ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი

ირაკლი თვალიაშვილი

ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვის საჭიროება და მოთხოვნები

სამაგისტრო პროგრამა - ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: ზურაბ ქოჩლაძე

თბილისი

2019

აბსტრაქტი

ნაშრომის მიზანია ორგანიზაციები დაარწმუნოს თუ რა მნიშვნელობის მატარებელია მათ ხელში არსებული ინფორმაციული აქტივები და რატომაა მათი დაცვა აუცილებელი. ნაშრომში განხილულია ინფორმაციული უსაფრთხოების მართვის სისტემის სტანდარტის მნიშვნელოვანი ასპექტები, რომლებიც განაპირობებენ ორგანიზაციაში არსებული ინფორმაციისა და მასთან დაკავშირებული პროცესებისა და ინდივიდების მთლიანობას, კონფიდენციალურობასა და ხელმისაწვდომობას.

ნაშრომი არ წამოადგენს სახელმძღვანელოს, მისი მიზანია ორგანიზაციების დარწმუნება ინფორმაციული უსაფრთხოების აუცილებლობაში და მისი განხორციელების შესაძლებლობაში.

ABSTRACT

The paper aims to assist organizations in understanding the vital importance of properly ensuring the safety of their information assets. The paper also reviews various important aspects of the information security management system and its general standards, which highly impact the integrity, confidentiality and availability of existing information and related processes or individuals within these organizations.

The paper is not presented as a manual or textbook, but rather serves as an instrument, with which organizations can reassure themselves about the significance and necessity of proper informational safety and the possibilities for practical implementation of said safety protocols.

სარჩევი

შესავალი

ორგანიზაციები იღებენ სტრატეგიულ გადაწყვეტილებებს, განკარგავენ რესურსებს და ინახავენ მომხმარებლებისა და თანამშრომლების პერსოალურ ინფორმაციას. შესაბამისად მათთვის მნიშვნელოვანია არსებული ინფორმაციული აქტივები იყოს მთლიანი, კონფიდენციალური და ხელმისაწვდომი, რასაც ინფორმაციული უსაფრთხოება უზრუნველყოფს. ინფორმაციული უსაფრთხოება არ არის ერთჯერადი პროცედურა, რომელიც წყვეტს ყველა პრობლემას. საჭიროა, რომ იყოს უწყვეტი და მუდმივად განვითარებადი პროცესი. ორგანიზაციაში საჭიროა დაინერგოს გარკვეული სისტემა, რომელიც უზრუნველყოფს ინფორმაციისა და მასთან დაკავშირებული რისკების მართვას. კონკრეტულად ამ მიზნით შეიქმნა საერთაშორისო სტანდარტების ორგანიზაციის მიერ სტანდარტი ISO27001. სტნდარტი არის ინფორმაციული უსაფრთხოების სტრუქტურირებული, თანმიმდევრული მართვის გადაწყვეტილება. ის შემუშავებულია, რათა ეფექტურად იურთიერთქმედოს უსაფრთხოების პოლიტიკის განხორციელების სამ ძირითად ასპექტთან: პროცესები (ან პროცედურები); ტექნოლოგიები; მომხმარებლების ქცევა; ნაშრომში განხილულია სტანდარტის ძირითადი და მნიშვნელოვანი ასპექტები, როგორებიცაა ინფორმაციული უსაფრთხოების მართვის სისტემის შინაარსი, განხოციელების PDCA მოდელი, მენეჯმენტისა და დოკუმენტაციის როლი მართვის სისტემაში, რა არის რისკი და როგორ შევარჩიოთ რისკის შესაბამისი კონტროლის მექანიზმები. ასევე როგორ შევინარჩუნოთ და განვავითაროთ ინფორმაციული უსაფრთხოება ორგანიზაციაში.

ნაშრომის მიზანია ორგანიზაციებს განუმარტოს თუ რა არის ინფორმაცია და რა მნიშვნელობის მატრებელია ის. ასევე დაანახოს ის რეალური რისკები, რაც ინფორმაციას ახლავს. დაანახოს ინფორმაციის უსაფრთხოების აუცილებლობა და მისი განხორციელების გზები.

ინფორმაციული უსაფრთხოება

ინფორმაცია

რა არის ინფორმაცია?

მონაცემები არის არაორგანიზებული ფაქტების მიმდევრობა, რომელიც საჭიროებს დამუშავებას. ის შეიძლება იყოს მარტივი და უსარგებლო სანამ დამუშავდება. დამუშავების ან მისი წარმოდგენის შემდგომ, როდესაც მას მიენიჭება გარკვეული კონტექსტი, მას ეწოდება **ინფორმაცია**. ანუ ინფორმაცია არის მონაცემთა ერთობლიობა, რომელთაც მინიჭებული აქვთ გარკვეული მნიშვნელობები და ქმნიან წარმოდგენას ამა თუ იმ საკითხზე. ინფორმაცია შესაძლოა არსებობდეს მრავალი ფორმით. იგი შეიძლება იყოს ქაღალდზე, ელექტრონული ფოსტის მეშვეობით ან სხვა საშუალებით გადაცემული, ფილმებში ნაჩვენები, საუბრისას ნათქვამი და ა.შ.

ინფორმაციის მნიშვნელობა

ინფორმაცია თამაშობს მთავარ როლს ორგანიზაციაში, რადგან ის წარმართავს ყველა ორგანიზაციულ გადაწყვეტილებებს. ანუ ინფორმაციაზე დაყრდნობით ხდება გადაწყვეტილების მიღება, ხოლო არასწორი ინფორმაცია იწვევს ორგანიზაციულ შეცდომებს.

ორგანიზაციას სჭირდება ინფორმაცია საკუთარ ძლიერ და სუსტ მხარეებზე, შესაძლებლობებზე და საფრთხეებზე რათა მიიღოს სტრატეგიული გადაწყვეტილებები. მას ასევე სჭირდება ინფორმაცია მომხმარებლებსა თუ თანამშრომლებზე რათა დაგეგმოს და წარმართოს საკუთარი რესურსები ეფექტურად.

ჭეშმარიტება იქნება თუ ვიტყვით რომ ინფორმაცია წარმოადგენს ვალუტას თანამედროვე სამყაროში. ხშირ შემთხვევაში ის წარმოადგენს ყველაზე ფასეულ აქტივს ორგანიზაციებში მიუხედავად იმისა მოიაზრება თუ არა მის ფორმალურ და საერთო ფინანსურ ღირებულებაში.

დაინტერესებული მხარეები და მათი მიზნები / ინციდენტები და მათი გავლენები

ვინაიდან და რადგანაც ინფორმაცია წარმოადგენს ფასეულ აქტივს, ბუნებრივია არსებობს დაინტერესებული მხარე, რომელიც გააზრებულად თუ გაუაზრებლად ცდილობს მის ხელში ჩაგდებას, დაზიანებას, განადგურებას და ა.შ. აქედან გამომდინარე მნიშვნელოვანია იცოდე ვინ ან რა შეილება იყოს ინფორმაციასთან დაკავშირებული საფრთხის უკან და რა მიზანს ემსახურებიან ისინი. დღეს მათი კლასიფიკაცია საკმაოდ რთულია თუმცა უმეტესობა შეგვიძლია მივაკუთვნოთ შემდეგ კატეგორიებს:

მთავრობის მიერ დაფინანსებული: ეს ჯგუფები საკმაოდ კარგად დაფინანსებულები არიან და ხშირად მიმართავენ კომპლექსურ და მიზანმიმართულ დარტყმებს. ისინი არიან პოლიტიკურად, ეკონომიკურად, ტექნიკურად ან მილიტარისტულად მოტივირებულები და ხშირად ეძებენ კონკურენტუნარიან ინფორმაციას, წყაროებს ან მოწყვლად მომხმარებლებს ჯაშუშური მიზნებისთვის.

ამ კატეგორიას მიეკუთვნება მაშტაბურად ცნობილი ვირუსი Stuxnet რომლის აღმოჩენაც სერგეი ულასენის სახელს უკავშირდება. 2010 წელს აღმოჩენილი ვირუსი რომლის გავრცელებაც ხდებოდა Windows ოპერაციულ სისტემებში გასავრცელებლად იყენებდა როგორც ინფორმაციის გარე მატარებლებს (USB flash) ასევე ქსელურ ინფრასტრუქტურას. მისი გაანალიზების შემდეგ აღმოჩნდა რომ ის ეკუთვნოდა ამერიკისა და ისრაელის კიბერ ქვედანაყოფების ერთობლივ ნაშრომს. ვირუსის კოდის ანალიზისას აღმოჩნდა, რომ მისი სამიზნე მხოლოდ პროგრამირებადი ლოგიკური კონტროლერი(PLC) იყო, რომელსაც ირანის ქალაქ ნატანზში არსებული ატომური სადგური ცენტრიფუგების კონტროლისთვის იყენებდა. მიუხედავად იმისა, რომ ატომურ სადგურს ინტერნეტთან კავშირი ფიზიკურად არ ქონდა, ვირუსმა მასში შეღწევა მაინც მოახერხა USB flash drive-ის გამოყენებით და 5000 ცენტრიფუგიდან 1000-ის მწყობრიდან გამოყვანა მოახერხა რამაც საგრძნობლად შეაფერხა ირანის ბირთვული პროგრამა. [1]

ორგანიზებული დანაშაული: ყველაზე ხშირად, ეს კიბერდამნაშავეები ახდენენ თავდასხმას ფინანსური ინტერესის მოტივით. მათი მიზანია პერსონალური მონაცემების, როგორიცაა პირადი ნომერი, სამედიცინო ისტორიები, საკრედიტო ბარათები და საბანკო ინფორმაცია, მოპოვება და მათი შავ ბაზარზე გაყიდვა.

ამ კატეგორიას მიეკუთვნება კიბერკრიმინალური ჯგუფი FIN7. მათ 2015 წლიდან დღემდე 16 მილიონზე მეტი საბანკო ბარათის მონაცემების მოპოვება შეძლეს, რომელთა უმეტესობაც შავ ბაზარზე იყიდება. მათი მთავარ სამიზნეს სწრაფი კვების ობიექტები, რესტორნები, სასტუმროები, კაზინოები და სხვა ბიზნესები წარმოადგენენ, სადაც მიმდინარეობს ხშირი საგადახდო ოპერაციები. ისინი იყენებენ როგორც სოციალურ ინჟინერიას ასევე საკუთარ შექმნილ პროგრამულ უზრუნველყოფებს, ინფორმაციის მოსაპოვებლად. [2]

ჰაკტივისტები(Hacktivists): ამ კატეგორიას აქვს პოლიტიკური ან პირადი მოტივები. მათი მიზანია განახორციელონ თავდასხმები, რომლებიც დაეხმარება პროპაგანდის გავრცელებაში ან ორგანიზაციებისთვის ზიანის მიყენებაში რომლის წინააღმდეგაც იბრძვიან.

2010 წელს სკანდალური ვებ გვერდი ვიკილიქსი ყურადღების ქვეშ კიდევ ერთხელ მოხვდა ამერიკის შეერთებული შტატების საიდუმლო დიპლომატიური ტელეგრამების გასაჯაროებისთვის. აღნიშნულთან დაკავშირებით ცნობილმა კომპანიებმა, როგორებიცაა Amazon, PayPal, BankAmerica, Swiss bank PostFinance, MasterCard და Visa, თანამშრომლობა შეწყვიტეს ვიკილიქსთან და გაუყინეს საბანკო ანგარიშები. დეცენტრალიზებულმა ჰაკტივისტურმა დაჯგუფებამ ანონიმუსმა(Anonymous), რომელიც ცნობილი გახდა ორგანიზაცია Church of Scientology-ს წინააღმდეგ კიბერ აქტივიზმით, ბრძოლა გამოუცხადა აღნიშნულ კომპანიებს ვიკილიკსის მხარდასაჭერად. 2010 წლის 8 და 9 დეკემბერს მათ განახორციელეს ეგრედწოდებული DDoS (Distributed Denial of Service) დარტყმები კომპანიის ვებ გვერდებზე. 10 დეკემბერს კი გაზეთმა The daily Telegraph-მა გაავრცელა აქტივისტების მიმართვა, სადაც ისინი იმუქრებოდნენ ბრიტანეთის სამთავრობო ვებ გვერდების დაზიანებით თუ ვიკილიქსის დამფუძნებელი ჟულიან ასანჟი ექსტრადირებული იქნებოდა შვედეთში. [3]

შიდაორგანიზაციული საფრთხე: ხშირად შურისძიების ან ფინანსური ინტერესის მოტივით აქტიური ან ყოფილი თანამშრომლები ოპერირებენ ორგანიზაციის შიგნით ამავე ორგანიზაციის წინააღმდეგ. ზოგჯერ ისინი თანამშრომლობენ ორგანიზებულ დამნაშავეებთან ან მთავრობის მიერ დაფინანსებულ ჯგუფებთან.

2015 წელს Canadian Pacific Railway(CPR)-ის სისტემური ადმინისტრატორის სამსახურიდან განთავისუფლების შემდეგ, განთავისუფლებულმა თანამშრომელმა მოლაპარაკებით მიაღწია, რომ მას თავად დაეწერა განცხადება წასვლის შესახებ. სამუშაო კომპიუტერთან წვდომის შემდეგ, მან კომპანიის ქსელურ ინფრასტრუქტურაში შეაღწია, წაშალა მნიშვნელოვანი ფაილები და სისტემების მართვისთვის განკუთვნილი მომხმარებლები. კვალის დასაფარად მან გაანადგურა მყარი დისკი და დატოვა პოსტი. როდესაც ინფორმაციული ტექნოლოგიების ინფრასტრუქტურას პრობლემები შეექმნა და მასთან კავშირს ვერავინ ახერხებდა, კომპანიამ დაიქირავა კომპანია პრობლემების გამოსასწორებლად. სისტემური ლოგების გაანალიზების შემდგომ დადასტურდა გათავისუფლებული თანამშრომლის ბრალეულობა და 1 წლით პატიმრობა მიესაჯა. [4]

ოპორტუნისტული მიდგომა: ძირითადად ამ კატეგორიას განეკუთვნებიან მოყვარული დამნაშავეები. მათი მიზანია სისტემებში სისუსტეების აღმოჩენა და მათში შეღწევა რათა მოიხვეჭონ სახელი. ზოგჯერ მათ აღმოჩენებს ორგანიზაციები იყენებენ სისტემების უსაფრთხოების გასაუმჯობესებლად.

16 წლის ჯონათან ჯეიმსი, ასევე ცნობილი როგორც “C0mrade”, 2000 წელს ამერიკის შეერთებული შტატების პოლიციამ დააკავა. მას ბრალად ედებოდა 1999 წელს კერძო კომპანიების, სკოლის სისტემების, თავდაცვის დეპარტამენტისა და ნასას (NASA) სისტემებში შეღწევა. როგორც გაირკვა, მან ნასას სერვერებიდან შეძლო კოსმოსური ხომალდის ტემპერატურისა და სხვა ფიზიკური მოწყობილობების სამართავი პროგრამის კოდის მოპარვა. მას 6 თვით შიდაპატიმრობა მიუსაჯეს. როგორც ჯონათანმა მოგვიანებით განაცხადა ეს მისთვის პატივი იყო. [5]

ინფორმაციული უსაფრთხოების აუცილებლობა

ზოგადად, ინფორმაციული უსაფრთხოება შეგვიძლია განვმარტოთ, როგორც ორგანიზაციის ან ინდივიდის კუთვნილი ინფორმაციის დაცვა. ინფორმაციის დაცვა ნიშნავს მასთან დაკავშირებული რისკების მართვას. რისკები კი ყოველდღიურად მატულობს. მითები იმის შესახებ რომ კიბერ ინციდენტები მხოლოდ დიდ კორპორაციებში ხდება არ შეესაბამება რეალობას. მაგალითად ავიღოთ 2017 წლის ცნობილი ვირუსი WannaCry რომლის სამიზნეც Windows ოპერაციული სისტემა წარმოადგენდა. როგორც Symantec იუწყება, მან 230 000-ზე მეტი კომპიუტერი დააზიანა 150 ქვეყანაში და დაახლოებით 4 მილიარდი დოლარის ექვივალენტის ზარალი მიაყენა ორგანიზაციებსა თუ ინდივიდებს. აქედან გამომდინარე თუ ორგანიზაციის მიზანია რომ უზრუნველყოს ორგანიზაციაში არსებული საინფორმაციო ტექნოლოგიების უსაფრთხოდ ფუნქციონირება, დაიცვას მათ მიერ შეგროვებული და გამოყენებული მონაცემები, ისევე როგორც ტექნოლოგიური აქტივები და ხელი შეუწყოს უწყვეტ ფუნქციონირებას, აუცილებელია იზრუნოს ინფორმაციულ უსაფრთხოებაზე.

ინფორმაციული უსაფრთხოების მართვის სისტემა

იუმს და ISO27001

ინფორმაციული უსაფრთხოების განმარტება

ISO27000 განმარტავს ინფორმაციულ უსაფრთხოებას, როგორც „კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დაცვას; ამას გარდა შესაძლოა სხვა ცნებების დამატება, როგორებიცაა ავთენტურობა, ანგარიშვალდებულება, ვერ უარყოფა და სანდოობა.“ [6]

ინფორმაციულმა რისკმა შეიძლება გავლენა იქონიოს ერთ ან მეტ ინფორმაციული აქტივის ფუნდამენტურ ატრიბუტზე შემდეგი სამიდან:

- ხელმისაწვდომობა
- კონფიდენციალურობა
- მთლიანობა

ეს ატრიბუტები ISO27000-ში განმარტებულია შემდეგნაირად:

- **ხელმისაწვდომობა:** „ავტორიზებული სუბიექტის მიერ მოთხოვნის შესაბამისად ხელმისაწვდომობისა და გამოყენებადობის მახასიათებელი“, რაც გულისხმობს, რომ ინფორმაცია ხელმისაწვდომი უნდა იყოს როგორც ადამიანებისთვის ასევე კომპიუტერული პროგრამისთვის.
- **კონფიდენციალურობა:** „მახასიათებელი იმისა რომ ინფორმაცია არ არის ხელმისაწვდომი არაავტორიზირებული ინდივიდების, სუბიექტების ან პროცესებისათვის“.
- **მთლიანობა:** „მახასიათებელი იმისა რომ დაცულია ინფორმაციული აქტივის სიზუსტე და სრულყოფილება“ [7]

ინფორმაციული უსაფრთხოების მართვის სისტემა (იუმს)

ინფორმაციული უსაფრთხოების მართვის სისტემა, რომელიც სტანდარტის მიხედვით შეიცავს „ორგანიზაციულ სტრუქტურას, პოლიტიკებს, დაგეგმარებით ქმედებებს, პასუხისმგებლობებს, პრაქტიკებს, პროცედურებს, პროცესებსა და რესურსებს“[1], არის ინფორმაციული უსაფრთხოების სტრუქტურირებული, თანამიმდევრული მართვის გადაწყვეტილება. ის შემუშავებულია რათა ეფექტურად იურთიერთქმედოს უსაფრთხოების პოლიტიკის განხორციელების სამ ძირითად ასპექტთან:

- პროცესები(ან პროცედურები)
- ტექნოლოგიები
- მომხმარებლების ქცევა

[1] ISO/IEC 27000:2012, terms and definitions, 2.34, note

სტანდარტის მოთხოვნაა რომ პოლიტიკის სტრუქტურა და განხორციელება პასუხობდეს ორგანიზაციის „მოთხოვნებს და მიზნებს, უსაფრთხოების საჭიროებებს, ორგანიზაციის პროცესებს, მის სტრუქტურასა და ზომას“ [1].

ISO27001 არ არის ერთი ზომის ორგანიზაციებზე მორგებული, რომელიც არ ითვალისწინებს მის განვითარებასა და გაზრდას. ის მკაფიოდ განმარტავს რომ :

- ინფორმაციული უსაფრთხოების მართვის სისტემა „შემცირდება ორგანიზაციული საჭიროებებიდან გამომდინარე
- მზადაა ხშირი ცვლილებებისთვის

სტანდარტის სრული სახელია „ISO/IEC 27001 ინფორმაციული ტექნოლოგიები - უსაფრთხოების ტექნიკები - ინფორმაციული უსაფრთხოების მართვის სისტემა - საჭიროებები”.

სტანდარტის სრული ვერსია 30 გვერდია. მისი ძირითადი ნაწილის მოცულობა 9 გვერდია, სადაც ჩამოყალიბებულია ინფორმაციული უსაფრთხოების მართვის სისტემის დიზაინი, სპეციფიკაციები და მართვა. 13 გვერდზე კი მოცემულია „დანართი ა“. ის შეიცავს 114 ინდივიდუალურ კონტროლს, რომლის გათვალისწინებაც სტანდარტის მიხედვით აუცილებელია. ინფორმაციული უსაფრთხოების მართვის სისტემის სპეციფიკაციები განსაზღვრულია მეოთხედან მეათე თავის ჩათვლით.

დოკუმენტაცია და ჩანაწერები

საგანგებო (ad hoc) ორგანიზაციები წარმოადგენენ ისეთ ორგანიზაციებს, რომლებსაც არ აქვთ განსაზღვრული პროცესები ან პროცედურები, შედეგი დამოკიდებულია ინდივიდუალურ შესრულებაზე, და ძირითადად რესურსები ხმარდება ინციდენტების აღმოფხვრასა და იმ დროისთვის არსებული პრობლემის გადაჭრას. მართვის სისტემის ერთ-ერთი ძირითადი მიზანი წარმოადგენს ამ პრაქტიკიდან გამოსვლას.

[1] ISO/IEC 27001:2013, Introduction General, 0.1

დოკუმენტაციის მართვის მოთხოვნები

ISO27001 მოითხოვს მართვის სისტემის დოკუმენტირებას. კონტროლი A.12.1.1-ის მოთხოვნაა, რომ უსაფრთხოების პროცედურები უნდა იყოს დოკუმენტირებული, შენარჩუნებული და ხელმისაწვდომი. „დანართი ა“ ასევე განსაზღვრავს ისეთი დოკუმენტების აუცილებლობას როგორებიცაა:

- A.5.1.1:ინფორმაციული უსაფრთხოების პოლიტიკები;
- A.6.1.1:ადამიანური რესურსების დოკუმენტირებული როლები და პასუხისმგებლობები;
- A.8.1.3:აქტივების დასაშვები გამოყენება;
- A.9.1.1:წვდომის კონტროლის პოლიტიკა;
- A18.1.1:გათვალისწინებული დოკუმენტების იდენტიფიკაცია.

ბევრი სხვა კონტროლები საჭიროებენ „ფორმალურ“ პროცედურებს ან „გამჭვირვალე“ კომუნიკაციას; ტექნიკურად ეს დოკუმენტირების გარეშეც მიღწევადია, თუმცა მიზანშეწონილია ყველა პროცესისა და პროცედურის დოკუმენტირება.

იუმს-ის დოკუმენტაციის შინაარსი

დოკუმენტაცია უნდა იყოს სრული, პასუხობდეს სტანდარტის მოთხოვნებს და ერგებოდეს ორგანიზაციის საჭიროებებს. მართვის სისტემა უნდა იყოს სრულად დოკუმენტირებული. ISO27001 განმარტავს იმ მინიმუმ დოკუმენტაციებს, რომლებიც უნდა იყოს დანერგილი.

არ არის აუცილებელი, რომ ყველა ორგანიზაციას ჰქონდეს ერთი სირთულის დოკუმენტაციათა სტრუქტურა. სტანდარტი მიუთითებს რომ „დოკუმენტირებული ინფორმაციის მოცულობა შესაძლოა განსხვავდებოდეს ორგანიზაციებში მათი ზომისა საქმიანობის მიხედვით.“[1] [6]

[1] ISO/IEC 27001:2013, 7.5.1, General, note b

ISO 27001:2013-ში 2005 წლის ვერსიისგან განსხვავებით, სტანდარტი არ განასხვავებს ჩანაწერებს დოკუმენტაციისგან და წარმოადგენს ერთი და იგივე მოთხოვნების საგანს.

არსებობს სპეციფიური ჩანაწერები, რომლებიც ორგანიზაციამ უნდა შეინახოს გარკვეული ხნის განმავლობაში და ეს რეგულირდება გარკვეული საკანონმდებლო ან მარეგულირებელი აქტებით. ჩანაწერები, რომლებიც შეიცავენ ინფორმაციული უსაფრთხოების მართვის სისტემის წარმადობის მტკიცებულებას, განსხვავდებიან მართვის სისტემის მიერ დასაცავი ჩანაწერებისგან, და უნდა იყოს წაკითხვადი, იდენტიფიცირებადი და ამოღებადი. განსაკუთრებით ელექტრონული ჩანაწერების შემთხვევაში, ის უნდა იყოს ამოღებადი და წაკითხვადი სისტემური ან ფიზიკური ცვლილებების შემდგომაც.

დოკუმენტის კონტროლები დანართ „ა“-ში

დანართ „ა“-ში მოცემულია დოკუმენტთან დაკავშირებული კონტროლის მექანიზმები, რომლებიც მიზანშეწონილია გათვალისწინებული იქნას დოკუმენტაციის კონტროლისას მართვის სისტემაში. ესენია:

- A.8.2.1 ინფორმაციის კლასიფიკაცია; რაც გულისმობს ინფორმაციის კონფიდენციალურობის ხარისხის განსაზღვრას.
- A.8.2.2 ინფორმაციის მარკირება; რაც გულისხმობს იმ მიდგომებს და მეთოდებს, რომელიც გამოყენებულია ინფორმაციის ან ინფორმაციის მატარებლების მარკირებისთვის
- A.8.2.3 აქტივების მოპყრობა; რაც გულისხმობს აქტივების მოპყრობის პროცედურებს კლასიფიკაციის მიხედვით
- A.18.1.3 ჩანაწერების დაცვა; რაც გულისხმობს დოკუმენტაციის შენახვის წესებს
- A.18.1.4 პირის მაიდენტიფიცერებელი ინფორმაციის კონფიდენციალურობა და დაცვა;

მენეჯმენტი

როგორც ISO27001 გვამცნობს, ინფორმაციული უსაფრთხოების მართვის სისტემის განხორციელება გავლენას იქონიებს მთლიან ორგანიზაციაზე. სტანდარტი ნათლად განმარტავს, რომ საჭიროა გავრცელების სფეროსა და პოლიტიკის დოკუმენტირება, სადაც განმარტებული უნდა იყოს გავრცელების სფეროში არ შესული აქტივების გარეთ დარჩენის მიზეზები. მისი მოთხოვნა იუმს-ის სტრატეგიის შესახებ, რომელიც უნდა ითვალისწინებდეს ორგანიზაციის კონტექსტს, ჩამოყალიბებულია 4.4 პუნქტში, სადაც ის მიუთითებს რომ ორგანიზაციამ „უნდა დაადგინოს, განახორციელოს, შეინარჩუნოს და შეუჩერებლად განავითაროს ინფორმციიული უსაფრთხოების მართვის სისტემა“. ამ საკითხების შესრულება შეუძლებელია მენეჯმენტის გარეშე.

მენეჯმენტის პასუხისმგებლობა იმდენად მნიშვნელოვანია, რომ სტანდარტის მე-5 თავში საუბარია მხოლოდ მენეჯმენტის მიმართ მოთხოვნებზე. ამ თავში გვხვდება შემდეგი მოთხოვნები, რომლებიც უფრო დაწვრილებით ჩაშლილია მის ქვეთავებში, რომ მენეჯმენტმა უნდა „გამოთქვას მზაობა ინფორმაციული უსაფრთხოების მართვის სისტემის მართვაზე“, “მიიღოს ინფორმაციული უსაფრთხოების პოლიტიკა“ და „იზრუნოს რომ ინფორმაციული უსაფრთხოების პასუხისმგებლობები გადანაწილებულია რელევანტურად“.

“დანართ ა“-ში მოცემულია კონტროლის მექანიზმები, რომლებიც საჭიროებენ მენეჯმენტის ჩართულობას. ესენია:

- A.5.1.1 ინფორმაციული უსაფრთხოების პოლიტიკები
- A.6.1.2 მოვალეობების გადანაწილება
- A.9.2.5 მომხმარებლების წვდომის უფლებების გადახედვა

- A.18.2.2 ინფორმაციული უსაფრთხოების პოლიტიკებისა და სტანდარტების დაცვა

გარდა ამ კონტროლის მექანიზმებისა, სტანდარტი 9.3 თავში განმარტავს, რომ მენეჯმენტმა დროის განსაზღვრულ ინტერვალებში უნდა „მიმოიხილოს ორგანიზაციის ინფორმაციული უსაფრთხოების მართვის სისტემა, რათა დარწმუნდეს მის სტანდარტთან შესაბამისობაში, ადეკვატურობასა და ეფექტურობაში“. ამ თავში განსაზღვრულია, როგორც განხილვისთვის საჭირო ნაბიჯები, ასევე განხილვის შემგომ გაკეთებული დასკვნის მნიშვნელობა და აუცილებლობა მართვის სისტემის სწორად ფუნქციონირებისათვის.

PDCA მოდელი

PDCA მოდელი არის დაგეგმვა(Plan)-შესრულება(Do)-შემოწმება(Check)-რეაგირება(Act) ციკლი, რომელიც შემუშავდა 1950-იან წლებში ედვარდ დემინგის მიერ. ის მდგომარეობს შემდეგში, რომ ბიზნეს პროცესები უნდა გვაძლევდნენ ინფორმაციას მის ფუნქციონირებაზე, რათა მენეჯმენტმა შეძლოს იდენტიფიკაცია და შეცვლა პროცესის იმ საკითხებისა, რომლებსაც სჭირდებათ გაუმჯობესება. პროცესი ან პროცესის გაუმჯობესება პირველ რიგში უნდა დაიგეგმოს, შემდეგ უნდა დაინერგოს და შეფასდეს მისი წარმადობა, თუ რამდენად შეესაბამება დაგეგმილს. გამოვლენილი შეუსაბამობები უნდა იქნეს იდენტიფიცირებული და განისაზღვროს მასზე რეაგირების გზები.

ISO27001-ის 2005 წლის ვერსია ხაზგასმით აღნიშნავდა, რომ ინფორმაციული უსაფრთხოების მართვის სისტემის ფუნქციონირება საჭიროებდა PDCA ციკლს. 2013 წლის ვერსია კი მხოლოდ მიუთითებს მუდმივი გაუმჯობესების აუცილებლობაზე, ხოლო რა მეთოდით იქნება ეს მიღწეული სრულ თავისუფლებას აძლევს ორგანიზაციებს. მიუხედავად PDCA მეთოდის სტანდარტიდან ამოღებისა, ის კვლავ რჩება როგორც იუმს-ის განხორციელების ეფექტური მეთოდი. ამ მეთოდით პროცესთან მიდგომა გულისხმობს, რომ არის საჭიროება, როგორც პროცესში

შემავალი, ასევე პროცესიდან გამომავალი მონაცემებისა. ინფორმაციული უსაფრთხოების მართვის სისტემისა და დაინტერესებული მხარეების მოთხოვნები/მოლოდინები, აუცილებელი ქმედებები და პროცესები წარმოადგენენ იუმს-ის პროცესის შემავალ მონაცემებს, რომლებიც წარმოქმნის მოსალოდნელ ინფორმაციულ უსაფრთხოებას.[1] [6]

ქვევით მოცემულია სტანდარტში წარმოდგენილი საკითხები, რომლებიც შეესაბამება PDCA ციკლის თითოეულ ეტაპს:

დაგეგმვა(იუმს-ის ჩამოყალიბება):

- განისაზღვროს ორგანიზაციის კონტექსტი (თავი 4.1)
- განისაზღვროს იუმს-ის გავრცელების სფერო (თავი 4.3)
- განისაზღვროს ინფორმაციული უსაფრთხოების პოლიტიკა (თავი 5.2)
- განისაზღვროს რისკების აღწერის სისტემატიური მოდელი (თავი 6.1.2)
- შემუშავდეს რისკების აღწერის მეთოდოლოგია რათა იდენტიფიცირდეს ორგანიზაციისათვის მნიშვნელოვანი ინფორმაციული აქტივები და მათზე არსებული რისკები, იუმს-ის კონტექსტიდან გამომდინარე (თავი 8.2)
- აღიწეროს რისკები(თავი 6.1.2d)
- იდენტიფიცირდეს და შეფასდეს რისკებთან მოპყრობის კრიტერიუმები (თავი 6.1.3)
- ყოველი რისკის მოპყრობისთვის შეირჩეს განსახორციელებელი კონტროლის მექანიზმები (თავი 6.1.3.b)
- შემუშავდეს კონტროლის მექანიზმების გამოყენებადობის განაცხადი(SoA)(თავი 6.1.3.d)

შესრულება(იუმს-ის დანერგვა და ფუნქციონირება):

- ფორმულირდეს რისკების მოპყრობის გეგმა და მისი დოკუმენტაცია, მათ შორის დაგეგმილი პროცესები და დეტალიზირებული პროცედურები (თავი 6.1.3.e)

[1] ISO/IEC 27001:2013, 4.2 და 4.3

- განხორციელდეს რისკების მოპყრობის გეგმა და დაგეგმილი კონტროლები (თავი 8.3)
- ჩაუტარდეს შესაბამისი ტრენინგები იუმს-ში ჩართულ თანამშრომლებს (თავი 7.2)
- იმართოს იუმს-ის რესურსები და პროცესები (თავი 7.2 და 8.1)
- დაინერგოს უსაფრთხოების ინციდენტების დეტექციისა და რეაგირების პროცედურები (თავი 8.1)

შემოწმება(იუმს-ის მონიტორინგი და განხილვა)

- შემოწმების ფაზას გააჩნია მხოლოდ შემდეგი საქმიანობები: მონიტორინგი, განხილვა, ტესტირება და აუდიტი (თავი 9)
- მონიტორინგი, განხილვა, ტესტირება და აუდიტი არის მუდმივად არსებული პროცესები რომლებმაც უნდა დაფაროს მთელი სისტემა.

რეაგირება(იუმს-ის შენარჩუნება და გაუმჯობესება)

- ტესტირებისა და აუდიტის შედეგების განხილვა უნდა მოხდეს მენეჯმენტის მიერ, რამაც შესაძლოა შეცვალოს რისკების არსებული გარემო, ტექნოლოგიები ან სხვა საკითხები. იუმს-ის გაუმჯობესებები უნდა იყოს იდენტიფიცირებული, დოკუმენტირებული და განხორციელებული (თავი 9)

კონტექსტი, გავრცელების სფერო და პოლიტიკა

დაგეგმვის პირველი ეტაპი გავრცელების სფეროს განსაზღვრაა.

გავრცელების სფეროს მოთხოვნები ჩამოყალიბებულია ISO27001-ის 4.3 თავში, სადაც წერია, რომ ორგანიზაციამ უნდა "დაადგინოს ინფორმაციული უსაფრთხოების მართვის სისტემის გამოყენებადობა და საზღვრები გავრცელების სფეროს განსასაზღვრად, სადაც გათვალისწინებული უნდა იყოს : ორგანიზაციის შიდა და გარე საკითხები, დაინტერესებული მხარეების საჭიროებები და ორგანიზაციის მიერ შესრულებულ აქტივობებს შორის კავშირები და დამოკიდებულებები."

გავრცელების სფეროს ჩამოყალიბებისას უნდა განისაზღვროს თუ რა შევა იუმს-

ში და რა არა. ფაქტობრივად ინფორმაციული უსაფრთხოების მართვის სისტემა ზღვარს ავლებს მასში შემავალ და გარეთ დარჩენილ ინფორმაციულ აქტივებს შორის. იუმს-ი ყველა იმ შეხების წერტილს, სადაც იკვეთება მასში შემავალი აქტივები გარეთ დარჩენილთან, განიხილავს როგორც პოტენციურ რისკს, რომელსაც სჭირდება შესაბამისი მოპყრობა. პროცესი, ისევე როგორც აქტივი შეუძლებელია იყოს ერთდროულად შიგნით და გარეთ. ის სრულად უნდა ეკუთვნოდეს იუმს-ს ან არა.

პოლიტიკის განსაზღვრა

ISO27001-ის თანახმად შემდეგი მთავარი ეტაპი პოლიტიკის ჩამოყალიბებაა. 5.2-ე თავში განსაზღვრულია ინფორმაციული უსაფრთხოების პოლიტიკის სპეციფიკაციები. სტანდარტის „დანართ ა“-ში 5.1 პუნქტი, რომელიც პირველი კონტროლის მექანიზმია სიაში, განმარტავს უსაფრთხოების პოლიტიკის როლს ორგანიზაციაში. 5.1.-ში წერია, რომ ინფორმაციული უსაფრთხოების პოლიტიკა არის დოკუმენტი, რომელიც ადასტურებს „მენეჯმენტის მიმართულებასა და ხელშეწყობას ინფორმაციული უსაფრთხოების მიმართ, ბიზნესის საჭიროებებისა და შესაბამისი საკანონმდებლო და მარეგულირებელი წესების გათვალისწინებით“. აუცილებელია, რომ პოლიტიკის დოკუმენტს ხელმოწერით ადასტურებდეს ორგანიზაციის მმართველი და ხელმისაწვდომი იყოს ყველა დაინტერესებული პირისთვის.

სტანდარტის გადმოსახედით, სწორად და წარმატებულად ის ინფორმაციული უსაფრთხოების მართვის სისტემა ითვლება, რომელიც ხელს არ უშლის და არ ზღუდავს ორგანიზაციის აქტივობებს. სისტემა, რომელიც ხელს უშლის ორგანიზაციის პროცესებს, თანამშრომლებს აიძულებს გვერდი აუარონ მას.

რისკების აღწერა

შემდეგ დაგეგმვის ეტაპს წარმოადგენს რისკების აღწერა, რომელიც სტანდარტში განხილულია 6.1.2 და 8.2 თავებში. რისკების მოპყრობა ემსახურება შემდეგ ოთხ მიზანს:

- რისკის სრულად აღმოფხვრა

- რისკის შემცირება მისაღებ დონემდე
- რისკის მიღება და მისი შენარჩუნება მისაღებ დონეზე
- რისკის გადაცემა მესამე მხარეზე, რაც გულისხმობს, რომ მასზე პასუხისმგებლობას იღებს ორგანიზაციის გარეთ არსებული სუბიექტი

რა არის რისკი? ინფორმაციული უსაფრთხოების რისკი არის „ალბათობა იმისა რომ საფრთხე ისარგებლებს ინფორმაციული აქტივის ან აქტივების ჯგუფის სისუსტით, რაც ზიანს მიაყენებს ორგანიზაციას“[1] [7]

საფრთხე ნებისმიერი რამ, რამაც შეიძლება ორგანიზაციას მიაყენოს ზიანი. ის შეიძლება იყოს როგორც შიდა ასევე გარე.

სისუსტე არის ინფორმაციული აქტივის მახასიათებელი, რომელიც საშუალებას აძლევს საფრთხეს რომ ზიანი მიაყენოს მას. სტანდარტის მიხედვით გავრცელების სფეროში შემავალ თითოეულ ინფორმაციულ აქტივზე უნდა იყოს გამოვლენილი ყველა სისუსტე და საფრთხე, რათა რისკების შეფასება მოხდეს ადეკვატურად.
ISO27001-ის მოთხოვნაა, რომ ორგანიზავიამ განსაზღვროს რისკის მისაღები დონე და მისი აღწერის კრიტერიუმები. მენეჯმენტის მიერ მიღებული ეს პროცესი უნდა „შეესაბამებოდეს ორგანიზაციის საჭიროებებს“[2] [6]. გარდა ამისა რისკების აღწერისა და შეფასების პროცესმა, რომელსაც ორგანიზაცია აირჩევს, უნდა უზრუნველყოს „კონსისტენტური, ვალიდური და შედარებდი შედეგი“.[3] [6]

რისკების აღწერისთვის სტანდარტში ჩამოყალიბებულია საკითხები რომელიც აუცილებლად უნდა იყოს გათვალისწინებული:

- იდენტიფიცირდეს რისკები რომელიც იწვევს იუმს-ში არსებული ინფორმაციის კონფიდენციალურობის, მთლიანობისა და ხელმისაწვდომობის დარღვევას
- იდენტიფიცირდეს რისკის მფლობელი

[1] ISO/IEC 27000, 2.61
[2] ISO/IEC 27001:2013,1
[3] ISO/IEC 27001:2003, 6.1.2b

- გაანალიზდეს შედეგები, რომლებიც შეიძლება გამოიწვიოს რისკის დადგომამ
- გაანალიზდეს რისკის დადგომის ალბათობა
- განისაზღვროს რისკის დონეები
- შედარდეს აღწერის შედეგები რისკის კრიტერიუმებთან
- პრიორიტიზირდეს რისკები მოპყრობისთვის.

გარდა იმისა, რომ საჭიროა ინფორმაციული აქტივის მფლობელის დადგენა, მნიშვნელოვანია გამოვლინდეს რისკის მფლობელი(6.1.2.c.2). როდესაც აქტივის მფლობელის პასუხისმგებლობაა, რომ აქტივი იყოს აღწერილი, კლასიფიცირებული, დაცული და კონტროლირებული, რისკის მფლობელის პასუხისმგებლობა მხოლოდ ამ აქტივზე გამოვლენილი რისკის მართვაა. საგულისხმოა, რომ ზოგიერთმა რისკმა გავლენა იქონიოს რამოდენიმე აქტივზე.

რისკის დადგომა გამოიწვევს აქტივის მთლიანობის, კონფიდენციალურობის ან ხელმისაწვდომობის რღვევას. საჭიროა შესაძლებლობისამებრ აღიწეროს ყველა ეს ზიანი და მიენიჭოს ღირებულება(6.1.2.d.1). ISO27001-ის თანახმად, ზიანი უნდა აღიწეროს ამ სამივე მახასიათებელთან მიმართებით, რადგან ერთმა საფრთხემ შესაძლოა ისარგებლოს ერთზე მეტი სისუსტით და აქტივს ზიანი მიადგეს ერთზე მეტი კრიტერიუმით. ასევე მნიშვნელოვანია გაანალიზდეს შესაძლო დანაკარგები, რათა რისკების მოპყრობისას მოხდეს ადეკვატური პრიორიტეტიზაცია.

რისკების აღწერისას მნიშვნელოვანია შეფასდეს მისი დადგომის ალბათობა(6.1.2.d.2). ალბათობები შესაძლოა რანჟირებდეს „ძალიან მცირე ალბათობა“-დან (მაგალითად თბილისში მეტეორის ჩამოვარდნა) „ძალიან დიდი ალბათობა“ (მაგალითად ავტომატიზირებული ჰაკერული თავდასხმები).

ამ კრიტერიუმების გათვალისწინებით რისკს უნდა მიენიჭოს გარკვეული ხარისხი(6.1.2.d.3). რისკისთვის ხარისხის მინიჭება ხდება რისკის შეფასების კრიტერიუმებთან დადარებით, სადაც განხილული იქნება ყველა შესაძლო ალბათობა. მაგალითად რისკის დადგომის ალბათობა თუ არის „ძალიან დიდი“ და მის მიერ მიყენებული ზიანიც არის მაღალი, რისკს მიენიჭება „მაღალი“ ხარისხი.

ხარისხის მინიჭების მეთოდოლოგია ორგანიზაციამ უნდა შეიმუშავოს ისეთი, რომელიც მოსახერხებელი იქნება მისთვის.

რისკების პრიორიტეტიზაციისას, რისკი რაც უფრო შორდება მისაღებ დონეს მატულობს მისი პრიორიტეტი. ასევე შესაძლოა რისკი ხვდებოდეს მისაღებ დონეში მაგრამ მიენიჭოს მაღალი პრიორიტეტი, რადგან მასზე მოპყრობით ის სრულად აღმოიფხვრება ან მზარდი იყოს მისი დადგომის ალბათობა.

6.1.3 თავში განხილულია რისკების მოპყრობის გეგმა. მან უნდა განსაზღვროს შესაფერისი ქმედებები, პასუხისმგებლობები და ინფორმაციული უსაფრთხოების რისკების მართვის პრიორიტეტები. ის უნდა იყოს დოკუმენტირებული, პასუხობდეს ორგანიზაციის კონტექსტსა და ინფორმაციული უსაფრთხოების პოლიტიკას, ორგანიზაციის რისკების მიმართ მიდგომასა და მისაღები რისკის კრიტერიუმებს.

გამოყენებადობის განაცხადი(SOA)

იმისათვის რომ ორგანიზაციამ მიიღოს ინფორმაციული უსაფრთხოების მართვის სისტემის სერტიფიკატი, აუცილებელია გამოყენებადობის განაცხადის დოკუმენტის არსებობა, რადგან დამოუკიდებელი აუდიტორი, რომელიც აფასებს დანერგილი კონტროლის მექანიზმების შესაბამისობას კონკრეტულ ორგანიზაციაში, შემოწმებას იწყებს გამოყენებადობის განაცხადით. ეს დოკუმენტი მუშავდება რისკების აღწერისა და შეფასების და რისკების მოპყრობის გეგმის შემუშავების შემდგომ და ადასტურებს იმ კონტროლის მექანიზმების გამოყენების შესაძლებლობასა და მზაობას, რომელიც მოცემულია სტანდარტის „დანართ ა“-ში. დოკუმენტში ასევე მითითებულია იმ კონტროლების არ გამოყენების მიზეზები რომელიც ორგანიზაციამ არ ჩათვალა საჭიროდ.

6.1.3.b თავის მოთხოვნაა, რომ ორგანიზაციამ შეარჩიოს კონტროლის მექანიზმები რისკების მოპყრობის მიზნით. 6.1.3.c თავში კი შედარდეს „დანართი ა“-ში არსებულ კონტროლებს. ამ მიდგომით მოხდება სტანდარტის მიერ შემოთავაზებული კონტროლების შერჩევა და იმ კონტროლების გამოვლენა რომლის დანერგვასაც არ საჭიროებს ორგანიზაცია. ეს მიდგომა ადასტურებს, რისკების

მოპყრობის გეგმასა და გამოყენებადობის განაცხადში „დანართ ა“-ში არ შესული კონტროლების მოხვედრის ალბათობასაც.

კონტროლი წარმოადგენს სისუსტეების საპირისპირო ცნებას. მისი ფორმალური განმარტება ISO27000-ში შემდეგნაირია: „კონტროლი ნიშნავს რისკის მართვას, პოლიტიკებით, პროცედურებით, სახელმძღვანელოებითა და სხვა და სხვა პრაქტიკებით, რომელიც შეიძლება იყოს ადმინისტრაციული, ტექნიკური, მენეჯერული ან იურიდიული ბუნების.“.[1] [7]

გარდა ორგანიზაციული გადაწყვეტილებისა რომ, მიიღონ რისკი, რომელიც არ ცდება განსაზღვრულ დასაშვები რისკის დონეს, ან აღმოფხვრას და მინიმუმზე დაიყვანოს მისი დადგომის ალბათობა, ან გადასცეს მის მართვაზე პასუხისმგებლობა მესამე მხარეს, ორგანიზაციას შეუძლია იზრუნოს რისკის დონის შემცირებაზე.

შეუძლებელია ყველა ორგანიზაციული რისკის სრულად აღმოფხვრა, მაგრამ შესაძლოა მათი დასაშვებ ზღვრამდე დაყვანა. აქედან გამომდინარე რისკის მფლობელმა ფორმალურად უნდა დაადასტუროს, რომ იღებს მოპყრობის შემდგომ დარჩენილ რისკებს.[2] [6]

თუ ვარჩევთ კონტროლს, რომელიც განკუთვნილია კონკრეტული გამოვლენილი უსაფრთხოების ინციდენტის აღმოსაფხვრელად, მნიშვნელოვანია რომ ეს ინციდენტი იყოს იდენტიფიცირებული, განხილული და დაგეგმილი. „დანართი ა“-დან კონტროლების შერჩევისას, აუცილებელია განისაზღვროს თუ რა მტკიცებულებები და ეფექტურობის საზომებია საჭირო იმის დასადგენად რომ:

- კონტროლი დანერგილია და მუშაობს ეფექტურად
- ყოველი რისკი შემცირებულია მისაღებ დონემდე.

რისკების შესამცირებლად აუცილებელია კონტროლი დაინერგოს ისე, რომ ფუნქციონირებისას დაშვებული შეცდომები ან გაუმართაობები იყოს მყისიერად იდენტიფიცირებული, რათა მასზე დაყრდნობით დაგეგმილი შემდგომი მაკორექტირებელი ქმედებები იყოს ეფექტური.

[1] ISO/IEC 27000, 2.16
[2] თავი 6.1.3.f

იუმს-ის დანერგვა

ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვა მოიცავს შემდეგ 5 ეტაპს:

- განხორციელდეს რისკების მოპყრობის გეგმა და გამოყენებადობის განაცხადში არსებული კონტროლები(8.3)
- განისაზღვროს თუ როგორ გაიზომოს და შეფასდეს კონტროლების ეფექტურობა(9.1.b)
- ჩატარდეს ტრენინგები და ცნობიერების ამაღლების პროგრამები (7.2 და 7.3)
- უნდა იმართოს იუმს-ი(8.1). ყველა პროცესმა და კონტროლმა უნდა იფუნქციონიროს, ახლად იდენტიფიცირებული საფრთხეები შეფასდეს და საჭიროების შემთხვევაში განეიტრალდეს.
- დაინერგოს ინციდენტის აღმოჩენისა და რეაგირების პროცედურა (10.1). ამ თემას ეხება „დანართი ა“-ს 16-ე თავი, ინფორმაციული უსაფრთხოების ინციდენტების მართვა.

შემოწმება და ქმედება

სტანდარტის მე-9 თავი მთლიანად დათმობილია მონიტორინგსა და განხილვაზე. ის შეიცავს მოთხოვნებს მენეჯმენტის მიმართ, რომ აქტიურად იყვნენ ჩართულნი ინფორმაციული უსაფრთხოების მართვის სისტემის მართვაში იმის გააზრებით, რომ ინფორმაციული უსაფრთხოების მიმართულებით არსებული საფრთხეები იმაზე ხშირად იცვლება ვიდრე ბიზნესს გარემოში. ამ თავში განიხილება ძირითადი სამი საკითხი: მონიტორინგი, აუდიტი და განხილვა.

მონიტორინგი

მონიტორინგის მიზანია მიმდინარე პროცესებში დროულად აღმოაჩინოს ხარვეზები და ინფორმაციული უსაფრთხოების მოლენები, რათა გატარდეს მაკორექტირებელი ქმედებები. „დანართი ა“-ს A.12.4 თავი (ლოგირება და მონიტორინგი) შეიცავს კონტროლებს, რომლებიც შეეხება ინფორმაციული ტექნოლოგიების მონიტორინგს, რაც პასუხობს სტანდარტის ამ ნაწილს. ასევე A.16 თავი, რომელიც შეეხება ინფორმაციული უსაფრთხოების ინციდენტების მართვას, რაც გვახსენებს რომ ორგანიზაციამ უნდა აღმოაჩინოს სისტემიდან გადახრები და ინციდენტები, მოახდინოს რეაგირება.

აუდიტი

აუდიტი უნდა დაიგეგმოს რათა ორგანიზაცია დარწმუნდეს გამოყენებადობის განაცხადში არსებული კონტროლები რამდენად ეფექტურადაა დანერგილი, კარგად ფუნქციონირებს და მზადაა გაუმჯობესებისთვის. „დანართი ა“-ს თავებში A.18.1 და A.18.2 წარმოდგენილია კონტროლები, რომელიც მოითხოვს წინასწარ დაგეგმილ, რეგულარულ შესაბამისობის განხილვებს როგორც პროცესებში, ისე ტექნიკურ სივრცეში. კონტროლს აუდიტის შესახებ წარმოადგენს A.12.7 თავი, რომელიც უფრო დეტალურად განხილულია სტანდარტის 9.2 თავში და აყალიბებს ორ ძირითად ასპექტს:

- ორგანიზაციამ უნდა „დაგეგმოს, ჩამოაყალიბოს, განახორციელოს და შეინარჩუნოს აუდიტის პროგრამა, რომელიც განსაზღვრავს მისი ჩატარების სიხშირეს, მეთოდოლოგიას, პასუხისმგებლობებს, დაგეგმვის მოთხოვნებსა და ანგარიშს“[1] [6]
- აუდიტმა უნდა გაითვალისწინოს წინა აუდიტის შედეგები

[1] ISO/IEC 27001:2013, თავი 9.2.c

განხილვა

შიდა და გარე აუდიტის, წარმადობის ანგარიშების, რისკების შეფასების რეპორტებისა და ყველა მასთან დაკავშირებული პროცედურის განხილვის ერთად-ერთ მიზანს წარმოადგენს, რომ ინფორმაციული უსაფრთხოების მართვის სისტემა უწყვეტად ფუნქციონირებდეს, იყოს ეფექტური და გაუმჯობესდეს.
ქვემოთ მოცემულია „დანართ ა“-ში არსებული კონტროლები რომელიც შეეხება ამ ეტაპს:

- A.5.1.2 ინფორმაციული უსაფრთხოების პოლიტიკების განხილვა
- A.9.2.5 მოხმარებლების სისტემებზე დაშვების უფლებების განხილვა
- A.12.4 ლოგირება და მონიტორინგი
- A.14.1 ინფორმაციული სისტემების უსაფრთხოების მოთხოვნები
- A.15.2.1 სერვისის მომწოდებლების მონიტორინგი და განხილვა
- A.16.1.6 ინფორმაციული უსაფრთხოების ინციდენტებზე სწავლა
- A.17.1.3 ინფორმაციული უსაფრთხოების უწყვეტობის შემოწმება, განხილვა და შეფასება
- A.18.2.1 ინფორმაციული უსაფრთხოების დამოუკიდებელი განხილვა

ყველა ეს კონტროლი უნდა იქნეს გათვალისწინებული იუმსის დანერგვისას. მონიტორინგისა და რეპორტინგის აღმოჩენებს და შედეგებს უნდა მოჰყვეს მაკორექტირებელი და გამაუმჯობესებელი ქმედებები. იუმს-ის გასაუმჯობესებლად რეკომენდირებულია აუდიტის ყოველი პროცესი და გადაწყვეტილების მიღება იყოს აღწერილი.

ქმედება

6.1.1.c თავის მოთხოვნაა რომ ორგანიზაციამ უნდა მიაღწიოს ინფორმაციული უსაფრთხოების მართვის სისტემის უწყვეტ განვითარებას. ასევე სტანდარტის 10-ე

თავში საუბარია მაკორექტირებელ ქმედებებზე და უწყვეტ განვითარებაზე, რომელიც უნდა იყოს იუმს-ის ყველდღიურობის შემადგენელი ნაწილი.

მენეჯმენტის მიერ განხილვა

სტანდარტის 9.3 თავი, რომელიც შეეხება მენეჯმენტის მიერ იუმს-ის განხილვას, ხაზს უსვამს რომ განხილვისას გათვალისწინებული უნდა იქნეს მონაცემები იუმს-ის წარმადობაზე, შეუსაბამობებზე და მაკორექტირებელ ქმედებებზე, ისევე როგორც ყველა სხვა ქმედებაზე რამაც შეიძლება გავლენა იქონიოს ინფორმაციული უსაფრთხოების მართვის სისტემაზე.

აქვე უნდა აღინიშნოს რომ ყველა მაკორექტირებელი და პრევენციული ქმედება უნდა პრიორიტეტიზირდეს რისკების შეფასებაზე დაყრდნობით.[1] [6]

კონტროლი A.18.2.1 რომელიც გულისხმობს ინფორმაციული უსაფრთხოების დამოუკიდებელ განხილვას, საჭიროა განხორციელდეს წინასწარ განსაზღვრული დროის ინტერვალებით ან მნიშვნელოვანი ცვლილებების შემდგომ. ის უნდა მოიცავდეს კონტროლის მიზნების, კონტროლების, პოლიტიკების, პროცესების და პროცედურების განხილვას. დამოუკიდებელი განხილვისთვის რეკომენდირებულია მესამე მხარის წარმომადგენელი, რომელსაც კავშირი არ აქვს ორგანიზაციასთან.

[1] ISO/IEC 27001:2013, 6.1.2.e.2

დასკვნა

ინფორმაცია თამაშობს მთავარ როლს, როგოც ორგანიზაციებისთვის ასევე ცალკეული სუბიექტებსთვის. მისი საშუალებით ხდება ახალი კონცეფციებისა და სტრატეგიული გადაწყვეტილების მიღება. ინფორმაციის მნიშვნელობიდან გამომდინარე, არსებობს რისკები, რომლებიც საფრთხეს უქმნიან მის კონფიდენციალურობას, ხელმისაწვდომობასა და მთლიანობას. ინფორმაციის დასაცავად აუცილებელია მასთან არსებული რისკების მართვა. მნიშვნელოვანია იცოდე რისკის წარმომქმნელი დაინტერესებული მხარეები და მათ გასამკლავებლად შეიმუშავო შესაბამისი დაცვის მექანიზმები. საერთაშორისო სტანდარტების ორგანიზაციის მიერ შემუშავებული სტანდარტი ISO/IEC 27001-ში თავმოყრილია მსოფლიო საუკეთესო პრაქტიკები ორგანიზაციაში ინფორმაციული უსაფრთხოების მართვის სისტემის დანერგვასა და მის გამოყენებაზე. სტანდარტი მოქნილია ყველა ტიპისა და ზომის ორგანიზაციაზე. ის არ ზღუდავს ორგანიზაციებს მართვის სისტემის დანერგვისა და გამოყენებისთვის საჭირო მეთოდოლოგიებს, თუმცა რეკომენდაციას უწევს დაგეგმვა-შესრულება-შემოწმება-რეაგირება (PDCA) ციკლს. სტანდარტის მოთხოვნაა ციკლის ყველა ეტაპში ჩართული იყოს ორგანიზაციის მმართველი გუნდი და თითოეული პროცესისა თუ პროცედურის ყოველი დეტალი იყოს დოკუმენტირებული. ვინაიდან სისტემის მიზანია მართოს ორგანიზაციაში არსებული რისკები, ISO 27001 განსაზღვრავს ყველა იმ პროცედურას რაც საჭიროა რისკების იდენტიფიკაციისათვის, შეფასებისთვის მოპყრობისთვისა და მართვისთვის. ასევე საგულისხმოა ის ფაქტი, რომ სტანდარტი „დანართ ა”-ში თავადვე გთავაზობს იმ ძირითად კონტროლებს, რომლებიც საჭიროა მართვის სისტემის სრულყოფილად განხორციელებისათვის.

ნაშრომის მიზანია ორგანიაზციებს დაანახოს თუ როგორი მნიშვნელოვანია ინფორმაციული უსაფრთხოება. ასევე გაამახვილოს ყურადღება იმ მნიშვნელოვან საკითხებზე სტანდარტში, რომლის გარეშეც პრაქტიკულად შეუძლებელია ინფორმაციის სათანადო დონეზე დაცვა.

ბიბლიოგრაფია

[1] D. Albright, P. Brannan and C. Walrond, "Did Stuxnet Take Out 1000 Centrifuges at the Natanz Enrichment Plant?," Institute for Science and International Security, 2010.

[2] U.S. Department of Justice, "www.justice.gov," U.S. Department of Justice, 1 August 2018. [Online]. Available: https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100. [Accessed 30 May 2019].

[3] Wikipedia, "www.wikipedia.org," The free Enciclopedia, 18 June 2019. [Online]. Available: https://en.wikipedia.org/wiki/Operation_Payback. [Accessed 28 June 2019].

[4] C. Wood, "Insider threat examples: 7 insiders who breached security," 19 March 2018. [Online]. Available: https://www.csoonline.com/article/3263799/insider-threat-examples-7-insiders-who-breached-security.html#slide4. [Accessed 30 May 2019].

[5] U.S. Department of Justice, "www.justice.gov," U.S. Department of Justice, 21 September 2000 . [Online]. Available: https://www.justice.gov/archive/opa/pr/2000/September/555crm.htm. [Accessed 30 May 2019].

[6] ISO/IEC, ISO/IEC 27001:2013 nformation technology -- Security techniques -- Information security management systems -- Requirements, ISO, 2013.

[7] ISO/IEC, ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, ISO, 2012.