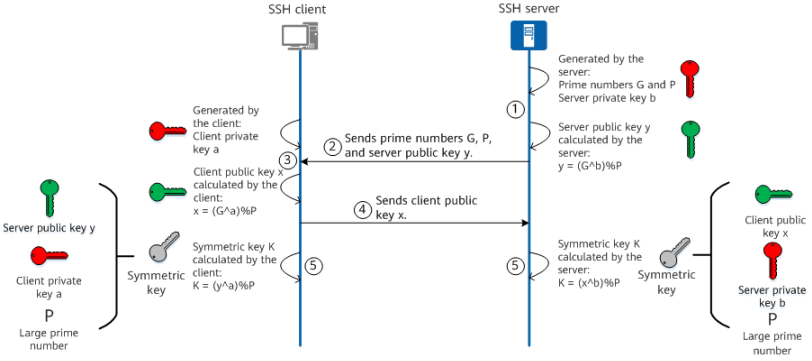
Windows- ის ინსტალაციის პროცესი არ ჩართავს დაშორებულ სამუშაო მაგიდას ნაგულისხმევად. ამ ფუნქციის ჩართვა ახორციელებს 3389 პორტის გახსნას და შეიძლება გამოიწვიოს მოწყვლადობა, თუ მომხმარებელი არ საჭიროებს ამ სერვისს.

უსაფრთხო გარსი (SSH - Secure Shell) წარმოადგენს პროტოკოლს, რომელიც უზრუნველყოფს უსაფრთხო (დაშიფრულ) მართვას დაშორებული მოწყობილობისათვის. SSH-მ უნდა ჩაანაცვლოს ტელნეტის მართვის შეერთება. ტელნეტი წარმოადგენს მოძველებულ პროტოკოლს, რომელიც ახორციელებს დაუშიფრავ, ღია ტექსტის გადაცემას ორივე (სახელისა და პაროლის) აუთენტიფიკაციისათვის და ასევე მონაცემთა გადაცემისათვის. SSH უზრუნველყოფს დაშორებული წვდომის უსაფრთხოებას ძლიერი დაშიფვრით მომხმარებლის აუთენტიფიკაციის პროცესში (სახელი და პაროლი) და მონაცემთა

ტრანზაქციისას კომუნიკაციაში მყოფ მოწყობილობათა შორის. SSH იყენებს TCP-ის 22-ე პორტს. ტელნეტი იყენებს TCP-ის 23-ე პორტს.

გასაღების გაცვლა წარმოადგენს SSH პროტოკოლის მნიშვნელოვან პროცესს. SSH სერვერი და კლიენტი იყენებენ გასაღების გაცვლის ალგორითმს, რათა დინამიურად დააგენერირონ საერთო სესიის გასაღები და სესიის ID, დაშიფრული არხის დასამყარებლად. სესიის გასაღები გამოიყენება გადასაცემი მონაცემების დასაშიფრად, ხოლო სესიის ID გამოიყენება ავთენტიფიკაციის დროს შესაბამისი SSH კავშირის იდენტიფიცირებისთვის. ამ ეტაპზე კლიენტი ასევე ასრულებს სერვერის იდენტიფიკაციას და ავთენტიფიკაციას. პროცესი იმაში მდგომარეობს, რომ სერვერი იყენებს თავის პირად გასაღებს შეტყობინებების ხელმოწერისთვის, ხოლო კლიენტი იყენებს სერვერის საჯარო გასაღებს ხელმოწერის დასადასტურებლად.

SSH სერვერმა და კლიენტმა უნდა შეინახონ ერთი და იგივე სესიის გასაღები შემდგომი სიმეტრიული დაშიფვრისთვის. გასაღების გაცვლის უსაფრთხოების უზრუნველსაყოფად, SSH წარმოქმნის სესიის გასაღებს უსაფრთხო მეთოდის გამოყენებით: SSH სერვერი და კლიენტი ერთობლივად ქმნიან სესიის გასაღებს. უფრო ზუსტად, მათემატიკური თეორიებიდან გამომდინარე, გასაღების გაცვლა ხორციელდება გასაღების პირდაპირი გადაცემის გარეშე, ამიტომ გასაღები არ საჭიროებს გადაცემას დაუცველ არხზე.



სურ. 7.2. SSH გასაღების გაცვლის პროცესი

1. SSH სერვერი აგენერირებს პირველ რიცხვებს G და P და სერვერის პირად გასაღებს b-ს და ითვლის სერვერის საჯარო გასაღებს y-ს შემდეგი ფორმულის გამოყენებით: y = (G^b)%P.

2. SSH სერვერი უგზავნის პირველ რიცხვებს G და P და სერვერის საჯარო გასაღებს y-ს, SSH კლიენტს.

3. SSH კლიენტი წარმოქმნის კერძო გასაღებს a და ითვლის კლიენტის საჯარო გასაღებს x შემდეგი ფორმულის გამოყენებით: x = (G^a)%P.

4. SSH კლიენტი აგზავნის კლიენტის საჯარო გასაღებს x-ს, SSH სერვერზე.

5. SSH სერვერი ითვლის K სიმეტრიულ გასაღებს K=(x^b)%P ფორმულის გამოყენებით, ხოლო SSH კლიენტი ითვლის K სიმეტრიულ გასაღებს K = (y^a)%P ფორმულის გამოყენებით. მათემატიკური კანონები უზრუნველყოფს, რომ SSH სერვერისა და კლიენტის მიერ გენერირებული სიმეტრიული გასაღებები ერთნაირია.

უსაფრთხო ასლი (SCP) უსაფრთხოდ გადასცემს კომპიუტერულ ფაილებს ორ დისტანციურ სისტემას შორის. SCP იყენებს SSH-ს მონაცემთა გადაცემისთვის (მათ შორის ავტორიზაციის ელემენტს), ამიტომ SCP უზრუნველყოფს გადაცემული მონაცემების ნამდვილობასა და კონფიდენციალურობას.

კიბერ დამნაშავეები იყენებენ სისტემაში გაშვებულ სერვისებს, რადგან იციან, რომ მოწყობილობათა უმეტესობა უფრო მეტ მომსახურებას ან პროგრამებს უშვებენ, ვიდრე მათ სჭირდებათ. ადმინისტრატორმა უნდა შეისწავლოს ყველა სერვისი, რათა შეამოწმოს მათი აუცილებლობა და შეაფასოს მათი გამოყენების რისკები. უმარტივესი მეთოდი, რომელსაც იყენებენ ქსელის ადმინისტრატორები არაავტორიზებული წვდომის თავიდან ასაცილებლად, არის გამოუყენებელი პორტების გამორთვა. მაგალითად, თუ კომუტატორს გააჩნია 24 პორტი და აქედან გამოყენებულია მხოლოდ 3 სწრაფი ეთერნეტის პორტი, დანარჩენი 21-ის გამორთვა იქნება მიზანშეწონილი. პორტის ჩართვისა და გამორთვის პროცესი მოითხოვს გარკვეულ დროს, მაგრამ ეს ამაღლებს ქსელის უსაფრთხოების უზრუნველყოფას.

კიბერ დამნაშავეები ცდილობენ წვდომა მოიპოვონ პრივილეგირებულ ანგარიშებზე, რადგან ისინი ყველაზე ძლიერი ანგარიშებია ორგანიზაციაში. პრივილეგირებულ ანგარიშებს გააჩნიათ სააღრიცხვო მონაცემები, რათა მიიღონ მაღალი დონის შეუზღუდავი წვდომა სისტემებზე. ადმინისტრატორები იყენებენ ამ ანგარიშებს ოპერაციული სისტემების, აპლიკაციებისა და ქსელური მოწყობილობების განთავსებასა და მართვაში.

ორგანიზაციამ უნდა მიიღოს პრივილეგირებული ანგარიშების უზრუნველყოფის შემდეგი საუკეთესო პრაქტიკა:

- პრივილეგირებული ანგარიშების რაოდენობის იდენტიფიცირება და შემცირება;
- ნაკლებად პრივილიგირებული სააღრიცხვო ანგარიშების შემუშავება;
- დასაქმების ადგილის დატოვების ან შეცვლისას უფლებების გაუქმების პროცესის ჩამოყალიბება;
- საერთო ანგარიშების წაშლა პაროლებით, რომელთა ვადა არ იწურება;
- პაროლების უსაფრთხო შენახვა;
- სხვადასხვა ადმინისტრატორებისთვის საერთო სააღრიცხვო ანგარიშების აღმოფხვრა;
- პრივილეგირებული ანგარიშის პაროლების ავტომატურად შეცვლა ყოველ 30 ან 60 დღეში;
- პრივილეგირებული სესიების ჩაწერა;
- პროცესის განხორციელება, რათა შეიცვალოს მიბმული პაროლები სკრიპტებისა და მომსახურების ანგარიშებისათვის;
- ყველა მომხმარებლის საქმიანობის ლოგირება;
- შეტყობინებების გენერირება უჩვეულო ქცევისთვის;
- არააქტიური პრივილეგირებული ანგარიშების გამორთვა;
- გამოიყენეთ მრავალ ფაქტორიანი აუთენტიფიკაცია ყველა ადმინისტრაციული წვდომისთვის;
- მოახდინეთ კარიბჭის გამართვა საბოლოო მომხმარებლებსა და მგრძნობიარე აქტივებს შორის, რათა შეზღუდოთ ქსელზე ზიანის მომტანი პროგრამების ზემოქმედების შესაძლებლობა.

პრივილეგირებული ანგარიშების გამორთვა კრიტიკულად მნიშვნელოვანია ორგანიზაციის უსაფრთხოებისთვის. ამ ანგარიშების

დაცვა უნდა იყოს უწყვეტი პროცესი. ორგანიზაციამ უნდა შეაფასოს ეს პროცესი უსაფრთხოების გასაუმჯობესებლად საჭირო ცვლილებების შესაქმნელად.

უმრავლეს ქსელებში, რომლებშიც გაერთიანებულნი არიან კომპიუტერები ვინდოუსის ოპერაციული სისტემებით, ადმინისტრატორი ახორციელებს აქტიური დირექტორიის შექმნას დომენით ვინდოუს სერვერის ოპერაციულ სისტემაში. Windows კომპიუტერები არიან დომენის წევრები. ადმინისტრატორი აკონფიგურირებს დომენის უსაფრთხოების პოლიტიკას, რომელიც გამოიყენება დომენში გაერთიანებული ყველა კომპიუტერისათვის. სააღრიცხვო ჩანაწერის პოლიტიკები ავტომატურადაა მომართული, როდესაც მომხმარებელი შედის Windows სისტემაში. როდესაც კომპიუტერი არ არის აქტიური დირექტორიის დომენის ნაწილი, მომხმარებელი ქმნის პოლიტიკას Windows-ის ლოკალური უსაფრთხოების პოლიტიკის მეშვეობით.

ლოგირების ჟურნალი აღწერს ყველა მოვლენას, მათი მოხდენის შემდეგ. სისტემაში შესვლის ჩანაწერები ქმნიან ჟურნალის ფაილს და ის შეიცავს ყველა ინფორმაციას, რომელიც დაკავშირებულია კონკრეტულ მოვლენასთან. მაგალითად, აუდიტის ჟურნალი აკონტროლებს მომხმარებლის ავტორიზაციის მცდელობებს, ხოლო წვდომის ჟურნალი უზრუნველყოფს ყველა დეტალს სისტემაში კონკრეტული ფაილების მოთხოვნის შესახებ. მონიტორინგის სისტემის ჟურნალების მეშვეობით შეიძლება დადგინდეს, როგორ მოხდა თავდასხმა და იყო თუ არა თავდაცვა განხორციელებული წარმატებულად.

კომპიუტერული უსაფრთხოების მიზნებისათვის გენერირებული ჟურნალის ფაილების რაოდენობის ზრდით, ორგანიზაციამ უნდა განიხილოს ჟურნალის მართვის პროცესი. ლოგირების მართვა განსაზღვრავს კომპიუტერის უსაფრთხოების ჟურნალის მონაცემების გენერირების, გადაცემის, შენახვის, ანალიზისა და განკარგვის პროცესს.

ორგანიზაციები იყენებენ ქსელებზე დაფუძნებულ ან სისტემებზე დაფუძნებულ უსაფრთხოების პროგრამულ უზრუნველყოფას. ეს

პროგრამა ქმნის უსაფრთხოების ჟურნალს კომპიუტერული უსაფრთხოების მონაცემების უზრუნველსაყოფად. ლოგები სასარგებლოა აუდიტის ანალიზის ჩატარებისა და ტენდენციების და გრძელვადიანი პრობლემების იდენტიფიცირებისათვის. ლოგები ასევე საშუალებას აძლევს ორგანიზაციას უზრუნველყოს დოკუმენტაცია, რომელიც აჩვენებს, რომ იგი შეესაბამება კანონებსა და მარეგულირებელ მოთხოვნებს.

HVAC სისტემები კრიტიკულად მნიშვნელოვანია ორგანიზაციაში ადამიანებისა და საინფორმაციო სისტემების უსაფრთხოებისათვის. თანამედროვე IT ობიექტების შექმნისას, ეს სისტემები ძალიან მნიშვნელოვან როლს ასრულებენ საერთო უსაფრთხოებაში. HVAC სისტემები აკონტროლებენ გარემოს (ტემპერატურას, ტენიანობას, ჰაერის ნაკადს და ჰაერის ფილტრაციას) და მათი დაგეგმვა უნდა მოხდეს და ოპერირდეს მონაცემთა ცენტრის სხვა კომპონენტებთან ერთად, როგორიცაა კომპიუტერული ტექნიკა, კაბელირება, მონაცემთა შენახვა, ხანძარსაწინააღმდეგო, ფიზიკური უსაფრთხოების სისტემები და ელექტროენერგია. თითქმის ყველა ფიზიკური კომპიუტერული ტექნიკის მოწყობილობა რეალიზდება გარემოსდაცვითი მოთხოვნებით, რომლებიც მოიცავენ მისაღებ ტემპერატურასა და ტენიანობის მერყეობას. გარემოსდაცვითი მოთხოვნები გაწერილია პროდუქტის სპეციფიკაციების დოკუმენტში ან ფიზიკური დაგეგმვის სახელმძღვანელოში. კრიტიკულად მნიშვნელოვანია ამ გარემოსდაცვითი მოთხოვნების შენარჩუნება, რათა თავიდან იქნას აცილებული სისტემის ჩავარდნები და გაგრძელდეს IT სისტემების ნორმალური ფუნქციონირება. კომერციული HVAC სისტემები და შენობის მართვის სხვა სისტემები ახლა დაკავშირებულნი არიან ინტერნეტით დისტანციური მონიტორინგისა და კონტროლისთვის. ბოლო დროს განვითარებულმა მოვლენებმა აჩვენა, რომ ასეთმა სისტემებმა (ხშირად „ჭკვიანი სისტემები“) ასევე გაზარდეს უსაფრთხოების პარამეტრები.

ჭკვიან სისტემებთან ასოცირებული ერთ-ერთი რისკი ის არის, რომ პირები, რომლებიც სისტემაში შედიან და მართავენ მას, წარმოადგენენ კონტრაქტორს ან მესამე მხარის ვენდორს. იმის გამო, რომ HVAC ტექნიკოსებმა უნდა უზრუნველყონ ინფორმაციის სწრაფად მოძიება,

გადამწყვეტი მონაცემები ინახება სხვადასხვა ადგილას, რის გამოც მათზე ხელი უფრო მეტ ადამიანს მიუწვდება. ასეთი სიტუაცია საშუალებას აძლევს ინდივიდების ფართო ქსელს, მათ შორის კონტრაქტორების თანამოაზრეებს, მიიღონ HVAC სისტემის სააღრიცხვო ანგარიშები. ამ სისტემების შეფერხებამ შეიძლება მნიშვნელოვანი რისკი შეუქმნას ორგანიზაციის საინფორმაციო უსაფრთხოებას.

აპარატურის მონიტორინგი ხშირად გვხვდება მსხვილი სერვერულ ფერმებში. სერვერული ფერმა არის ობიექტი, სადაც წარმოდგენილია ასობით ან ათასობით სერვერი კომპანიისათვის. Google-ს ბევრი სერვერული ფერმა აქვს მთელს მსოფლიოში, რათა უზრუნველყოს ოპტიმალური მომსახურება. პატარა კომპანიებიც კი ქმნიან ადგილობრივ სერვერულ ფერმებს, რათა უზრუნველყონ თავიანთი ბიზნესის საჭიროებანი. აპარატურის მონიტორინგის სისტემები გამოიყენება ამ სისტემების გამართულობის მონიტორინგისა და სერვერისა და აპლიკაციის სამუშაო დროის დანაკარგის შემცირების მიზნით. თანამედროვე აპარატურის მონიტორინგის სისტემები იყენებენ USB და ქსელურ პორტებს CPU ტემპერატურის, ელექტროენერგიის მიწოდების სტატუსის, გაგრილების სიჩქარისა და ტემპერატურის, მეხსიერების სტატუსის, დისკზე და ქსელის ბარათის სტატუსის გადაცემის მიზნით. აპარატურის მონიტორინგის სისტემები საშუალებას აძლევს ტექნიკოსს მონიტორინგი გაუწიოს ასობით ან ათასობით სისტემას ერთი ტერმინალიდან. სერვერული ფერმების რაოდენობის ზრდასთან ერთად ტექნიკის მონიტორინგის სისტემები წარმოადგენენ აუცილებელ კომპონენტს უსაფრთხოების კონტრღონისძიების რეალიზებაში.

7.3 ქსელური მოწყობილობების დაცვა

ქსელის ოპერაციის ცენტრი (NOC) არის ადგილი, რომელიც შეიცავს იმ ინსტრუმენტებს, რომლებიც უზრუნველყოფენ ადმინისტრატორებს ორგანიზაციის ქსელის დეტალური სტატუსით. NOC განკუთვნილია ნულოვანი ქსელის პრობლემების, მწარმოებლობის მონიტორინგის,

პროგრამული უზრუნველყოფის განაწილებისა და განახლებების, კომუნიკაციებისა და მოწყობილობის მართვისთვის.

უსაფრთხოების ოპერაციის ცენტრი (SOC) არის გამოყოფილი საიტი, რომელიც აკვირდება, აფასებს და იცავს ორგანიზაციის საინფორმაციო სისტემებს, როგორიცაა ვებ-გვერდები, აპლიკაციები, მონაცემთა ბაზები, მონაცემთა ცენტრები, ქსელები, სერვერები და მომხმარებლის სისტემები. SOC წარმოადგენს უსაფრთხოების ანალიტიკოსების გუნდს, რომელიც ახდენს კიბერუსაფრთხოების ინციდენტების გამოვლენას, ანალიზს, რეაგირებას, ანგარიშს და პრევენციას.

სურ. 7.3. NOC და SOC იერარქიული სტრუქტურა

ორივე ეს სუბიექტი იყენებს იერარქიული იარუსის სტრუქტურას მოვლენების დასამუშავებლად. პირველი იარუსი ამუშავებს ყველა მოვლენას და გადასცემს ნებისმიერ მოვლენას, რომელსაც ის ვერ უმკლავდება, მეორე იარუსს. მე-2 იარუსის პერსონალი განიხილავს ღონისძიებას დეტალურად მისი გადაჭრის მიზნით. თუ ისინიც ვერ ახერხებენ მოვლენის დამუშავებას, იგი გადაეცემა მე-3 იარუსის ექსპერტებს.

ქსელის კომუტატორები (Switch) წარმოადგენენ თანამედროვე მონაცემთა საკომუნიკაციო ქსელის გულს. ქსელის კომუტატორების ძირითადი საფრთხეებია ქურდობა, ჰაკერული თავდასხმა და დისტანციური წვდომა, ქსელური პროტოკოლების წინააღმდეგ თავდასხმები, როგორიცაა ARP/STP ან თავდასხმები მწარმოებლობასა და ხელმისაწვდომობაზე. რამდენიმე კონტრზომას და მართვას შეუძლია დაიცვას ქსელური კონცენტრატორები, მათ შორისაა გაუმჯობესებული ფიზიკური უსაფრთხოება, გაფართოებული

კონფიგურირება და შესაბამისი სისტემის განახლებები და პატჩები. კიდევ ერთი ეფექტური მართვაა პორტის უსაფრთხოების განხორციელება. ადმინისტრატორმა უნდა განახორციელოს კომუტატორის ყველა პორტის (ინტერფეისის) დაცვა მის ექსპლუატაციაში შეყვანამდე. ერთ-ერთი გზა პორტზე უსაფრთხოების პარამეტრების რეალიზებისა არის პორტის უსაფრთხოება (port security). პორტის უსაფრთხოება ზღუდავს იმ MAC მისამართთა რიცხვს, რომელნიც დაშვებულია მოცემული პორტის წვდომაზე. კომუტატორი დაუშვებს წვდომას თავის პორტებზე მხოლოდ ლეგიტიმური MAC მისამართებიდან და აღკვეთს მას არალეგიტიმური MAC მისამართებიდან.

VLAN-ები უზრუნველყოფენ მოწყობილობების ლოგიკურ დაჯგუფებას ლოკალური ქსელის ფარგლებში. VLAN-ები იყენებენ ლოგიკურ შეერთებებს და არა ფიზიკურს. კომუტატორის ინდივიდუალური პორტები შეიძლება ასოცირდნენ კონკრეტულ VLAN-ებთან. სხვა პორტები შეიძლება გამოყენებულ იქნან კომუტატორთა ფიზიკური კავშირებისათვის, რაც უზრუნველყოფს VLAN-თა შორის მონაცემთა ტრაფიკს. ამ პორტებს ეწოდება trunk-პორტები.

მაგალითად, HR დეპარტამენტს შეიძლება დასჭირდეს მგრძნობიარე მონაცემების დაცვა. VLAN-ები საშუალებას აძლევს ადმინისტრატორს, დაჰყოს ქსელი შესაბამისი ფაქტორების გათვალისწინებით, როგორებიცაა ფუნქცია, პროექტის ჯგუფი, აპლიკაცია და სხვა, მიუხედავად მოწყობილობის ან მომხმარებლის ფიზიკური ლოკაციისა. VLAN-ის შიგნით მოწყობილობები მოქმედებენ ისე, თითქოს არიან დამოუკიდებელი ქსელის წევრები იმ შემთხვევაშიც კი, როდესაც ისინი იზიარებენ ერთ ქსელურ ინფრასტრუქტურას სხვა VLAN-ებთან. VLAN-ს აქვს შესაძლებლობა, გამოჰყოს მგრძნობიარე მონაცემთა მქონე ჯგუფი ქსელის სხვა ჯგუფებისაგან და შესაბამისად, შეამციროს ინფორმაციის გაჟონვის ალბათობა. Trunk საშუალებას აძლევს პირებს სხვადასხვა VLAN-დან ფიზიკურად დაუკავშირდნენ მრავალჯერად კომუტატორებს.

არსებობს მრავალი სხვადასხვა სახის VLAN მოწყვლადობა და თავდასხმების ტიპები. ეს შეიძლება მოიცავდეს VLAN და Trucking პროტოკოლებზე თავდასხმას. ჰაკერებს ასევე შეუძლიათ განახორციელონ თავდასხმები VLAN-ის მწარმოებლობასა და ხელმისაწვდომობაზე. საერთო კონტროლონისძიებების ჩამონათვალი მოიცავს VLAN-ის ცვლილებებისა და მწარმოებლობის მონიტორინგს, გაფართოებულ კონფიგურირებას და IOS განახლებების განხორციელებას.

ფაიერვოლები (დამცავი ეკრანები). არსებობს ფაიერვოლის პროგრამული და აპარატურული გადაწყვეტები, რომლებიც შეესაბამებიან ქსელის უსაფრთხოების პოლიტიკებს. დამცავი ეკრანი ახდენს ქსელში შემომავალი არაავტორიზებული და პოტენციურად საფრთხის შემცველი ტრაფიკის ბლოკირებას. მარტივი დამცავი ეკრანი უზრუნველყოფს ძირითადი ტრაფიკის ფილტრაციას დაშვების კონტროლის სიების (ACLs) შესაძლებლობების გამოყენებით. ადმინისტრატორი იყენებს ACL-ს, რათა შეაჩეროს ქსელში არასასურველი ტრაფიკი ან დართოს შემოსვლის ნება მხოლოდ სპეციფიურ ნაკადებს. ACL წარმოადგენს დაშვებისა და უარყოფის შემცველ ბრძანებათა მიმდევრობას, რომელიც ეხება მისამართებსა და პროტოკოლებს. ACL უზრუნველყოფს ქსელში შემომავალი ან გამავალი ტრაფიკის მართვას. დამცავი ეკრანები იგერიებენ თავდასხმებს კერძო ქსელზე და წარმოადგენენ ჰაკერების საერთო სამიზნეს. მთავარი საფრთხე დამცავი ეკრანებისათვის არის ქურდობა, ჰაკერული თავდასხმა და დისტანციური წვდომა, თავდასხმები ACL-ის წინააღმდეგ ან თავდასხმები მწარმოებლობასა და ხელმისაწვდომობაზე. რამოდენიმე კონტრზომას და მართვას შეუძლია დაიცვას ეკრანები, მათ შორისაა გაუმჯობესებული ფიზიკური უსაფრთხოება, გაფართოებული კონფიგურირება, უსაფრთხო დისტანციური წვდომა და ავტორიზაციის და შესაბამისი სისტემის განახლებები.

მარშრუტიზატორები ქმნიან ინტერნეტის ხერხემალს და უზრუნველყოფენ კომუნიკაციებს სხვადასხვა ქსელებს შორის. მარშრუტიზატორები ერთმანეთთან კომუნიკაციას ახდენენ, რათა გამოავლინონ საუკეთესო მარშრუტი ტრაფიკის გადასაცემად ქსელებს

შორის. მარშრუტიზატორები იყენებენ მარშრუტიზაციის პროტოკოლებს მარშრუტიზაციის გადაწყვეტილების მისაღებად. მარშრუტიზატორებს ასევე შეუძლიათ სხვა სერვისების ინტეგრირება, როგორიცაა კომუტაცია და დამცავი ეკრანის შესაძლებლობები. ეს ოპერაციები მარშრუტიზატორს გადააქცევს კიბერშემტევთა სამიზნედ. მთავარი საფრთხე ქსელის მარშრუტიზატორებისათვის - ქურდობა, ჯჰაკერული თავდასხმა და დისტანციური წვდომა, თავდასხმები მარშრუტიზაციის პროტოკოლებზე ან თავდასხმები მწარმოებლობასა და ხელმისაწვდომობაზე. რამდენიმე კონტრზომასა და მართვას შეუძლია დაიცვას ქსელური მარშრუტიზატორები, მათ შორის გაუმჯობესებული ფიზიკური უსაფრთხოება, გაფართოებული კონფიგურაციის პარამეტრები, უსაფრთხო მარშრუტიზაციის პროტოკოლების გამოყენება ავტორიზაციით და შესაბამისი სისტემის განახლებები და პატჩები საჭიროების შემთხვევაში.

უსადენო და მობილური მოწყობილობები გახდნენ ყველაზე გამოყენებადი დღეისათვის არსებულ ქსელის მოწყობილობებს შორის. ისინი უზრუნველყოფენ მობილობას და მოხერხებულობას, მაგრამ არიან მოწყვლადები თავდასხმების მიმართ. ეს მოწყვლადობა მოიცავს ქურდობას, ჰაკერულ თავდასხმებს და არასანქცირებული დისტანციური წვდომას, სნიფინგს, man-in-the-middle თავდასხმებსა და თავდასხმებს მწარმოებლობასა და ხელმისაწვდომობაზე. საუკეთესო გზა დავიცვათ უსადენო ქსელი, გახლავთ აუთენტიფიკაციისა და შიფრაციის გამოყენება. ორიგინალური უსადენო სტანდარტი 801.11 უზრუნველყოფს ორი ტიპის აუთენტიფიკაციას:

1. ღია სისტემების აუთენტიფიკაცია - ნებისმიერ უსადენო მოწყობილობას შეუძლია შეუერთდეს უსადენო ქსელს. ეს მეთოდი გამოიყენეთ იმ სიტუაციებში, როდესაც უსაფრთხოება არაა პრიორიტეტული.

2. გაზიარებული გასაღების აუთენტიფიკაცია - უზრუნველყოფს აუთენტიფიკაციისა და დაშიფვრის მექანიზმებს უსადენო კლიენტსა და აპლიკაციას ან უსადენო მარშრუტიზატორს შორის.

უსადენო ლოკალური ქსელებისთვის გვაქვს საზიარო კოდის აუთენტიფიკაციის სამი მეთოდი:

1. WEP - ეს იყო WLAN-ების უსაფრთხოების ორიგინალური 802.11 სპეციფიკაცია. ვინაიდან, დაშიფრვის კოდი არასოდეს იცვლება, პაკეტების გაცვლისას კოდის გატეხვა ხდება ადვილი.

2. Wi-Fi დაცული წვდომა (WPA) - ეს სტანდარტი იყენებს WEP-ს, მაგრამ უზრუნველყოფს უსაფრთხოებას შედარებით ძლიერი დროებითი გასაღების ინტეგრირების პროტოკოლის (TKIP) დაშიფვრით. TKIP ცვლის კოდს თითოეული პაკეტისთვის, შესაბამისად კოდის გატეხვა ხდება უფრო რთული.

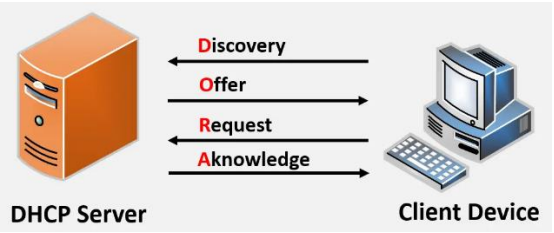
3. IEEE 802.11i/WPA2 - IEEE 802.11i წარმოადგენს დღეისათვის ინდუსტრიულ სტანდარტს WLAN-ების უსაფრთხოებისათვის.. 802.11i და WPA2 იყენებენ გაფართოებული დაშიფვრის სტანდარტს (AES), რომელიც წარმოადგენს უძლიერეს დაშიფვრის პროტოკოლს.

2006 წლიდან, ნებისმიერი მოწყობილობა რომელიც Wi-Fi სერტიფიცირების ლოგოს ატარებს, არის WPA2 სერტიფიცირებული. მაშასადამე, თანამედროვე უსადენო ლოკალურ ქსელებში უნდა იყოს გამოყენებული 802.11i/WPA2 სტანდარტი. სხვა კონტრზომები მოიცავენ გაუმჯობესებულ ფიზიკურ უსაფრთხოებასა და რეგულარულ სისტემის განახლებებს.

კიბერ დამნაშავეები იყენებენ მოწყვლად ქსელის სერვისებს მოწყობილობაზე შეტევის მიზნით. არასაიმედო ქსელური სერვისების შესამოწმებლად, საჭიროა გამოყენებულ იქნას პორტის სკანერი. პორტის სკანერი წარმოადგენს პროგრამას, რომელიც ამოწმებს მოწყობილობას ღია პორტებზე შეტყობინებების გაგზავნით და მათზე პასუხის მოლოდინით. კიბერ დამნაშავეები იყენებენ პორტის სკანერებს იმავე მიზეზით. ქსელური სერვისების უსაფრთხოება მოითხოვს მხოლოდ საჭირო პორტების გახსნას და ხელმისაწვდომობას.

ჰოსტის დინამიური მართვის პროტოკოლი (DHCP - Dynamic Host Configuration Protocol)

DHCP იყენებს სერვერს, რათა მიანიჭოს IP მისამართი და სხვა კონფიგურაციული ინფორმაცია ავტომატურად ქსელურ მოწყობილობებს. ფაქტობრივად, მოწყობილობა იღებს ნებართვას DHCP სერვერისაგან ქსელის გამოყენებაზე. თავდამსხმელებს შეუძლიათ მიზანში ამოიღონ DHCP სერვერები, რათა არ დაუშვან მოწყობილობები ქსელში. როდესაც ჰოსტს (DHCP კლიენტს) სჭირდება IP კონფიგურაცია, ის უკავშირდება DHCP სერვერს და ითხოვს IP კონფიგურაციას. DHCP სერვერი შეიცავს რამდენიმე წინასწარ კონფიგურირებულ IP კონფიგურაციას. როდესაც ის იღებს DHCP მოთხოვნას DHCP კლიენტისგან, ის უზრუნველყოფს კლიენტს IP კონფიგურაციას ყველა ხელმისაწვდომი IP კონფიგურაციიდან. ეს პროცესი შედგება ოთხი ეტაპისგან: აღმოჩენა, შეთავაზება, მოთხოვნა და დადასტურება.



სურ. 7.4. DHCP კომუნიკაციის ოთხი ეტაპი.

როდესაც ჩვენ მოწყობილობას ვრთავთ ინტერნეტში, ის ამოწმებს, არის თუ არა სწორი IP კონფიგურაცია. თუ ის არ არის ხელმისაწვდომი, მოწყობილობა წარმოქმნის სპეციალურ შეტყობინებას, რომელიც ცნობილია როგორც DHCPDISCOVER შეტყობინება და ავრცელებს ამ შეტყობინებას LAN ქსელზე.

ამ შეტყობინებაში მოწყობილობა იყენებს მისამართებს 0.0.0.0 და 255.255.255.255 წყაროსა და დანიშნულების მისამართის ველებში, შესაბამისად. 0.0.0.0 და 255.255.255.255 არის ორი სპეციალური მისამართი. ნებისმიერ მოწყობილობას, აქვს თუ არა მას სწორი IP კონფიგურაცია, შეუძლია გამოიყენოს ეს მისამართები ადგილობრივი სამაუწყებლო შეტყობინებების გასაგზავნად. ამ მისამართებიდან წყაროს მისამართად გამოიყენება 0.0.0.0. თუ მოწყობილობას არ აქვს წყაროს მისამართი, მას შეუძლია გამოიყენოს ეს მისამართი

სამაუწყებლო შეტყობინებების გასაგზავნად. 255.255.255.255 არის ადგილობრივი სამაუწყებლო მისამართი. ამ მისამართზე გაგზავნილი ნებისმიერი შეტყობინება მიიღება ლოკალური ქსელის ყველა კვანძის მიერ.

ვინაიდან კლიენტი აგზავნის DHCPDISCOVER შეტყობინებას ლოკალურ სამაუწყებლო მისამართზე, თუ DHCP სერვერი კონფიგურირებულია ლოკალურ ქსელში, ის ასევე მიიღებს ამ შეტყობინებას. თუ რამდენიმე DHCP სერვერი არის კონფიგურირებული ლოკალურ ქსელში, ისინი ყველა მიიღებენ DHCPDISCOVER შეტყობინებას. ერთმა ან ყველამ შეიძლება უპასუხოს DHCPDISCOVER შეტყობინებას. DHCPDISCOVER შეტყობინების საპასუხოდ, DHCP სერვერი უგზავნის DHCPOFFER შეტყობინებას კლიენტს.

იმის გამო, რომ კლიენტს არ აქვს IP მისამართი, DHCP სერვერს არ შეუძლია გაგზავნოს DHCPOFFER შეტყობინება პირდაპირ კლიენტთან. ამიტომ, სერვერი ადგენს დანიშნულების მისამართს 255.255.255.255. სხვა სიტყვებით რომ ვთქვათ, სერვერი ასევე ავრცელებს DHCPOFFER შეტყობინებას ადგილობრივ ქსელში.

DHCPOFFER შეტყობინება შეიცავს პროტოკოლის სპეციფიკურ ინფორმაციას, ასევე IP მისამართს, ქვექსელის ნიღაბს, ნაგულისხმევი კარიბჭის IP მისამართს, DNS სერვერის IP მისამართს და სხვა კონფიგურირებული სერვერების IP მისამართებს, როგორიცაა TFTP და FTP.

ლოკალურ ქსელში ყველა ჰოსტი იღებს DHCPOFFER შეტყობინებას. ჰოსტი, რომელმაც გაგზავნა DHCPDISCOVER შეტყობინება, იღებს DHCPOFFER შეტყობინებას. წყაროს ჰოსტის გარდა, ყველა სხვა ჰოსტი უგულებელყოფს DHCPOFFER-ს. DHCPDISCOVER შეტყობინება შეიცავს ჰოსტის MAC მისამართს. როდესაც DHCP სერვერი აგზავნის DHCPOFFER შეტყობინებას, ის ასევე მოიცავს ჰოსტის MAC მისამართს პარამეტრში, რომელიც ცნობილია როგორც კლიენტის ID. როდესაც ჰოსტები იღებენ DHCPOFFER შეტყობინებას, ისინი ამოწმებენ კლიენტის ID ველს შეტყობინებაში. თუ ჰოსტი ხედავს მის MAC მისამართს Client ID ველში, მან იცის, რომ შეტყობინება მისთვის არის

განკუთვნილი. თუ ჰოსტი ხედავს სხვა ჰოსტის MAC მისამართს Client ID ველში, მან იცის, რომ შეტყობინება მისთვის არ არის განკუთვნილი.

DHCP სერვერების რაოდენობის მიხედვით, ჰოსტს შეუძლია მიიღოს მრავალი DHCPOFFER შეტყობინება. თუ ჰოსტი იღებს რამდენიმე DHCPOFFER შეტყობინებას, ის იღებს მხოლოდ ერთ შეტყობინებას და ატყობინებს სერვერს DHCPREQUEST შეტყობინებით, რომ მას სურს გამოიყენოს შემოთავაზებული IP კონფიგურაცია.

როდესაც DHCP სერვერი იღებს DHCPREQUEST შეტყობინებას კლიენტისგან, კონფიგურაციის პროცესი გადადის საბოლოო ეტაპზე. ამ დროს სერვერი უგზავნის DHCPACK შეტყობინებას კლიენტს. DHCPACK შეტყობინება არის კლიენტის აღიარება, რომელიც მიუთითებს, რომ DHCP სერვერმა მიიღო კლიენტის DHCPREQUEST შეტყობინება და კლიენტს შეუძლია გამოიყენოს შემოთავაზებული IP კონფიგურაცია.

დომენურ სახელთა სისტემა (DNS)

DNS გარდაქმნის ერთიანი რესურსების ლოკატორის URL ან ვებ-გვერდის მისამართს საიტის IP მისამართში. როდესაც მომხმარებლები მისამართების საძიებო ველში შეიტანენ ვებ-მისამართს, ისინი დამოკიდებულნი ხდებიან DNS სერვერებზე, რათა მათ მოახდინონ მისი ფაქტობრივ IP მისამართში ტრანსლაცია. თავდამსხმელებმა შეიძლება მიზანში ამოიღონ DNS სერვერები, რათა უარყონ ქსელური რესურსების ხელმისაწვდომობა ან მოახდინონ გადამისამართება ყალბ საიტებზე.

ინტერნეტის კონტროლის გზავნილთა პროტოკოლი (ICMP)

ქსელური მოწყობილობები იყენებენ ICMP-ს შეცდომის შეტყობინებების გაგზავნისთვის, როგორიცაა მოთხოვნილი სერვისის მიუწვდომლობა ან ჰოსტის ხელმიუწვდომლობა მარშრუტიზატორზე. ping ბრძანება არის ქსელის უტილიტა, რომელიც იყენებს ICMP-ს ქსელის ჰოსტის ხელმისაწვდომობის შესამოწმებლად. Ping აგზავნის ICMP შეტყობინებებს ჰოსტზე და ელოდება პასუხს. სერვისზე უარის მიღების თავდასხმები იყენებენ ICMP-ს, შესაბამისად, ბევრ ქსელში

ხდება ICMP-ს ფილტრაცია, რათა თავიდან იქნას აცილებული მსგავსი თავდასხმები.

Network Time Protocol (NTP)

მნიშვნელოვანი ფაქტორია ქსელების ფარგლებში სწორი დროის ინსტალირება. სწორი დრო საშუალებას იძლევა ზუსტად აკონტროლოთ ქსელის მოვლენები, როგორიცაა უსაფრთხოების დარღვევები. გარდა ამისა, საათის სინქრონიზაცია კრიტიკულად მნიშვნელოვანია მოვლენების სწორი ინტერპრეტაციისთვის ლოგის მონაცემთა ფაილებში, ასევე ციფრული სერთიფიკატებისთვის.

ქსელის დროის პროტოკოლი (NTP) არის პროტოკოლი, რომელიც ახდენს კომპიუტერული სისტემების საათების სინქრონიზაციას მონაცემთა ქსელებში. NTP საშუალებას აძლევს ქსელის მოწყობილობებს, მოახდინონ დროის სინქრონიზაცია დროის სერვერთან. კიბერ დამნაშავეები თავს ესხმიან დროის სერვერს, რათა ჩაშალონ ის უსაფრთხო კომუნიკაციები, რომლებიც დამოკიდებულნი არიან ციფრულ სერტიფიკატებზე.

Voice over IP (VoIP) იყენებს ქსელებს, როგორიცაა ინტერნეტი, რათა განახორციელოს და მიიღოს სატელეფონო ზარები. VoIP-ისთვის საჭირო აპარატურა მოიცავს ინტერნეტ კავშირს და ტელეფონს. რამდენიმე ვარიანტი ხელმისაწვდომია ტელეფონის კომპლექტისთვის. უმრავლესი სამომხმარებლო VoIP მომსახურება იყენებს ინტერნეტს სატელეფონო ზარებისთვის. თუმცა, მრავალი ორგანიზაცია სარგებლობს კერძო ქსელებით, რადგან ისინი უზრუნველყოფენ მეტ უსაფრთხოებასა და მომსახურების ხარისხს. VoIP უსაფრთხოება ისევე საიმედოა, როგორც ძირითადი ქსელის უსაფრთხოება. კიბერ დამნაშავეები ამ სისტემებს იღებენ მიზანში, რათა მიიღონ უფასო სატელეფონო სერვისებზე წვდომა, სატელეფონო ზარებზე წვდომა, ან გავლენა მოახდინონ მწარმოებლობასა და ხელმისაწვდომობაზე.

ვიდეოკონფერენცია საშუალებას აძლევს ორ ან მეტ ლოკაციას ერთდროულად დაუკავშირდნენ ერთმანეთს სატელეკომუნიკაციო ტექნოლოგიების გამოყენებით. ეს ტექნოლოგიები სარგებლობენ

ახალი მაღალი დეფინიციის ვიდეო სტანდარტებით და საშუალებას იძლევიან, ადამიანთა ერთმა ჯგუფმა კონკრეტული ლოკაციიდან დაამყაროს კავშირი სხვა ჯგუფთან სხვა ლოკაციაზე რეალურ დროში. ვიდეოკონფერენციები დღეისათვის წარმოადგენენ ჩვეულებრივი ყოველდღიური ოპერაციების ნაწილს ისეთ ინდუსტრიებში, როგორიცაა სამედიცინო სფერო. ექიმებს შეუძლიათ განიხილონ პაციენტის სიმპტომები და კონსულტაციები გაუწიონ ექსპერტებს პოტენციური მკურნალობის იდენტიფიცირების მიზნით.

ბევრი საწარმოო ორგანიზაცია იყენებს ტელეკომუნიკაციას, რათა დაეხმაროს ინჟინრებს და ტექნიკოსებს კომპლექსური ოპერაციების ან ტექნიკური ამოცანების შესასრულებლად. ვიდეოკონფერენციის აპარატურა შეიძლება იყოს ძალიან ძვირი და წარმოადგენენ მაღალი ღირებულების სამიზნეებს ქურდებისა და კიბერ დამნაშავეებისათვის. კიბერ დამნაშავეები ამ სისტემებს იღებენ მიზანში, რათა მოახდინონ ვიდეო ზარების მოსმენა და გავლენა მოახდინონ მწარმოებლობასა და ხელმისაწვდომობაზე.

საინფორმაციო ტექნოლოგიების ერთ-ერთი ყველაზე სწრაფად განვითარებადი სექტორია ინტელექტუალური მოწყობილობებისა და სენსორების გამოყენება. კომპიუტერული ინდუსტრია უწოდებს ამ სექტორს **საგანთა ინტერნეტს (IoT)**. ბიზნესი და მომხმარებლები იყენებენ IoT მოწყობილობებს პროცესების ავტომატიზირებისათვის, გარემოს პირობების მონიტორინგისა და მომხმარებლის გაფრთხილებისთვის გარკვეული საფრთხის შემცველი პირობების წარმოქმნისას. უმრავლესი IoT მოწყობილობები უკავშირდებიან ქსელს უსადენო ტექნოლოგიის მეშვეობით და მოიცავენ კამერებს, კარის საკეტებს, მიახლოების სენსორებს, განათებას და სხვა სახის სენსორებს, რომლებიც გამოიყენებიან გარემოს ინფორმაციის შეგროვების ან მოწყობილობის სტატუსის განსაზღვრის მიზნით. ზოგიერთი მოწყობილობის მწარმოებლები იყენებენ IoT ტექნოლოგიას მომხმარებლების ინფორმირების მიზნით, რომ აპარატურის ნაწილები საჭიროებენ ჩანაცვლებას ან გამოსულნი არაინ მწყობრიდან.

ბიზნესი იყენებს ამ მოწყობილობებს ინვენტარის, სატრანსპორტო საშუალებებისა და პერსონალის გასაკონტროლებლად. IoT

მოწყობილობები შეიცავენ გეოსივრცულ სენსორებს. მომხმარებელს შეუძლია გლობალურად განათავსოს, მონიტორინგი ჩაუტაროს და აკონტროლოს გარემოს ცვლადები, როგორიცაა ტემპერატურა, ტენიანობა და განათება. IoT ინდუსტრია უზარმაზარ გამოწვევას უქმნის ინფორმაციული უსაფრთხოების პროფესიონალებს, რადგან ბევრი IoT მოწყობილობა იღებს და გადასცემს მგრძნობიარე ინფორმაციას. კიბერ დამნაშავეები მიზანში იღებენ ამ სისტემებს, რათა ხელი შეუშალონ მონაცემების გადაცემას ან იმოქმედონ მწარმოებლობასა და ხელმისაწვდომობაზე.

7.4 ფიზიკური უსაფრთხოების ზომები

ფიზიკური ბარიერები პირველია, რაც ფიზიკურ უსაფრთხოებაზე ფიქრის დროს მოსდის ადამიანს თავში. ეს არის უსაფრთხოების ყველაზე გარე ფენა და ეს გადაწყვეტილებები ყველაზე საჯაროდ ხილვადია.

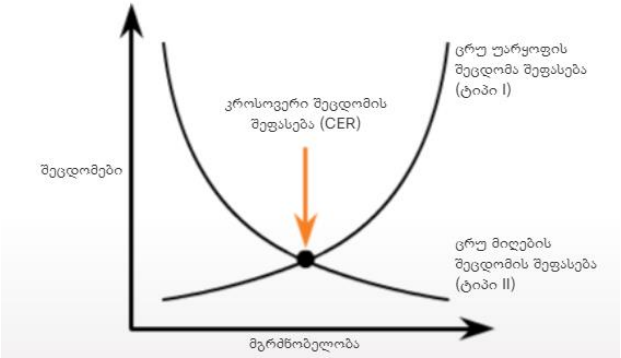
ღობე არის ბარიერი, რომელიც მოიცავს უსაფრთხო ტერიტორიებს და განსაზღვრავს საკუთრების საზღვრებს. ყველა ბარიერი უნდა აკმაყოფილებდეს სპეციფიკურ დიზაინის მოთხოვნებს და ქარხნულ სპეციფიკაციებს. მაღალი შრის უსაფრთხოების სფეროები ხშირად ითხოვენ „ზედა მცველს“, როგორიცაა მავთულხლართები ან გოფრირებული მავთული.

შეღობვა მოითხოვს რეგულარულ მხარდაჭერას. ცხოველები შეიძლება შეძვრნენ ღობის ქვეშ ან მოხდეს ღობის გამორეცხვა, რაც ქმნის მათ არასტაბილურობას. ღობესთან ახლოს გაჩერებული მანქანა ხელს შეუწყობს ღობეზე გადაძრომას ან დაზიანებას. დაცის მაღალი დონეები უზრუნველყოფენ დამატებით შემაკავებელ ფაქტორებს და შეუძლიათ შეაჩერონ არასანქცირებული შეღწევა.

ბიომეტრიკა აღწერს ფიზიოლოგიური ან ქცევითი მახასიათებლების საფუძველზე ინდივიდის ამოცნობის ავტომატიზირებულ მეთოდებს. ბიომეტრიული ავტორიზაციის სისტემები მოიცავს სახის, თითის ანაბეჭდის, ხელის გეომეტრიის, ირისის, ბადურის, ხელმოწერისა და ხმის გაზომვებს. ბიომეტრიული ტექნოლოგიები შეიძლება იყოს

უაღრესად უსაფრთხო იდენტიფიკაციისა და პირადი გადამოწმების გადაწყვეტილებების საფუძველი. ბიომეტრიული სისტემების პოპულაროზა და გამოყენება გაიზარდა უსაფრთხოების დარღვევებისა და გარიგების თაღლითობის გაზრდის გამო. ბიომეტრიკა უზრუნველყოფს კონფიდენციალური ფინანსური ოპერაციებისა და პირადი მონაცემების პრივატულობას. მაგალითად, Apple იყენებს სახის/თვალის ამოცნობის ტექნოლოგიას თავისი სმარტფონებზე. მომხმარებლი ხსნის მოწყობილობას და იყენებს სხვადასხვა აპებს, როგორიცაა ონლაინ საბანკო ან გადახდის აპები.

ბიომეტრიული სისტემების შედარებისას არსებობს რამდენიმე მნიშვნელოვანი ფაქტორი, რომელიც მოიცავს სიზუსტის, სიჩქარის ან გამტარუნარიანობის მაჩვენებელს. ყველაზე მნიშვნელოვანი ფაქტორია სიზუსტე.



სურ. 7.5 ცრუ უარყოფისა და ცრუ მიღების მაჩვენებელის დამოკიდებულება

პირველი შეცდომა არის I-ლი ტიპის შეცდომა ან ცრუ უარყოფა. ამ ტიპის შეცდომა უარყოფს პირს, რომელიც რეგისტრირდება და არის ავტორიზებული მომხმარებელი. წვდომის მართვაში, თუ მოთხოვნა არის ბოროტგანმზრახველთა წვდომის თავიდან აცილება, ცრუ უარყოფა არის ყველაზე ნაკლებად მნიშვნელოვანი შეცდომა. თუმცა, მრავალ ბიომეტრულ აპლიკაციაში ცრუ უარყოფის დაფიქსირებამ შეიძლება ძალიან უარყოფითი გავლენა იქონიოს ბიზნესზე. მაგალითად, საბანკო ან საცალო მაღაზია საჭიროებს მომხმარებელთა

იდენტობისა და ანგარიშის ბალანსის დამოწმებას. ცრუ უარყოფა ნიშნავს, რომ გარიგება ან გაყიდვა დაკარგულია, რაც იწვევს მომხმარებლის განრისხებას.

მიღების მაჩვენებელი პროცენტული მაჩვენებელია და ის წარმოადგენს რეიტინგს, რომელიც განსაზღვრავს, რამდენი მატყუარა (იმპოსტერი) იქნა იდენტიფიცირებული, როგორც აუთენტიფიცირებული მომხმარებელი. ცრუ მიღება არის მე-II ტიპის შეცდომა. ამ ტიპის შეცდომა საშუალებას აძლევს ბოროტგანმზრახველს, თავი გაასაღოს ავტორიზებულ მომხმარებლად, შესაბამისად, ეს არის ყველაზე მნიშვნელოვანი შეცდომა ბიომეტრიულ სისტემაში.

ბიომეტრიული აუთენტიფიკაციის სიზუსტის გაზომვისას ყველაზე ფართოდ გამოიყენება კროსოვერი შეცდომის შეფასება (CER). CER არის რეიტინგი, სადაც ცრუ უარყოფისა და ცრუ მიღების მაჩვენებელი თანაბარია (სურ.7.5).

წვდომის **სამკერდე ნიშანი** საშუალებას აძლევს ინდივიდს, მიიღოს დაშვება ფართობზე ავტომატური შესვლის წერტილით. წვდომის სამკერდე ნიშნები იყენებენ სხვადასხვა ტექნოლოგიებს, როგორიცაა მაგნიტური ზოლი, შტრიხკოდი ან ბიომეტრიკა. ბარათის მკითხველი კითხულობს ნომერს, რომელსაც შეიცავს წვდომის სამკერდე ნიშანი. სისტემა აგზავნის ნომერს კომპიუტერზე, რომელიც უზრუნველყოფს დაშვების კონტროლის გადაწყვეტილებებს სააღრიცხვო ანგარიშის საფუძველზე. სისტემა მოგვიანებით ქმნის ამ დაშვების ლოგს. ლოგის ანგარიშები ცხადყოფს შემსვლელის ვინაობას, შესვლათა რაოდენობას და დროს.

ვიდეო და ელექტრონული სათვალთვალო დანამატი ზოგიერთ შემთხვევაში ცვლის დაცვის პერსონალს. ვიდეო და ელექტრონული მეთვალყურეობის უპირატესობად შეიძლება ჩაითვალოს ტერიტორიების მონიტორინგის უნარი, მაშინაც კი, როდესაც არ არსებობს მესაზღვრეები ან პერსონალი, ასევე ხანგრძლივი პერიოდის განმავლობაში სათვალთვალო ვიდეოებისა და მონაცემების ჩაწერისა და მოკვლევის უნარი მოძრაობის გამოვლენისა და შეტყობინების ჩათვლით.

ვიდეო და ელექტრონული მეთვალყურეობა ასევე შეიძლება უფრო ზუსტი იყოს მოვლენების მოხდენის შემდეგაც კი. კიდევ ერთი მთავარი უპირატესობა ის არის, რომ იგი უზრუნველყოფს სათვალთვალო არეალის გაზრდის შესაძლებლობას, რაც ძნელი მისაღწევია დაცვის პერსონალის არსებობის დროს. ასევე კამერების გამოყენება ობიექტის მთელი პერიმეტრის მონიტორინგისთვის შეიძლება ბევრად უფრო ეკონომიური იყოს. უაღრესად უსაფრთხო გარემოს ორგანიზების მიზნით, ორგანიზაციამ უნდა განათავსოს ვიდეო და ელექტრონული მეთვალყურეობა ყველა შესასვლელში, გასასვლელებზე, საფეხურებზე და ნარჩენთა შეგროვების ადგილებში. უმეტეს შემთხვევაში, ვიდეო და ელექტრონული მეთვალყურეობა ეხმარება დაცვის პერსონალს.

მნიშვნელოვანი საინფორმაციო სისტემის აქტივების მართვა და განთავსება მთავარი გამოწვევაა ორგანიზაციების უმრავლესობისთვის. მობილური მოწყობილობებისა და IoT მოწყობილობების რაოდენობის ზრდამ ეს სამუშაო კიდევ უფრო რთული გახადა. კრიტიკული აღჭურვილობის ძიების დრომ შეიძლება გამოიწვიოს ძვირადღირებული შეყოვნება ან სამუშაო დროის დაკარგვა. **რადიოსიხშირული იდენტიფიკაციის (RFID)** აქტივების ტეგების გამოყენებას შეიძლება დიდი მნიშვნელობა ჰქონდეს უსაფრთხოების პერსონალისათვის. ორგანიზაციას შეუძლია განათავსოს RFID მკითხველი ისე, რომ ისინი არ იყოს ხილული ადამიანებისათვის..

RFID აქტივების ტეგების სარგებელი არის ის, რომ მათ შეუძლიათ აკონტროლონ ნებისმიერი აქტივი, რომელიც ფიზიკურად ტოვებს დაცულ არეალს. უახლეს RFID აქტივების ტეგ სისტემებს შეუძლიათ წაიკითხონ მრავალჯერადი ტეგი ერთდროულად. RFID სისტემები არ საჭიროებს მხედველობის არეალს სკანირების მიზნით. მისი სკიდევ ერთი უპირატესობაა უნარი წაიკითხოს ტეგი, რომელიც უშუალოდ არაა ხილული. ბარკოდებისა და ადამიანის წაკითხვადი ტეგებისგან განსხვავებით, რომლებიც ფიზიკურად უნდა იყვნენ განთავსებულნი და ხილულნი წაკითხვისთვის, RFID ტეგების ხილვადობა არაა აუცილებელი სკანირებისთვის. მაგალითად, მაგიდის ქვეშ მყოფი კომპიუტერის ტეგირება მოითხოვს პერსონალს მაგიდის ქვეშ, რათა

ფიზიკურად იქნას დათვალიერებული ტეგი ბარკოდის პროცესის განსახორციელებლად. RFID ტეგის გამოყენება საშუალებას მისცემს პერსონალს, მოახდინოს ტეგის სკანირება მისი ფიზიკური ხილვის გარეშე.

თავი 8 კიბერუსაფრთხოების ორგანიზაციულ-სამართლებრივი ასპექტები

ტექნოლოგიის წინსვლამ უზრუნველყო მთელი რიგი მოწყობილობების შექმნა, რომელიც გამოიყენება საზოგადოების მიერ და რომელიც მუდმივ კავშირშია მთელი მსოფლიოს მასშტაბით. ამან გაზარდა კავშირები, თუმცა, გამოიწვია ქურდობის, თაღლითობისა და ბოროტად გამოყენების რისკი მთელი ტექნოლოგიური ინფრასტრუქტურის მასშტაბით. ამიტომ საინფორმაციო ტექნოლოგიების ინფრასტრუქტურის კატეგორიზაცია ხდება შვიდ დომენად. თითოეული დომენი მოითხოვს უსაფრთხოების სათანადო მართვას CIA (confidentiality, integrity and availability) ტრიადის მოთხოვნების დასაკმაყოფილებლად.

8.1 კიბერუსაფრთხოების ოპერაციების არეალი CIA ტრიადის ფარგლებში

კონფიდენციალურობა, მთლიანობა და ხელმისაწვდომობა, ეს არის CIA ტრიადის სამი კომპონენტი, ინფორმაციული უსაფრთხოების მოდელი, რომელიც შექმნილია სენსიტიური ინფორმაციის დასაცავად მონაცემთა დარღვევისგან. CIA ტრიადა არის მნიშვნელოვანი კონცეფცია ინფორმაციული უსაფრთხოების ინდუსტრიაში და გამოიყენება ISO 27001-ში, გლობალური სტანდარტი ინფორმაციის უსაფრთხოების მართვისთვის.

GDPR (General Data Protection Regulation) ასევე აღნიშნავს CIA-ს ტრიადას 32-ე მუხლში, რომელიც ავალდებულებს ორგანიზაციებს გამოიყენონ შესაბამისი ზომები მათი ინფორმაციის დამუშავების სისტემებისა და სერვისების კონფიდენციალურობის, მთლიანობის, ხელმისაწვდომობისა და გამძლეობის დასაცავად. მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR) არის კანონი, რომელიც არეგულირებს, თუ როგორ ამუშავებენ ორგანიზაციები პერსონალურ მონაცემებს (Brexit-ის შემდეგ, ახლა არსებობს ორი კანონი: ევროკავშირის GDPR და დიდი ბრიტანეთის GDPR).

კონფიდენციალურობა არის CIA ტრიადის პირველი ელემენტი, რაც გულისხმობს სენსიტიური ინფორმაციის კონფიდენციალურობას და უსაფრთხოებას. მისი მიზანია აღკვეთოს მონაცემების არაავტორიზებული წვდომა კიბერ კრიმინალების ან თანამშრომლების მიერ ლეგიტიმური წვდომის გარეშე.

კონფიდენციალურობის უზრუნველსაყოფად, ორგანიზაციებს სჭირდებათ უსაფრთხოების ზომები, რომლებსაც შეუძლიათ არაავტორიზებული პერსონალის იდენტიფიცირება და მათ მონაცემებზე წვდომის თავიდან აცილება.

მონაცემთა კონფიდენციალურობა ჩვეულებრივ ეხება პერსონალურ ინფორმაციას, როგორიცაა კლიენტების სახელები, საკონტაქტო ინფორმაცია და გადახდის ბარათის ინფორმაცია. ეს დეტალები უნდა იყოს შენახული შესაბამის მონაცემთა ბაზებში და ხელმისაწვდომი იყოს მხოლოდ მათთვის, ვისაც ეს სჭირდება. ეს შეიძლება გულისხმობდეს ფაილების პაროლით დაცვას ან წვდომის კონტროლის დაყენებას. თქვენ ასევე უნდა განიხილოთ სხვადასხვა ინფორმაციის შენახვა ცალკეულ მონაცემთა ბაზაში.

თუმცა კონფიდენციალურობა არ ეხება მხოლოდ პერსონალურ მონაცემებს. ის მოიცავს ნებისმიერ სენსიტიური ხასიათის ინფორმაციას. ეს შეიძლება შეიცავდეს ისეთ საკითხებს, როგორიცაა ინტელექტუალური საკუთრება და კორპორატიული ჩანაწერები. მათაც უნდა მიეცეს ადეკვატური დაცვა, რათა უზრუნველყოფილი იყოს მხოლოდ უფლებამოსილი პერსონალის წვდომა.

CIA ტრიადის მეორე ელემენტი არის **მთლიანობა**. ეს ეხება მონაცემთა სისრულესა და სიზუსტეს, ასევე ორგანიზაციის უნარს დაიცვას იგი კორუფციისგან.

მონაცემთა მთლიანობა მნიშვნელოვან და უნიკალურ როლს ასრულებს მონაცემთა დაცვაში. ჩვენ ხშირად ვფიქრობთ იმაზე, თუ ვის აქვს (ან არ აქვს) ინფორმაციაზე წვდომა. თუმცა, ისეთივე მნიშვნელოვანია გავითვალისწინოთ არის თუ არა თავად ინფორმაცია სწორი. თუ არსებობს შეცდომები მონაცემებში, ორგანიზაციებმა შეიძლება შემთხვევით გაუზიარონ საიდუმლო ინფორმაცია არასწორ

პირს. ასევე არსებობს შესაძლებლობა, რომ ინფორმაცია საერთოდ არ მიეწოდება.

მონაცემთა მთლიანობის მაგალითი შეიძლება მოხდეს ჯანდაცვის ფირმასთან დაკავშირებით, რომელიც უგზავნის პაციენტს ინფორმაციას მათი ჯანმრთელობის მდგომარეობის შესახებ. ორგანიზაცია დარწმუნებული უნდა იყოს, რომ მათი ჩანაწერები სწორია, წინააღმდეგ შემთხვევაში მიმღები მიიღებს არასწორ ინფორმაციას მათი ჯანმრთელობის მდგომარეობის შესახებ, ან შესაძლოა საერთოდ არ მიიღოს.

CIA ტრიადის მესამე ელემენტია **ხელმისაწვდომობა.** ეს ეხება ორგანიზაციის უნარს საჭიროების შემთხვევაში ინფორმაციის წვდომას. ეს შეიძლება იყოს, მაგალითად, თუ ელექტროენერგიის გათიშვა არღვევს ორგანიზაციის სერვერებს ან თუ Cloud ჰოსტინგის პროვაიდერის სისტემები შეფერხებულია.

მიუხედავად იმისა, რომ მონაცემთა ხელმისაწვდომობა ხშირად ეხება ამ სახის ორგანიზაციის საკითხებს, ის ასევე შეიძლება ეხებოდეს ინდივიდუალურ გარემოებებს. მაგალითად, თანამშრომელს შეიძლება ჰქონდეს ტექნიკური პრობლემა, რომელიც ხელს უშლის მათ მგრძნობიარე ფაილის ნახვას, ან სხვა.

სურ. 8.1. CIA ტრიადა

ორგანიზაციის სისტემები, აპლიკაციები და მონაცემები ხელმისაწვდომი უნდა იყოს ავტორიზებული მომხმარებლებისთვის მოთხოვნის შემთხვევაში. თუ, მაგალითად, ორგანიზაცია განიცდის ელექტროენერგიის გათიშვას, რომელიც წყვეტს მათ სისტემებს, მათი ოპერაციები შეჩერდება.

ხელმისაწვდომობა ასევე შეიძლება ეხებოდეს კონკრეტული თანამშრომლის ინფორმაციის ნახვის შესაძლებლობას. თუ მათ ანგარიშთან ან აპარატურასთან დაკავშირებული პრობლემაა, მათ შესაძლოა ვერ შეძლონ წვდომა ინფორმაციაზე, რომელიც აუცილებელია სამუშაოს შესასრულებლად.

CIA ტრიადის თითოეული ასპექტი წარმოადგენს ინფორმაციის უსაფრთხოების ფუნდამენტურ პრინციპებს. მათ შორის, ისინი მოიცავს ყველა შესაძლო გზას, რომ სენსიტიური მონაცემები შეიძლება იყოს კომპრომეტირებული. მაგრამ ტრიადა უფრო მეტს ეხება, ვიდრე მონაცემთა დაცვის ცალკეულ ასპექტებს. სამი კომპონენტის ერთობლივად გათვალისწინება ტრიადის ფარგლებში ეხმარება ორგანიზაციებს გაიგონ მათი საჭიროებები და მოთხოვნები ინფორმაციული უსაფრთხოების კონტროლის შემუშავებისას.

გავრცელებული მომხმარებლის საფრთხეები და მოწყვლადობა

მომხმარებლის დომენი მოიცავს მომხმარებლებს, რომლებიც შედიან ორგანიზაციის საინფორმაციო სისტემაში. მომხმარებლები შეიძლება იყვნენ თანამშრომლები, მომხმარებლები, ბიზნეს კონტრაქტორები და სხვა პირები, რომლებიც საჭიროებენ მონაცემებზე ხელმისაწვდომობას. მომხმარებელი ხშირად ყველაზე სუსტი კავშირია ინფორმაციული უსაფრთხოების სისტემებში და მნიშვნელოვან საფრთხეს უქმნის ორგანიზაციის მონაცემების კონფიდენციალურობას, მთლიანობასა და ხელმისაწვდომობას.

სარისკო ან ცუდი მომხმარებლის პრაქტიკა ხშირად ძირს უთხრის თვით საუკეთესო უსაფრთხოების სისტემას. ქვემოთ ჩამოთვლილია გავრცელებული მომხმარებლის საფრთხეები, გამოვლენილი ბევრ ორგანიზაციაში:

უსაფრთხოების შესახებ ცნობიერების ამაღლება - მომხმარებელმა უნდა იცოდეს ინფორმაციული და საინფორმაციო სისტემების დაცვის მიზნით მოწოდებული მგრძნობიარე მონაცემების, უსაფრთხოების პოლიტიკისა და პროცედურების, ტექნოლოგიებისა და კონტრზომების შესახებ.

ცუდად აღსრულებული უსაფრთხოების პოლიტიკა - ყველა მომხმარებელმა უნდა იცოდეს უსაფრთხოების პოლიტიკა და შედეგები, რომლებიც არ შეესაბამებიან ორგანიზაციის პოლიტიკას.

მონაცემთა ქურდობა — მომხმარებლების მიერ მონაცემთა ქურდობამ შეიძლება დააზარალოს ორგანიზაციები ფინანსურად, რაც იწვევს ორგანიზაციის რეპუტაციის შელახვას ან მგრძნობიარე ინფორმაციის გამჟღავნებასთან დაკავშირებულ სამართლებრივ პასუხისმგებლობას.

არასანქცირებული ჩამოტვირთვები — მრავალი ქსელისა და სამუშაო სადგურის ინფექცია აზარალებს იმ მომხმარებლებს, რომლებიც ახდენენ არასანქცირებული ელ-ფოსტის, ფოტოების, მუსიკის, თამაშების, აპების, პროგრამებისა და ვიდეოების ჩამოტვირთვას სამუშაო სადგურებზე, ქსელებზე ან შენახვის მოწყობილობებში.

არასანქცირებული მედია - არასანქცირებული მედიის გამოყენებამ, როგორიცაა CD, USB დისკები და ქსელური შენახვის მოწყობილობები, შეიძლება გამოიწვიოს მავნე ინფექციები და თავდასხმები.

არასანქცირებული VPNs — VPN-მა შეიძლება გამოიწვიოს არასანქცირებული ინფორმაციის ქურდობის დამალვა. დაშიფვრა ჩვეულებრივ გამოიყენება IT უსაფრთხოების დასაცავად პერსონალის მიერ მონაცემთა გადაცემისას სათანადო უფლებამოსილების გარეშე მასზე წვდომის აღსაკვეთად.

არასანქცირებული ვებ-გვერდები - არასანქცირებული ვებსაიტების წვდომას შეუძლია საფრთხე შეუქმნას მომხმარებლის მონაცემებს, მოწყობილობებს და ორგანიზაციას. ბევრი ვებ საიტი სტუმრებს სთავაზობს სკრიპტების ან პლაგინების ჩამოტვირთვას, რომლებიც შეიცავს ბოროტგანზრახულ კოდს ან adware-ს. ზოგიერთმა ამ საიტებთაგან შეიძლება წვდომა მოიპოვონ მოწყობილობებზე, როგორიცაა კამერები და აპლიკაციები.

სისტემების, აპლიკაციების ან მონაცემების განადგურება - სისტემების, აპლიკაციისა და მონაცემების შემთხვევითი ან განზრახ განადგურება ან დივერსიული განადგურება ყველა ორგანიზაციას დიდ რისკს უქმნის. აქტივისტებს, უკმაყოფილო თანამშრომლებსა და ინდუსტრიის კონკურენტებს შეუძლიათ წაშალონ მონაცემები, გაანადგურონ მოწყობილობები ან მოახდინონ მათი არასწორი კონფიგურირება, რათა მონაცემები და საინფორმაციო სისტემები გახადონ მიუწვდომელნი.

ტექნიკური გადაწყვეტა, კონტროლი ან კონტრზომები არ იძლევა საინფორმაციო სისტემების დაცვის უფრო დიდ შესაძლებლობას, ვიდრე იმ ადამიანების ქცევები და პროცესები, რომლებიც იყენებენ ამ სისტემებს. ორგანიზაციებს შეუძლიათ განახორციელონ სხვადასხვა ზომები მომხმარებლის მიმართ წარმოქმნილი საფრთხეების მართვის მიზნით.

საფრთხეების მართვა

ორგანიზაციებს შეუძლიათ განახორციელონ სხვადასხვა ზომები მომხმარებლისმიმართ წარმოქმნილი საფრთხეების მართვის მიზნით. მათ უნდა უზრუნველყონ უსაფრთხოების ცნობიერების ტრენინგი. დაუკავშირონ უსაფრთხოების შესახებ ცოდნა მწარმოებლობის ანალიზის მიზნებს. გამოიყენონ კონტენტის ფილტრაცია კონკრეტული დომენური სახელების ნებართვის ან უარყოფისთვის მისაღები გამოყენების პოლიტიკის (AUP) შესაბამისად. ჩართონ ავტომატური ანტივირუსული სკანირება მედია დისკების, ფაილებისა და ელ. ფოსტის ბმულებისათვის. მომხმარებლებისთვის წვდომა დაუშვან მხოლოდ იმ სისტემებზე, აპლიკაციებსა და მონაცემებზე, რომლებიც საჭიროა მათი სამუშაოს შესასრულებლად.

განახორციელონ მონიტორინგი თანამშრომლის არანორმალურ ქცევაზე, არაეთიკურ სამუშაოს შესრულებაზე და IT ინფრასტრუქტურის გამოყენებაზე არასამუშაო საათებში. განახორციელონ დაშვების მართვის პროცედურები AUP მონიტორინგისა და შესაბამისობის საფუძველზე. ჩართონ შეღწევის გამოვლენის სისტემა/შეჭრის პრევენციის სისტემა (IDS/IPS)

თანამშრომელთა მგრძნობიარე პოზიციებისა და ხელმისაწვდომობის მონიტორინგის მიზნით.

საფრთხეები მოწყობილობებისთვის

მოწყობილობა არის ნებისმიერი დესკტოპ კომპიუტერი, ლეპტოპი, ტაბლეტი ან სმარტფონი, რომელნიც დაკავშირებულნი არიან ქსელთან. ამიტომ მათ შეიძლება დაემუქროს სხვადასხვა საფრთხეები: უყურადღებოდ დარჩენილი სამუშაო ადგილი ელექტროქსელში, მომხმარებლის ჩამოტვირთვები, განუახლებელი პროგრამული უზრუნველყოფა, მავნე კოდის პროგრამა, არასანქცირებული მედია, გამოყენების პოლიტიკის დარღვევა და სხვა.

მოწყობილობის საფრთხეების მართვა

ორგანიზაციებს შეუძლიათ განახორციელონ სხვადასხვა ზომები მოწყობილობებისთვის საფრთხის მართვის მიზნით: პაროლის დაცვა და ღურბლების პოლიტიკის შექმნა ყველა მოწყობილობაზე; მომხმარებლებისთვის ადმინისტრატორის უფლებების გამორთვა; დაშვების მართვის პოლიტიკა, სტანდარტები, პროცედურები და სახელმძღვანელო პრინციპები; ავტომატური ანტივირუსული განახლებების განხორციელება.

საფრთხეები ლოკალური ქსელისათვის

ლოკალური ქსელი (LAN) დომენი მოითხოვს ძლიერ უსაფრთხოებას და წვდომის მართვას, მას შემდეგ, რაც მომხმარებლებს შეუძლიათ მიიღონ ორგანიზაციის სისტემები, აპლიკაციები და მონაცემები LAN დომენიდან: არასანქცირებული LAN წვდომა; უსადენო ქსელებზე მომხმარებლების მიერ არასანქცირებული წვდომა; არასანქცირებული ქსელის გამოკვლევა და პორტის სკანირება; დამცავი ეკრანის უზრუნველყოფა.

საფრთხეები კერძო ღრუბელში

კერძო ღრუბლოვანი დომენი მოიცავს კერძო სერვერებს, რესურსებს და IT ინფრასტრუქტურას, რომელიც ხელმისაწვდომია ორგანიზაციის წევრებისთვის ინტერნეტის მეშვეობით. შემდეგი პოზიციები საფრთხეს უქმნის კერძო ღრუბელს: არასანქცირებული ქსელის

გამოკვლევა და პორტის სკანირება; რესურსების არასანქცირებული ხელმისაწვდომობა; მარშრუტიზატორის, დამცავი ეკრანის, ან ქსელის მოწყობილობის ოპერაციული სისტემის პროგრამული მოწყვლადობა; დაშორებული მომხმარებლები, რომლებიც ახდენენ ორგანიზაციის ინფრასტრუქტურაზე წვდომას და მგრძნობიარე მონაცემების ჩამოტვირთვას.

საფრთხეები საჯარო ღრუბლისათვის

საჯარო ღრუბლოვანი დომენი მოიცავს ღრუბლოვანი პროვაიდერის, სერვისის პროვაიდერის ან ინტერნეტ პროვაიდერის მიერ განთავსებულ მომსახურებას. ქლაუდ პროვაიდერები ახორციელებენ უსაფრთხოების კონტროლს ღრუბლოვანი გარემოს დაცვის მიზნით, მაგრამ ორგანიზაციები პასუხისმგებელნი არიან მათ მიერ ღრუბლებზე განთავსებული რესურსების დაცვაზე. არსებობს სამი განსხვავებული მომსახურების მოდელი, საიდანაც ორგანიზაციას შეუძლია აირჩიოს:

პროგრამული უზრუნველყოფა, როგორც სერვისი (SaaAs) — გამოწერაზე დაფუძნებული მოდელი, რომელიც უზრუნველყოფს პროგრამულ უზრუნველყოფას, რომელიც ცენტრალურადაა განთავსებული და მომხმარებლებს შეუძლიათ განახორციელონ წვდომა ვებ-ბრაუზერის საშუალებით.

პლატფორმა, როგორც სერვისი (PaaS) — უზრუნველყოფს პლატფორმას, რომელიც საშუალებას აძლევს ორგანიზაციას განავითაროს, აწარმოოს და მართოს თავისი აპლიკაციები სერვისის აპარატურაზე იმ ინსტრუმენტების გამოყენებით, რომლებსაც სერვისი უზრუნველყოფს.

ინფრასტრუქტურა, როგორც სერვისი (IAs) — უზრუნველყოფს ვირტუალიზებულ კომპიუტერულ რესურსებს, როგორიცაა აპარატურა, პროგრამული უზრუნველყოფა, სერვერები, შენახვა და სხვა ინფრასტრუქტურული კომპონენტები ინტერნეტში.

ქვემოთ ჩამოთვლილია პოზიციები, რომლებიც საფრთხეს უქმნიან საჯარო ღრუბელს:

- მონაცემთა გაჟონვა;
- ინტელექტუალური საკუთრების დაკარგვა ან ქურდობა;

- კომპრომეტირებული სააღრიცხვო ანგარიში;
- ფედერალური საიდენტიფიკაციო სავავები წარმოადგენენ მაღალი ღირებულების სამიზნეებს;
- საარრიცხვო ანგარიშის გატაცება;
- ორგანიზაციის მხრიდან გაგების ნაკლებობა;
- სოციალური საინჟინრო თავდასხმები;
- შესაბამისობის დარღვევა.

ფიზიკური ობიექტების საფრთხეები

ფიზიკური ობიექტების დომენი მოიცავს ორგანიზაციის მიერ გამოყენებულ ყველა სერვისს, მათ შორის წყალდიდობის და ხანძრის გამოვლენას. ეს დომენი ასევე მოიცავს ფიზიკური უსაფრთხოების ზომებს, რომლებიც რეალიზებულნი არიან ობიექტის დასაცავად. შემდეგი პოზიციები საფრთხეს უქმნიან ორგანიზაციის ობიექტებს: ბუნებრივი საფრთხეები, მათ შორის ამინდის პრობლემები და გეოლოგიური საფრთხე; ელექტროდენის მიწოდების შეფერხებები; სოციალური ინჟინერია უსაფრთხოების პროცედურებისა და საოფისე პოლიტიკის შესახებ; ქურდობა; გახსნილი მონაცემთა ცენტრი; მეთვალყურეობის ნაკლებობა.

საფრთხეები აპლიკაციათა დომენებისათვის

აპლიკაციათა დომენი მოიცავს ყველა კრიტიკულ სისტემას, აპლიკაციებსა და მონაცემებს. გარდა ამისა, იგი მოიცავს ტექნიკას და ნებისმიერ ლოგიკურ რეალიზაციას. ორგანიზაციებს საჯარო ღრუბელში გადააქვთ აპლიკაციები, როგორიცაა ელ. ფოსტა, უსაფრთხოების მონიტორინგი და მონაცემთა ბაზის მართვა. აპლიკაციებს საფრთხეს უქმნიან: მონაცემთა ცენტრების, კომპიუტერული ოთახების და გაყვანილობის კარადების არასანქცირებული წვდომა; ქსელის ოპერაციული სისტემის პროგრამული უზრუნველყოფის მოწყვლადობა; სისტემებზე არასანქცირებული წვდომა; მონაცემთა დაკარგვა; დიდი ხნის განმავლობაში IT სისტემების სამუშაო დროის მოცდენა; კლიენტი/სერვერი ან ვებ აპლიკაციის შემუშავების მოწყვლადობა.

8.2 ეთიკა და სახელმძღვანელო პრინციპები

ეთიკა ხელმძღვანელობს კიბერუსაფრთხოების პროფესიონალს იმაზე, თუ რა უნდა გააკეთოს ან არ უნდა გააკეთოს, მიუხედავად იმისა, არის თუ არა ეს ლეგალური. ორგანიზაცია ენდობა კიბერუსაფრთხოების სპეციალისტს თავისი ყველაზე მგრძნობიარე მონაცემებითა და რესურსებით. კიბერუსაფრთხოების პროფესიონალმა უნდა გაიგოს, როგორ ეხმარება კანონი და ორგანიზაციული ინტერესები ეთიკური გადაწყვეტილებების მიღებაში.

კიბერ დამნაშავეები, რომლებიც სისტემაში შედიან, საკრედიტო ბარათის ნომრებს იპარავენ და აინსტალირებენ ვორმებს, ჩადიან რა არაეთიკურ ქმედებებს. მაგალითად, კიბერუსაფრთხოების სპეციალისტს შეიძლება ჰქონდეს შესაძლებლობა, წინასწარ შეაჩეროს ვორმის გავრცელება შესაბამისი პატჩების ინსტალაციის გზით.

უტილიტარული ეთიკა - მე-19 საუკუნის განმავლობაში ჯერემი ბენთანმა და ჯონ სტიუარტ წილმა შექმნეს უტილიტარული ეთიკა. სახელმძღვანელო პრინციპი ისაა, რომ ნებისმიერი ქმედება, რომელიც უზრუნველყოფს გაცილებით მეტ სიკეთეს, ვიდრე ცუდს ან ბოროტს, ითვლება ეთიკურ არჩევანად.

უფლებრივი მიდგომა - უფლებრივი მიდგომის სახელმძღვანელო პრინციპია ის, რომ პირებს აქვთ უფლება გააკეთონ საკუთარი არჩევანი. ეს მიდგომა აფასებს, თუ როგორ მოქმედებს ქმედება სხვების უფლებებზე, შესაბამისად, ადგენს ქმედება ეთიკურად სწორია თუ არასწორი. ეს უფლებები მოიცავს სიმართლის, პირადი ცხოვრების, უსაფრთხოების უფლებას, და რომ საზოგადოება სამართლიანად იყენებს კანონებს საზოგადოების ყველა წევრისთვის.

საერთო სიკეთის მიდგომა - საერთო სიკეთის მიდგომა გულისხმობს, რომ ეთიკურად გამართლებულია ქცევა, რომელსაც სარგებელი მოაქვს მთელი საზოგადოებისათვის. ასეთ შემთხვევაში კიბერუსაფრთხოების სპეციალისტი აფასებს, თუ რს გავლენას ახდენს მისი ქმედება საზოგადოების საერთო კეთილდღეობაზე.

არ არსებობს მკაფიო პასუხები ეთიკურ საკითხებზე, რომლებსაც კიბერუსაფრთხოების სპეციალისტები აწყდებიან. პასუხი, თუ რა არის

სწორი ან არასწორი, შეიძლება შეიცვალოს სიტუაციისა და ეთიკური პერსპექტივის მიხედვით.

კომპიუტერული ეთიკის ინსტიტუტი (CEI) არის საინფორმაციო ტექნოლოგიების ინდუსტრიის მასშტაბით ეთიკური საკითხების იდენტიფიცირების, შეფასებისა და რეაგირების რესურსი. CEI იყო ერთ-ერთი პირველი ორგანიზაცია, რომელმაც აღიარა ინფორმაციული ტექნოლოგიების სფეროს სწრაფი ზრდის შედეგად წარმოქმნილი ეთიკური და საჯარო პოლიტიკის საკითხები.

კიბერუსაფრთხოების ეთიკის არსებობა, როგორც ორგანიზაციის კულტურის ნაწილი, ხელს უწყობს ნდობის ჩამოყალიბებას და შენარჩუნებას. როდესაც კომპანიები თავიანთ პროცესებში აჩვენებენ ეთიკურ პრაქტიკას, როგორიცაა სენსიტიური მონაცემების დამუშავება და უსაფრთხოების სისტემები, ძირითადი დაინტერესებული მხარეები, როგორიცაა მომხმარებლები და პარტნიორები, უფრო მეტად ენდობიან მათ, რაც იწვევს დაინტერესებული მხარეების კმაყოფილებას და მათ შენარჩუნებას.

კიბერუსაფრთხოების ეთიკური პრაქტიკის დანერგვა ხელს უწყობს ციფრული სისტემების, მონაცემებისა და ტექნოლოგიების გრძელვადიან მდგრადობას. კიბერუსაფრთხოებაში ეთიკური მოსაზრებების პრიორიტეტიზაციამ შეიძლება ხელი შეუწყოს მონაცემთა დარღვევის შემცირებას და სენსიტიური მონაცემების უსაფრთხოების გაუმჯობესებას.

მთლიანობა ფუნდამენტური სტანდარტია ეთიკურ კიბერუსაფრთხოებაში, რადგან ის უზრუნველყოფს მონაცემთა კონფიდენციალურობის შესანარჩუნებლად და უსაფრთხოების დარღვევის შანსების შესამცირებლად შექმნილი სისტემებისა და ოპერაციების სანდოობას, სიზუსტეს და საიმედოობას. მთლიანობის შენარჩუნება გადამწყვეტია იმისთვის, რომ მონაცემები დარჩეს ზუსტი და უცვლელი მთელი მისი სიცოცხლის ციკლის განმავლობაში, ან თუ საჭიროა მისი შეცვლა, ეს ხდება ავტორიზებული მხარის მიერ.

კიბერუსაფრთხოებაში ორგანიზაციული მთლიანობის უზრუნველყოფა გულისხმობს საჭირო ნაბიჯების გადადგმას

მონაცემების უსაფრთხოდ შენახვის უზრუნველსაყოფად, მაგრამ ასევე პოლიტიკის განხორციელებას იმის შესახებ, თუ როგორ ამუშავებენ მათ მონაცემებს, რათა მომხმარებელს ჰქონდეს სრული გამჭვირვალობა იმის შესახებ, თუ როგორ დარჩება მათი მონაცემები დაცული.

ეთიკური პრაქტიკის კიდევ ერთი მთავარი ასპექტია პროფესიონალიზმი, რომელიც მოიცავს გამჭვირვალობას ორგანიზაციის მიერ შეგროვებული მონაცემების ტიპზე, რატომ სჭირდებათ მათ და როგორ ინახება ისინი უსაფრთხოდ. ორგანიზაციებმა უნდა უზრუნველყონ, რომ მათ მომხმარებლებმა გაიგონ ზუსტად რა ინფორმაცია იქნება შეგროვებული და როგორ იქნება გამოყენებული. უფრო მეტიც, ორგანიზაციებმა ასევე უნდა განახორციელონ შიდა პოლიტიკა და პროცესები, რომლებიც უზრუნველყოფენ შეგროვებული მონაცემების გამოყენებას მხოლოდ მითითებული მიზნებისთვის.

გარდა ამისა, ორგანიზაციებმა ასევე უნდა მართონ ცვლილებების პოლიტიკა მონაცემთა შეგროვებისთვის. ციფრული ტექნოლოგიების სწრაფი წინსვლის გამო, გარდაუვალია მონაცემთა შეგროვების, შენახვის ან გაზიარების გზების ცვლილება. იმის გამო, რომ ეს გავლენას მოახდენს მომხმარებლის კონფიდენციალურობაზე, მომხმარებლები წინასწარ უნდა იყვნენ ინფორმირებულები მათი მონაცემების დამუშავების შესახებ ნებისმიერი ცვლილების შესახებ, რათა გადაწყვიტონ, სურთ თუ არა მათი მონაცემების შენარჩუნება ან გატანა ორგანიზაციიდან.

კიბერუსაფრთხოების პრაქტიკაში ეთიკის გარდაქმნის საბოლოო სტანდარტი სანდოობაა. თუ თქვენი ორგანიზაცია ეფექტურად იცავს მთლიანობისა და პროფესიონალიზმის ეთიკურ სტანდარტებს, სავარაუდოდ, სანდოობა მოჰყვება, რადგან კლიენტებს სავარაუდოდ ექნებათ გაზრდილი ნდობა თქვენი ორგანიზაციის, როგორც კიბერუსაფრთხოების პროვაიდერის მიმართ, რომელსაც აქვს ცოდნის, უნარებისა და მთლიანობის დადასტურებული გამოცდილება.

ორგანიზაციული სანდოობის შემდგომი ასამაღლებლად, მნიშვნელოვანია, რომ ყველა შესრულებულ სამუშაოს თან ახლდეს

ანგარიშვალდებულება და პასუხისმგებლობა. ეს მოიცავს დარწმუნდეს, რომ ანგარიშვალდებულების კულტურა და პასუხისმგებლობის აღება შესრულებულ სამუშაოზე არის ჩანერგილი კომპანიაში. ამ კულტურის ჩამოყალიბების მიზნით, კომპანიის აღმასრულებლებმა უნდა გამოიჩინონ მაგალითი, მკაცრად დაიცვან ორგანიზაციული პოლიტიკა, რომლებიც დაკავშირებულია კიბერუსაფრთხოების პროცესებთან და პასუხისმგებლობით მოეკიდონ რაიმე შეცდომის ან პრობლემის წარმოშობას.

გარდა ამისა, ორგანიზაციის შიგნით ანგარიშვალდებულების მაღალი დონე გამოიწვევს თანამშრომლების მიერ გადაწყვეტილების მიღების გაუმჯობესებას, რადგან ეს შექმნის მათ ქმედებებზე პასუხისმგებლობის გრძნობას, გაზრდის გადაწყვეტილების სიზუსტეს და ყურადღებას დეტალებზე.

ამ ეთიკური სტანდარტების დანერგვა ხელს შეუწყობს მომხმარებლებისთვის ოპტიმალური ნდობის, გამჭვირვალობისა და ექსპერტიზის უზრუნველყოფას, სენსიტიური მონაცემების დაცვით.

ტექნოლოგიური ცვლილებების ტემპმა შეიძლება გადააჭარბოს ეთიკური მითითებებისა და რეგულაციების შემუშავებას, რაც რთულს გახდის მიმდინარე ეთიკური საკითხებისა და პრობლემების პოლიტიკის განხილვასა და განხორციელებას მონაცემთა უსაფრთხოდ შესანახად გამოყენებული პროცესებისა და მეთოდების მუდმივი ცვლილების გამო.

ბევრ ინდივიდს და ორგანიზაციას არ გააჩნია ეთიკური მოსაზრებების სრული გაგება კიბერუსაფრთხოების ფარგლებში. ამ ცნობიერების ნაკლებობამ შეიძლება გამოიწვიოს უსაფრთხოების უნებლიე დარღვევა, ტექნოლოგიის ბოროტად გამოყენება ან მონაცემთა დამუშავების პოლიტიკის დარღვევა ბიზნესსა და მომხმარებლებს შორის, რაც პოტენციურად შელახავს ორგანიზაციის აღქმულ მთლიანობას და სანდოობას.

მონაცემთა განზრახ ან შემთხვევითი დარღვევის თავიდან აცილება მოითხოვს ნდობასა და კონტროლს შორის დელიკატურ ბალანსს, რაც შეიძლება ეფექტურად განხორციელდეს როლზე დაფუძნებული

სასწავლო პროგრამების მეშვეობით, რომლებიც შექმნილია სპეციალურად თქვენი ორგანიზაციისა და მისი საჭიროებებისთვის.

მოწინავე ტექნოლოგიური გადაწყვეტილებების მიუხედავად, ადამიანური შეცდომა რჩება მნიშვნელოვან ფაქტორად კიბერუსაფრთხოების დარღვევებში. ადამიანური ელემენტის მიმართვა გულისხმობს უსაფრთხოების ცნობიერების, განათლებისა და ანგარიშვალდებულების კულტურის განვითარებას.

8.3 ინფორმაციულ უსაფრთხოებასთან დაკავშირებული კანონმდებლობა და პასუხისმგებლობა

კანონები კრძალავენ არასასურველ ქცევას. სამწუხაროდ, საინფორმაციო სისტემის ტექნოლოგიებში წინსვლა ბევრად აღემატება სამართალწარმოების სამართლებრივი სისტემის განვითარებას. რიგი კანონები და რეგულაციები გავლენას ახდენენ კიბერსივრცეზე. რამდენიმე კონკრეტული კანონი ხელმძღვანელობს ორგანიზაციის მიერ შემუშავებულ პოლიტიკასა და პროცედურებს, რათა უზრუნველყონ, რომ ისინი შესაბამისობაში იყვნენ.

კიბერდანაშაული

კომპიუტერი შეიძლება ჩართული იყოს კიბერდანაშაულში რამდენიმე სხვადასხვა გზით. არსებობს კომპიუტერის დახმარებით ჩადენილი დანაშაული, კომპიუტერული მიზნობრივი დანაშაული და კომპიუტერული შემთხვევითი დანაშაული. ბავშვთა პორნოგრაფია არის კომპიუტერული შემთხვევითობის დანაშაულის მაგალითი - კომპიუტერი არის შენახვის მოწყობილობა და არ არის დანაშაულის ჩადენისთვის გამოყენებული ფაქტობრივი ინსტრუმენტი.

კიბერდანაშაულის ზრდა რიგი სხვადასხვა მიზეზებითაა განპირობებული. ინტერნეტში ფართოდაა ხელმისაწვდომი მრავალი ინსტრუმენტი და პოტენციურ მომხმარებლებს არ სჭირდებათ დიდი ექსპერტული ცოდნა ამ ინსტრუმენტების გამოყენებისათვის. კიბერდანაშაულის წინააღმდეგ ბრძოლაში არაერთი უწყება და ორგანიზაციას ჩართული.

Internet Crime Complaint Center (IC3). ინტერნეტ დანაშაულის საჩივრების ცენტრი, ან IC3, არის ერის ცენტრალური ცენტრი კიბერდანაშაულის შესახებ შეტყობინებისთვის. მას მართავს FBI, წამყვანი ფედერალური სააგენტო კიბერდანაშაულის გამოძიებისთვის.

ნებისმიერს შეუძლია გახდეს ინტერნეტ დანაშაულის მსხვერპლი. იმოქმედეთ საკუთარი თავისთვის და სხვებისთვის ამის შეტყობინებით. ინტერნეტ დანაშაულების შესახებ შეტყობინებას შეუძლია დამნაშავეების პასუხისგებაში მიცემა და ინტერნეტის ჩვენთვის უფრო უსაფრთხო ადგილად გადაქცევა.

InfraGard. არის პარტნიორობა გამოძიების ფედერალურ ბიუროს (FBI) და კერძო სექტორის წევრებს შორის აშშ-ს კრიტიკული ინფრასტრუქტურის დასაცავად. უწყვეტი თანამშრომლობის საშუალებით, InfraGard აკავშირებს კრიტიკულ ინფრასტრუქტურის მფლობელებს და ოპერატორებს FBI-სთან, რათა უზრუნველყონ განათლება, ინფორმაციის გაზიარება, ქსელები და სემინარები განვითარებადი ტექნოლოგიებისა და საფრთხეების შესახებ. InfraGard-ის წევრობაში შედიან: ბიზნესის აღმასრულებლები, მეწარმეები, იურისტები, უსაფრთხოების პერსონალი, სამხედრო და სამთავრობო მოხელეები, IT პროფესიონალები, აკადემიური წრეები და სახელმწიფო და ადგილობრივი სამართალდამცავი ორგანოები - ეს ყველაფერი ეძღვნება ინდუსტრიის სპეციფიკურ ცოდნას და ეროვნული უსაფრთხოების წინსვლას.

NW3C. 1978 წლიდან NW3C-მ გააძლიერა სისხლის სამართლის პროფესიონალები მთელ მსოფლიოში, საექსპერტო სწავლებისა და ტექნიკური დახმარების გაწევით, რომელიც ფოკუსირებულია ეკონომიკურ და მაღალტექნოლოგიურ დანაშაულზე, კრიმინალურ დაზვერვაზე და იურიდიულ სტრატეგიებზე.

The Bureau of Justice Assistance (BJA) - აძლიერებს ერის სისხლის სამართლის სისტემას და ეხმარება ამერიკის სახელმწიფოს, ადგილობრივ და ტომობრივ იურისდიქციებს შეამცირონ და თავიდან აიცილონ დანაშაული, შეამცირონ რეციდივიზმი და ხელი შეუწყონ სამართლიან და უსაფრთხო სისხლის სამართლის სისტემას.

ამერიკის შეერთებულ შტატებში არსებობს კანონებისა და რეგულაციების სამი ძირითადი წყარო: ნორმატიული კანონი, ადმინისტრაციული სამართალი და საერთო კანონი. სამივე წყარო მოიცავს კომპიუტერულ უსაფრთხოებას. აშშ-ის კონგრესმა ჩამოაყალიბა ფედერალური ადმინისტრაციული ორგანოები და მარეგულირებელი ჩარჩო, რომელიც მოიცავს როგორც სამოქალაქო, ასევე სისხლის სამართლის ჯარიმებს წესების შეუსრულებლობისთვის.

სისხლის სამართლის კანონები აღასრულებენ საყოველთაოდ მიღებულ მორალურ კოდექსს, რომელსაც მხარს უჭერს მთავრობის უფლებამოსილება. რეგულაციები ადგენს წესებს, რომლებიც მიზნად ისახავენ შედეგების მოგვარებას სწრაფად ცვალებად საზოგადოებაში, და რომლებიც ახორციელებენ ჯარიმებს ამ წესების დარღვევისთვის. მაგალითად, კომპიუტერული თაღლითობისა და ბოროტად გამოყენების აქტი არის ნორმატიული კანონი. ადმინისტრაციულად, FCC და ფედერალური სავაჭრო კომისია მსჯელობს ისეთ საკითხებზე, როგორიცაა ინტელექტუალური საკუთრების ქურდობა და თაღლითობა. საბოლოო ჯამში, საერთო სამართლის საქმეები სასამართლო სისტემის მეშვეობით ამუშავებენ პრეცედენტებისა და კანონების კონსტიტუციურ საფუძვლებს.

ფედერალური საინფორმაციო უსაფრთხოების მართვის აქტი (FISMA). კონგრესმა 2002 წელს შექმნა FISMA, რათა შეეცვალა აშშ-ის მთავრობის მიდგომა ინფორმაციული უსაფრთხოებისადმი. როგორც უმსხვილესი შემოქმედი და ინფორმაციის მომხმარებელი, ფედერალური IT სისტემები წარმოადგენენ მაღალი ღირებულების სამიზნეებს კიბერ დამნაშავეებისთვის.

მრავალ ინდუსტრიულ სპეციფიურ კანონებს გააჩნიათ უსაფრთხოების და/ან კონფიდენციალურობის კომპონენტი. ამერიკის მთავრობა მოითხოვს შესაბამისობას ორგანიზაციებისგან ამ ინდუსტრიებში. კიბერუსაფრთხოების სპეციალისტებმა უნდა შეძლონ სამართლებრივი მოთხოვნების ტრანსლაცია უსაფრთხოების პოლიტიკასა და პრაქტიკაში.

გრამ-ლეჩ-ბლილის აქტი (GLBA)

გრამ-Leach-Bliley აქტი წარმოადგენს კანონმდებლობის ნაწილს, რომელიც ძირითადად გავლენას ახდენს ფინანსურ ინდუსტრიაზე. თუმცა, ამ კანონმდებლობის ნაწილი მოიცავს კერძო პირებისთვის კონფიდენციალურობის დებულებებს. დებულება ითვალისწინებს ალტერნატიული მეთოდების გამოყენებას ისე, რომ პირებს შეუძლიათ გააკონტროლონ ბიზნეს გარიგებაში მოცემული ინფორმაციის გამოყენება, რაც წარმოადგენს ფინანსური ინსტიტუტის ნაწილს. GLBA ზღუდავს ინფორმაციის გაზიარებას მესამე მხარის ფირმებთან.

სარბანეს-ოქსლის აქტი (SOX)

აშშ-ში რამდენიმე გახმაურებული კორპორატიული აღრიცხვის სკანდალის შემდეგ, კონგრესმა შეიმუშავა Sarbanes-Oxley აქტი (SOX). SOX-ის მიზანი იყო ფინანსური და კორპორატიული აღრიცხვის სტანდარტების ძირეული გადახედვა და კონკრეტულად მიზნად ისახავდა აშშ-ში საჯაროდ მოვაჭრე ფირმების სტანდარტების დახვეწას.

გადახდის ბარათის ინდუსტრიის მონაცემთა უსაფრთხოების სტანდარტი (PCI DSS)

კერძო ინდუსტრია ასევე აღიარებს, თუ რამდენად მნიშვნელოვანია ერთიანი და სააღსრულებო სტანდარტები. უსაფრთხოების სტანდარტების საბჭო, რომელიც შედგება ზედა კორპორაციებისგან გადახდის ბარათის ინდუსტრიაში, შექმნილია კერძო სექტორის ინიციატივით ქსელური კომუნიკაციების კონფიდენციალობის გასაუმჯობესებლად.

საგადახდო ბარათის ინდუსტრიის მონაცემთა უსაფრთხოების სტანდარტი (PCI DSS) არის სახელშეკრულებო წესების კომპლექტი, რომელიც განსაზღვრავს საკრედიტო ბარათის მონაცემებს, როგორც სავაჭრო ობიექტებსა და ბანკებს გარიგების გაცვლას. PCI DSS არის ნებაყოფლობითი სტანდარტი (თეორიულად) და ვაჭრები/მოვაჭრეებს შეუძლიათ აირჩიონ, სურთ თუ არა მათ დაიცვან სტანდარტი. თუმცა, გამყიდველის შეუსაბამობამ შეიძლება გამოიწვიოს მნიშვნელოვნად

მაღალი გარიგების საფასური, ჯარიმები $500,000-მდე, და შესაძლოა, საკრედიტო ბარათების დამუშავების უნარის დაკარგვა.

იმპორტ/ექსპორტის შეზღუდვა

მეორე მსოფლიო ომის შემდეგ აშშ-მა ეროვნული უსაფრთხოების მოსაზრებების გამო მოაწესრიგა კრიპტოგრაფიის ექსპორტი. კომერციის დეპარტამენტში მრეწველობისა და უსაფრთხოების ბიურო ახლა აკონტროლებს არასამხედრო კრიპტოგრაფიის ექსპორტს. ჯერ კიდევ არსებობს საექსპორტო შეზღუდვები არააღიარებულ სახელმწიფოებსა და ტერორისტულ ორგანიზაციებზე. ქვეყნებს შეუძლიათ გადაწყვიტონ კრიპტოგრაფიის ტექნოლოგიების იმპორტის შეზღუდვა შემდეგი მიზეზების გამო:

- ტექნოლოგია შეიძლება შეიცავდეს ბექდორ-კოდს ან უსაფრთხოების დაუცველობას.
- მოქალაქეებს შეუძლიათ ანონიმურად დაუკავშირდნენ ერთმანეთს და თავიდან აიცილონ მონიტორინგი.
- კრიპტოგრაფიამ შესაძლოა გაზარდოს კონფიდენციალურობის ხარისხი მისაღები დონის ზემოთ.

ბიზნესი აგროვებს მუდმივად მზარდი რაოდენობით პერსონალურ ინფორმაციას მათი კლიენტების შესახებ, ანგარიშის პაროლებიდან და ელექტრონული ფოსტის მისამართებიდან უაღრესად მგრძნობიარე სამედიცინო და ფინანსურ ინფორმაციამდე. როგორც დიდი, ასევე პატარა კომპანიები აღიარებენ დიდი მონაცემებისა და მონაცემთა ანალიტიკის ღირებულებას. ეს ამაღლებს ორგანიზაციების მოტივაციას ინფორმაციის შეგროვებისა და შენახვის მიზნით. კიბერ დამნაშავეები ყოველთვის ეძებენ გზებს, მიიღონ ასეთ ინფორმაციზე წვდომა და გამოიყენონ კომპანიის ყველაზე მგრძნობიარე, კონფიდენციალური მონაცემები. ორგანიზაციები, რომლებიც აგროვებენ მგრძნობიარე მონაცემებს, უნდა იყვნენ კარგი მონაცემების შემნახველნი. მონაცემთა შეგროვების ამ ზრდის საპასუხოდ, რამდენიმე კანონი მოითხოვს ორგანიზაციებისაგან, რომლებიც აგროვებენ პერსონალურ ინფორმაციას, აცნობონ პირებს მათი პირადი მონაცემების დარღვევის ფაქტის შესახებ.

ელექტრონული კომუნიკაციების კონფიდენციალურობის აქტი (ECPA) მიმართავს უამრავი სამართლებრივი კონფიდენციალურობის საკითხებს, რის შედეგადაც ხდება სატელეკომუნიკაციო კომპიუტერებისა და სხვა ტექნოლოგიების მზარდი გამოყენება. ამ კანონის სექციები მიმართულია ელექტრონული ფოსტის, ფიჭური კავშირგაბმულობის, სამუშაო ადგილის კონფიდენციალურობისა და ელექტრონულ კომუნიკაციასთან დაკავშირებული სხვა ჰოსტებისადმი.

კომპიუტერული თაღლითობისა და ძალადობის შესახებ აქტი (CFAA) მოქმედებს 20 წელზე მეტი ხნის განმავლობაში. CFAA უზრუნველყოფს აშშ-ს კანონებს, რომლებიც კომპიუტერულ სისტემებზე არასანქცირებული წვდომის კრიმინალიზაციას ახდენენ. CFAA თვლის დანაშაულად შეგნებულად წვდომას კომპიუტერზე, რომელიც განიხილება, როგორც სამთავრობო კომპიუტერი ან კომპიუტერი, რომელიც გამოიყენება სახელმწიფოთაშორისი კომერციაში, ნებართვის გარეშე. CFAA ასევე კრიმინალურ ქმედებად თვლის კომპიუტერის გამოყენებას, რომელიც ატარებს სახელმწიფოთაშორისი ხასიათს. აქტი ასევე დანაშაულად თვლის პაროლების ტრეფიკინგს ან მსგავს ინფორმაციაზე არასანქცირებულ წვდომას და პროგრამის, კოდის ან ბრძანების გადაცემას, რამაც შესაძლოა გამოიწვიოს გარკვეული ზიანი.

ქვემოთ ჩამოთვლილია კანონები, რომლებიც იცავენ კონფიდენციალურობას.

1974 წლის კონფიდენციალურობის აქტი - ეს აქტი ადგენს სამართლიანი საინფორმაციო პრაქტიკის კოდექსს, რომელიც არეგულირებს ფედერალური სააგენტოების მიერ ჩანაწერების სისტემებში შენარჩუნებული პირების შესახებ პერსონალური იდენტიფიცირებადი ინფორმაციის შეგროვებას, შენარჩუნებას, გამოყენებას და გავრცელებას.

ინფორმაციის თავისუფლების აქტი (FOIA) - FOIA იძლევა მერიკის შეერთებული შტატების მთავრობის ჩანაწერებზე საჯარო ხელმისაწვდომობის საშუალებას. FOIA ახდენს გამჟღავნების პრეზუმფციას, ამიტომ ინფორმაციის გაუვრცელებლობის

პასუხისმგებლობა ეკისრება ხელისუფლებას. არსებობს ცხრა გამონაკლისი ინფორმაციის გამჟღავნებისა, რომელიც ეხება FOIA-ს.

1. ინფორმაცია ეროვნული უსაფრთხოებისა და საგარეო პოლიტიკის შესახებ;
2. სააგენტოს შინაგანი პერსონალის წესები და პრაქტიკა;
3. კონკრეტულად წესდებით გამჟღავნებული ინფორმაცია;
4. კონფიდენციალური ბიზნეს ინფორმაცია;
5. უწყებათაშორისი ან შიდა სააგენტო კომუნიკაცია, რომელიც ექვემდებარება გაწზრახ პროცესს, სამართალწარმოებას და სხვა პრივილეგიებს;
6. ინფორმაცია, რომელიც გამჟღავნების შემთხვევაში იქნებოდა აშკარად არაგარანტირებული შეჭრა პირადი კონფიდენციალურობის სივრცეში;
7. სამართალდამცავი ჩანაწერები, რომლებიც ითვალისწინებენ მთელ რიგ ჩამოთვლილ პრობლემებს;
8. სააგენტოს ინფორმაცია ფინანსური ინსტიტუტებისგან;
9. გეოლოგიური და გეოფიზიკური ინფორმაცია ჭაბურღილების შესახებ.

საოჯახო განათლების ჩანაწერები და კონფიდენციალურობის აქტი (FERPA) - ეს ფედერალური კანონი აძლევს სტუდენტებს წვდომას თავიანთი განათლების ჩანაწერებზე. FERPA მუშაობს რეგისტრაციის საფუძველზე, ვინაიდან სტუდენტმა უნდა დაადასტუროს ინფორმაციის გამჟღავნება ფაქტობრივი გამჟღავნების დაწყებამდე. როდესაც სტუდენტი გახდება 18 წლის ან სკოლის დამთავრების შემდეგ, ნებისმიერ ასაკში, ეს უფლებები FERPA- ს ფარგლებში სტუდენტის მშობლებისგან გადაეცემა სტუდენტს.

აქტი აშშ კომპიუტერული თაღლითობისა და ძალადობის შესახებ (CFAA) - 1984 წლის ყოვლისმომცველი დანაშაულის კონტროლის აქტის ეს ცვლილება კრძალავს კომპიუტერზე არასანქცირებული წვდომას. CFAA აფართოებს წინა აქტის შემთხვევების კრებულს, გამომდინარე დიდი ფედერალური ინტერესიდან. ეს შემთხვევები განისაზღვრება, როგორც ფედერალური მთავრობის ან ფინანსური ინსტიტუტების კუთვნილი კომპიუტერების გამოყენება, თუ დანაშაული სახელმწიფოთაშორისი ხასიათისაა.

აშშ ბავშვთა კონფიდენციალურობის დაცვის აქტი (COPPA) - ეს ფედერალური კანონი ვრცელდება პერსონალური ინფორმაციის ონლაინ შეგროვებაზე ამერიკის იურისდიქციის ქვეშ მყოფი პირების ან პირების მიერ 13 წლამდე ასაკის ბავშვებისგან. სანამ ინფორმაცია შეგროვება და გამოყენება მოხდება ბავშვებისგან (13 წლის და წლამდე), მშობლის ნებართვა უნდა იყოს მიღებული.

აშშ ბავშვთა ინტერნეტ დაცვის აქტი (CIPA) - აშშ-ის კონგრესმა 2000 წელს შეიმუშავა CIPA, რათა 17 წლამდე ასაკის ბავშვები დაეცვა შეურაცხმყოფელი ინტერნეტ კონტენტისა და უცენზურო მასალის ზემოქმედებისგან.

ვიდეო კონფიდენციალურობის დაცვის აქტი (VPPA) - ვიდეო კონფიდენციალურობის დაცვის აქტი იცავს ინდივიდს ვიდეოფირების, DVD-ის და სხვა მხარესთან გამჟღავნებული ინფორმაციის გამოყენებისაგან. წესდება ითვალისწინებს ნაგულისხმევ დაცვას, რაც მოითხოვს ვიდეოგაქირავების კომპანიისაგან, მიიღოს მოქირავნობის თანხმობა, თუ კომპანიას სურს დამქირავებლის შესახებ პირადი ინფორმაციის გამჟღავნება. ბევრი კონფიდენციალურობის დამცველი მიიჩნევს, რომ VPPA აშშ-ს კონფიდენციალურობის ყველაზე ძლიერი კანონია.

ჯანმრთელობის დაზღვევის პორტაბელურობა და ანგარიშვალდებულება - სტანდარტების მანდატი უზრუნველყოფს ფიზიკური შენახვის, მოვლა-შენახვის, გადაცემის და ხელმისაწვდომობის პირთა ჯანმრთელობის ინფორმაციას. HIPAA იღებს პასუხისმგებლობას, რომ ორგანიზაციები, რომლებიც იყენებენ ელექტრონულ ხელმოწერებს, უნდა აკმაყოფილებდნენ ინფორმაციის მთლიანობას, ხელმომწერთა აუთენტიფიკაციას და არა-უარყოფის უზრუნველყოფას.

კალიფორნიის სენატის ბილი 1386 (SB 1386) - კალიფორნია იყო პირველი შტატი, რომელმაც შეიმუშავა კანონი პირადად ამოცნობადი ინფორმაციის არასანქცირებული გამჟღავნების შესახებ. მას შემდეგ, ბევრმა სხვა შტატმა მიჰბაძა მათ. თითოეული ამ კანონთაგანი სხვადასხვაა, თუმცა ერთიანდებიან ერთ სრულ ფედერალურ კანონში. ეს აქტი მოითხოვს, რომ სააგენტოებმა მომხმარებელს აცნობონ

თავიანთი უფლებებისა და მოვალეობების შესახებ. იგი იღებს პასუხისმგებლობას, რომ სახელმწიფო აცნობებს მოქალაქეებს, როდესაც PII დაკარგულია ან გამჟღავნებულია. მას შემდეგ, რაც მიღებულ იქნა SB 1386, მრავალმა სხვა შტატმა შექმნა ამ ბილის მოდელი.

კონფიდენციალურობის პოლიტიკა

პოლიტიკა არის საუკეთესო საშუალება, რათა უზრუნველყოფილ იქნას ორგანიზაციის მასშტაბით შესაბამისობა და კონფიდენციალურობის პოლიტიკა მნიშვნელოვან როლს ასრულებს ორგანიზაციის შიგნით, განსაკუთრებით კი კონფიდენციალურობის დაცვის მიზნით მიღებულ უამრავ კანონთან დაკავშირებით. კონფიდენციალურობასთან დაკავშირებული სამართლებრივი დებულებების ერთ-ერთი პირდაპირი შედეგი იყო მონაცემთა შეგროვებასთან დაკავშირებული კორპორატიული კონფიდენციალურობის პოლიტიკის საჭიროება.

ინტერნეტისა და გლობალური ქსელური კავშირების ზრდით, კომპიუტერულ სისტემაში არასანქცირებული შესვლის ან კომპიუტერის არასასურველი წვდომის შედეგად წარმოიშვა შეშფოთება, რომელსაც შეიძლება ჰქონდეს ეროვნული და საერთაშორისო შედეგები. ეროვნული კანონები კომპიუტერულზე არასასურველი წვდომისა არსებობს ბევრ ქვეყანაში, მაგრამ ყოველთვის შეიძლება მოიძებნოს ხარვეზები, რომლის მეშვეობითაც სახელმწიფოები მაინც ახორციელებენ ამ ტიპის დანაშაულს.

კიბერდანაშაულის კონვენცია არის პირველი საერთაშორისო ხელშეკრულება ინტერნეტ დანაშაულების შესახებ (ევროკავშირი, აშშ, კანადა, იაპონია და სხვა). საერთო პოლიტიკა ეხება კიბერდანაშაულს და ეხება შემდეგს: საავტორო უფლებების დარღვევა, კომპიუტერთან დაკავშირებული თაღლითობა, ბავშვთა პორნოგრაფია და ქსელური უსაფრთხოების დარღვევა.

ელექტრონული კონფიდენციალურობის საინფორმაციო ცენტრი (EPIC) ხელს უწყობს კონფიდენციალურობას და ღია სამთავრობო კანონებსა და პოლიტიკას გლობალურად და აქცენტს აკეთებს ევროკავშირი-აშშ-ის ურთიერთობებზე.

8.4 ინფორმაციული უსაფრთხოების პროცესის დანერგვა ორგანიზაციაში

მოწყვლადობის ეროვნული მონაცემთა ბაზა (NVD) არის აშშ-ის სამთავრობო საცავი სტანდარტებზე დაფუძნებული მოწყვლადობის მართვის მონაცემები, რომელიც იყენებს უსაფრთხოების კონტენტის ავტომატიზაციის პროტოკოლს (SCAP). SCAP არის მეთოდი, რომელიც იყენებს სპეციფიკურ სტანდარტებს მოწყვლადობის მართვის, გაზომვისა და პოლიტიკის შესაბამისობის შეფასების ავტომატიზირებისათვის. დააჭირეთ აქ, რათა ეწვიოთ ეროვნული დაუცველობის მონაცემთა ბაზის ვებ-გვერდს.

SCAP იყენებს ღია სტანდარტებს უსაფრთხოების პროგრამული უზრუნველყოფის ხარვეზებისა და კონფიგურაციის საკითხების დასადგენად. სპეციფიკაციები ახდენენ ორგანიზებას და ზომავენ უსაფრთხოებასთან დაკავშირებულ ინფორმაციას სტანდარტიზებული გზებით. SCAP საზოგადოება არის პარტნიორობა კერძო და საჯარო სექტორს შორის, რაც ხელს უწყობს ტექნიკური უსაფრთხოების ოპერაციების სტანდარტიზაციას. დააჭირეთ აქ, რათა ეწვიოთ უსაფრთხოების კონტენტის ავტომატიზაციის პროტოკოლის ვებ-გვერდს

NVD იყენებს საერთო დაუცველობის ქულათა მინიჭების სისტემას, რათა შეაფასოს მოწყვლადობის გავლენა. ორგანიზაციას შეუძლია გამოიყენოს ქულები, რათა განისაზღვროს მოწყვლადობის სიმძიმე, რომელიც მის ქსელშია აღმოაჩენილი.

კარნეგი მელონის უნივერსიტეტის პროგრამული ინჟინერიის ინსტიტუტი (SEI) ეხმარება მთავრობასა და ინდუსტრიულ ორგანიზაციებს ინოვაციური, ხელმისაწვდომი და სანდოობის პროგრამული უზრუნველყოფის სისტემების შემუშავებაში, ფუნქციონირებასა და შენარჩუნებაში. იგი არის ფედერალური დაფინანსებული კვლევებისა და განვითარების ცენტრი, რომელსაც აშშ-ის თავდაცვის დეპარტამენტი აფინანსებს.

CERT დივიზიის SEI ცენტრის სამმართველო სწავლობს და წყვეტს კიბერუსაფრთხოების არენაზე არსებულ პრობლემებს, მათ შორის

პროგრამული პროდუქტების უსაფრთხოების ხარვეზებს, ქსელური სისტემების ცვლილებებს და ტრენინგებს კიბერუსაფრთხოების გაუმჯობესების მიზნით. CERT უზრუნველყოფს შემდეგ მომსახურებას:

- ეხმარება პროგრამული უზრუნველყოფის მოწყვლადობის მოგვარებას;
- შეიმუშავებს ინსტრუმენტებს, პროდუქტებსა და მეთოდებს სასამართლო ექსპერტიზის ჩასატარებლად;
- შეიმუშავებს ინსტრუმენტებს, პროდუქტებსა და მეთოდებს მოწყვლადობის გასაანალიზებლად;
- შეიმუშავებს ინსტრუმენტებს, პროდუქტებს და მეთოდებს დიდი ქსელების მონიტორინგისთვის;
- ეხმარება ორგანიზაციებს განსაზღვრონ რამდენად ეფექტურია მათი უსაფრთხოებასთან დაკავშირებული პრაქტიკა.

CERT ფლობს ინფორმაციის ფართო მონაცემთა ბაზას პროგრამული ხარვეზებისა და მუქარის კოდის შესახებ, რათა დაეხმაროს გადაწყვეტილებების და გამოსწორების სტრატეგიების შემუშავებას.

ინტერნეტ შტორმის ცენტრი (ISC) უზრუნველყოფს უფასო ანალიზსა და გამაფრთხილებელ მომსახურებას ინტერნეტ მომხმარებლებსა და ორგანიზაციებს შორის. იგი ასევე მუშაობს ინტერნეტ მომსახურების პროვაიდერებთან კიბერ დამნაშავეების წინააღმდეგ. ინტერნეტ შტორმის ცენტრი ყოველდღიურად აგროვებს მილიონობით ჟურნალის ჩანაწერს შეღწევის გამოვლენის სისტემებიდან, სენსორების გამოყენებით, რომელიც მოიცავს 500,000 IP მისამართს 50-ზე მეტ ქვეყანაში. ISC განსაზღვრავს საიტებს, რომლებიც გამოიყენება თავდასხმებისთვის და უზრუნველყოფს მონაცემებს მსოფლიოს სხვადასხვა ინდუსტრიებისა და რეგიონების წინააღმდეგ დაწყებული თავდასხმების ტიპებზე.

გაფართოებული კიბერ უსაფრთხოების ცენტრი (ACSC) წარმოადგენს არაკომერციულ ორგანიზაციას, რომელიც აერთიანებს ინდუსტრიას, აკადემიას და მთავრობას, რათა მიმართონ ძალისხმევა მოწინავე კიბერ საფრთხეების წინააღმდეგ. ორგანიზაცია აზიარებს ინფორმაციას კიბერ საფრთხეებზე, ეწევა კიბერუსაფრთხოების კვლევასა და

განვითარებას და ქმნის საგანმანათლებლო პროგრამებს კიბერუსაფრთხოების პროფესიის პოპულარიზაციისთვის.

ACSC განსაზღვრავს ოთხ გამოწვევას, რომელიც ხელს შეუწყობს მის პრიორიტეტებს:

1. შეიქმნას სტაბილური სისტემები თავდასხმებისა და წარუმატებლობებისგან.
2. გაძლიერდეს მობილური უსაფრთხოება.
3. მოხდეს რეალურ დროში საფრთხის გაზიარების განვითარება.
4. მოხდეს კიბერ რისკების ინტეგრირება საწარმოს რისკების ჩარჩოებთან.

მოწყვლადობის სკანერი აფასებს კომპიუტერების, კომპიუტერული სისტემებისა და ქსელების მოწყვლადობებს. მოწყვლადობის სკანერები ხელს უწყობენ უსაფრთხოების აუდიტის ავტომატიზირებას უსაფრთხოების რისკების ქსელის სკანირებით და ქმნიან პრიორიტეტული სიებს შექმნას სუსტი მხარეების მოსაგვარებლად.

მოწყვლადობის სკანერის შეფასებისას შეგიძლიათ გამოიკვლიოთ, თუ როგორ არის შეფასებული სიზუსტე, საიმედოობა, სკალირება და ანგარიშგება. არსებობს ორი სახის მოწყვლადობის სკანერი, პროგრამულ უზრუნველყოფაზე დაფუძნებული ან ღრუბელზე დაფუძნებული.

მოწყვლადობის სკანირება კრიტიკულად მნიშვნელოვანია ქსელების ორგანიზაციებისთვის, რომლებიც მოიცავს მთელ რიგ ქსელის სეგმენტებს, როგორებიცაა მარშრუტიზატორები, დამცავი ეკრანები, სერვერები და სხვა ბიზნეს მოწყობილობები.

შეღწევადობის ტესტირება (pen testing) არის სისტემაში მოწყვლადი ადგილების ტესტირების მეთოდი სხვადასხვა მავნე კოდის ტექნიკის გამოყენებით. შეღწევადობის ტესტირება არ არის იგივე, რაც დაუცველობის ტესტირება. დაუცველობის ტესტირება მხოლოდ პოტენციურ პრობლემებს განსაზღვრავს. შეღწევადობის ტესტირება მოიცავს კიბერუსაფრთხოების სპეციალისტს, რომელიც "ტეხავს" ვებსაიტს, ქსელს ან სერვერს ორგანიზაციის ნებართვით, რათა შეეცადოს მოიპოვოს რესურსებზე ხელმისაწვდომობა მომხმარებლის

სახელების, პაროლების ან სხვა ნორმალური საშუალებების ცოდნით. კიბერ კრიმინალებსა და კიბერუსაფრთხოების სპეციალისტებს შორის მნიშვნელოვანი განსხვავებაა ის, რომ კიბერუსაფრთხოების სპეციალისტებს ტესტების ჩატარების ნებართვა აქვთ.

ერთ-ერთი ძირითადი მიზეზი, რომელსაც ორგანიზაცია იყენებს შეღწევადობის ტესტირებაში, არის რაიმე დაუცველობის პოვნა და დაფიქსირება, სანამ ამას კიბერ დამნაშავეები მოახერხებდნენ. შეღწევადობის ტესტირება ასევე ცნობილია, როგორც ეთიკური გარჩევა.

პაკეტის ანალიზატორები (ან პაკეტის სნიფერები) ახდენენ ქსელის ტრაფიკის "დაჭერას" და ლოგირებას. პაკეტის ანალიზატორი იღებს თითოეულ პაკეტს, აფასებს პაკეტში სხვადასხვა ველის ღირებულებებს და აანალიზებს მის შინაარსს. სნიფერის საშუალებით შეიძლება როგორც სადენიანი, ასევე უსადენო ქსელების მონაცემების "დაჭერა".

პაკეტების სნიფერი წარმოადგენს გამოყენებით პროგრამას, რომელიც იყენებს ქსელურ ადაპტერს, რომელიც მუშაობს თვალთვალის რეჟიმში (Promiscuous mode - ამ რეჟიმში ადაპტერი ყველა პაკეტს, მიღებული ფიზიკური არხის მიერ, უგზავნის აპლიკაციას დამუშავებისათვის) ამ დროს სნიფერი იჭერს ყველა ქსელურ პაკეტს, რომელიც გადაიცემა განსაზღვრულ დომეინში. ამ დროისთვის სნიფერები ქსელებში სავსებით კანონიერად მუშაობენ ქსელებში. ისინი გამოიყენება დიაგნოსტიკისათვის და ტრაფიკის ანალიზისათვის, მაგრამ თუ მხედველობაში მივიღებთ იმას, რომ ზოგიერთი ამლიკაცია გადასცემს მონაცემებს ტექსტურ ფორმაში (Ftp, Telnet, SMTP, POP3 და სხვა) სნიფერის საშუალებით შესაძლებელია გავიგოთ კონფიდენციალური ინფორმაცია (მაგ. მომხმარებლის სახელი და პაროლი).

სახელებისა და პაროლის დადგენა იძლევა დიდ საშიშროებას, რადგანაც მომხმარებლები ხშირად იყენებენ ერთი და იგივე სახელს და პაროლს მრავალი პროგრამისთვის, მრავალ მომხმარებელს საერთოდ აქვს მხოლოდ ერთი სახელი და პაროლი. თუ პროგრამა მუშაობს როგორც კლიენტ-სერვერი, ხოლო აუტენტიფიცირებული მონაცემები გადაეცემა ქსელის საშუალებით და კითხვადი ტექსტური ფორმატით, მაშინ ეს ინფორმაცია დიდი ალბათობით შეიძლება გამოყენებულ

იქნას კორპორატიულ და გარე რესურსებზე წვდომისათვის (შეტევის მეთოდები ხშირად ბაზირდება სოციალური ინჟინერიის საფუძველზე). მათ კარგად აქვთ წარმოდგენილი, რომ ჩვენ ვიყენებთ ერთი და იგივე პაროლს მარვალი რესურსის წვდომისათვის, ჩვენი პაროლის გაგებით, მას შეუძლია ჩვენი რესურსის გამოყენება ყველაზე ცუდ ვარიანტში ის მიიღებს წვდომას სამომხმარებლო დონეზე და მისი სასუალებით შექმნის ახალ მომხმარებელს, რომლის საშუალებით მას შეეძლება ნებისმიერ მომენტში შემოვიდეს ქსელში და მის რესურსებში. პაკეტის ანალიზატორები ასრულებენ შემდეგ ფუნქციებს:

- ✓ ქსელის პრობლემის ანალიზი;
- ✓ ქსელში შეღწევის მცდელობის გამოვლენა;
- ✓ ექსპლოატირებული სისტემის იზოლაცია;
- ✓ ტრაფიკის ლოგირება;
- ✓ ქსელის არასწორად გამოყენების გამოვლენა.

არ არსებობს ერთი მიდგომა, რომელიც შეესაბამება ყველაფერს, როდესაც საქმე ეხება საუკეთესო უსაფრთხოების ინსტრუმენტებს. ბევრი რამ დამოკიდებულია სიტუაციაზე, გარემოებებსა და პირად გადაწყვეტილებებზე. კიბერუსაფრთხოების სპეციალისტმა უნდა იცოდეს, ვის უნდა მიმართოს ღირებული ინფორმაციის მისაღებად.

8.5 კიბერუსაფრთხოების პროფესიონალების როლების განსაზღვრა

ISO სტანდარტი განსაზღვრავს კიბერუსაფრთხოების პროფესიონალების როლს. ISO 27000 ჩარჩო მოითხოვს:

- IT და ISM პასუხისმგებელი უფროსი მენეჯერი (ხშირად აუდიტის სპონსორი)
- ინფორმაციული უსაფრთხოების პროფესიონალები
- უსაფრთხოების ადმინისტრატორები
- საიტის/ფიზიკური უსაფრთხოების მენეჯერი და ობიექტების კონტაქტები
- HR კონტაქტი ადამიანური რესურსების საკითხებზე, როგორიცაა დისციპლინური ქმედება და ტრენინგი

- სისტემებისა და ქსელის მენეჯერები, უსაფრთხოების არქიტექტორები და სხვა IT პროფესიონალები

ინფორმაციული უსაფრთხოების პოზიციების სახეები შეიძლება ჩამოყალიბდეს შემდეგნაირად:

- განმსაზღვრელები უზრუნველყოფენ პოლიტიკას, სახელმძღვანელო პრინციპებს და სტანდარტებს და მოიცავენ კონსულტანტებს, რომლებიც ახორციელებენ რისკების შეფასებას და განავითარებენ პროდუქტსა და ტექნიკურ არქიტექტურას, და უფროსი დონის პირებს ორგანიზაციის ფარგლებში, რომლებსაც გაჩნიათ ფართო, მაგრამ არა სიღრმისეული ცოდნა.
- მშენებლები არიან ნამდვილი ტექნიკოსები, რომლებიც ქმნიან და გამართავენ უსაფრთხოების გადაწყვეტილებებს.
- მონიტორები ახორციელებენ უსაფრთხოების ინსტრუმენტებს, ასრულებენ უსაფრთხოების მონიტორინგის ფუნქციას და გააუმჯობესებენ პროცესებს.

მრავალფეროვანი საიტები და მობილური პროგრამები რეკლამირებას უწევენ საინფორმაციო ტექნოლოგიების სამუშაო ადგილებს. თითოეული საიტი მიმართულია სხვადასხვა სამუშაოს განმცხადებლების მიმართ და უზრუნველყოფს სხვადასხვა ინსტრუმენტებს კანდიდატებისთვის, რომლებიც ეძებენ თავიანთ იდეალურ სამუშაო პოზიციას. მრავალი საიტი წარმოადგენს სამუშაო ძებნის საიტს, რომელიც აგროვებს განცხადებებს სხვა სამუშაო ფორუმებზე და კომპანიის კარიერულ საიტებზე და გამოსახავს მათ ერთ ლოკაციაზე.

Indeed.com - რეკლამირდება რა, როგორც მსოფლიოს #1 სამუშაო საიტი-აგრეგატორი, Indeed.com იზიდავს 180 მილიონ უნიკალურ ვიზიტორს ყოველთვიურად 50-ზე მეტი ქვეყნიდან. ეს მართლაც მსოფლიოში გავრცელებული სამუშაოს საძიებო საიტია. ის მართლაც ეხმარება კომპანიებს ყველა სახის ვაკანსიის მოძიებაში და სთავაზობს საუკეთესო შესაძლებლობებს სამუშაოს მაძიებლებს.

CareerBuilder.com - ემსახურება ბევრ მსხვილ და პრესტიჟულ კომპანიას. შედეგად, ეს საიტი იზიდავს კონკრეტულ კანდიდატებს,

რომლებიც, როგორც წესი, გააჩნიათ უფრო მეტი განათლება და მაღალი სააღრიცხვო ანგარიშები. CareerBuilder-ზე გამოქვეყნებულ დამსაქმებლებს უფრო მეტი კანდიდატი ჰყავთ კოლეჯის ხარისხით, მოწინავე სააღრიცხვო ანგარიშებითა და ინდუსტრიის სერთიფიცირებით.

USAJobs.gov - ფედერალური მთავრობა აქვეყნებს პოსტებს ნებისმიერი ვაკანსიებით USAJobs-ზე. დააჭირეთ აქ, რათა შეიტყოთ მეტი განაცხადის პროცესის შესახებ, რომელიც გამოიყენება ამერიკის მთავრობის მიერ.

Hr.gov.ge - მეშვეობით საქართველოს ნებისმიერ მოქალაქეს აქვს შესაძლებლობა, ონლაინ გააკეთოს განაცხადი საჯარო სამსახურში არსებულ ნებისმიერ ვაკანსიაზე და დასაქმდეს. ეს არის ერთ-ერთი გზა, მიიღო მონაწილეობა კონკურსში და დაიწყო შენი კარიერა საჯარო სამსახურში. ამ ვებ–გვერდზე დარეგისტრირებულია 199384 სამსახურის მაძიებელი და 383 საჯარო უწყება/დამსაქმებელი.

საჯარო სამსახურის შესახებ საქართველოს კანონის შესაბამისად, ბიუროს ვალდებულება, ამ ეტაპისთვის, შემოიფარგლება ვებ-გვერდზე ვაკანსიების განთავსების ადმინისტრირებით. საკვალიფიკაციო მოთხოვნების დადგენა და კონკურსის გამოცხადება მხოლოდ დამსაქმებელი უწყების უფლებამოსილებაა.

Jobs.ge - არის ვებ-გვერდი, სადაც ქვეყნდება განცხადებები ვაკანსიების, ტრენინგების, გაცვლითი პროგრამების, გრანტებისა და ტენდერების შესახებ. ჯობს.გე შეიქმნა 1998 წელს, როგორც დასაქმების ხელშემწყობი არამომგებიანი პროექტი, და შემდგომში გარდაიქმნა ყველაზე წარმატებულ ინტერნეტ-ბიზნესად საქართველოში. დღეს-დღეობით ჯობს.გე ერთ-ერთი ყველაზე პოპულარული ინტერნეტ-გვერდია ქვეყნის ფარგლებში. დღეს-დღეობით ჯობს.გე ემსახურება ინტერნეტის ასიათასობით მომხმარებელს და ათიათასობით დამქირავებელს.

გამოყენებული ლიტერატურა

- S. Sexton, R. Lacoste. Cisco Press: CCST Cybersecurity. ISBN-13: 978-0-13-820392-4. 2023.
- Awais Rashid, George Danezis, Howard Chivers, Emil Lupu and Andrew Martin. CyBOK - The Cyber Security Body of Knowledge. 2019;
- Michael E.Whitman, Hernert J.Mattord – Principles of Information Security, 6th edition. 2017.
- Suliman Hawamdeh. Cybersecurity for Information Professionals: concepts and Applications. 2020.
- Omar Santos. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, 2nd Edition. Cisco Press. 2023.
- N. Arabuli, V. Adamia, R. Galdava. About One Approach To The Security Of Wireless Communication. 2023;
- ნ. არაბული, ვ. ადამია. მონაცემთა დაცვა. საქართველოს ტექნიკური უნივერსიტეტი. ISBN 978-99940-957-8-0.
- ნ. არაბული., ა. მიგინეიშვილი. დინამიკურ ქსელში სისუსტეების აღმოჩენის და პრევენციის მოდელის ანალიზი. Automated Control Systems - No 1(33), 2022.
- ნ. არაბული., დ. გულუა., ვ. ადამია., რ. გალდავა. სამეცნიერო მოხსენებათა კრებული „კიბერუსაფრთხოების ახალი გამოწვევები გლობალურ საინფორმაციო სივრცეში“. 2020წ. ISBN 978-9941-8-2048-9.
- ა. შეყელაძე. ინფორმაციული უსაფრთხოების რისკების მართვა: სტანდარტები და გამოწვევები, სამეცნიერო-პრაქტიკული კიბერუსაფრთხოების ჟურნალი - Scientific & practical cyber security journal, N3, 2022.
- ა. შეყელაძე. საჯარო ადმინისტრირების ინფორმაციული უსაფრთხოების გამოწვევები და მათი მართვის ინოვაციური საშუალებები, საქართველოს ტექნიკური უნივერსიტეტი, 2023.

დანართი: პრაქტიკული დავალებები

საფრთხეების იდენტიფიკაცია

თქვენ გამოიკვლევთ იმ საფრთხეებს, რომლებსაც ქმნიან კიბერ დამნაშავეები და განსაზღვრავთ კიბერუსაფრთხოების სპეციალისტად გახდომისთვის საჭირო თვისებებსა და მოთხოვნებს.

სცენარი

კიბერ სამყაროს მიერ გამოწვეული საფრთხეები რეალურია. ამ საფრთხეებს გააჩნიათ პოტენციალი, დიდი ზიანი მიაყენონ კომპიუტერებზე ორიენტირებულ სამყაროს. ამ საფრთხეების გააზრება მნიშვნელოვანია ყველასთვის და მათთან ბრძოლის მიზნით, მსოფლიოს სჭირდება ჩამოყალიბებული პროფესიონალები, რომლებსაც შეუძლიათ გამოავლინონ საფრთხეები და მოიგერიონ კიბერდამნაშავეები. საჭირო უნარების განსავითარებლად ორგანიზაციებმა, როგორიცაა Comptia, Cisco Systems და ISC2, შექმნეს პროგრამები კიბერ პროფესიონალების განათლებსა და სერტიფიცირებისათვის.

ნაწილი 1: კიბერშეტევების საფრთხის შესწავლა

კიბერთავდასხმები მსოფლიოს წინაშე მდგარი საფრთხეების ჩამონათვალის სათავეშია. როდესაც ადამიანები ფიქრობენ საფრთხეებზე ეროვნული ან მსოფლიო უსაფრთხოებისთვის, მათი უმრავლესობა ფიქრობს ფიზიკურ თავდასხმებზე ან მასობრივი განადგურების იარაღზე. კომპიუტერული სისტემები აკონტროლებენ ჩვენი ცხოვრების თითქმის ყველა ასპექტს. კომპიუტერული სისტემებისა და კომპიუტერული ქსელების ჩამოშლამ შეიძლება მოახდინოს დამანგრეველი გავლენა თანამედროვე ცხოვრებაზე. იხილეთ ვიდეო და უპასუხეთ კითხვებს.

- გამოიკვლიეთ საფრთხეები. უყურეთ ვიდეოს

(https://www.youtube.com/watch?v=TQoKFovvigI&ab_channel=GoogleWorkspace)

და უპასუხეთ შემდეგ კითხვებს: რომელია ყველაზე საშიში იარაღი მსოფლიოში? რატომ? ეთანხმებით?

- ჩამოთვალეთ ხუთი გზა, რომელთა საშუალებითაც კიბერ კრიმინალს შეუძლია გამოიყენოს კომპიუტერები კანონის დასარღვევად. რომელიმე თქვენს მიერ ჩამოთვლილ დანაშაულს

- დაუზარალებიხართ თქვენ პირადად? თქვენ ან თქვენი ოჯახის წევრები დაზარალდნენ ამ დანაშაულების ჩადენის შედეგად?

ნაწილი 2: CIA ტრიადა

კონფიდენციალობა, მთლიანობა და ხელმისაწვდომობა არის კიბერუსაფრთხოების სამი ფუნდამენტური პრინციპი. ეს სამი პრინციპი ქმნის CIA ტრიადას. ტრიადის ელემენტები უსაფრთხოების სამი ყველაზე მნიშვნელოვანი კომპონენტია. კიბერუსაფრთხოების ყველა პროფესიონალი უნდა იცნობდეს ამ ძირითად პრინციპებს.

- რატომ არის მონაცემთა კონფიდენციალობა ამდენად მნიშვნელოვანი ადამიანებისა და ორგანიზაციებისათვის?

- რას წარმოადგენს მონაცემთა მთლიანობა? დაასახელეთ სამი გზა მონაცემთა მთლიანობის ან სანდოობის დასაზარალებლად.

- რა არის სისტემის ხელმისაწვდომობა? რა შეიძლება მოხდეს, თუ კრიტიკულად მნიშვნელოვანი კომპიუტერული სისტემა აღარ არის ხელმისაწვდომი?

- იხილოთ ვიდეო

(https://www.youtube.com/watch?v=LXHSQ9aAp_4&list=PL6FEA443253B44EC2&index=2&ab_channel=Cisco).

რის განხორციელებას აპირებდნენ კიბერკრიმინალები? დღის რომელ დროს მოხდა თავდასხმა? შესაძლოა თუ არა ქსელის შეტევები სავარაუდოდ განხორციელდნენ რამდენიმე საათის შემდეგ? რატომ?

კიბერუსაფრთხოების პროფესიონალთა სამყაროს შესწავლა

შეისწავლით კიბერუსაფრთხოების პროფესიონალის ყოველდღიურ მოვალეობებს, კონტროლისა და უსაფრთხოების ზომების ტიპებს, რომლებიც მსხვილმა ორგანიზაციებმა უნდა შეიმუშაონ თავიანთი საინფორმაციო სისტემების დაცვის მიზნით.

ვიდეოები:

https://www.youtube.com/watch?v=TQoKFovvigI&ab_channel=GoogleWorkspace

https://www.youtube.com/watch?v=LUHOs_ggvi4&ab_channel=GoogleWorkspace

ნაწილი 1: თქვენი მონაცემების დაცვა

გახსენით ბრაუზერი და იხილეთ პირველი ვიდეო

- როგორ გვარწმუნებს Google, რომ მათ მიერ მონაცემთა ცენტრებში განთავსებული სერვერები არ არიან ინფიცირებულები მავნე კოდის პროგრამებითა და ვირუსებით?

- როგორ აღკვეთს Google მონაცემთა ცენტრებში მდებარე სერვერებზე არასანქცირებულ ფიზიკურ წვდომას?

- როგორ იცავს Google მომხმარებლის მონაცემებს სერვერულ სისტემაში?

ნაწილი 2: თქვენი Google ანგარიშის უსაფრთხოების გაუმჯობესება

გახსენით ბრაუზერი და იხილეთ მეორე ვიდეოს.

- რა არის ორსაფეხურიანი შემოწმება? როგორ შეიძლება მან დაიცვას თქვენი Google ანგარიში?

- რა არის უსაფრთხოების გასაღები და რას აკეთებს ის? შეგიძლიათ გამოიყენოთ უსაფრთხოების გასაღები მრავალ სისტემებში?

დაიცავით Gmail ანგარიშის წვდომა.

- Gmail-ის ანგარიშის გამოყენება ძალიან პოპულარული გახდა. Google-ს ახლა აქვს 1 მილიარდზე მეტი აქტიური Gmail ანგარიში. Gmail-ის ანგარიშების ერთ-ერთი მოსახერხებელი მახასიათებელია სხვა მომხმარებლებისთვის წვდომის უნარი. ეს წვდომის გაზიარების ფუნქცია ქმნის გაზიარებულ ელ. ფოსტის ანგარიშს. ჰაკერებს შეუძლიათ გამოიყენონ ეს ფუნქცია თქვენს Gmail ანგარიშზე წვდომისთვის. თქვენი ანგარიშის შესამოწმებლად, შედით თქვენს Gmail ანგარიშზე და დააჭირეთ ღილაკს Gear ზედა მარჯვენა კუთხეში (პარამეტრები). როდესაც პარამეტრების ეკრანი იხსნება, მენიუს ბარი გამოჩნდება პარამეტრების ეკრანის სათაურით. (General – Labels – Inbox – Accounts and Import – Filters and Blocked Addresses …)

- დააჭირეთ Accounts and Import მენიუს. შეამოწმეთ Grant access to your account ოფცია. წაშალეთ თქვენი ანგარიშის არასანქცირებულად გაზიარებული მომხმარებლები.

შეამოწმეთ თქვენი Gmail-ის ანგარიშის აქტიურობა.

Gmail-ის მომხმარებლებს ასევე შეუძლიათ შეამოწმონ ანგარიშის საქმიანობა, რათა დარწმუნდნენ, რომ სხვა მომხმარებლებს არ მიუწვდებათ ხელი მათ პირადი Gmail ანგარიშზე. ეს ფუნქცია ახდენს იდენტიფიცირებას, ვინ მოახდინა წვდომა ანგარიშზე და რა ლოკაციიდან. გამოიყენეთ Last account activity ოფცია, რათა განსაზღვროთ, ჰქონდა თუ არა სხვა პირს წვდომა თქვენს ანგარიშზე. Last account activity წვდომისათვის შეასრულეთ შემდეგი ნაბიჯები:

1) შედით თქვენს Gmail ანგარიშზე.

2) აირჩიეთ Last account activity: გვერდის ბოლოში. შედეგად გამოჩნდება წვდომა არასანქცირებული მომხმარებლის მიერ და ლოკაცია, საიდანაც ეს წვდომა განხორციელდა.

3) ზუსტად ამ გზავნილის ქვემოთ არის განთავსებულია დეტალური ჰიპერბმული. დააჭირეთ დეტალურ ჰიპერბმულს.

იხილეთ ანგარიშის აქტივობა. თუ არასანქცირებულ მომხმარებელს იპოვით, შეგიძლიათ გააუქმოთ არასანქცირებული მომხმარებელი ზედა მარცხენა ღილაკზე დაჭერით Sign out all other web sessions. ახლა შეცვალეთ თქვენი პაროლი, რათა თავიდან აიცილოთ არასანქცირებული მომხმარებლის მიერ შესაძლო წვდომა თქვენს ანგარიშზე.

აუთენტიფიკაციის, ავტორიზაციისა და სააღრიცხვო ანგარიშების გამოკვლევა

შეისწავლით, განსაზღვრავთ და გამართავთ შესაბამის აუთენტიფიკაციას, ავტორიზაციას ან დაშვების კონტროლს. გამართავთ უსაფრთხოების მართვას.

წინაპირობები: პროგრამირების ენების (მაგ., Python, JavaScript) და HTTP პროტოკოლების ცოდნა.

ნაწილი 1: შესავალი ავთენტიფიკაციასა და ავტორიზაციაში (ცნებები და განმარტებები)

ავთენტიფიკაცია: მომხმარებლის იდენტურობის გადამოწმების პროცესი.

ავტორიზაცია: იმის დადგენის პროცესი, თუ რისი უფლება აქვს დამოწმებულ მომხმარებელს.

ავთენტიფიკაციის საერთო მეთოდები:

- მომხმარებლის სახელი და პაროლი
- OAuth (მაგ., Google, Facebook შესვლა)
- მრავალფაქტორიანი ავთენტიფიკაცია (MFA)

ავტორიზაციის ტექნიკა

- როლებზე დაფუძნებული წვდომის კონტროლი (RBAC)
- ატრიბუტებზე დაფუძნებული წვდომის კონტროლი (ABAC)

ნაწილი 2: გარემოს შექმნა

ინსტრუმენტები და ტექნოლოგიები

- პროგრამირების ენა: Python (Flask) ან JavaScript (Node.js Express-თან ერთად)
- მონაცემთა ბაზა: SQLite სიმარტივისთვის

გარემოს დაყენება

- დააინსტალირეთ საჭირო პროგრამული უზრუნველყოფა (Python, Node.js, Git)
- დააყენეთ ვირტუალური გარემო (პითონისთვის) ან დააინსტალირეთ Node.js

– დააინსტალირეთ საჭირო ბიბლიოთეკები და დამოკიდებულებები (Flask, Flask-Login, Flask-SQLAlchemy Python-ისთვის; Express, Passport.js Node.js-ისთვის)

ნაწილი 3: ავთენტიფიკაციის განხორციელება

მომხმარებლის რეგისტრაცია

```python
# Flask example
from flask import Flask, request, render_template, redirect, url_for
from flask_sqlalchemy import SQLAlchemy
from werkzeug.security import generate_password_hash

app = Flask(__name__)
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///users.db'
db = SQLAlchemy(app)

class User(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(150), unique=True, nullable=False)
    password = db.Column(db.String(150), nullable=False)

@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']
        hashed_password = generate_password_hash(password, method='sha256')
        new_user = User(username=username, password=hashed_password)
        db.session.add(new_user)
        db.session.commit()
        return redirect(url_for('login'))
    return render_template('register.html')
```

შექმენით შესვლის ფორმა

```python
# Flask example continued
from werkzeug.security import check_password_hash
from flask_login import LoginManager, login_user, login_required, logout_user, current

login_manager = LoginManager()
login_manager.init_app(app)

@login_manager.user_loader
def load_user(user_id):
    return User.query.get(int(user_id))

@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']
        user = User.query.filter_by(username=username).first()
        if user and check_password_hash(user.password, password):
            login_user(user)
            return redirect(url_for('dashboard'))
    return render_template('login.html')
```

ნაწილი 4: ავტორიზაციის განხორციელების უფლება

როლებზე დაფუძნებული წვდომის კონტროლი

- განსაზღვრეთ როლები (მაგ., ადმინი, მომხმარებელი)
- მიანიჭეთ როლები მომხმარებლებს

```
# Flask example
class User(db.Model):
    id = db.Column(db.Integer, primary_key=True)
    username = db.Column(db.String(150), unique=True, nullable=False)
    password = db.Column(db.String(150), nullable=False)
    role = db.Column(db.String(50), nullable=False, default='user')

@app.route('/admin')
@login_required
def admin():
    if current_user.role != 'admin':
        return 'Access Denied', 403
    return 'Welcome to the admin page'
```

ატრიბუტზე დაფუძნებული დაშვების კონტროლი

- შეამოწმეთ მომხმარებლის ან რესურსის ატრიბუტები

```
@app.route('/profile')
@login_required
def profile():
    if not current_user.is_active:
        return 'Account not active', 403
    return f'Welcome to your profile, {current_user.username}'
```

ფაილის და მონაცემთა დაშიფვრის შესწავლა

ფაილის დავაშიფრვა Windows 11-ში

მიუხედავად იმისა, რომ Windows 11-ში დაცული ხართ უსაფრთხოების ყოვლისმომცველი ფუნქციებით, შეიძლება დაგჭირდეთ დამატებითი გარანტიები თქვენი ფაილების კონფიდენციალურობისა და უსაფრთხოების შესანარჩუნებლად. ფაილის დაშიფვრა კიდევ ერთი ძლიერი ინსტრუმენტია თქვენი დაცვისთვის.

დაცვის ეს დამატებითი დონე განსაკუთრებით სასარგებლოა ფაილების დასაცავად, რომლებიც გაზიარებულია ონლაინ ელექტრონული ფოსტით, ჩეთით და ა.შ. ეს არხები შეიძლება უფრო მიდრეკილი იყოს ჰაკერების ან კიბერშეტევებისკენ, მაგრამ თქვენი დაშიფრული ფაილები წაუკითხავი იქნება ნებისმიერი მავნე აქტორის მიერ. თუ თქვენ აგზავნით სენსიტიურ ფინანსურ ან პერსონალურ მონაცემებს, დაშიფვრა ამ ინფორმაციას უფრო უსაფრთხოდ ინახავს.

თქვენი ფაილების დასაცავად მრავალი გზა არსებობს, მათ შორის, პაროლის გამოყენება თქვენს მოწყობილობებზე წვდომისთვის. დაშიფვრა ამ დაცვას კიდევ უფრო აძლიერებს. ფაილის დაშიფვრისას, მისი შინაარსი ირევა, რაც მას გაუშიფრავს ხდის უსაფრთხოების უნიკალური სერტიფიკატის გარეშე. სანამ შესული ხართ Windows მოწყობილობაში, თქვენი ფაილი გაიხსნება და ნორმალურად იმუშავებს, რადგან უსაფრთხოების სერთიფიკატი მიმაგრებულია თქვენს ანგარიშზე. თუ ვინმე შეეცდება ამ ფაილის გახსნას თქვენს Windows ანგარიშში შესვლის გარეშე, ის წაუკითხავი იქნება.

ფაილის ან საქაღალდის დაშიფვრისთვის:

1. დააწკაპუნეთ მაუსის მარჯვენა ღილაკით ხატულაზე ფაილის ან საქაღალდის, რომლის დაშიფვრაც გსურთ.
2. აირჩიეთ **Okay**.
3. **Properties** ფანჯრის ბოლოში აირჩიეთ **Advanced.**
4. მონიშნეთ **Encrypt contents to secure data**. შიგთავსის დაშიფვრის გვერდით მონაცემების დასაცავად.
5. აირჩიეთ **Apply**.

6. თქვენ მოგეცემათ არჩევანი, გამოყენებული იქნას თუ არა დაშიფვრა დაკავშირებულ საქაღალდეებსა და ფაილებზე. მას შემდეგ რაც გადაწყვეტთ, აირჩიეთ **Okay.**
7. **Properties** ფანჯრის ბოლოში აირჩიეთ კვლავ **Apply.**
8. თქვენი ფაილი ან საქაღალდე ახლა დაშიფრულია და ახლავს დაბლოკვის ხატულა.
9. დეშიფრაციისთვის მიჰყევით იგივე ნაბიჯებს და მოხსენით ველი **Encrypt contents to secure data**.

თუ კონტენტის დაშიფვრის ვარიანტი მონაცემების დასაცავად მიუწვდომელია (რაც ნიშნავს, რომ ის ნაცრისფერია და თქვენ ვერ შეძლებთ ველის მონიშვნას), დაშიფვრა შეიძლება არ იყოს ჩართული ან ხელმისაწვდომი თქვენს მოწყობილობაზე. თუ ეს ასეა, წაიკითხეთ ეს სახელმძღვანელო, რათა გაიგოთ როგორ ჩართოთ დაშიფვრა Windows 11-ში.

უსაფრთხოების სერთიფიკატების სარეზერვო ასლის შექმნა დაშიფრული ფაილებისთვის

დაშიფვრა საოცრად უსაფრთხოა, რის გამოც გსურთ გქონდეთ უსაფრთხოების სერთიფიკატების სარეზერვო ასლი, რომელიც საშუალებას მოგცემთ შეხვიდეთ დაშიფრულ ფაილებსა და საქაღალდეებში. ეს სარეზერვო ასლები გამოდგება, თუ თქვენი მოწყობილობა დაზიანდა, მოიპარეს ან როგორმე წაშლილია. სარეზერვო ასლის შესაქმნელად მიჰყევით ამ ნაბიჯებს:

1. Windows-ის საძიებო ველში შეიყვანეთ “**certificate**”.
2. აირჩიეთ კომპიუტერის სერთიფიკატების მართვა.
3. აირჩიეთ **Personal** > **Certificates.** თქვენი ხელმისაწვდომი სერთიფიკატები გამოჩნდება მარჯვენა მხარეს პანელში.
4. ფანჯრის ზედა ნაწილში გადადით **Action** > **All Tasks** > **Export**.
5. ახლა თქვენ გაქვთ შესაძლებლობა შეინახოთ ეს სერთიფიკატები USB-ზე, გარე მოწყობილობაზე ან ღრუბელში შესანახად.

მომავალში ამ სერთიფიკატების ახალ მოწყობილობაზე გამოსაყენებლად, მიჰყევით ზემოთ მოცემულ ნაბიჯებს, მაგრამ აირჩიეთ **Import**..

ფაილების დაშიფვრა კიდევ ერთი გზაა Windows 11 თქვენი ციფრული ცხოვრების დაცვით. რჩევების, ხრიკებისა და ინფორმაციის მისაღებად Windows 11-ის მაქსიმალური სარგებლობისთვის, გადადით Windows Learning Cent-ზე

ფაილის და მონაცემთა მთლიანობის შემოწმების გამოყენება

ფაილის და მონაცემთა მთლიანობის შემოწმების გამოყენება გადამწყვეტი ასპექტია მობილური და უკაბელო მოწყობილობების უსაფრთხოებისა და საიმედოობის შესანარჩუნებლად. აი, როგორ შეგიძლიათ ეფექტურად განახორციელოთ ეს შემოწმებები:

1. Checksums და Hash ფუნქციები

MD5, SHA-256: გამოიყენეთ ჰეშის ფუნქციები, როგორიცაა MD5, SHA-256 ან SHA-3, რომ შექმნათ უნიკალური ჰეშები ფაილებისთვის. შეადარეთ ფაილის მიმდინარე ჰეში ორიგინალურ ჰეშთან, რათა აღმოაჩინოთ რაიმე ცვლილება.

ინსტრუმენტები: გამოიყენეთ ინსტრუმენტები, როგორიცაა md5sum, sha256sum, ან ოპერაციული სისტემების ჩაშენებული ფუნქციები ჰეშების გენერირებისთვის და შესამოწმებლად.

2. ციფრული ხელმოწერები

საჯარო გასაღების ინფრასტრუქტურა (PKI): გამოიყენეთ ციფრული ხელმოწერები ფაილების და მონაცემების მთლიანობისა და ავთენტურობის შესამოწმებლად. ციფრული ხელმოწერები უზრუნველყოფს, რომ ფაილი არ არის შეცვლილი და ადასტურებს ფაილის წყაროს.

პროგრამული უზრუნველყოფის განახლებები: დარწმუნდით, რომ პროგრამული უზრუნველყოფის განახლებები და პატჩები ციფრულად არის ხელმოწერილი მათი მთლიანობის შესამოწმებლად ინსტალაციამდე.

3. ფაილის მთლიანობის მონიტორინგი (FIM)

ინსტრუმენტები: დანერგეთ FIM გადაწყვეტილებები, როგორიცაა Tripwire, OSSEC ან AIDE, რათა დააკვირდეთ და შეატყობინოთ ფაილებში ნებისმიერი არაავტორიზებული ცვლილების შესახებ.

კონფიგურაცია: დააკონფიგურირეთ FIM ინსტრუმენტები კრიტიკული სისტემის ფაილების, კონფიგურაციის ფაილების და დირექტორიების მონიტორინგისთვის, სადაც ინახება მგრძნობიარე მონაცემები.

4. ვერსიის კონტროლის სისტემები

Git, SVN: გამოიყენეთ ვერსიების კონტროლის სისტემები ფაილებსა და კოდებში ცვლილებების სამართავად. ეს სისტემები აკონტროლებენ ცვლილებებს და შეუძლიათ აღმოაჩინონ და აღადგინონ არაავტორიზებული ცვლილებები.

შეასრულეთ ჰეშები: ვერსიის კონტროლის სისტემაში თითოეულ ჩადენას აქვს უნიკალური ჰეში, რომელიც გეხმარებათ კოდის ბაზის მთლიანობის გადამოწმებაში.

5. მონაცემთა ბაზის მთლიანობის შემოწმება

საკონტროლო ჯამები: გამოიყენეთ საკონტროლო ჯამები და ჰეშები მონაცემთა ბაზის ჩანაწერების მთლიანობის შესამოწმებლად.

აუდიტის ჟურნალები: ჩართეთ და რეგულარულად გადახედეთ მონაცემთა ბაზის აუდიტის ჟურნალებს ნებისმიერი არაავტორიზებული ცვლილების გამოსავლენად.

6. სარეზერვო მთლიანობის შემოწმება

Hashing და Checksums: შექმენით ჰეშები სარეზერვო ფაილებისთვის და შეადარეთ ისინი ორიგინალურ ფაილებს, რათა დარწმუნდეთ, რომ სარეზერვო ასლი არ არის დაზიანებული ან გაყალბებული.

რეგულარული ტესტირება: რეგულარულად შეამოწმეთ სარეზერვო ასლები მათი აღდგენით, რათა დარწმუნდეთ, რომ ისინი სრული და უცვლელია.

7. ბოლოდან ბოლომდე დაშიფვრა

მონაცემთა გადაცემა: გამოიყენეთ ბოლოდან ბოლომდე დაშიფვრა, რათა დარწმუნდეთ, რომ მონაცემები არ შეიცვლება გადაცემის დროს. პროტოკოლებს, როგორიცაა TLS/SSL, შეუძლია დაეხმაროს მონაცემთა მთლიანობის შენარჩუნებას ქსელებში.

უსაფრთხო შენახვა: დაშიფრეთ მონაცემები დასვენების დროს, რათა დაიცვათ ისინი არაავტორიზებული ცვლილებებისგან.

8. ქსელზე დაფუძნებული მთლიანობის შემოწმება

შეჭრის აღმოჩენის სისტემები (IDS): განათავსეთ IDS ქსელის ტრაფიკის მონიტორინგისთვის ხელყოფის ან მავნე აქტივობის ნიშნებისთვის.

ქსელის სეგმენტაცია: ქსელის ცალკეულ სეგმენტებზე კრიტიკული სისტემების და მგრძნობიარე მონაცემების იზოლირება, მთლიანობის პოტენციური დარღვევის ზემოქმედების შესამცირებლად.

9. მომხმარებლის წვდომის კონტროლი

როლებზე დაფუძნებული წვდომის კონტროლი (RBAC): განახორციელეთ RBAC, რათა დარწმუნდეთ, რომ მხოლოდ ავტორიზებულ მომხმარებლებს შეუძლიათ შეცვალონ კრიტიკული ფაილები და მონაცემები.

აუდიტის ბილიკები: შეინახეთ მომხმარებლის საქმიანობის დეტალური აუდიტის ბილიკი არაავტორიზებული ცვლილებების აღმოსაჩენად და გამოსაკვლევად.

10. რეგულარული უსაფრთხოების აუდიტი

დაუცველობის შეფასება: ჩაატარეთ დაუცველობის რეგულარული შეფასებები და შეღწევადობის ტესტირება მთლიანობის პოტენციური საფრთხის იდენტიფიცირებისთვის და შესამცირებლად.

შესაბამისობის შემოწმება: უზრუნველყოს ინდუსტრიის სტანდარტებისა და რეგულაციების შესაბამისობა, რომლებიც ავალდებულებს მონაცემთა და ფაილების მთლიანობის ზომებს (მაგ., HIPAA, PCI-DSS).

ფაილის და მონაცემთა მთლიანობის შემოწმების განხორციელება: ნაბიჯ-ნაბიჯ მიდგომა

კრიტიკული ფაილების და მონაცემების იდენტიფიცირება: დაადგინეთ, რომელ ფაილებსა და მონაცემებს სჭირდება მთლიანობის შემოწმება.

აირჩიეთ ხელსაწყოები და ტექნიკა: აირჩიეთ შესაბამისი ინსტრუმენტები და ტექნიკა მთლიანობის შემოწმებისთვის (მაგ., ჰეშინგი, ციფრული ხელმოწერები).

პროცესების ავტომატიზაცია: მთლიანობის შემოწმების ავტომატიზაცია სკრიპტებისა და დაგეგმილი ამოცანების გამოყენებით.

მონიტორინგი და გაფრთხილება: დააყენეთ მონიტორინგის სისტემები და გაფრთხილებები არაავტორიზებული ცვლილებებისთვის.

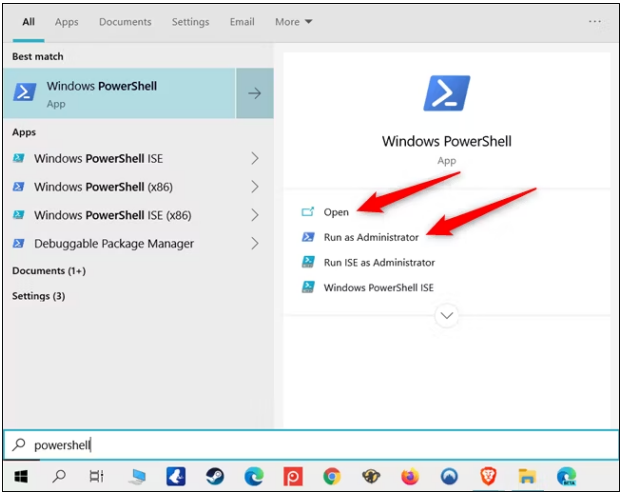
განხილვა და განახლება: რეგულარულად გადახედეთ მთლიანობის შემოწმების პოლიტიკას და განაახლეთ ისინი საჭიროებისამებრ.

ამ მთლიანობის შემოწმების განხორციელებით, შეგიძლიათ ეფექტურად დაიცვათ თქვენი მობილური და უკაბელო მოწყობილობები არაავტორიზებული ცვლილებებისგან და უზრუნველყოთ თქვენი მონაცემების სანდოობა.

როგორ შევამოწმოთ გადმოწერილი ფაილის ან ინსტალერის SHA256 მთლიანობა?

Windows მაგალითზე ვნახოთ გადმოწერილი ფაილის ან ინსტალერის SHA256 მთლიანობის შესამოწმებლი პროცედურა:

გახსენით Windows PowerShell. მაგალითად, Windows Start მენიუს ბრძანების ველში აკრიფეთ **PowerShell**.



ჩაწერეთ **Get-FileHash**, რასაც მოჰყვება სივრცე.

გადმოიტანეთ გადმოწერილი ფაილი ან ინსტალერი Windows PowerShell-ის ფანჯარაში Get-FileHash ბრძანებისა და სივრცის შემდეგ. ალტერნატიულად, შეიყვანეთ ფაილის ან ინსტალერის სრული გზა ორმაგი ბრჭყალებით, სივრცის შემდეგ.

მაგალითად:

```
PS C:\Users\SESA142775> Get-FileHash "C:\My_Software.exe"
```

დააჭირეთ Enter. გამომავალი მსგავსია შემდეგი:

```
PS C:\Users\SESA142775> Get-FileHash "C:\My_Software.exe"

Algorithm       Hash
---------       ----
SHA256          E99322006F6538D35CC0D504F5920C36540CB6FAB88D505352A7288
```

შეადარეთ PowerShell-ის გამოთვლილი მნიშვნელობა მოწოდებულ ჰეშის მნიშვნელობას. თუ ჰეშის მნიშვნელობები ემთხვევა, ფაილის მთლიანობა ნორმალურია.

მონაცემთა მთლიანობის უზრუნველყოფა გადამწყვეტია ჯანსაღი და საიმედო Windows 11 სისტემის შესანარჩუნებლად. მოდით გამოვიკვლიოთ ორი მეთოდი მონაცემთა მთლიანობის შემოწმების შესასრულებლად:

<u>დაზიანებული სისტემის ფაილების სკანირება და შეკეთება:</u>

სისტემის ფაილების შემოწმება (SFC) და გამოსახულების განლაგების სერვისი და მენეჯმენტი (DISM) მძლავრი უტილიტებია ამ მიზნით.

აი, როგორ გამოიყენოთ ისინი:

გახსენით ადმინისტრაციული დონის ბრძანების ხაზი:

Windows 11 დესკტოპის საძიებო ინსტრუმენტში ჩაწერეთ “command prompt”

დააწკაპუნეთ მაუსის მარჯვენა ღილაკით Command Prompt აპზე და აირჩიეთ **Run as administrator**.

შეასრულეთ შემდეგი ბრძანება Windows 11-ის სარეზერვო სისტემის ფაილების განახლებისთვის Microsoft-ის სერვერებიდან DISM-ის გამოყენებით:

DISM.exe /Online /Cleanup-image /Restorehealth

ამ პროცესს შეიძლება რამდენიმე წუთი დასჭირდეს, თქვენი ინტერნეტ კავშირის მიხედვით.

სარეზერვო სისტემის ფაილების განახლების შემდეგ, შეამოწმეთ შეცდომები და განახორციელეთ შეკეთება SFC-ის გამოყენებით:

sfc / scannow

კიდევ ერთხელ, ამ გადამოწმების პროცესს შეიძლება რამდენიმე წუთი დასჭირდეს1.

MD5 ან SHA256 საკონტროლო ჯამების შემოწმება:

თქვენ შეგიძლიათ შეამოწმოთ ფაილის მთლიანობა საკონტროლო ჯამების გამოყენებით.

გახსენით ბრძანების ხაზი და შეასრულეთ შემდეგი ბრძანებები:

ფაილის MD5 საკონტროლო ჯამის შესამოწმებლად:

certutil -hashfile "C:\Path\To\File.ext" MD5

ფაილის SHA256 საკონტროლო ჯამის შესამოწმებლად:

certutil -hashfile "C:\Path\To\File.ext" SHA256

საკონტროლო ჯამი გამოჩნდება, რაც უზრუნველყოფს მონაცემთა მთლიანობას.

გახსოვდეთ, ეს ნაბიჯები დაგეხმარებათ Windows 11-ის ჯანსაღი სისტემის შენარჩუნებაში დაზიანებული ფაილების გამოვლენით.

საფრთხეებისა და მოწყვლადობის გამოვლენა

ქსელის Mapper, ან Nmap, არის ღია წყაროს უტილიტა, რომელიც გამოიყენება ქსელის აღმოჩენისა და უსაფრთხოების აუდიტის განსახორციელებლად. ადმინისტრატორები ასევე იყენებენ Nmap-ს ჰოსტის მონიტორინგის განსახორციელებლად ან მომსახურების განახლების დაგეგმვის სამართავად. Nmap განსაზღვრავს, რა ჰოსტების ხელმისაწვდომი ქსელში, რა სერვისებია გაშვებული, რა ოპერაციული სისტემებია ინსტალირებული და რა პაკეტის ფილტრები ან დამცავი ეკრანებია გამართული.

წინაპირობები: კომპიუტერი Ubuntu 16.0.4 LTS ინსტალირებული ვირტუალური მანქანა

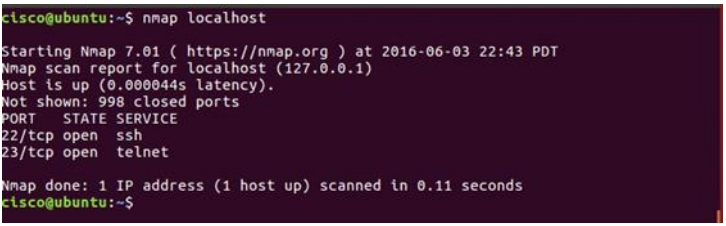
ნაბიჯი 1: გახსენით ტერმინალის ფანჯარა Ubuntu- ში.

1. შედით Ubuntu- ში სააღრიცხვო ანგარიშის გამოყენებით.
2. დააჭირეთ **terminal**ნიშნულს ტერმინალის გასახსნელად.

ნაბიჯი 2: გაუშვით Nmap.

ბრძანების სტრიქონზე შეიყვანეთ შემდეგი ბრძანება, რომ დაიწყოთ ძირითადი სკანირება ამ Ubuntu-ს ამსისტემის საშუალებით:

cisco @ubuntu: ~$ **nmap localhost**



მივიღებთ პირველი 1024 TCP პორტის სკანირების შედეგს. რა TCP პორტებია ღია?

ნაბიჯი 3: გამოიყენეთ ადმინისტრაციული პრივილეგიები Nmap-ის გასაშვებად.

1. ჩაწერეთ შემდეგი ბრძანება ტერმინალში კომპიუტერის UDP პორტების სკანირებისთვის (გახსოვდეთ,Ubuntu არის კლავიშებზე მგრძნობიარე) და შეიყვანეთ პაროლი **password** მოთხოვნისამებრ:

cisco@ubuntu:~$ **sudo nmap –sU localhost**

```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

რომელი UDP პორტებია ღია?

---

2. შეიტანეთ შემდეგი ბრძანება ტერმინალში:

cisco@ubuntu:~$ **nmap –sV localhost**

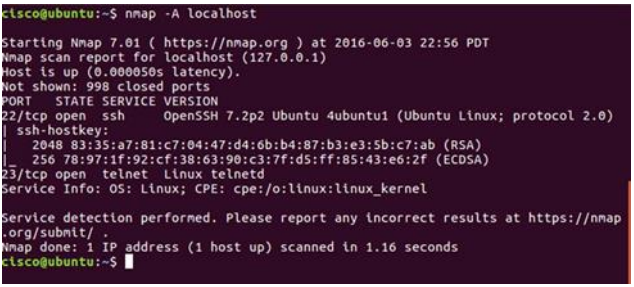
```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
cisco@ubuntu:~$
```

გამოიყენეთ **–sV** switch with the **nmap** ბრძანება, რომელიც გამოიკვლევს უბუნტუს ვერსიას და რომელსაც გამოიყენებთ მოწყვლადობების აღმოსაჩენად.

ნაბიჯი 4: მოიპოვეთ SSH გასაღებები.

ჩაწერეთ შემდეგი ბრძანება ტერმინალში სკრიპტის სკანირების დასაწყებად:

cisco@ubuntu:~$ **nmap –A localhost**



თქვენ მოიპოვებთ SSH გასაღებებს ჰოსტის სისტემისათვის. ბრძანება გაუშვებს სკრიპტების კომპლექტს, რომლებსაც შეიცავს Nmap-ს კონკრეტული ხარვეზების შესამოწმებლად.

მობილური და უსადენო მოწყობილობებზე თავდასხმების თავიდან აცილება

მობილურ და უკაბელო მოწყობილობებზე თავდასხმების პრევენცია მოიცავს მრავალ ფენიან მიდგომას, რომელიც მოიცავს როგორც ტექნიკურ ზომებს, ასევე მომხმარებლის ინფორმირებულობას. აქ არის რამდენიმე ძირითადი სტრატეგია:

1. რეგულარულად განახლება და პატჩი

ოპერაციული სისტემის და პროგრამული უზრუნველყოფის განახლებები: დარწმუნდით, რომ ოპერაციული სისტემა და ყველა დაინსტალირებული აპი რეგულარულად განახლდება ცნობილი დაუცველობების დასაფარად.

Firmware განახლებები: განაახლეთ მოწყობილობის firmware.

2. გამოიყენეთ ძლიერი ავთენტიფიკაცია

მრავალფაქტორიანი ავთენტიფიკაცია (MFA): ჩართეთ MFA უსაფრთხოების დამატებითი ფენის დასამატებლად.

ძლიერი პაროლები: გამოიყენეთ ძლიერი, უნიკალური პაროლები სხვადასხვა ანგარიშებისთვის და რეგულარულად შეცვალეთ ისინი.

3. უსაფრთხო კავშირები

VPN-ები: გამოიყენეთ ვირტუალური პირადი ქსელები (VPN) საჯარო Wi-Fi-ზე წვდომისას თქვენი ინტერნეტ ტრაფიკის დაშიფვრისთვის.

უსაფრთხო Wi-Fi: სახლისა და ბიზნესის Wi-Fi ქსელების კონფიგურაცია ძლიერი დაშიფვრით (WPA3 თუ შესაძლებელია).

4. აპის უსაფრთხოება

სანდო წყაროები: ჩამოტვირთეთ აპლიკაციები მხოლოდ ოფიციალური აპების მაღაზიებიდან, როგორიცაა Google Play Store ან Apple App Store.

აპის ნებართვები: გადახედეთ და შეამცირეთ აპის ნებართვები მგრძნობიარე მონაცემებზე წვდომის შესაზღუდად.

5. ანტივირუსი და მავნე პროგრამა

უსაფრთხოების აპლიკაციები: დააინსტალირეთ რეპუტაციის მქონე ანტივირუსული და მავნე პროგრამული უზრუნველყოფის პროგრამები მავნე პროგრამებისგან დასაცავად.

6. დაშიფვრა

მონაცემთა დაშიფვრა: ჩართეთ დაშიფვრა თქვენს მოწყობილობაზე, რათა დაიცვან მონაცემები დასვენების დროს. თანამედროვე მოწყობილობების უმეტესობა გთავაზობთ სრული დისკის დაშიფვრას.

ბოლოდან ბოლომდე დაშიფვრა: გამოიყენეთ საკომუნიკაციო აპლიკაციები, რომლებიც უზრუნველყოფენ ბოლოდან ბოლომდე დაშიფვრას.

7. სარეზერვო მონაცემები

რეგულარული სარეზერვო ასლები: რეგულარულად შექმენით თქვენი მონაცემების სარეზერვო ასლები უსაფრთხო ადგილას, რათა თავიდან აიცილოთ მონაცემთა დაკარგვა ისეთი შეტევებისგან, როგორიცაა გამოსასყიდი პროგრამა.

8. ინფორმირებულობა და ტრენინგი

ფიშინგის ინფორმირებულობა: ფრთხილად იყავით ფიშინგის მცდელობებთან ელფოსტის, SMS-ის ან სხვა შეტყობინებების პლატფორმების საშუალებით.

უსაფრთხო დათვალიერება: მოერიდეთ საეჭვო ბმულებზე დაწკაპუნებას და უცნობი წყაროებიდან დანართების ჩამოტვირთვას.

9. მოწყობილობების მართვა

დისტანციური წაშლა: ჩართეთ დისტანციური წაშლის შესაძლებლობები, რათა წაშალოთ მონაცემები, თუ მოწყობილობა დაიკარგება ან მოიპარეს.

მოწყობილობის დაბლოკვა: გამოიყენეთ ძლიერი პაროლები, PIN-ები ან ბიომეტრიული ავთენტიფიკაცია თქვენი მოწყობილობის დასაბლოკად.

10. ქსელის უსაფრთხოება

Firewall: გამოიყენეთ firewalls შემომავალი და გამავალი ქსელის ტრაფიკის მონიტორინგისა და კონტროლისთვის.

შეჭრის აღმოჩენის სისტემები (IDS): განათავსეთ IDS უსაფრთხოების პოტენციური დარღვევების აღმოსაჩენად და რეაგირებისთვის.

11. რეგულარული აუდიტი და მონიტორინგი

უსაფრთხოების აუდიტი: ჩაატარეთ რეგულარული უსაფრთხოების აუდიტი დაუცველობის იდენტიფიცირებისა და შესამცირებლად.

მონიტორინგის ხელსაწყოები: გამოიყენეთ მონიტორინგის ხელსაწყოები თქვენს ქსელში საეჭვო მოქმედებების გამოსავლენად.

12. IoT მოწყობილობის უსაფრთხოება

უსაფრთხო კონფიგურაცია: შეცვალეთ ნაგულისხმევი პაროლები და პარამეტრები IoT მოწყობილობებზე.

სეგმენტაცია: მოათავსეთ IoT მოწყობილობები ცალკე ქსელში კრიტიკულ სისტემებზე წვდომის შესაზღუდად.

ამ სტრატეგიების კომბინაციით, ინდივიდებსა და ორგანიზაციებს შეუძლიათ მნიშვნელოვნად შეამცირონ მობილურ და უკაბელო მოწყობილობებზე თავდასხმების რისკი.

დაშიფრული და დაუშიფრავი ტრაფიკის გადაცემა

ტექსტური შეტყობინების დაშიფვრა და გაშიფვრა OpenSSL გამოყენებით

OpenSSL არის ღია კოდის პროგრამული უზრუნველყოფა, რომელიც უზრუნველყოფს სატრანსპორტო ფენის (TLS) და სოკეტების ფენის (SSL) უსაფრთხოებას. OpenSSL არის პროგრამული ბიბლიოთეკა აპლიკაციებისთვის, რომლებიც უზრუნველყოფენ უსაფრთხო კომუნიკაციას კომპიუტერულ ქსელებში მოსმენის საწინააღმდეგოდ. მას ფართოდ იყენებენ ინტერნეტ სერვერები, მათ შორის HTTPS ვებსაიტების უმრავლესობა.

წინაპირობა: ვირტუალური მანქანა.

ნაბიჯი 1: ტექსტური ფაილის დაშიფვრა.

- გაუშვით Security Workstation VM და შედით მომხმარებლის სახელით sec_admin და პაროლი net_secPW .

- გახსენით ტერმინალის ფანჯარა.

- გადადით დირექტორიაში, სადაც შენახულია ტექსტური ფაილი. (ამ მაგალითში დაშიფრული ტექსტური ფაილი არის /home/sec_admin/lab.support.files/ დირექტორიაში):

```
[sec_admin@secOps ~]$ cd /home/sec_admin/lab.support.files/
[sec_admin@secOps lab.support.files]$
```

- ჩაწერეთ ქვემოთ მოცემული ბრძანება, რათა ეკრანზე გამოიტანოთ დასაშიფრი ტექსტური ფაილის შინაარსი (ჩვენ შემთხვევაში letter_to_grandma.txt):

```
[sec_admin@secOps lab.support.files]$ cat letter_to_grandma.txt
გამარჯობა ბებო,
ამ წერილს ვწერ, რომ მადლობა გადაგიხადოთ თქვენ მიერ გამოგზავნილი შოკოლადის
მე. დღეს დილით მივიღე და ყუთის ნახევარი უკვე ვჭამე! მათ
აბსოლუტურად გემრიელია!
ყველაფერს საუკეთესოს გისურვებ. სიყვარული,
შენი ფუნთუშა მჭამელი შვილიშვილი.
[sec_admin@secOps lab.support.files]$
```

- იმავე ტერმინალის ფანჯრიდან გაუშვით ქვემოთ მოცემული ბრძანება ტექსტური ფაილის დაშიფვრისთვის. ბრძანება გამოიყენებს AES-256-ს ტექსტური ფაილის დასაშიფრად და დაშიფრული ვერსიის შესანახად, როგორც message.enc. OpenSSL ითხოვს პაროლს და პაროლის დადასტურებას. მიუთითეთ პაროლი მოთხოვნის შესაბამისად და დარწმუნდით, რომ დაიმახსოვრეთ პაროლი.

```
[sec_admin@secOps lab.support.files]$ openssl aes-256-cbc -in
letter_to_grandma.txt -out message.enc
შეიყვანეთ aes-256-cbc დაშიფვრის პაროლი:
დადასტურება - შეიყვანეთ aes-256-cbc დაშიფვრის პაროლი:
[sec_admin@secOps lab.support.files]$
```

როდესაც პროცესი დასრულდება, გამოიყენეთ **cat** ბრძანება message.enc ფაილის შინაარსის საჩვენებლად.

ნაწილი 2: შეტყობინებების გაშიფვრა OpenSSL-ით

- გამოიყენეთ ქვემოთ მოცემული ბრძანება message.enc-ის გასაშიფრად.

```
[sec_admin@secOps lab.support.files]$ openssl aes-256-cbc –a -d -in
message.enc -out decrypted_letter.txt
```

- OpenSSL ითხოვს პაროლს, რომელიც გამოიყენეთ ფაილის დაშიფვრისთვის. ისევ შეიყვანეთ იგივე პაროლი.

- როდესაც OpenSSL დაასრულებს **message.enc** ფაილის გაშიფვრას, ის ინახავს გაშიფრულ შეტყობინებას ტექსტურ ფაილში, სახელწოდებით **decrypted_letter.txt**. გამოიყენეთ **cat** ბრძანება **decrypted_letter.txt** შინაარსის საჩვენებლად.

```
[sec_admin@secOps lab.support.files]$ cat decrypted_letter.txt
```

პაროლის გატეხვა

პაროლის სიძლიერე არის პაროლის ეფექტურობის საზომი, რათა გაუძლოს პაროლის გატეხვის შეტევებს. პაროლის სიძლიერე განისაზღვრება:

სიგრძე: სიმბოლოების რაოდენობა, რომელსაც შეიცავს პაროლი.

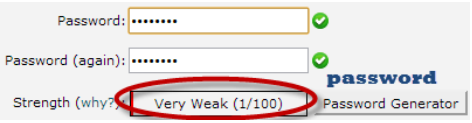
სირთულე: იყენებს ასოების, რიცხვების და სიმბოლოების კომბინაციას ?

არაპროგნოზირებადობა: არის თუ არა ეს ისეთი რამ, რისი გამოცნობაც თავდამსხმელს ადვილად შეუძლია?

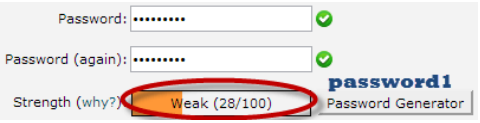
ჩვენ გამოვიყენებთ სამ პაროლს:

1. password
2. password1
3. #password1$

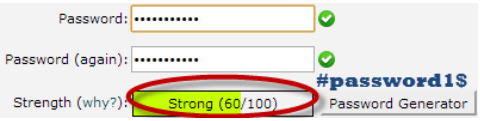
პაროლების შექმნისას გამოვიყენებთ Cpanel-ის პაროლის სიძლიერის ინდიკატორს. ქვემოთ მოცემულ სურათებში ნაჩვენებია თითოეული ზემოთ ჩამოთვლილი პაროლის ძლიერი მხარე.



შენიშვნა: გამოყენებული პაროლი არის პაროლი, სიძლიერე არის 1 და ის ძალიან სუსტია.



შენიშვნა: გამოყენებული პაროლი არის password1, სიმძლავრე არის 28 და ის ჯერ კიდევ სუსტია.



შენიშვნა: გამოყენებული პაროლი არის #password1$, სიმძლავრე არის 60 და ის ძლიერია.

რაც უფრო მაღალია სიძლიერის რიცხვი, მით უკეთესი პაროლი.

იმისათვის, რომ ზემოაღნიშნული პაროლები შევინახოთ md5 ჰეშირების გამოყენებით, გამოვიყენებთ ონლაინ md5 ჰეშის გენერატორს, რომ გადავიყვანოთ ჩვენი პაროლები md5 ჰეშებად.

ქვემოთ მოყვანილი ცხრილი აჩვენებს პაროლის ჰეშებს.

პაროლი	MD5 ჰეში	Cpanel Strength Indicator
password	5f4dcc3b5aa765d61d8327deb882cf99	1
password1	7c6a180b36896a0a8c02787eeafb0e4c	28
#password1$	29e08fb7103c327d68327f23d8d9256c	60

გამოიყენეთ https://md5hashing.net/ ზემოხსენებული ჰეშების გასატეხად. ქვემოთ მოყვანილი სურათები აჩვენებს პაროლის გატეხვის შედეგებს ზემოხსენებული პაროლების შესახებ.

როგორც ზემოაღნიშნული შედეგებიდან ხედავთ, ჩვენ მოვახერხეთ პირველი და მეორე პაროლების გატეხვა, რომლებსაც უფრო დაბალი სიძლიერის ნომრები ჰქონდათ. ჩვენ ვერ მოვახერხეთ მესამე პაროლის გატეხვა, რომელიც უფრო გრძელი, რთული და არაპროგნოზირებადი იყო. მას უფრო მაღალი სიძლიერის რიცხვი ჰქონდა.

პაროლის გატეხვის ტექნიკა

არსებობს მთელი რიგი **ტექნიკა, რომელიც შეიძლება გამოყენებულ იქნას პაროლების გასატეხად** . ქვემოთ აღვწერთ ყველაზე ხშირად გამოყენებულს:

ლექსიკონის შეტევა – ეს მეთოდი გულისხმობს სიტყვების სიის გამოყენებას მომხმარებლის პაროლების შესადარებლად.

უხეში ძალის შეტევა - ეს მეთოდი ლექსიკონის შეტევის მსგავსია . უხეში ძალის შეტევები იყენებს ალგორითმებს, რომლებიც აერთიანებს ალფა-ციფრულ სიმბოლოებს და სიმბოლოებს თავდასხმის პაროლების შესაქმნელად. მაგალითად, პაროლის მნიშვნელობის „პაროლი“ ასევე შეიძლება სცადოთ როგორც p@$$word უხეში ძალის შეტევის გამოყენებით.

Rainbow table attack – ეს მეთოდი იყენებს წინასწარ გამოთვლილ ჰეშებს. დავუშვათ, რომ გვაქვს მონაცემთა ბაზა, რომელიც ინახავს პაროლებს md5 ჰეშებად. ჩვენ შეგვიძლია შევქმნათ სხვა მონაცემთა ბაზა, რომელსაც აქვს md5 ხშირად გამოყენებული პაროლების ჰეშები. ჩვენ შეგვიძლია შევადაროთ პაროლის ჰეში, რომელიც გვაქვს მონაცემთა ბაზაში შენახულ ჰეშებთან. თუ შესატყვისი ნაპოვნია, მაშინ ჩვენ გვაქვს პაროლი.

გამოიცანით - როგორც სახელიდან ჩანს, ეს მეთოდი გულისხმობს გამოცნობას. პაროლები, როგორიცაა qwerty, პაროლი, admin და ა.შ. ჩვეულებრივ გამოიყენება ან დაყენებულია ნაგულისხმევ პაროლად. თუ ისინი არ შეცვლილა ან თუ მომხმარებელი უყურადღებოა პაროლების შერჩევისას, მაშინ ისინი შეიძლება ადვილად დაზარალდნენ.

Spidering – ორგანიზაციების უმეტესობა იყენებს პაროლებს, რომლებიც შეიცავს კომპანიის ინფორმაციას. ეს ინფორმაცია შეგიძლიათ იხილოთ კომპანიის ვებსაიტებზე, სოციალურ მედიაში, როგორიცაა facebook , twitter და ა.შ. Spidering აგროვებს ინფორმაციას ამ წყაროებიდან სიტყვების სიების შესაქმნელად. სიტყვების სია შემდეგ გამოიყენება ლექსიკონისა და უხეში ძალის შეტევების შესასრულებლად.

როგორ დავიცვათ თავი პაროლის გატეხვის შეტევებისგან?

- პაროლების გატეხვის შანსების შესამცირებლად ორგანიზაციას შეუძლია გამოიყენოს შემდეგი მეთოდები
- მოერიდეთ მოკლე და ადვილად პროგნოზირებად პაროლებს

- მოერიდეთ პაროლების გამოყენებას პროგნოზირებადი შაბლონებით, როგორიცაა 11552266.
- მონაცემთა ბაზაში შენახული პაროლები ყოველთვის უნდა იყოს დაშიფრული. md5 დაშიფვრებისთვის, უმჯობესია პაროლის ჰეშების დამარილება მათ შენახვამდე. Salting გულისხმობს რაიმე სიტყვის დამატებას მითითებულ პაროლზე ჰეშის შექმნამდე.
- სარეგისტრაციო სისტემების უმეტესობას აქვს პაროლის სიძლიერის ინდიკატორები, ორგანიზაციებმა უნდა მიიღონ პოლიტიკა, რომელიც ხელს უწყობს პაროლის მაღალი სიძლიერის ნომრებს.

ჰაკერული აქტივობა: გატეხე ახლავე!

ამ პრაქტიკულ სცენარში ხორციელდება **Windows ანგარიშის გატეხვა მარტივი პაროლით**. **Windows იყენებს NTLM ჰეშებს პაროლების დასაშიფრად**.

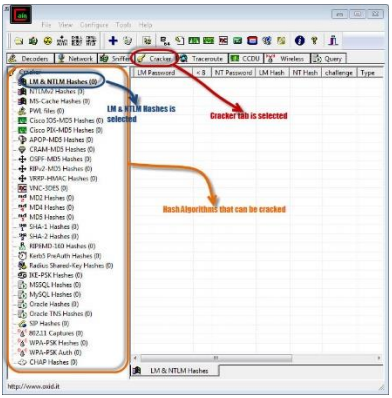
გამოიყენეთ ლექსიკონის შეტევა. თქვენ უნდა ჩამოტვირთოთ ლექსიკონის თავდასხმის სიტყვების სია აქ 10k-Most-Common.zip

ამ დემონსტრაციისთვის ჩვენ შევქმენით ანგარიში სახელწოდებით Accounts პაროლით qwerty Windows 7-ზე.

როგორ გავტეხოთ პაროლი

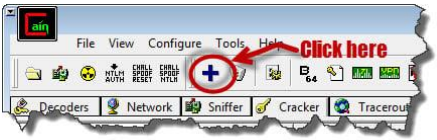
ნაბიჯი 1. გახსენით პროგრამა კაენი და აბელი.

თქვენ მიიღებთ შემდეგ მთავარ ეკრანს



ნახატი 2. იპოვეთ დამატების ღილაკი.

დარწმუნდით, რომ კრეკერის ჩანართი არჩეულია, როგორც ეს ნაჩვენებია ზემოთ და დააჭირეთ ღილაკს **დამატება** ინსტრუმენტთა პანელზე.



ნახატი 3. შეამოწმეთ დიალოგური ფანჯარა.

შემდეგი დიალოგური ფანჯარა გამოჩნდება. ადგილობრივი მომხმარებლების იმპორტი და დააჭირეთ შემდეგ ღილაკს.

ნახატი 4. ადგილობრივი მომხმარებლის ანგარიშები გამოჩნდება შემდეგნაირად.

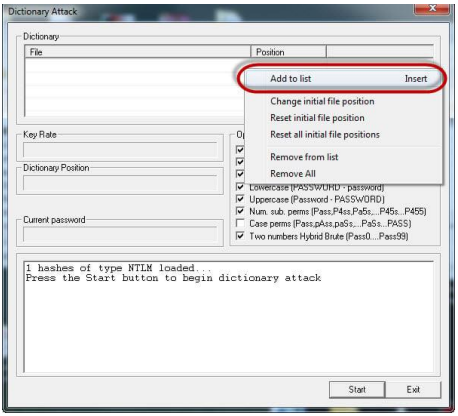
გაითვალისწინეთ, რომ ნაჩვენები შედეგები იქნება თქვენი ადგილობრივი აპარატის მომხმარებლის ანგარიშები.

ნაბიჯი 5. დააწკაპუნეთ მარჯვენა ღილაკით ანგარიშზე, რომლის გატეხვა გსურთ.

ჩვენ გამოვიყენებთ ანგარიშებს, როგორც მომხმარებლის ანგარიშს.

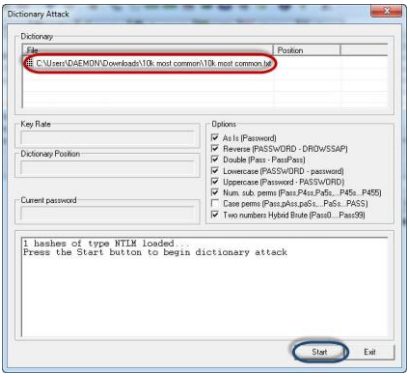
ნაბიჯი 6. შეამოწმეთ ქვემოთ მოცემული ეკრანი.

დააწკაპუნეთ მარჯვენა ღილაკით ლექსიკონის განყოფილებაში და აირჩიეთ მენიუს დამატება სიაში, როგორც ეს ზემოთ არის ნაჩვენები.



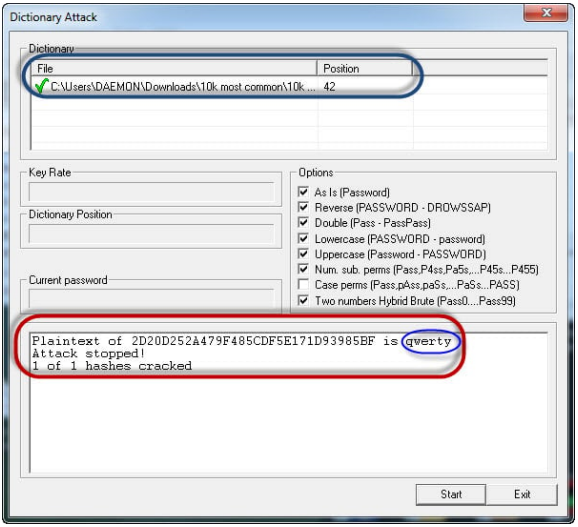
ნაბიჯი 7. დაათვალიერეთ ფაილი.

გადახედეთ 10k ყველაზე common.txt ფაილს, რომელიც ახლახან გადმოწერეთ



ნაბიჯი 8. შეამოწმეთ შედეგები.

თუ მომხმარებელმა გამოიყენა მარტივი პაროლი, როგორიცაა qwerty, მაშინ თქვენ უნდა მიიღოთ შემდეგი შედეგები.



შენიშვნა: პაროლის გატეხვის დრო დამოკიდებულია თქვენი პაროლის სიძლიერეზე, სირთულესა და დამუშავების ძალაზე. თუ პაროლი არ არის გატეხილი ლექსიკონის შეტევის გამოყენებით, შეგიძლიათ სცადოთ უხეში ძალის ან კრიპტოანალიზის შეტევები.

ციფრული ხელმოწერების გამოყენება

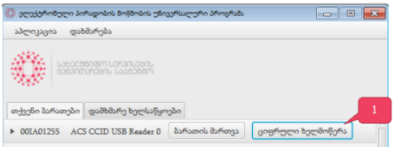
კვალიფიციური ელექტრონული ხელმოწერა არის ციფრული ხელმოწერა, რომელიც შესრულებულია კვალიფიციური ელექტრონული ხელმოწერის შექმნის საშუალებით, კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის გამოყენებით. იგი არის ელექტრონული მონაცემების ერთობლიობა რომლითაც დამოწმებულია ელექტრონული დოკუმენტი და მტკიცე რწმუნებით ადასტურებს ხელმომწერის ვინაობას, ასევე იცავს დოკუმენტს გაყალბებისა და მანიპულაციებისაგან. საქართველოს კანონმდებლობით კვალიფიციურ ელექტრონულ ხელმოწერას აქვს პირადი ხელმოწერის თანაბარი იურიდიული ძალა.

კვალიფიციური ელექტრონული ხელმოწერის შესასრულებლად დაგჭირდებათ პირადობის (ბინადრობის) ელექტრონული მოწმობა, პირადობის ელექტრონული მოწმობის უნივერსალური პროგრამა და წამკითხველი მოწყობილობა.

საქართველოში აღიარებული კვალიფიციური ელექტრონული ხელმომწერის სერტიფიკატებზე და ხელმოწერის შექმნის საშუალებებზე ინფორმაცია მოცემულია საქართველოს სანდო მომსახურების მიმწოდებლებისა და მათ მიერ შეთავაზებულ მომსახურებათა სია (ე.წ. Trusted List of Georgia)-ში. კვალიფიციური ელექტრონული ხელმოწერის შესახებ.

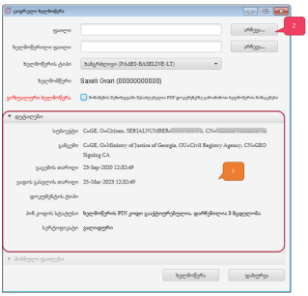
1. ციფრული ხელმოწერა პირადობის ელექტრონული მოწმობის უნივერსალურ პროგრამაში

პირადობის ელექტრონული მოწმობის უნივერსალურ პროგრამაში შესაძლებელია ციფრული ხელმოწერის განხორციელება. ამისათვის დააჭირეთ ღილაკს **[ციფრული ხელმოწერა] (1)**.



გამოსულ ფანჯარაში ბლოკში **[დეტალები] (ა)** მოცემულია ინფორმაცია ხელმოწერის სერტიფიკატის შესახებ.

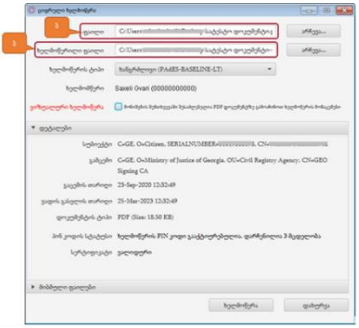
შემდეგ შეარჩიეთ ხელმოსაწერი ფაილი. ამისათვის დააჭირეთ ღილაკს **[არჩევა] (2)**



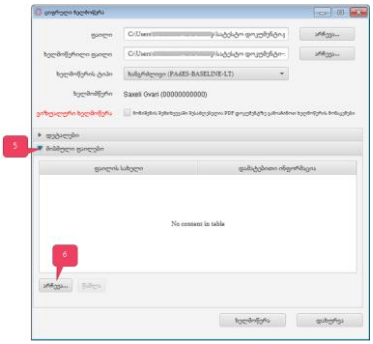
გამოსულ ფანჯარაში შეარჩიეთ ფაილი (3) და დააჭირეთ ღილაკს **[Open]**.

ციფრული ხელმოწერა შესაძლებელია .pdf ფორმატის ფაილებზე.

ხელმოსაწერი ფაილი ჩაჯდება ველში **[ფაილი] (ბ)**, ხოლო ხელმოწერილი ფაილის მისამართი განისაზღვრება ველში - **[ხელმოწერილი ფაილი] (გ)**.



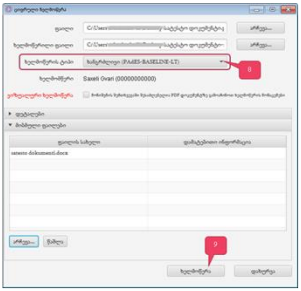
დოკუმენტზე შესაძლებელია ფაილების მიბმაც, ამისათვის გახსენით ბლოკი **[მიბმული ფაილები] (5)** და დააჭირეთ ღილაკს **[არჩევა] (6)**



გამოსულ ფანჯარაში შეარჩიეთ ფაილი და დააჭირეთ ღილაკს [**Open**]. არჩეული ფაილი ჩაჯდება ბლოკში [**მიბმული ფაილები**].

შენიშვნა, *ფაილების მიბმა არ არის შესაძლებელი უკვე ხელმოწერილ დოკუმენტზე.*

მიუთითეთ ხელმოწერის ტიპი **(8)** და დააჭირეთ ღილაკს [**ხელმოწერა**] **(9)**.



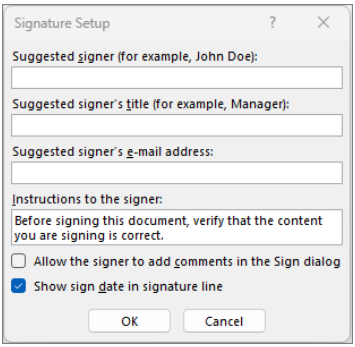
შემდეგ შეიყვანეთ ელექტრონული ხელმოწერის PIN კოდი **(PIN3) (10)** და დააჭირეთ ღილაკს [**დადასტურება**] **(11)**.

ხელმოწერის პროცესის დასრულებისას პროგრამა გამოიტანს შეტყობინებას **„გსურთ თუ არა ხელმოწერილი ფაილის გახსნა?"** ღილაკზე [**Yes**] დაჭერით დაიხურება ფანჯარა და გაიხსნება ხელმოწერილი დოკუმენტი. ღილაკზე [**No**] დაჭერით დაიხურება ფანჯარა.

2. ციფრული ხელმოწერა Microsoft 365 ფაილებისთვის

შექმენით ხელმოწერის ხაზი Word ან Excel-ში.

- დოკუმენტში ან სამუშაო ფურცელში მოათავსეთ თქვენი მაჩვენებელი იქ, სადაც გსურთ ხელმოწერის ხაზის შექმნა.
- ჩანართზე **Insert** აირჩიეთ **Signature Line Text** ჯგუფში .
- **Signature Setup** დიალოგურ ფანჯარაში აკრიფეთ ინფორმაცია, რომელიც გამოჩნდება ხელმოწერის ხაზის ქვეშ:



შემოთავაზებული ხელმომწერი: ხელმომწერის სრული სახელი.

შემოთავაზებული ხელმომწერის სათაური: ხელმომწერის სათაური, ასეთის არსებობის შემთხვევაში.

შემოთავაზებული ხელმომწერის ელექტრონული ფოსტის მისამართი: საჭიროების შემთხვევაში ხელმომწერის ელექტრონული ფოსტის მისამართი.

ინსტრუქციები ხელმომწერისთვის: დაამატეთ ინსტრუქციები ხელმომწერისთვის, როგორიცაა "დოკუმენტზე ხელმოწერამდე, შეამოწმეთ, რომ შინაარსი სწორია".

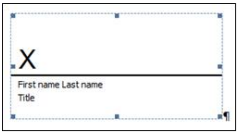
- აირჩიეთ ერთი ან ორივე ქვემოთ ჩამოთვლილი ველი:
  - მიეცით საშუალება ხელმომწერს დაამატოს კომენტარები ხელმოწერის დიალოგურ ფანჯარაში. ნება მიეცით ხელმომწერს აკრიფოს ხელმოწერის მიზანი.
  - ხელმოწერის ხაზში ხელმოწერის თარიღის ჩვენება დოკუმენტის ხელმოწერის თარიღი გამოჩნდება ხელმოწერით.

დამატებითი ხელმოწერის ხაზების დასამატებლად, გაიმეორეთ ეს ნაბიჯები.

შენიშვნა: თუ დოკუმენტი ხელმოუწერელი რჩება, გამოჩნდება **Signatures Message Bar.** აირჩიეთ **ხელმოწერების ნახვა** ხელმოწერის პროცესის დასასრულებლად.

ხელი მოაწერეთ ხელმოწერის ხაზს Word ან Excel-ში.

როდესაც ხელს აწერთ ხელმოწერის ხაზს, თქვენ ამატებთ თქვენი ხელმოწერის თვალსაჩინო წარმოდგენას და ციფრულ ხელმოწერას.



1. ფაილში დააწკაპუნეთ მარჯვენა ღილაკით ხელმოწერის ხაზზე და აირჩიეთ **ხელმოწერა**. თუ ფაილი იხსნება დაცულ ხედში, აირჩიეთ **Edit Anyway**, თუ ფაილი არის სანდო წყაროდან.

2. გააკეთეთ ერთი ან მეტი შემდეგი:

   - X- ის გვერდით მდებარე ველში .

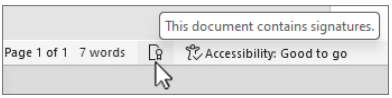
   - X- ის გვერდით მდებარე ველში მარკირების ფუნქციის გამოყენებით.

   - თქვენი წერილობითი ხელმოწერის გამოსახულების გამოსაყენებლად აირჩიეთ **სურათის არჩევა**. **სურათების ჩასმა** დიალოგური ფანჯრიდან აირჩიეთ თქვენი ხელმოწერის გამოსახულების ფაილის მდებარეობა , აირჩიეთ ფაილი და შემდეგ აირჩიეთ არჩევა .

   შენიშვნა: მომხმარებლებისთვის, რომლებიც იყენებენ ჩინურ (ტრადიციულ ან გამარტივებულ), კორეულ ან იაპონურ ვერსიებს, გამოჩნდება Stamp Signature Line ვარიანტი.

3. აირჩიეთ **ხელმოწერა**.

ხელმოწერების **ღილაკი** გამოჩნდება დოკუმენტის ან სამუშაო ფურცლის ბოლოში.



შენიშვნა: ხელმოწერის ხაზის ხელმოწერა შეგიძლიათ ხელმოწერის ხაზზე ორჯერ დაწკაპუნებით. ჩაწერეთ თქვენი სახელი **X**- ის გვერდით. ან **ხელმოწერის პანელში** მოთხოვნილი ხელმოწერების

განყოფილებაში აირჩიეთ ხელმოწერის გვერდით მდებარე ისარი . მენიუდან აირჩიეთ **ხელმოწერა**.

ამოიღეთ ციფრული ხელმოწერები Word-დან ან Excel-დან

1. გახსენით დოკუმენტი ან სამუშაო ფურცელი, რომელიც შეიცავს ხილულ ხელმოწერას, რომლის წაშლა გსურთ.
2. დააწკაპუნეთ მარჯვენა ღილაკით ხელმოწერის ხაზზე და აირჩიეთ **Remove Signature** და აირჩიეთ **დიახ**.

შენიშვნა: გარდა ამისა, თქვენ შეგიძლიათ წაშალოთ ხელმოწერა ხელმოწერის პანელში ხელმოწერის გვერდით მდებარე ისრის არჩევით. აირჩიეთ **ხელმოწერის წაშლა**.

ხელმოწერილ დოკუმენტებს ექნება ღილაკი **ხელმოწერები** დოკუმენტის ბოლოში. გარდა ამისა, ხელმოწერილი დოკუმენტებისთვის, ხელმოწერის ინფორმაცია გამოჩნდება **ინფორმაციის** განყოფილებაში, რომელსაც ხედავთ მას შემდეგ, რაც დააწკაპუნებთ **ფაილი** ჩანართზე.

დაამატეთ უხილავი ციფრული ხელმოწერები Word, Excel ან PowerPoint-ში

დოკუმენტის შინაარსის ავთენტურობის დასაცავად, შეგიძლიათ დაამატოთ უხილავი ციფრული ხელმოწერა. ხელმოწერილ დოკუმენტებს აქვს ღილაკი **ხელმოწერები** დოკუმენტის ბოლოში.

1. **ფაილის** ჩანართზე აირჩიეთ **ინფორმაცია** .
2. აირჩიეთ **დოკუმენტის დაცვა** , **სამუშაო წიგნის დაცვა** ან **პრეზენტაციის დაცვა**.
3. **აირჩიეთ ციფრული ხელმოწერის დამატება**.
4. წაიკითხეთ Word, Excel ან PowerPoint შეტყობინება და შემდეგ აირჩიეთ **OK**.
5. **ხელმოწერის დიალოგურ** ფანჯარაში ჩაწერეთ მიზანი **ამ დოკუმენტის ხელმოწერის** ველში.
6. აირჩიეთ **ხელმოწერა**.

ფაილის ციფრული ხელმოწერის შემდეგ, გამოჩნდება **Signatures** ღილაკი და ფაილი ხდება მხოლოდ წაკითხვადი, რათა თავიდან აიცილოს ცვლილებები.

წაშალეთ უხილავი ციფრული ხელმოწერები Word, Excel ან PowerPoint-დან

1. გახსენით დოკუმენტი, სამუშაო ფურცელი ან პრეზენტაცია, რომელიც შეიცავს უხილავ ხელმოწერას, რომლის წაშლა გსურთ.
2. **ფაილის** ჩანართზე აირჩიეთ **ინფორმაცია**.
3. აირჩიეთ  **ხელმოწერების ნახვა**.
4. დოკუმენტი, სამუშაო ფურცელი ან პრეზენტაციის ხედი ბრუნდება და გამოჩნდება **ხელმოწერების** პანელი.
5. ხელმოწერის სახელის გვერდით აირჩიეთ **ისარი**.
6. აირჩიეთ **Remove Signature** და შემდეგ აირჩიეთ **დიახ**.

ქსელის მდგრადობის უზრუნველყოფა

ქსელის საიმედოობის უზრუნველყოფა გადამწყვეტია ქსელის თანმიმდევრული და საიმედო სერვისების შესანარჩუნებლად., განსაკუთრებით დღევანდელ ურთიერთდაკავშირებულ სამყაროში, სადაც შეფერხებები შეიძლება მოხდეს სხვადასხვა წყაროსგან, როგორიცაა ბუნებრივი კატასტროფები, კიბერშეტევები ან აღჭურვილობის გაუმართაობა. აქ არის მაგალითი იმისა, თუ როგორ შეიძლება ორგანიზაციამ უზრუნველყოს ქსელის მდგრადობა:

- ✓ დუბლირებული ინფრასტრუქტურა: მათ შეუძლიათ დანერგონ დუბლირებული აპარატურა და ქსელის კომპონენტები, როგორიცაა სერვერი, სვიჩი და მარშრუტიზატორი. ეს სიჭარბე უზრუნველყოფს, რომ თუ ერთი კომპონენტი ვერ ახერხებს ფუნქციონირებას, არსებობს სარეზერვო სისტემები ქსელის ფუნქციონირების შესანარჩუნებლად.
- ✓ მრავალფეროვანი ქსელის კავშირები: მრავალფეროვანი ქსელის კავშირების დადგენა ხელს უწყობს ერთი წერტილის მარცხის რისკის შემცირებას. ეს შეიძლება მოიცავდეს სხვადასხვა ინტერნეტ სერვისის პროვაიდერების (ISP) გამოყენებას ან მრავალი საკომუნიკაციო მედიის გამოყენებას, როგორიცაა ბოჭკოვანი ოპტიკა, უკაბელო კავშირები და სატელიტური ბმულები.
- ✓ Load Balancing: დატვირთვის დაბალანსების განხორციელება ანაწილებს ქსელის ტრაფიკს მრავალ სერვერზე ან ქსელის ბმულზე. გაზრდილი ტრაფიკის ან ერთი სერვერის/ბმულის წარუმატებლობის შემთხვევაში, დატვირთვა შეიძლება სხვაზე გადაიტანოს, რაც თავიდან აიცილებს ქსელის გადატვირთულობას და შეფერხებას.
- ✓ რეგულარული სარეზერვო ასლები: კრიტიკული მონაცემების რეგულარული სარეზერვო ასლების შენახვა უზრუნველყოფს, რომ ქსელის უკმარისობის ან კიბერშეტევის შემთხვევაშიც კი შესაძლებელი იქნება არსებითი ინფორმაციის სწრაფად აღდგენა, რაც ამცირებს ოპერაციების შეფერხებას.
- ✓ ქსელის მონიტორინგი: ქსელის მონიტორინგის ხელსაწყოების გამოყენება საშუალებას იძლევა რეალურ დროში გამოავლინოს

ანომალიები ან პოტენციური პრობლემები ქსელში. ეს პროაქტიული მიდგომა საშუალებას აძლევს ადმინისტრატორებს ამოიცნონ და მოაგვარონ პრობლემები, სანამ ისინი უფრო დიდ საკითხებში გადაიქცევიან.

- ✓ უსაფრთხოების ზომები: უსაფრთხოების მძლავრი ზომების განხორციელება, როგორიცაა firewalls, შეჭრის აღმოჩენის სისტემები (IDS) და დაშიფვრის პროტოკოლები, ეხმარება ქსელის დაცვას კიბერ საფრთხეებისგან და არაავტორიზებული წვდომისგან, რაც აძლიერებს მთლიან მდგრადობას.
- ✓ რეგულარული ტესტირება და მოვლა: ქსელის ინფრასტრუქტურის რეგულარული ტესტირება და ტექნიკური სამუშაოების ჩატარება უზრუნველყოფს სისტემების ოპტიმალურად ფუნქციონირებას და მზადყოფნას გაუმკლავდეს მოულოდნელ მოვლენებს. ეს მოიცავს პროგრამული უზრუნველყოფის განახლებებს, ტექნიკის შემოწმებას და კატასტროფის სიმულირებულ სცენარებს.

ასვე ქსელის საიმედო სერვისების შესანარჩუნებლად ორგანიზაციამ უნდა უზრუნველყოს:

- ✓ მაღალი ხარისხის აღჭურვილობა: მაღალი ხარისხის ქსელის აღჭურვილობის გამოყენება სანდო მომწოდებლებისგან უზრუნველყოფს საიმედოობას. ეს მოიცავს მარშრუტიზატორებს, სვიჩებს/კომუტატორებს, სერვერებს და კაბელებს, რომლებიც აკმაყოფილებენ ინდუსტრიის სტანდარტებს და აქვთ საიმედოობის დადასტურებული გამოცდილება.
- ✓ დუბლირებული კვების წყაროები: კრიტიკული ქსელის აღჭურვილობისთვის დუბლირებული კვების წყაროების გამოყენება ხელს უწყობს შეფერხებების თავიდან აცილებას ელექტროენერგიის გათიშვის ან რყევების გამო. უწყვეტი დენის წყაროს (UPS) სისტემებს ასევე შეუძლიათ უზრუნველყონ დროებითი ელექტროენერგია გათიშვის დროს, რაც საჭიროების შემთხვევაში მოხდენილი გამორთვის საშუალებას იძლევა.
- ✓ რეგულარული მოვლა და განახლებები: ქსელის ინფრასტრუქტურის რეგულარული მოვლისა და განახლების

გრაფიკის დანერგვა აუცილებელია პოტენციური პრობლემების იდენტიფიცირებისთვის და მოსაგვარებლად, სანამ ისინი შეფერხებებს გამოიწვევს. ეს მოიცავს firmware განახლებებს, ტექნიკის ინსპექტირებას და შესრულების ოპტიმიზაციას.

- ✓ სერვისის ხარისხის (QoS) პოლიტიკა: QoS პოლიტიკის დანერგვა ხელს უწყობს ქსელის ტრაფიკის პრიორიტეტიზაციას კონკრეტული კრიტერიუმების საფუძველზე, როგორიცაა განაცხადის ტიპი, მომხმარებლის ან მომსახურების დონის შეთანხმებები (SLA). ეს უზრუნველყოფს, რომ კრიტიკულმა აპლიკაციებმა მიიღონ საკმარისი გამტარობა და რესურსები, შეინარჩუნონ საიმედოობა მაღალი მოთხოვნის პერიოდშიც კი.
- ✓ შეცდომის მიმართ მედეგობა და სიჭარბე: შეცდომის მიმართ მედეგი ქსელის არქიტექტურისა და ჭარბი(ერთზე მეტი) კომპონენტების დანერგვა ხელს უწყობს ტექნიკის გაუმართაობის ან ქსელის შეფერხების ზემოქმედების შემცირებას. უწყვეტი მუშაობის უზრუნველსაყოფად შეიძლება გამოყენებულ იქნას ტექნოლოგიები, როგორიცაა Spanning Tree Protocol (STP), ბმულის აგრეგაცია (LACP) და ზედმეტი მარშრუტიზაციის პროტოკოლები (მაგ., OSPF, BGP).
- ✓ კატასტროფის შემთხვევაში აღდგენის მეთოდების დაგეგმვა: კატასტროფისას აღდგენის ყოვლისმომცველი გეგმის შემუშავება ასახავს პროცედურებსა და პროტოკოლებს, რომლებიც უნდა დაიცვათ ქსელის გათიშვის ან კატასტროფის შემთხვევაში. ეს მოიცავს სარეზერვო და აღდგენის პროცედურებს, უკმარისობის მექანიზმებს და კომუნიკაციის გეგმებს, რათა მინიმუმამდე დაიყვანოს შეფერხება და მონაცემთა დაკარგვა.

ამ სტრატეგიების განხორციელებით, ორგანიზაციებს შეუძლიათ უზრუნველყონ თავიანთი ქსელის ინფრასტრუქტურის საიმედოობა, უზრუნველყონ მომხმარებლებისთვის თანმიმდევრული და საიმედო სერვისები, მინიმუმამდე დაიყვანონ შეფერხების რისკი და უზრუნველყონ უწყვეტი ფუნქციონირება გაუთვალისწინებელი გამოწვევების შემთხვევაშიც კი.

დამცავი ეკრანები

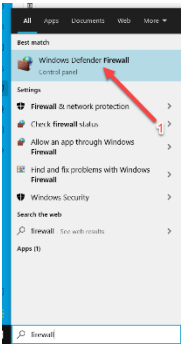
Windows Firewall არის უსაფრთხოების ფუნქცია, რომელიც დაგეხმარებათ დაიცვათ თქვენი მოწყობილობა ქსელის ტრაფიკის გაფილტვრით, რომელიც შედის და გამოდის თქვენს მოწყობილობაში. ამ ტრაფიკის გაფილტვრა შესაძლებელია რამდენიმე კრიტერიუმის საფუძველზე, მათ შორის წყაროსა და დანიშნულების IP მისამართის, IP პროტოკოლის ან წყაროსა და დანიშნულების პორტის ნომრის ჩათვლით. Windows Firewall-ის კონფიგურაცია შესაძლებელია დაბლოკოს ან დაუშვას ქსელის ტრაფიკი თქვენს მოწყობილობაზე დაინსტალირებული სერვისებისა და აპლიკაციების საფუძველზე. ეს საშუალებას გაძლევთ შეზღუდოთ ქსელის ტრაფიკი მხოლოდ იმ აპლიკაციებსა და სერვისებზე, რომლებსაც ცალსახად აქვთ ნებადართული კომუნიკაცია ქსელში.

Windows Firewall არის ჰოსტზე დაფუძნებული firewall, რომელიც შედის ოპერაციულ სისტემაში და ჩართულია ნაგულისხმევად Windows-ის ყველა გამოცემაში. Windows Firewall შედის ოპერაციულ სისტემაში, ამიტომ არ არის საჭირო დამატებითი აპარატურა ან პროგრამული უზრუნველყოფა.

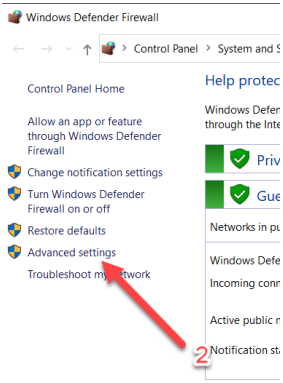
Firewall-ის წესები განსაზღვრავს დაშვებული ან დაბლოკილი იქნას ქსელის ტრაფიკი. წესები გთავაზობთ პირობების ფართო არჩევანს ტრაფიკის იდენტიფიცირებისთვის.

აქ მოცემულია მაგალითი, თუ როგორ უნდა გახსნათ პორტები Windows 10/11 Firewall-ში:

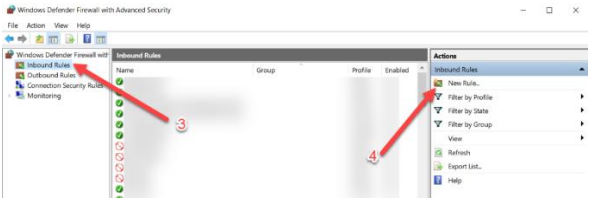
1. გახსენით **Windows Defender Firewall** თქვენს კომპიუტერში.



2. დააწკაპუნეთ **Advanced settings** .

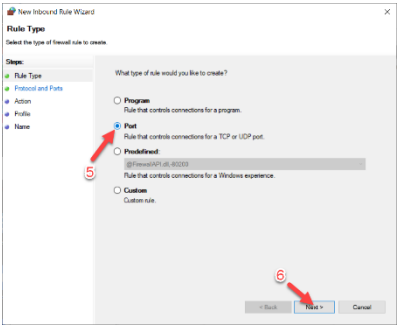


3. გადადით **Inbound Rules- ზე ახალი წესის** შესაქმნელად.



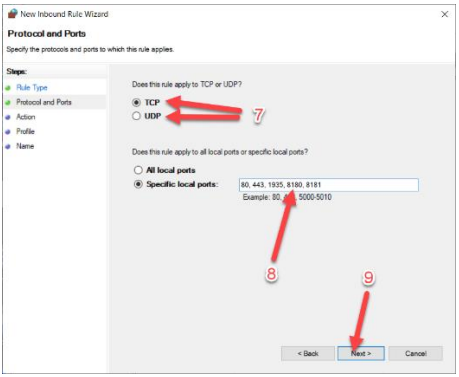
5. აირჩიეთ **პორტი**

6. დააწკაპუნეთ **შემდეგი.**



7. აირჩიეთ **TCP** ან **UDP** . Warrior Trading-ის სერვისებისთვის , ეს პარამეტრები უნდა იქნას გამოყენებული როგორც TCP , ასევე UDP-ზე.

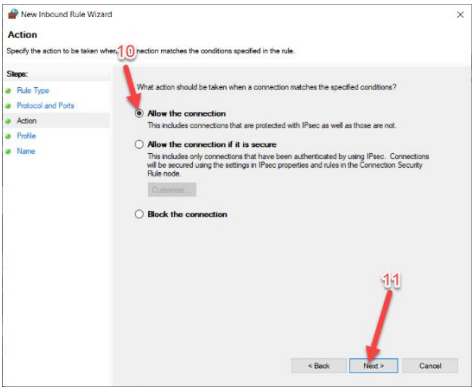
(აირჩიეთ ერთი ამჯერად და შემდეგ დაუბრუნდით ამ საფეხურს და აირჩიეთ მეორე).



8. შეიყვანეთ **კონკრეტული ადგილობრივი პორტები** ამ პარამეტრების გამოსაყენებლად. მაგ შეიყვანეთ ეს პორტები: **80, 443, 1935, 8180, 818**

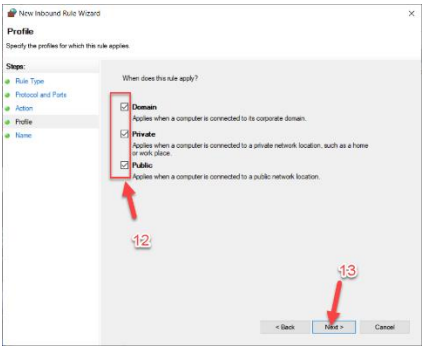
9. დააწკაპუნეთ შემდეგი.

10. დააწკაპუნეთ **კავშირის დასაშვებად**



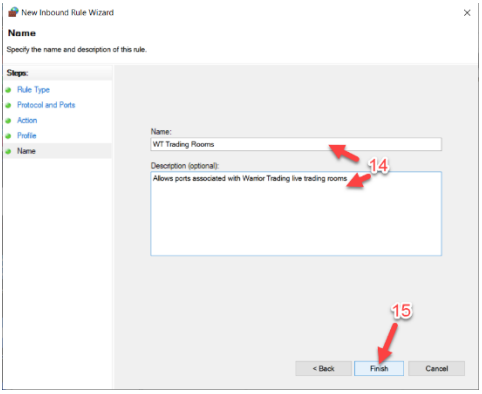
11. დააწკაპუნეთ **შემდეგი**.

12. გამოიყენეთ წესი ყველა ვარიანტზე ველის მონიშვნით: **Domain, Private Public**



13. დააწკაპუნეთ **შემდეგი**.

14. შეიყვანეთ თქვენი არჩევანის **სახელი** და **აღწერა** , რათა დაგეხმაროთ თქვენ მიერ შექმნილი წესის იდენტიფიცირებაში.



15. დააწკაპუნეთ **Finish-ზე**.

16. Warrior Trading-ის ცოცხალი სავაჭრო ოთახებისთვის, ახლა მოგინდებათ დაბრუნდეთ და გაიმეოროთ ნაბიჯები, აირჩიოთ სხვა ვარიანტი TCP/UDP-სთვის (ნაბიჯი 7), რომელიც პირველად არ აირჩიეთ.

საგამომცემლობა „სამშობლო“.

ტირაჟი 200 ეგზ.