ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

შალვა ანანიაშვილი

ქსელური უსაფრთხოების პოლისების იმპლემენტაცია ქსელის ეფექტური მართვისათვის

სამაგისტრო პროგრამა: ინფორმაციული ტექნოლოგიები

ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის ხარისხის მოსაპოვებლად

ხელმძღვანელი: ასოცირებული პროფესორი
ლელა მირცხულავა

თბილისი
2017

ანოტაცია

თანამედროვე ორგანიზაციების საქმიანობა სულ უფრო უფრო დამოკიდებული ხდება ციფრულ გარემოზე და ამ სფეროში ნებისმიერმა შეფერხებამ შეიძლება მნიშვნელოვანი ზარალი მიაყენოს მას. ინფორმაციის მოცულობის ზრდასთან ერთად იზრდება ინფორმაციის დატაცების, არასანქცირებული წვდომის, გამიზნული შეცვლის და მათი დანაშაულებრივი მიზნებით გამოყენების რისკები. აქედან გამომდინარე, ორგანიზაციებს უხდებათ გამოყონ დრო და რესურსები ინფორმაციისა და ქსელური უსაფრთხოების დაცვის უზრუნველსაყოფად, შესაბამისად ინფორმაციული უსაფრთხოება დღეისათვის ყველაზე მოთხოვნადი და აქტუალური საკითხია.

ეს ნაშრომი ეხება ორგანიზაციებში ინფორმაციული უსაფრთხოების პოლიტიკის შექმნასთან დაკავშირებულ საკითხებს. ინფორმაციული უსაფრფთხოება - ეს არის ინფორმაციისა და ინფორმაციული სისტემების დაცვა მათი დაზიანებისა და განადგურებისაგან. დღეისათვის, როდესაც ინფორმაციულ სისტემებს მნიშვნელოვანი როლი აკისრია ჩვენს ცხოვრებაში, დგება მასში შემავალი ინფორმაციის უსაფრთხოების საკითხი. ინფორმაციული უსაფრთხოება არ უზრუნველყოფს აბსოლუტურ დაცვას, უსაფრთხოების პოლიტიკა წარმოადგენს გამაფრთხილებელ მოქმედებათა ერთობლიობას, რომელიც, სწორად შემუშავებისა და დანერგვის შემთხვევაში, საშუალებას გვაძლევს დავიცვათ ინფორმაცია და მოწყობილობები საფრთხეებისგან, რომელიც შესაძლებელია მათი სუსტი ადგილების გამოყენებით. ამ საფრთხეებთან საბრძოლველად საჭიროა ინფორმაციული რესურსების დაცვის პროცესის მიზანმიმართული ორგანიზება, რაშიც უნდა მონაწილეობდნენ პროფესიონალი სპეციალისტები, ადმინისტრაცია, თანამშრომლები და მომხმარებელი, რაც აამაღლებს საკითხის ორგანიზაციულ მხარეს. ნაშრომში მოცემულია მეთოდები და პრინციპები, რომლის შესრულება აუცილებელია, რათა შეიქმნას დაცული ქსელური ინფრასტუქტურა.

Annotation

The activities of Modern organizations increasingly depend on digital environment and any disruption in this area can cause a significant loss. The growth of information can lead to the growth of the risk of information theft, an unauthorized access, misuse and use for illegal puposes of this information. Organizations have to spend much time and resources for information and network security. This makes the problem of information security one of the most relevant and important issues today.

The given thesis is devoted to the problem of creating information security policy in organizations. Information security implies protection of information and information systems from damages and destruction. Today, as the role of information systems has grown in our lives, information security has become a very important issue. Information security does not provide absolute protection. Security policy is an aggregation of preventive actions, that protect information and appliances from danger arised from their weak points when it's correctly developed and instilled. Organizing the successful sets of security policies and frameworks are nessecary to protect an information from the threts and requires involvement of professionals, administration, management, employees and users. The methods and principles that are necessary for creating the secure network infrastructure are described in the given thesis.

შინაარსი

შესავალი

თანამედროვე სამყაროს წარმოდგენა გამოთვლითი ტექნიკის საშუალებების გარეშე შეუძლებელია. ინფორმაციული ტექნოლოგიები ვითარება ძალიან სწრაფად და ისინი მოიცავენ ადამიანური შემოქმედების კიდევ უფრო ფართო არეალს. ამდენად, ინფორმაციული ტექნოლოგიების უსაფრთხოება მათი ფუნქციონირების უზრუნველყოფის უმნიშვნელოვანეს საკითხს წარმოადგენს.

ნებისმიერი ორგანიზაცია შეიძლება შევადაროთ პატარა სახელმწიფოს და თუ სახელმწიფოში არსებობს კანონები, რომელსაც ემორჩილებიან მოქალაქეები. ორგანიზაციაში ამ კანონების როლს ასრულებს უსაფრთხოების პოლიტიკა, რომლის წესებიც უნდა დაიცვას კომპანიის ყველა თანამშრომლემა. ინფორმაციული უსაფრთხოების პოლიტიკა განსაზღვრავს სტრატეგის და ტაქტიკას, კორპორატიული ინფორმაციის უსაფრთხოების სისტემების შემუშავებისას. ინფორმაცია ორგანიზაციისთვის ისეთივე არსებითი აქტივია, როგორც საქმიანობის მართვის სხვა მნიშვნელოვანი აქტივები და მას შესაბამისი დაცვა სჭირდება. თითოეული კომპანია ფლობს გარკვეული ღირებულების მქონე ინფორმაციას, რომელიც, გასაგები მიზეზების გამო, საჭიროებს დაცვას. მაგალითად, ბანკებმა უნდა უზრუნველყონ საკუთარი მომხმარებლების საბანკო ინფორმაციის საიდუმლოება, სადაზღვევო კომპანიებმა უნდა დაიცვან, საკუთარ კლიენტებზე არსებული, სადაზღვევო ინფორმაცია და ასე შემდეგ. გარდა ამისა ორგანიზაციამ უნდა უზრუნველყოს თანამშრომლების პირადი მონაცემების და კომპანიის ქსელში არსებული სვდასხვა, ბიზნესისათვის საჭირო, ინფორმაციის დაცვა. ინფორმაცია შესაძლოა არსებობდეს მრავალი ფორმით. იგი შეიძლება იყოს ქაღალდზე, ელექტრონული ფოსტის მეშვეობით ან სხვა საშუალებებით გადაცემული, რა ფორმითაც არ უნდა არსებობდეს ან რა საშუალებებითაც არ უნდა ხდებოდეს მისი გადაცემა, ინფორამცია ყოველთვის უნდა იყოს შესაბამისად დაცული. ორგანიზაციები, მათი ინფორმაციული სისტემები და ქსელები უშუალოდ დგანან ისეთი საფრთხეების წინაშე, როგორებიცაა კომპიუტერული თაღლითობა, ჯაშუშობა, მავნე კოდის შემცველი პროგრამები, კომპიუტერულ პროგრამაზე თავდასხმა სერვისის შეფერხების მიზნით, ხანძარი ან წყალდიდობა და ასეთი ქმედებებიდან გამოწვეული ზარალი სულ უფრო იზრდება.

ინფორმაციული უსაფრთხოება არის ინფორმაციის და ინფორმაციული სისტემების დაცვა მთელი რიგი საფრთხეებისაგან, რათა უზრუნველყოფილი იყოს ორგანიციის უწყვეტი საქმიანობა, რისკების შემცირება და ბიზნესის მოგების გაზრდა. კომპიუტერი და

ქსელური უსაფრთხოების პოლიტიკა განსაზღვრავს სათანადო და არასათანადო ქცევას, განმარტავს, თუ რაა ნებადართულია და რა არა. პროცედურები დეტალურად აღწერენ, პოლიტიკის მხარდასაჭერად და აღსრულებისათვის საჭირო, მეთოდებს და აღწერს კონკრეტულ ნაბიჯებს. ინფორმაციული უსაფრთხოება მიიღწევა შესაბამისი პოლიტიკის, პროცედურების, პროგრამული უზრუნველყოფის და კომპიუტერული ტექნიკის დანერგვით. უნდა მოხდეს აღნიშნული პოლიტიკის, დანერგვა, მონიტორინგი, და საჭიროების შემთხვევაში, გაუმჯობესება, რათა ამით უზრუნველყოფილი იყოს ორგანიზაციისთვის უნფორმაციული უსაფრთხოება. სათანადოდ შემუშავებულ და განხორციელებულ უსაფრთხოების პოლიტიკას შეუძლია გაცილებით ეფექტური და ხელმისწვდომი გახადოს კომპანიის სერვისები, რაც ზრდის ორგანიზაციის სიცოცხლისუნარიანობას და უზრუნველყოფს ბიზნესის უწყვეტობას. ინფორმაციული უსაფრთხოება წარმოადგენს, ბიზნესის სტაბილურობის მთავარ ფაქტორს. ქსელური უსაფრთხოების პოლიტიკა სუბიექტურია და შეიძლება განსხვავებული იყოს სხვადასხვა ორგანიზაციებისთვის, თუმცა არსებობს გარკვეული საკითხები, რომლებიც დაკავშირებულია უმეტესად პოლიტიკასთან.

- წვდომის კონტროლი განსაზღვრავს, ვის რაზე უნდა ჰქონდეს წვდომა.
- ქსელის უსაფრთხოება განსაზღვრავს თუ როგორ უნდა იქნას დაცული ქსელში შენახული აქტივები. ასევე შეიძლება შეიცავდეს უსაფრთხოების ზომებს ხელმისაწვდომობის კონტროლის, ეკრანის, ქსელის აუდიტის, დისტანციური წვდომის, ინტერნეტის სერვისების და ფაილური სისტემის სტრუქტურების შესახებ.
- ფიზიკური უსაფრთხოების გარეშე, ქსელური უსაფრთხოების სხვა საკითხები, როგორიცაა კონფიდენციალობა, ხელმისაწვდომობა და მთლიანობა, იქნება საფრთხის ქვეშ.
- ფიზიკური უსაფრთხოება გულისხმობს, თუ როგორ უნდა იყოს დაცული ობიექტები და აპარატურა, თუ რომელ თანამშრომელს უნდაჰქონდეს წვდომა შეზღუდულ ტერიტორიებზე, როგორიცაა სერვერები და სადენები.
- აუდიტი: უსაფრთხოების პოლიტიკის დენერგვის შემდეგ აუცილებელია შემოწმება იმისათვის, რომ უზრუნველყოფილ იქნას უსაფრთხოების ყველა კომპონენტი და თანამშრომელი.
- უსაფრთხოების ინციდენტებზე რეაგირება: რეაგირების გეგმა განმარტავს, თუ როგორ უნდა იმოქმედოს ორგანიზაციამ ნებისმიერი სახის სტიქიური უბედურების

ან ჰაკერული თავდასხმის დროს. მაგალითად, შეიძლება შეიცავდეს სერვერების მხარდაჭერის ზომებს, სარეზერვო ასლების გადაღების გეგმას.

უსაფრთხოება, რომელიც ტექნიკური საშუალებებით მიიღწევა, შეზღუდულია და მისი მხარდაჭერა უნდა მოხდეს შესაბამისი მენეჯმენტისა და პროცედურების მეშვეობით. სასურველი და საჭირო კონტროლის მექანიზმების გამოვლენა მოითხოვს ფრთხილ დაგეგმვას, დეტალების გათვალისწინებით, ინფორმაციული უსაფრთხოების მართვა მოითხოვს ყველა თანამშრომლის თანამონაწილეობას.

1. უსაფრთხოების პოლისების დეველოპმენტი

პირველი რაც უნდა გავაკეთოთ უსაფრთხოების პოლიტიკის შექმნისას: შევკრიბოთ გუნდი, რომელიც უნდა შედგებოდეს იმ ადამიანებისგან, რომლებიც მუშობენ კომპანიის ქსელთან და ინტერნეტთან, კომპანიის სხვადასხვა ფუნქციონალური სფეროებიდან. უსაფრთხოების პოლიტიკას უნდა ქმნიდნენ არა მარტო IT დეპარტამენტის წარმომადგენლები არამედ პერსონალი, რომელიც იცნობს კომპანიის საქმიანობის სფეროს და მოთხოვნებს, თითოეულ დეპარტამენტის ხელმძღვანელს და მენეჯერს აქვს კომპანიის საჭიროებების და რისკების უნიკალური ხედვა, რომელიც უნდა იქნას გათვალისწინებული უსაფრთხოების შემუშვებისას. ორგანიზაციის ბიზნეს მოთხოვნები უსაფრთხოების პოლიტიკის ერთერთი ყველაზე მნიშვნელოვანი ნაწილია. ბიზნეს-ფაქტორების გაცნობა გვეხმარება განასხვავოთ თუ რას საჭიროებს ორგანიზაცია სინამდვილეში და ცალკეული თანამშრომელი. ამიტომ სანამ დავიწყებთ ინფორმაციული უსაფრთხოების პოლიტიკის წერას, უნდა გავარკვიოთ კომპანიის ბიზნეს-მოთხოვნები, რა წესები ვრცელდება მოცემულ ინდუსტრიაში, გავეცნოთ ჯარიმებს ნებისმიერი შეუსაბამობისთვის, რაც დაგვეხმარება პრიორიტეტების გადანაწილებაში და სათანადო დონის დისციპლინარული სანქციის შექმნაში კადრისათვის, რომელიც არ იცავს უსაფრთხოების პოლიტიკას. უნდა იქნას გათვალისწინებული შემდეგი საკითხები:

- რა მომსახურებაა საჭირო კომპანიის საქმიანობისთვის და როგორ შეიძლება მათი უსაფრთხოების უზრუნველყოფა
- რამდენად არიან თანამშრომელები დამოკიდებული ინტერნეტზე, ელ-ფოსტის გამოყენებაზე და ინტრანეტ სერვისების ხელმისაწვდომობაზე
- საჭიროა რუ არა შიდა ქსელში დისტანციური წვდომა
- არსებობს თუ არა ბიზნეს-მოთხოვნა - ყველა თანამშრომლისათვის ინტერნეტთან წვდომაზე
- აქვთ თუ არა მომხმარებლებს კომპანიის სერვისებზე წვდომა ინტერნეტის მეშვეობით

კიდევ ერთი მნიშვნელოვანი ასპექტი, რაც უნდა გვახსოვდესი უსაფრთხოების პოლისის შექმნისას, დოკუმენტი უნდა იყოს დაწერილი მარტივი ენით, უნდა იყოს ადვილად გასაგები, არ იყოს ზედმეტად რთული და უნდა მიეწოდოს ორგანიზაციაში ყველა მომხმარებელს იმ ფორმით, რომელიც ხელმისაწვდომი და გასაგები იქნება სამიზნე აუდიტორიისთვის. Cisco-ს რეკომენდაციით ინფორმაციული უსაფრთხოების პოლიტიკის

დოკუმენტი უნდა მოიცავდეს 5-6 გვერდს. იდეალურ შემთხვევაში, უსაფრთხოების პოლიტიკა უნდა იყოს რეალისტური, განხორციელებადი, მოკლე და გასაგები. მას შემდეგ რაც დავასრულებთ პოლიტიკის შემუშავებას, უნდა განხორციელდეს პოლიტიკის შეფასება, რათა დადგინდეს, მიღწეულია თუ არ პოლიტიკის ამოცანები. ინფორმაციული უსაფრთხოების პოლიტიკის საბოლოო დოკუმენტი უნდა იყოს დამტკიცებული მენეჯმენტის მიერ, რის შემდეგაც უნდა გამოიცეს და მიეწოდოს ყველა თანამშრომელს. ინფორმაციის უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს შემდეგ მინიმლურ მოთხოვნებს:

- ✓ მოიცავდეს ინფორმაციული ქმედების მთელ ტექნოლოგიურ კომპლექსს
- ✓ იყოს გათვალისწინებული ცვლილებების და დამატებების შეტანა
- ✓ იყოს მარტივი და მოხერხებული ტექნიკური მომსახურების და მომხმარებელთა მიერ ექსპუატაციის თვალსაზრისით
- ✓ იყოს საიმედო
- ✓ ცხადად იყოს განსაზღვრული მომხმარებლის უფლებები ინფორმაციის წვდომაზე
- ✓ მიანიჭოს მომხმარებელს მინიმალური უფლება, რომელიც სჭირდება დაკისრებული სამუშაოს შესასრულებლად

1.1 რისკის ანალიზი და შეფასება

ინფორმაციულ სისტემებზე ზეგავლენას ახდენს სხვადასხვა ტიპის სერიოზული საფრთხე, რომლებმაც შეიძლება უარყოფითად ომოქმედონ ორგანიზაციის საოპერაციო გარემოზე, აქტივებსა თუ ინდივიდებზე სხვადასხვა სისუსტეების გამოყენებით, რომლებიც არღვევენ ინფორმაციულ სისტემებში შენახული, დამუშავებული თუ გადაცემული ინფორმაციის კონფიდენციალურობას, მთლიანობასა თუ ხელმისაწვდომობას. ინფორმაციული სისტემების საფრთხეებს მიეკუთვნება: მიზანმიმართული შემოტევები, გარემოსდაცვითი ხასიათის დარღვევები, ადამიანური შეცდომები და სხვა, რომლებიც საბოლოოდ დიდ ან საერთოდ გამოუსწორებელ ზიანს აყენებენ ორგანიზაციას. ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება უნდა დაიწყოს ამ საფრთხეების ანალიზით. ორგანიზაციის მიზნებიდან გამომდინარე რიკსების შეფასების შედეგად უნდა გამოვლინდეს, შეფასდეს და განისაზღვროს რისკების

პრიორიტეტი, შედეგებმა უნდა განსაზღვროს ქმედებები და პრიორიტეტები, რომლებმაც ორგანიზაცია უნდა დაიცვან ინფორმაციული უსაფრთხოების რისკებისგან. უნდა დადგინდეს და დაცულ იქნას ინფორმაციული უსაფრთხოების რისკების მართვის პროცესისთვის საჭირო ორგანიზაციული სტრუქტურა და პასუხისმგებლობები:

- ორგანიზაციაზე მორგებული ინფორმაციული უსაფრთხოების რისკების მართვის პროცესის შემუშავება
- დაინტერესებული პირების გამოვლენა და ანალიზი
- ყველა მხარის როლებისა და პასუხისმგებლობების განსაზღვრა ორგანიზაციისათვის
- გადაწყვეტილების მიღების წესის განსაზღვრა

ინფორმაცული უსაფრთხოების რისკის შეფასებას უნდა გააჩნდეს მკაფიოდ დადგენილი ფარგლები, იმისათვის, რომ იყოს ეფექტიანი და ჰქონდეს კავშირი სხვა სფეროებში ჩატარებულ რისკების შეფასებებებთან. რისკების შეფასებები უნდა ხორციელდებოდეს პერიოდულად, რათა შეფასების დროს აისახოს მომხდარი ცვლილებები. მაგალითად, უნდა შეფასდეს აქტივები, საფრთხეები, სისუსტეები, რისკის ზემოქმედება. უნდა დადგინდეს რისკის დონე იმ შემთხვევებისთვის, როდესაც ხორციელდება მნიშვნელოვანი ცვლილებები. რისკების შეფასება უნდა განხორციელდეს იმ მეთოდური მიდგომით, რომლებიც შედარებად შედეგებს იძლევა. რისკების შეფასება შეიძლება განხორციელდეს მთელი ორგანიზაციის მაშტაბით, მოიცავდეს ორგანიზაციის ნაწილს, ინდივიდუალურ საინფორმაციო სისტემას, კონკრეტული სისტემის კომპონენტებს, ან რომლიმე სერვისს.

რისკების მართვა წარმოადგენს პროცესს, რომლის დროსაც ერთად სხდებიან ორგანიზაციის მთავარი წევრები და აანალიზებენ ყველა იმ რისკს, რომელიც არსებობს ორგანიზაციაში. აღნიშნულ რისკებში განიხილება როგორც კრიტიკული, ასევე უმნიშვნელო რისკები: დაწყებული ხანძრიდან, დამთავრებული ბუნებრივ კატასტროფამდე. განსაკუთრებული მნიშვნელობა აქვს უსაფრთხოების შესაბამისი მუქარების სისტემურ ანალიზს. ასეთი ანალიზის საფუძველი უნდა იყოს მუქარების კლასიფიკაცია გარკვეული ბაზური პარამეტრების მიხედვით, რომლებიც საშუალებას აძლევს მკვლევარს ერთიანობაში წარმოადგინონ დესტრუქციული ზემოქმედებები და მათი შედეგები. უნდა განსაზღვროს რისკების მისაღებობის კრიტერიუმები, რისკი შეიძლება იყოს მიღებული თუ მაგალითად, მის მიერ მიყენებული პოტენციური ზარალი არის მცირე ან მისი თავიდან აცილების დანახრჯი არის დიდი. თითოეული რესურს უნდა მივანიჭოთ რისკის შესაბამისი დონე:

- დაბალი რისკი - სისტემები და მონაცემები, რომელთა არასანქცირებული დათვალიერება, დაკარგვა ან განადგურება არ გამოიწვევს იურიდიულ და ფინანსურ პრობლემებს
- საშუალო რისკი - სისტემები და მონაცემები, რომელთა არასანქცირებული დათვალიერების, დაკარგვის ან განადგურების შედეგად ორგანიზაცია განიცდის უმნიშვნელო ზიანს იურიდიული ან ფინანსური თვალსაზრისით
- მაღალი რისკი - სისტემები და მონაცემები, რომელთა არასანქცირებული დათვალიერება, დაკარგვა ან განადგურება საფრთხეს უქმნის ორგანიზაციის ფუნქციონირებას, იწვევს სერიოზულ დარღვევას იურიდიულ და ფინანსურ სფეროში ან საფრთხეს უქმნის ადამიანის ჯანმრთელობას

თითოეული იდენტიფიცირებული რისკითვის, მათი შეფასების შესაბამისად უნდა განხორციელდეს გარკვეული რეაგირება. რისკზე რეაგირება და მასთან მოპყრობა შესაძლოა მოიცავდეს შემდეგს:

- კონტროლის მექანიზმების დანერგვა რისკის შესამცირებლად
- რისკის მიღება შეგნებულად და ობიექტურად, რაც ცალსახად შეესაბამება რისკის მიღების კრიტერიუმს
- რისკების თავიდან აცილება, მათი გამომწვევი მოვლენების არდაშვების შედეგად
- რიკების გადაცემა ასოცირებული მხარეებისათვის, მაგალითად სადაზღვევო, სერვისების მომწოდებლი, ან სხვა ორგანიზაციებისთვის

ინფორმაციული უსაფრთხოების რისკების მართვა უნდა იყოს უწყვეტი პროცესი. პროცესმა უნდა დაადგინოს ორგანიზაციული გარემო, შეაფასოს და გადაჭრას რისკები რისკებთან მოპყრობის გეგმის მიხედვით, რეკომენდაციების და გადაწყვეტილებების დასანერგად. რისკების დასაშვებ დონეზე დაყვანისათვის რისკების მართვა აანალიზებს შესაძლო უარყოფით მოვლენებს და განსაზღვრავს სამოქმედო გეგმას რეაგირების არქონის შემთხვევაში.

ინფორმაციული უსაფრთხოების რისკების მართვამ ხელი უნდა შეუწყოს:

1. რისკების იდენტიფიცირებას
2. რისკებთან მოპყრობის პრიორიტეტულობის დადგენას
3. რისკების შემცირების შესახებ ქმედებების პრიორიტეტულობას
4. რისკებისა და რისკების მართვის პროცესის რეგულარულ მონიტორინგსა და განხილვას

5. რისკების მართვისადმი მიდგომის გაუმჯობესების მიზნით საჭირო ინფორმაციის შეგროვებას
6. მენეჯერებისა და თანამშრომლების ინფორმირებულობას რისკებისა და მათი შემცირების შესახებ.

2. IT უსაფრთხოების პოლისები

2.1 მომხმარებლის კონტროლი

ინფორმაციული უსაფრთხოების წარმატება და წარუმატებლობა მნიშვნელოვნათაა დაკავშირებული თანამშრომლისათვის ინფორმაციაზე წვდომის დონის სწორ მინიჭებაზე. თუ მომხმარებელს მივანიჭებთ საჭიროზე მაღალ წვდომის უფლებას, რამაც შეიძლება გამოიწვიოს ინფორმაციის უსაფრხოების დარღვევა, ხოლო დაბალმა კი სამუშაო პროცესში შეფერხება. შესაბამისად, ინფორმაციაზე, მისი დამუშავების მოწყობილობებსა და პროცესებზე წვდომა უნდა შემოწმდეს საქმიანობის და უსაფრთხოების მოთხოვნების საფუძველზე. თითოეული მომხმარებლისთვის მკაფიოდ უნდა განისაზღვროს ინფორმაციაზე წვდომის წესები. წვდომის კონტროლის მექანიზმები უნდა მოიცავდნენე როგორც ფიზიკური, ასევე ლოგიკური წვდომის კონტროლის მექანიზმებს. იმისათვის რომ შეგვეძლოს ინფორმაციულ სისტემებსა და მომსახურებებზე წვდომის უფლებების კონტროლი, უნდა არსებობდეს პროცედურები, რომელიც მოიცავს მომხმარებელთა წვდომის უფლებების მთლიანი სასიცოცხლო ციკლს, დაწყებული ახალი მომხმარებლის რეგისტრაციიდან, დამთავრებული მისი გაუქმებით. ყველა მომხმარებელს უნდა ჰქონდეს უნიკალური იდენტიფიკატორი (ID, Username) მხოლოდ პირადი გამოყენებისათვის და მომხმარებლის პიროვნების დადასტურებისთვის, შერჩეული უნდა იყოს შესაბამისი აუთენტიფიკაციის მეთოდი. კონტროლის ეს მექანიზმი უნდა იყოს გამოყენებული ყველა ტიპის მომხმარებლისათვის (როგორიცაა ტექნიკური მხარდაჭერის პერსონალი, ოპერატორები, ქსელის ადმინისტრატორები, სისტემის პროგრამისტები და მონაცმენთა ბაზების ადმინისტრატორები). მომხმარებლის ID, Username გამოყენებული უნდა იყოს პასუხისმგებელი პირის ქმედებებზე თავლყურის დევნის მიზნით. მრავალმომხმარებლიან სისტემებში, რომლებიც დაცული უნდა იყვნენ არაავტორიზირებული წვდომისგან, უნდა არსებობდეს მომხმარებელთა უფლებების რეესტრი, რომელიც კონტროლირებადია ფორმალური ავტორიზაციის პროცესის მიერ. უნდა შეიქმნას ზოგადი პროფილითითოეულ მომხმარებლისათვის, რომლისთვისაც წვდომის უფლებები განისაზღვრება საქმიანობის მოთხოვნების შესაბამისად. მსგავსი პროფილებით წვდომის უფლებების მოთხოვნების მართვა გაცილებით მარტივი და მოსახერხებელი ხდება. დადგენილი პერიოდულობით უნდა ხდებოდეს მომხმარებლების წვდომის უფლებების

რეგულარული გადახედვა, რათა შესაძლებელი იყოს ინფორმაციულ მომსახურებებსა და მონაცემებზე წვდომის ეფექტური კონტროლის განხორციელება:

1. თითოეულ მომხმარებელს უნდა მიენიჭოს მომხმარებლის უნიკალური იდენტიფიქატორი (ID, Username)
2. მომხმარებლებს არ უნდა მიენიჭოს ზედმეტი იდენტიფიქატორები (ID, Username);
3. უნდა იყოს განსაზღვრული თითოეულ სისტემასთან წვდომის უფლებები და მომხმარებლები, რომელთაც ეს უფლებები ენიჭებათ
4. წვდომის უფლებები მომხმარებლებს უნდა მიენიჭოს მხოლოდ იმ მინიმალური ოდენობით, რაც საჭიროებიდანაა გამომდინარე
5. ავტორიზაციის პროცესი და წვდომის უფლებების რეესტრი უნდა იყოს შენახული და დაცული
6. წვდომის უფლებები უნდა დაებლოკოს იმ მომხმარებლებს, რომლებმაც დატოვეს ორგანიზაცია.

მომხმარებლებს გაცნობიერებული უნდა ჰქონდეთ საკუთარი პასუხისმგებლობები წვდომის ეფექტიანი კონტროლის მხადაჭერისთვის, განსაკუთრებით პაროლების გამოყენებისას, რომელიც წარმოადგენს მომხმარებლის ნამდვილობის შემოწმების საშუალებას მანამ, სანამ მათ მიეცემათ წვდომა ინფორმაციულ სისტემაზე და მომხმარებელთა მოწყობილობების უსაფრთხოების გათვალისწინებით:

1. პაროლების კონფიდენციალურობის დაცვა;
2. მომხმარებლებს მიეცეთ საკუთარი პაროლის შერჩევისა და შეცვლის შესაძლებლობა
3. ხარისხიანი პაროლების შერჩევა შესაბამისი საკმარისი მინიმალური სიმბოლოები
4. მოხდეს პაროლების შეცვლა რეგულარულად
5. პაროლების დაუყოვნებელი შეცვლა, იმ შემთხვევებში როდესაც არსებობს რაიმე მინიშნება პაროლის შესაძლო საფრთხის ქვეშ დაყენების შესახებ
6. არ უნდა მოხდეს ინდივიდუალური პაროლების გაზიარება.

პაროლები წარმოადგენენ ყველაზე გავრცელებულ წესს იდენტიფიკაციისა და აუტენტიფიკაციის უზრუნველსაყოფად, რაც გასაიდუმლოებულია და მხოლოდ მომხმარებელმა იცის. იმავე შედეგის მიღწევა შესაძლებელია კრიპტოგრაფიული საშუალებებით და აუთენტიფიკაციის ოქმებით. მომხმარებლის იდენტიფიკაციისა და აუთენტიფიკაციის სიმძლავრე უნდა შეესაბამებოდეს იმ ინფორმაციის სენსიტიურობას, რომელზეც ხორციელდება წვდომა.

2.2 ქსელზე წვდომის კონტროლი

ქსელის კონტროლი უზრუნველყოფს ინფორმაციისა და სერვისების უსაფრთხოებას, ქსელებსა და ქსელურ მომსახურებებზე. კომპანიის ქსელის უსაფრთხოება უნდა შეიცავდეს: (1)ქსელში არსებული ყველა მოწყობილობის და კავშირის იდენტიფიცირებას; (2)კომპანიის შიდა ქსელის საზღვრების დადგენას; და (3)კონტროლი, რომელიც უზრუნველყოფს, რომ არასანქცირებული შეღწევის, არასწორად გამოყენების ან სერვისზე უარის თქმის შემთხვევების აღკვეთას, ხოლო მოხდენის შემთხვევაში მათი სწრაფად შეჩერება და აღდგენა იყოს შესაძლებელი. მომხმარებლის წვდომა საფრთხის ქვეშ არ უნდა აყენებდეს ქსელის უსაფრთხოებას, ქსელურ მომსახურებებზე არაავტორიზებულმა წვდომამ და საფრთხის შემცველმა კავშირებმა შესაძლოა გავლენა იქონიოს მთელ ორგანიზაციაზე. კომპიუტერულ ქსელებზე უსაფრთხოების მისაღწევად და შენარჩუნებისთვის საჭიროა კონტროლის მექანიზმები, რომლის მიზანი იქნება შიდა ქსელში არსებული ინფორმაციის და სერვისის დაცვა არასანქცინირებული წვდომისგან ან დაზიანებისგან. კომპანიის შიდა ქსელმა უნდა უზრუნველყოს მხოლოდ იმ სერვისებისა და რესურსების ინტერნეტში ჩართვა, რომლებიც აუცილებელია ბიზნესისა და თანამშრომლების საჭიროებებზე.

დიდი ქსელების უსაფრთხოების კონტროლის ერთ-ერთი მეთოდი არის მისი დაყოფა ცალკეულ დომენებად, რომლიც დაცული იქნება უსაფრთხოების დადგენილი პერიმეტრით. დახარისხებული კონტროლის მექანიზმების ნაკრები შესაძლოა გამოყენებული იყოს სხვადასხვა ლოგიკურ ქსელურ დომენებში, რათა შემდგომ მოხდეს ქსელის უსაფრთხოების გარემოს იზოლირება, მაგალითად, საჯაროდ ხელმისაწვდომი სისტემები, შიდა ქსელები და კრიტიკული აქტივები. დომენები უნდა განისაზღვროს რისკების შეფასების და უსაფრთხოების სხვადასხვა მოთხოვნების საფუძველზე. ამგვარი ქსელური პერიმეტრი შესაძლოა დაინერგოს ორ ქსელს შორის დამცავი ბარიერის, firewall-ის დაინსტალირებით, დამცავი ბარიერი უნდა იყოს დაკონფიგურირებული ისე, რომ გაფილტროს ამ დომენებს შორის ტრაფიკი წინასწარ დადგენილი ცხრილებისა თუ წესების მეშვეობით და დაბლოკოს არაავტორიზებული წვდომა. ლოგიკური დომენების დაყოფის სხვა მეთოდია ქსელური წვდომის შეზღუდვა ვირტუალური პირადი ქსელის გამოყენებით ორგანიზაციის ფარგლებში არსებული მომხმარებელთა ჯგუფისთვის. ასევე უნდა იყოს გათვალისწინებული უსადენო ქსელების შიდა და პირადი ქსელებისგან გამოცალკევება. იმდენად, რამდენადაც უსადენო ქსელების პერიმეტრები არ არის მკაფიოდ დადგენილი.

თუ კომპანია იყენებს უკაბელო ლოკალურ ქსელს (WLAN) სტუმრებისთვის და კლიენტებისათვის, მნიშვნელოვანია, რომ ასეთი WLAN გამოყოფილი იყოს კომპანიის მთავარი ქსელიდან, ისეთნაირად რომ ტრაფიკმა ვერ გადაკვეთოს კომპანიის შიდა სისტემის ნებისმიერი წერტილი საჯარო ქსელიდან. ხოლო შიდა, არასაჯარო WLAN-ზე წვდომა უნდა იყოს შეზღუდული კონკრეტული მოწყობილობების და კონკრეტული მომხმარებლებისთვის.

ქსელების დომენებად დანაწილება უნდა ეფუძნებოდეს ქსელებში დაცული, ან დამუშავებული ინფორმაციის ფასეულობას და კლასიფიკაციას, სანდოობის დონეს, ან საქმიანობის მიმართულებებს, რათა შემცირდეს მომსახურების შეწყვეტით გამოწვეული მთლიანი გავლენა, ასევე უნდა ითვალისწინებდეს შესაბამის ხარჯებსა და წარამდობის გავლენას შესაბამის ქსელურ მარშრუტში ჩართვის, ან დამცავი ბარიერის ტექნოლოგიის თვალსაზრისით.

მნიშვნელოვან კონტროლს მოითხოვს დისტანციური კავშირი კომპანიის შიდა ქსელთან და რესურსებთან, განსაკუთრებით მაშინ, როდესაც დაკავშირებისას გამოიყენება ქსელი/კავშირი, რომელიც არ ექვემდებარება ორგანიზაციის უსაფრთხოების მართვას. დისტანციური მომხმარებლების აუთენტიფიკაცია შესაძლოა განხორციელდეს კრიპტოგრაფიული ტექნიკის, კომპიუტერული ტექნიკის ბარათების ან რეაგირების სხვა ოქმების გამოყენებით. ამგვარი ტექნიკის დანერგვა შესაძლოა შეგვხვდეს სხვადასხვა ვირტუალური პირადი ქსელის (VPN) გადაწყვეტებში. სპეციალურად გამოყოფილი პირადი ხაზები შეიძლება ასევე გამოიყენებოდეს კავშირის წყაროს სანდოობის უზრუნველსაყოფად. აბონენტთან დისტანციური კავშირის პროცედურებმა და კონტროლის მექანიზმებმა, უნდა უზრუნველყოს ორგანიზაციის ინფორმაციის დამუშავების მოწყობილობებთან არაავტორიზებული და არასასურველი დაკავშირების საწინააღმდეგო დაცვა. ამ ტიპის კონტროლის მექანიზმი ახდენს მომხმარებლების აუთენტიფიკაციას, რომლებიც დისტანციურად, ორგანიზაციის გარედან, ცდილობენ დაამყარონ კავშირი ორგანიზაციის ქსელთან. კვანძის (ქსელის) აუთენტიფიკაცია შესაძლოა დისტანციური მომხმარებლის აუტენტიფიკაციის ალტერნატიული საშუალება იყოს, როდესაც ისინი დაკავშირებული არიან უსაფრთხო, ზიარ კომპიუტერულ მოწყობილობებთან. კრიპტოგრაფიული მეთოდები, მაგალითად, მანქანის სერთიფიკატები შეიძლება გამოყენებული იყოს კვანძის აუთენტიფიკაციისთვის. ეს არის სხვადასხვა ვირტუალურ პირად ქსელზე დაფუძნებული გადაწყვეტების ნაწილი.

აუთენტიფიკაციის დამატებითი კონტროლის მექანიზმებია საჭირო უსადენო ქსელებზე წვდომის გასაკონტროლებლად. ზოგიერთ შემთხვევაში, განსაკუთრებული ყურადღებაა საჭირო უსადენო ქსელებისთვის კონტროლის მექანიზმების არჩევის დროს, რადგან არსებობს დიდი ალბათობა და შესაძლებლობა იმისა, რომ მოხდეს ფარული მოსმენა და ქსელის ტრაფიკში ჩართვა.

არსებობს აუთენტიფიკაციის მეთოდის სხვადასხვა ტიპი, ზოგიერთი მათგანი უფრო მაღალი დონის დაცვას უზრუნველყოფს, ვიდრე სხვა დანარჩენი, მაგალითად, კრიპტოგრაფიულ მეთოდებზე დაფუძნებული მეთოდები უზრუნველყოფენ მკაცრ აუტენტიფიკაციას. მნიშვნელოვანია, რისკების შეფასების საფუძველზე განისაზღვროს დაცვის საჭირო დონე, რაც თავის მხრივ, აუცილებელია აუტენტიფიკაციის შესაბამისი მეთოდის შერჩევისთვის.

2.3 ელ-ფოსტის უსაფრთხოება

ელ-ფოსტა წარმოადგენს ბიზნესის განუყოფელ ნაწილს, როგორც შიდა მენეჯმენტში ასევე კლიენტებთან ურთიერთობისას, უპირატესობები, რომლებიც დაკავშირებულია ელ-ფოსტასთან, როგორც ბიზნეს-ინსტრუმენტთან, ბევრად წონის მის ნეგატიურ მხარეებს. მიუხედავად ამისა, უნდა გავითვალისწინოთ, რომ წარმატებული e-mail პლატფორმა ეფუძნება ელფოსტის უსაფრთხოების ძირითად პრინციპებს, უზრუნველყოს კლიენტისა და საქმიანი ინფორმაციის კონფიდენციალურობის დაცვა. ელ-ფოსტა ვირუსების და მავნე კოდის შემცველი პროგრამების გავრცელების ძირითადი მეთოდია, მაგრამ მისის დაცვა საკმაოდ მარტივია. ელ-ფოსტის უსაფრთხოებისათვის გამოყენებული უნდა იქნას ფოსტის ფილტრაციის სერვისი, რომელსაც გვთავაზობს ელ-ფოსტის სერვისის მომწოდებელი, ჰოსტინგ პროვაიდერი, ან სხვა "ღრუბლოვანი" ინფრასტრუქტურის პროვაიდერები. ფოსტის ფილტრაციის ადგილობრივი პროგრამა - ასევე მნიშვნელოვანი კომპონენტია საფუძვლიანი ანტივირუსული სტრატეგიის. უნდა ხდებოდეს იმეილ პროგრამების, ფოსტის ფილტრების და ანტივირუსული პროგრამების, ავტომატური განახლება, და რეგულარულად შემოწმდებოდეს ფილტრები რათა მნიშვნელოვანი იმელები ან/და დომენები არ დაბლოკოს შეცდომით.

ელექტრონული ფოსტა, როგორც კომუნიკაციის ძირითადი ინსტრუმენტი, ორგანიზაციის შიგნით და გარეთ, ხშირად შეიცავს მგრძნობიარე ინფორმაციას. ამიტო მნიშვნელოვანია იმის უზრუნველყოფა, რომ კომპანიის ინფოემაცია, რომელის დაკარგვამ ან გამჟღავნებამ შეიძლება ზიანი მიაყენოს ბიზნესს, გაგზავნილი და ხელმისაწვდომი იქნას მათთვის, ვისთვისაც განკუთვნილია. ამისათვის პოლიტიკამ უნდა განიხილოს რა სახის ინფორმაციის გადაცემა შეიძლება განიხილოს ელ.ფოსტის საშუალებით. ასევე შესაძლებელია განხილული იქნას ელექტრონული ფოსტის დაშიფვრის გამოყენება. ასეთ შემთხვევაში ინფორმაციის მიღება შეუძლიათ მხოლოდ პირებს ან ორგანიზაციებს, რომლებსაც გააჩნიათ შიფრირების გასაღები.

2.4 მავნე კოდისგან დაცვა

პროგრამული ინფორმაცია და ინფორმაციის დამუშავების გარემო მგრძნობიარეა ისეთი მავნე კოდების მიმართ, როგორიცაა კომპიუტერული ვირუსი, ქსელური ჭიები, ტროიანები. მომხმარებლები უნდა აცნობიერებდნენ მავნე კოდებიდან მომდინარე საფრთხეებს, მენეჯერებმა საჭიროების შემთხვევაში უნდა შემოიღონ კონტროლის მექანიზმები, იმისთვის, რომ თავიდან აიცილონ, გამოავლინონ და გაანადგურონ მავნე კოდები. მავნე კოდისგან დაცვა უნდა ეფუძნებოდეს მისი აღმოჩენისა და განადგურების პროგრამულ უზრუნველყოფებს, აგრეთვე სისტემაზე წვდომის კონტროლის შესაბამის მექანიზმებს და ცვლილებების მართვას. ვირუსებისგან, ტროიანებისგვან და სხვა მავნე კოდებისგან დაცვა საჭიროებს მრავალ დონიან უსფრთხოების სიტემას. ანტივირუსული პროგრამული უზრუნველყოფა აუცილებელია, მაგრამ ის არ უნდა იყოს უსაფრთხოების ერთადერთი გარანტი. ვებ ფილტრაცია, ანტივირუსული ხელმოწერები, ეკრანები, ძლიერი უსაფრთხოების პოლიტიკა და თანამშრომელი ტრენინგი მნიშვნელოვნად ამცირებს ინფექციის რისკს. მნიშვნელოვანია ანტივირუსების, ოპერაციული სუსტემების და პროგრამული უზრუნველყოფის მუდმივი განახლება, რის შედეგად იზრდება უსაფრთხოება. სხვადასხვა მომწოდებლისგან მავნე კოდისგან დამცავი ორი ან მეტი პროგრამული პროდუქტის მიღებამ შეიძლება გაზარდოს მავნე კოდისგან დაცვის ეფექტიანობა. მავნე კოდისგან დამცავი პროგრამული უზრუნველყოფა იმგვარად უნდა დავაინსტალირდეს, რომ უზრუნველყოს განმსაზღვრელი ფაილების ავტომატური

განახლება სკანირების მექანიზმების დაცვის სიზუსტის გასაზრდელად. უნდა ვიზრუნოთ დაცვის მექანიზმებზე ტექნიკური მომსახურების, ან საგანგებო ვითარებების პროცედურების დროს, რომლებმაც შეიძლება გვერდი აუარონ დაცვის ჩვეულებრივ საშუალებებს. მავნე კოდისგან დაცვის პოლიტიკა უნდა მიცავდეს შემდეგს:

1. პოლიტიკის შექმნა, რომელიც არ დაუშვებს ისეთი პროგრამული უზრუნველყოფის გამოყენებას, რომელიც არ იქნება ნებადართული
2. მავნე კოდის აღმომჩენი და გამანადგურებელი პროგრამის დაყენება და მუდმივად განახლება კომპიუტერისა და ინფორმაციის მატარებლების სკანირებისთვის,
    - ელექტრონულ ან ოპტიკურ მატარებელზე არსებული, აგრეთვე ქსელიდან მიღებული ნებისმიერი ფაილის შემოწმება;
    - ელექტრონულ წერილებზე მიმაგრებული და ჩამოტვირთული ფაილების შემოწმება გამოყენების წინ; ასეთი შემოწმება სხვადასხვა ადგილზე უნდა განხორციელდეს, მაგალითად ელექტრონული ფოსტის სერვერზე, პერსონალურ კომპიუტერში და ორგანიზაციის ქსელში მოხვედრის დროს;
    - ვებ-გვერდების შემოწმება მავნე კოდის აღმოჩენის მიზნით.

2.5 მობილური ტექნოლოგიები

თუ კომპანიის თანამშრომლები იყენებენ მობილურ მოწყობილობებს, ლეპტოპი, პლანშეტი, მობილური ტელეფონი, კომპანიის საქმიანობისათვის, როგორიცაა კომპანიის ელ.ფოსტის ან მგრძნობიარე მონაცემებზე წვდომა, ყურადღება უნდა მიაქციეს მობილურ უსაფრთხოებას და პოტენციურ საფრთხეებს. მობილური ტექნოლოგიების პოლიტიკა უნდა მოიცავდეს წვდომის კონტროლის მექანიზმების, კრიპტოგრაფიული ტექნიკის, და ვირუსისგან დაცვის მოთხოვნებს. პოლიტიკა უნდა განიხილავდეს ქსელში მობილური მოწყობილობების ჩართვის წესებსა, რეკომენდაციებს და მითითებებს იმის შესახებ, თუ როგორ უნდა ხდებოდეს ამ მოწყობილობების გამოყენება. ყურადღება უნდა დაეთმოს მობილური ტექნოლოგიების გამოყენებას საჯარო ადგილებში, საკონფერენციო ოთახებსა და სხვა დაუცველ ადგილებში ორგანიზაციის ფარგლებს გარეთ. უნდა არსებობდეს არაავტორიზებული წვდომის, ან ამ მოწყობილობებზე შენახული და მათი მეშვეობით დამუშავებული ინფორმაციის გამჟღავნების თავიდან ასარიდებელი დაცვის მექანიზმები,

მაგალითად, კრიპტოგრაფიული ტექნოლოგიების გამოყენება. ასევე უნდა არსებობდეს მავნე კოდის საწინააღმდეგო პროცედურები და უზრუნველყოფილი იყოს მათი განახლება. საჯარო ქსელის მეშვეობით მობილური ტექნოლოგიების გამოყენება ინფორმაციაზე დისტანციური წვდომის განსახორციელებლად მხოლოდ მაშინ უნდა იყოს შესაძლებელი, როდესაც წარმატებულად განხორციელდება იდენტიფიკაცია და აუთენტიფიკაცია.

მობილური ქსელის უსადენო დაკავშირება ისეთივე ტიპის ქსელური კავშირია, როგორც სხვა დანარჩენი, მაგრამ მას ასევე გააჩნია მნიშვნელოვანი განსხვავებები, რაც აუცილებლად უნდა იქნას გათვალისწინებული კონტროლის მექანიზმების დადგენისას. ტიპიური განსხვავებებია:

- ზოგიერთი უსადენო კავშირის უსაფრთხოების ოქმები არ არის ბოლომდე ჩამოყალიბებული და გააჩნიათ სუსტი წერტილები;
- შეიძლება არ მოხდეს მობილურ კომპიუტერებზე შენახული ინფორმაციის სარეზერვო ასლების გადაღება, რადგანაც შეზღუდულია ქსელის გამტარი ხაზი და/ან მობილური აპარატურის დაკავშირება არ ხდება იმ დროს, როდესაც გრაფიკით დაგეგმილია სარეზერვო ასლების გადაღება.

2.6 სარეზერვო ასლების გადაღება

ინფორმაციისა და პროგრამული უზრუნველყოფის სარეზერვო ასელბის გადაღება უნდა ხორციელდებოდეს რეგულარულად და შესაბამისი აპარატურა მუდმივად ხელმისაწვდომი უნდა იყოს ინფორმაციის სარეზერვო ასლების სწრაფი და მარტივი გადაღებისათვის. თავად სარეზერვო ასლები შესაბამისად უნდა იყოს დაცული, მაგალითად, გამოყენებული უნდა იქნას ინფორმაციის დაკარგვის ან დატაცების საწინააღმდეგო დაცვა. კრიტიკული სისტემებისთვის სარეზერვო ასლების გადაღების ღონისძიებები უნდა მოიცავდეს სისტემის სრულ ინფორმაციას, ყველა პროგრამულ პროდუქტს და მონაცემებს, რომლებიც აუცილებელია სისტემის სრული აღდგენისთვის. გათვალისწინებული უნდა იქნას სარეზერვო ასლების შექმნის ადეკვატური საშუალებები იმისათვის, რომ მთელი არსებული ინფორმაცია და პროგრამული უზრუნველყოფა აღდგენილი იქნას უბედური შემთხვევის შემდეგ, ან ინფორმაციის მატარებლის

დაზიანების შემთხვევაში. ინფორმაციის სარეზერვო ასლების გადაღებისას უნდა გავითვალისწინოთ შემდეგი საკითხები:

- უნდა განისაზღვროს ინფორმაციის სარეზერვო ასლების შექნის აუცილებელი დონე;
- სარეზერვო ასლები დაშორებული უნდა იყოს ძირითად ინფორმაციასაგან იმისთვის, რომ არ მოხდეს მათი დაზიანება;
- მნიშვნელოვანი ინფორმაციისთვის უნდა არსებობდეს შენახვის განსაზღვრული ვადები;
- აღდგენის პროცედურები რეგულარულად უნდა შემოწმდეს და გამოიცადოს, იმის უზრუნველსაყოფად, რომ მათი განხორციელება შესაძლებელია დროის განსაზღვრულ შუალედში;
- სარეზერვო ასლების მედია-მატარებლები რეგულარულად უნდა ექვემდებარებოდეს ტესტირებას, იმის უზრუნველსაყოფად, რომ ავარიული გამოყენების დროს გარანტირებული იყოს მათი საიმედოობა;

სარეზერვო ასლების გადაღების ღონისძიებები შეიძლება ავტომატიზირებული იქნას იმისათვის, რომ გაამარტივოს ასლის გადაღებისა და აღდგენის პროცესები. ასეთი ავტომატიზირებული გადაწყვეტები უნდა გადიოდეს ტესტირებას, როგორც უშუალოდ დანერგვის წინ, ასევე პერიოდულად.

2.7 აპარატურის უსაფრთხოება

აპარატურის დაცვა აუცილებელია ინფორმაციაზე არაავტორიზებული წვდომის რისკის შესამცირებლად, ზიანისა და დანაკარგის თავიდან ასარიდებლად, ასევე უნდა ითვალისწინებდეს აპარატურის განთავსებასა და კონტროლს. საჭიროა სპეციალური კონტროლი ფიზიკური საფრთხისგან დაცვის და დამხმარე საშუალებების უსაფრთხოების მიზნით, როგორიცაა ელექტრო ენერგიის მოწოდება და კაბელების ინფრასტრუქტურა. რეკომენდირებულია უწყვეტი ელექტრო კვების (UPS) სისტემის უზრუნველყოფა იმ აპარატურისთვის, რომელიც კრიტიკული ბიზნეს-ოპერაციის მხარდაჭერას ახორციელებს. ელექტრო ენერგიასთან დაკავშირებული გაუთვალისწინებელი შემთხვევების გეგმა უნდა მოიცავდეს იმ ქმედებებს, რომლებიც უნდა განხორციელდეს უწყვეტი ელექტრო კვების

(UPS) სისტემის მუშობის შეფერხებისას. მაქსიმალური უსაფრთხოებისათვის გათვალისწინებული უნდა იყოს სარეზერვო გენერატორი, ელექტრო ენერგიის ხანგრძლივი შეწყვეტის შემთხვევაში. უნდა მოხდეს უწყვეტი ელექტრო-კვების (UPS) სისტემის შემოწმება მწარმოებლის რეკომენდაციების გათვალისწინებით. აპარატურის უსაფრთხოებისათვის გასათვალისწინებელია შემდეგი პრინციპები:

- აპარატურა ისე უნდა დაინსტალირდეს, რომ სამუშაო ზონაში შემცირდეს არააუცილებელი წვდომა;
- აპარატურა, რომელიც განსაკუთრებულ დაცვას მოითხოვს, უნდა იყოს იზოლირებული
- უნდა დაწესდეს შესაბამისი კონტროლი, რათა შემცირდეს პოტენციური ფიზიკური საფრთხის რისკი, მაგ.: ქურდობა, ხანძარი, აფეთქება, წყალი (წყლის მარაგის შეფერხება), კვამლი, მტვერი, ვიბრაცია, ქიმიური ეფექტი, ელექტროენერგიის მიწოდების შეფერხება, ელექტრომაგნიტური რადიაცია და ვანდალიზმი;
- უნდა განხორციელდეს ტემპერატურის, ტენიანობის მონიტორინგი;
- ელექტროენერგიისა და ტელეკომუნიკაციების ხაზები, ინფორმაციის დამუშვების საშუალებები, სადაც შესაძლებელია, მიწის წვეშ უნდა იყოს განთავსებული, ან უზრუნველყოფილ იქნას დაცვის ალტერნატიული საშუალებები;
- ქსელის კაბელი დაცული უნდა იყოს არაავტორიზებული მოსმენისა და დაზიანებისაგან, მაგ.: გადაცემის დაცული არხის გამოყენება, ან მთავარი მარშრუტის საჯარო ადგილებისგან არიდება;
- კვების კაბელები უნდა გამოცალკევდეს კომუნიკაციების კაბელებისგან;

2.8 ადამიანური რესურსების უსაფრთხოება

აუცილებელია რომ, თანამშრომლებამდე მივიტანოთ იდეა, რომ ინფორმაციული უსაფრთხოების უზრუნველყოფა - ყველა თანამშრომლის მოვალეობაა. რაც მიიღწევა მათთვის ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტის გაცნობით და შესაბამის დოკუმენტზე ხელმოწერით. თანამშრომლები უნდა აცნობიერებდნენ ინფორმაცასთან დაკავშირებულ საფრთხეებს, მათ პასუხისმგებლობებსა და ვალდებულებებს, აგრეთვე მზად უნდა იყვნენ ორგანიზაციის უსაფრთხოების პოლიტიკის

მხარდასაჭერად და ადამიანური ფაქტორით გამოწვეული შეცდომის რისკის შემცირებლად. საინფორმაციო უსაფრთხოების ძლიერი პროგრამა უნდა შეიცავდეს IT ტრენინგების პოლიტიკას, უსაფრთხოების შესახებ ტრენინგები, თანამშრომლებს ეხმარება, გააცნობიერონ სისტემის სისუსტეები და საფრთხეები, რომელიც თან ახლავს ბიზნეს ოპერაციებში, ინფორმაციული ტექნოლოგიების გამოყენებას. უნდა განისაზღვროს უსაფრთხოების პროცედურების შესახებ ცოდნისა და სწავლების შესაბამისი დონე და დასაქმებულს, უნდა მიეცეს შესაბამისი ცოდნა ინფორმაციის დამუშავების საშუალებების სწორი გამოყენების შესახებ, რათა შემცირდეს უსაფრთხოების შესაძლო რისკები, უსაფრთხოების ტრენინგებმა უნდა მოიცვას უსაფრთხოების პოლიტიკის ყველა ასპექტი. უნდა ჩამოყალიბდეს ფორმალური დისციპლინარული პროცესი უსაფრთხოების დარღვევების მართვის მიზნით. ორგანიზაციის ყველა თანამშრომელმა, ფუნქციების შესაბამისად უნდა გაიარონ სათანადო ტრენინგი და მიიღონ რეგულარულად განახლებული ინფორმაცია ორგანიზაციის პოლიტიკისა და პრიცედურების შესახებ, ტრენინგები უნდა მოიცავდეს უსაფრთხოების მოთხოვნებს, პასუხისმგებლობებსა და ბიზნეს-პროცესების კონტროლის მექანიზმებს, ინფორმაციის დამუშავების საშუალებების მაგალითად: სისტემაში შესვლის პრიცედურებს, პროგრამული პაკეტების გამოყენების და დისციპლინარული პროცესის შესახებ ინფორმაციებს. აუცილებელია რომ თანამშრომლები:

- გაერკვიონ და დაემორჩილონ უსაფრთხოების პოლიტიკას და პროცედურებს;
- სათანადოდ იყვნენ გაცნობიერებული ინფორმაციული უსაფრთხოების ქცევის წესაბში, იმ სისტემებისადა აპლიკაციებისთვის რომლებთანაც მათ აქვთ წვდომა;
- თანამშრომლობდნენ მენეჯმენტთან ტრენინგების საშუალებით უსაფრთხოების შესახებ ცოდნის ასმაღლებლად;
- იცოდნენ თუ რა ზომებს შეუძლიათ მიმართონ კომპანიის ინფორმაციის უკეთ დასაცავად ეს ზომები მოიცავს: პაროლების სწორ გამოყენებას, ინციდენტების ან უსაფრთხოების პოლიტიკის დარღვევის შესახებ შეტყობინებას, დადგენილი წესების დაცვას, რათა თავიდან იქნას აცილებული სპამის და ვირუსების გავრცელება.

უსაფრთხოების სწავლების უგულვებელყოფა ორგანიზაციას დიდი რისკის ქვეშ აყენებს, რადგან ბიზნესის რესურსების უსაფრთხოება იმდენადაა ადამიანურ გარემოზე დამოკიდებული რამდენადაც ტექნოლოგიურ ინფრასტრუქტურაზე.

ორგანიზაციის ის თანამშრომლები, რომლებმაც უსაფრთხოების ნორმების დაცვის დროს დაუშვეს შეცდომები, ჩართულნი უნდა იყვნენ დისციპლინარულ პროცესში. დისციპლინარულმა პროცესმა უნდა უზრუნველყოს სწორი და სამართლიანი მოპყრობა იმ თანამშრომლების მიმართ, რომლებიც ეჭვმიტანილნი არიან უსაფრთხოების პოლიტიკის დარღვევაში. ასევე უნდა უზრუნველყოს სრულყოფილი პასუხის მიღება იმ საკითხებზე, რომლებიც მოიცავენ ისეთ ფაქტორებს, როგორიცაა დარღვევის ტიპი, სიმძიმე და მისი გავლენა ორგანიზაციაზე, სერიოზული დარღვევისას უნდა დავუშვათ მოვალეობების მყისიერი ჩამორთმევა.

უნდა არსებობდეს პასუხისმგებლობები, რათა დასაქმებულის ორგანიზაციიდან წასვლის პროცესი განხორციელდეს ორგანიზებულად. ასევე უზრუნველყოფილ იქნას დასაქმებულზე გადაცემული მოწყობილობების დაბრუნება და მასზე გაწერილი წვდომის ყველა უფლების ჩამორთმევა. თანამშრომლის სამსახურიდან წასვლისას უნდა გადაიხედოს ინფორმაციულ სისტემაზე წვდომის უფლებები. ამით განისაზღვრება აუცილებელია თუ არა წვდომის უფლებების ჩამორთმევა. სამუშაოსთან დაკავშირებული ცვლილებები უნდა აისახოს წვდომის უფლებების ჩმორთმევაში, რომელიც არ არის დაშვებული ახალი პოზიციისთვის. წვდომის უფლებები, რომელიც თანამშრომელს უნდა, ჩამოერთვას ან მოხდეს მისი ადაპტაცია, გულისხმობს ფიზიკურ და ლოგიკურ წვდომას, გასაღებს, საიდენტიფიკაციო ბარათებს, ინფორმაციის დამუშავების საშუალებებს, მომახმარებელთა ჯგუფებში გაწევრიანება და ნებისმიერი ტიპის დოკუმენტაციიდან ჩამოშორება, რომელიც ახდენს პიროვნების ორგანიზაციის მიმდინარე თანამშრომლად იდენტიფიცირებას. თუ თანამშრომელმა იცოდა მოქმედი მომხმარებლის პაროლი, შრომითი ურთიერთობების შეწყვეტის ან შეცვლის შემდეგ უნდა მოხდეს მათი შეცვლა ან გაუქმება.

3. ინფორმაციული უსაფრთხოების მონიტორინგი

მუდმივად უნდა ხორციელდებოდეს სისტემის მონიტორინგი და ინფორმაციული უსაფრთხოების შემთხვევების ჩაწერა. სისტემის მონიტორინგი უნდა გამოიყენებოდეს იმისთვის, რომ შემოწმდეს კონტროლის დამტკიცებული მექანიზმების ეფექტიანობა. მონიტორინგის პროცედურების გამოყენება აუცილებელია იმისათვის, რომ მომხმარებელმა განახორციელოს მხოლოდ ის ქმედება, რომელიც ცალსახად ნებადართულია. აუდიტის ლოგები, რომლებიც არეგისტრირებენ მომხმარებლების ქმედებებს, ინფორმაციის დაცვის სისტემებში დაფიქსირებულ შემთხვევებსა და გამონაკლისებს, უნდა ინახებოდეს გარკვეული პერიოდის მანძლზე იმისათვის, რომ ხელი შეუწყოს მუდმივ მონიტორინგს ინფორმაცია, რომელსაც ლოგები შეიცავს, დაცული უნდა იყოს საიდუმლო ჩარევისა და არასანქცირებული წვდომისგან და უნდა ხდებოდეს მონიტორინგის შედეგების რეგულარული გადაიხედვა. აუდიტის ლოგები უნდა მოიცავდეს შემდეგს:

1. მომხმარებლების იდენტიფიკატორებს (ID, Username);
2. შემთხვევების თარიღი, დრო და დეტალები,
3. ჩანაწერები სისტემაში შესვლის წარმატებული და წარუმატებელი მცდელობების შესახებ
4. ფაილები, რომლებზეც განხორციელდა წვდომა და წვდომის ტიპი;
5. ქსელური მისამართები და ოქმები;
6. დამხმარე პროგრამებისა და აპლიკაციების გამოყენება;
7. დაცვის სისტემის აქტივაცია და დეაქტივაცია, როგორიცაა ანტი-ვირუსული სისტემები და შეღწევის აღმომჩენი სისტემები.

სისტემური ლოგები ხშირად შეიცავენ დიდი მოცულობის ინფორმაციას, რომლის დიდი ნაწილიც არ განეკუთვნება უსაფრთხოების მონიტორინგის ინტერესის სფეროს. იმისათვის, რომ უსაფრთხოების მონიტორინგისთვის გამოვლენილი იქნას მნიშვნელოვანი შემთხვევები, განხილული უნდა იქნას ჩანაწერების სათანადო ტიპების კოპირება მეორე ჟურნალში ან/და შესაბამისი დამხმარე სისტემური პროგრამების გამოყენება.

3.1 ინფორმაციული უსაფრთხოების ინციდენტების მართვა

კარგად დაგეგმილმა და განხორციელებულმა უსაფრთხოების გეგმამაც კი შეიძლება ვერ შეძლოს ინფორმაციიის დაცვა დაზიანებისგან ამიტომ უნდა არსებობდეს უსაფრთხოების დარღვევებზე რეაგირებისას პროცედურები. უნდა დაინერგოს და განვითარდეს ინფორმაციული უსაფრთხოების შემთხვევებზე რეაგირების მუდმივი მექანიზმი, რომლიც უზრუნველყოფს ინფორმაციული ტექნოლოგიების ინფრასტრუქტურის დაცვას მოახდენს საფრთხეებისა და რისკების სწრაფ იდენტიფიცირებას, მათზე რეაგირებას, საჭიროების შემთხვევაში პრევენციული ზომების გატარებას, პრევენციული, დაცვითი, და აღდგენითი მექანიზმების საშუალებებით. ყველა თანამშრომელს უნდა მოეთხოვებოდეს ინფორმაციული უსაფრთხოების ნებისმიერი შემთხვევის და სისუსტის შესახებ შეტყობინება სპეციალურ საკონტაქტო პირთან რაც შეიძლება სწრაფად. ჩამოყალიბებული ინდა იქნას ინფრმაციული უსაფრთხოების შემთხთხვის შესახებ ანგარიშგების პროცედურა, რაც ასევე მოიცავს ინციდენტზე რეაგირების პროცედურას, რომელიც განსაზღვრავს ინფორმაციული უსაფრთხოების შემთხვევის შესახებ რეაგირების ღონისძიებებს. ქსელისა და სისტემის უსაფრთხოების დარღვევების შემთხვევაში, აღმოფხვრა ჩვეულებრივ ნიშნავს ქსელისგან არასანქცირებული პროგრამების ყველა ინსტანციის მოხსნას და მომხმარებლის დაშვების პრივილეგიების შეჩერებას, რომლიც დაკავშირებულია მავნე აქტივობებთან. ყველა მომხმარებელს უნდა ჰქონდეს გაცნობიერებული პასუხისმგებლობა ნებისმიერი სახის ინფორმაციული უსაფრთხოების შემთხვევების შესახებ მყისიერი რეაგირების თაობაზე. ინფორმაციული უსაფრთხოების შემთხვევებისა და ინციდენტების მაგალითებია:

- მომსახურების, აპარატურისა, ან მოწყობილობის დაკარგვა;
- სისტემის გაუმართაობა, ან გადატვირთვა;
- ადამიანური ფაქტორით გამოწვეული შეცდომები;
- პოლიტიკებთან ან სახელმძღვანელო მითითებებთან შეუსაბამობები;
- ფიზიკური უსაფრთხოების ღონისძიებების დაღვევა;
- არაკონტროლირებადი სისტემური ცვლილებები;
- პროგრამული უზრუნველყოფის, ან კომპიუტერული ტექნიკის გაუმართაობა;
- წვდომის უფლებების დარღვევა.

მას შემდეგ, რაც დაფიქსირდება დარღვევა, ტექნიკურმა პერსონალმა და ბიზნეს გადაწყვეტილების მიმღებებმა უნდა ითანამშრომლონ იმისათვის, რომ გადაწყდეს

ყველაზე პრაქტიკული და ეფექტური შეკავების გეგმა. კომპიუტერულ ინციდენტებზე რეაგირების მომსახურების განყოფილება უნდა ღებულობდეს შეტყობინებას კომპიუტერული ინციდენტის შესახებ, ახდენდეს მის რეგისტრაციას ინციდენტების მართვის სისტემში და დახარისხებას. ინციდენტის რეგისტრაციის შემდეგ უნდა მოხდეს მისი ვერიფიკაცია და პირველადი კლასიფიცირება. ინციდენტის ვერიფიკაციის მიზანია, განისაზღვროს, რამდენად არის ეს შემთხვევა კომპიუტერული ინციდენტი. ინციდენტის პირველადი კლასიფიცირება ხორციელდება ინციდენტის კრიტიკულობის დონის განსაზღვრის მიზნით. ინფორმაციული უსაფრთხოების ინციდენტების შეფასებიდან მიღებული ინფორმაცია გამოყენებული უნდა იქნას მაღალი დონის გავლენის მქონე ინციდენტების, ან გამეორებებთი ინციდენტების გამოსავლენად. ინფორმაციული უსაფრთხოების ინციდენტების შეფასება შესაძლოა მიუთითებდეს კონტროლის დამატებითი, ან გაფართოებული მექანიზმების აუცილებლობაზე, იმისათვის, რომ შეიზღუდოს მათი სიხშირე, ასევე შემცირდეს ზარალი და შემდგომი ხარჯები, ან ეს საკითხები გათვალისწინებული უნდა იყოს უსაფრთხოების პოლიტიკის გადახედვის პროცესში.

ინფორმაციული უსაფრთხოების ინციდენტები შესაძლოა გამოყენებული იყოს მომხმარეებლთა ტრენინგის დროს, როგორც მაგალითი იმისა, თუ რა შეიძლება მოხდეს, როგორი რეაგირება უნდა განხორციელდეს ინციდენტებზე და როგორ ავირიდოთ ისინი მომავალში თავიდან. გაუმართაობები, ან სხვა სახის ანომალური სისტემური ქცევები შესაძლოა იყოს უსაფრთხოებაზე შეტევის, ან უსაფრთხოების დარღვევის ინდიკატორი, ამდენად, უნდა მოხდეს მისი, როგორც ინფორმაციული უსაფრთხოების შემთხვევის ანგარიშგება და მათზე რეაგირება. ინფორმაციული უსაფრთხოების ინციდენტებზე რეაგირებისთვის, მათზე მონიტორინგის განსახორციელებლად, შესაფასებლად და სამართავად უნდა გამოიყენებოდეს უწყვეტი გაუმჯობესების პროცესი.

3.3 ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა

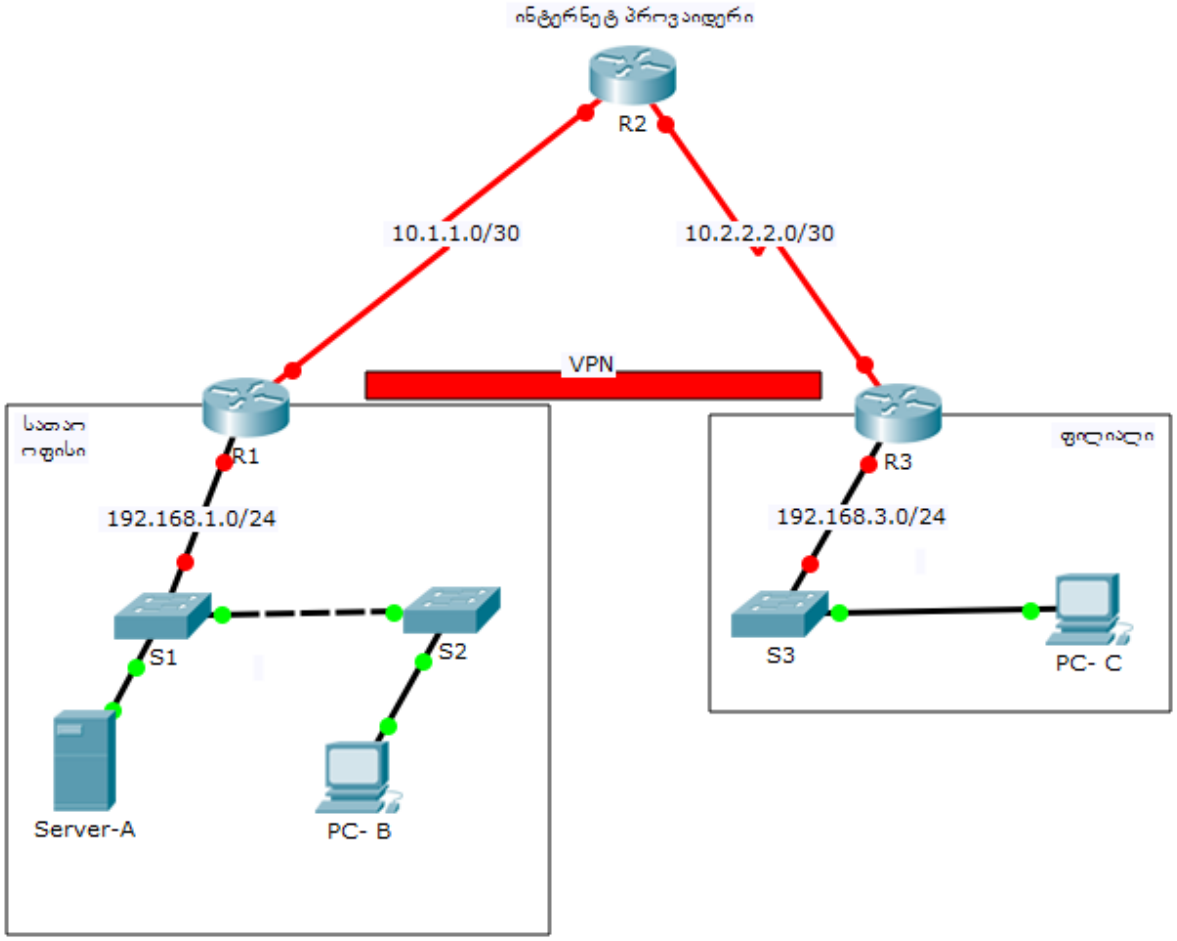
ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა წარმოადგენს დასკვნით ნაწილს უსაფრთხოების პოლიტიკის შექმნასა და უზრუნველყოფაში, განხილვისა და ანალიზის მეშვეობით დგინდება თუ რამდენად მიღწეულია უსაფრთხოების მიზნები.

ინფორმაციული უსაფრთხოების პოლიტიკის განხილვა უნდა მოხდეს დაგეგმილი პერიოდულობით, ან მნიშვნელოვანი ცვლილებების შემთხვევაში, რათა უზრუნველყოფილი იყოს მისი შემდგომი გამოყენებადობა, ადეკვატურობა და ეფექტიანობა. განხილვა უნდა მოიცავდეს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკის გაუმჯობესების შესაძლებლობებს და ინფორმაციული უსაფრთხოების მართვისადმი მიდგომის გარემოს, ბიზნესის მდგომარეობის, საკანონმდებლო, ან ტექნიკური გარემოს ცვლილებების საპასუხოდ.

ინფრორმაციული უსაფრთხოების გეგმები წარმოადგენენ რეალურ, ''ცოცხალ'' დოკუმენტაციას, რომლებიც მოითხოვენ პერიოდულ გადახედვას, განახლებას და ქმედებებს უსაფრთხოების კონტროლის მექანიზმების დასანერგად. ასევე, უნდა არსებობდეს პროცედურები, რომლებიც აფიქსირებენ, თუ ვის მიერ განხორციელდა გეგმის გადახედვა და მოცემული მომენტისათვის ვინ არის გეგმაზე პასუხისმგებელი, ასევე ვინ მეთვალყურეობს პერიოდულად უსაფრთხოების კონტროლის დაგეგმილ მექანიზმებს. ამას გარდა, პროცედურები უნდა ავალდებულებდნენ იმასაც, რომ სისტემის უსაფრთხების გეგმები შექმნილი და გადახედილ იქნას მათთვის უსაფრთოების სერტიფიკატის მინიჭებამდე. უსაფრთხოების სერტიფიცირების დროს ხდება სისტემის უსაფრთხოების გეგმის ანალიზი, განახლება და დამტკიცება. უსაფრთოხების სერტიფიცირების შედეგები გამოიყენება რისკების ხელმეორედ შესაფასებლად და ასევე გეგმის შესადგენად, რომელიც აუცილებელია გამოსასწორებელი სამუშაობის და ასევე უსაფრთხების გეგმის განსაახლებლად. ინფორმაციული უსაფრთხოების პოლიტიკის განხილვის დროს გათვალისწინებული უნდა იყოს მენეჯმენტის მიერ ჩატარებული განხილვების შედეგები. უნდა განისაზღვროს მენეჯმენტის მხრიდან ჩასატარებელი განხილვების პროცედურები, განხილვების პერიოდულობა ან განრიგი. განხილვის შედეგები უნდა მოიცავდეს შემდეგ საკითხებთან დაკავშირებულ გადაწყვეტილებებსა და ქმედებებს:

- ინფორმაციული უსაფრთხოების მართვისადმი ორგანიზაციის მიდგომის და მისი პროცესების გაუმჯობესება;
- კონტროლის მიზნებისა და მექანიზმების გაუმჯობესება;
- რესურსებისა და/ან პასუხისმგებლობების განაწილების გაუმჯობესება.

4. მარსრუტიზატორების და კომუტატორის მინიმალური უსაფრთხოების კონფიგურაცია



პაროლის და გამფრთხილებელი ბანერის კონფიგურაცია მარშრუტიზატორზე

R1(config)#**banner motd $ არასანქცირებული წვდომა აკრძალულია და ისჯება კანონით $**
R1(config)#**security passwords min-length 10**
R1(config)#**enable secret samag12345**
R1(config)#**service password-encryption**

R1(config)#**line console 0**
R1(config-line)#**password samagistro01**
R1(config-line)#**exec-timeout 5 0**
R1(config-line)#**login**
R1(config-line)#**logging synchronous**
R1(config-line)#**exit**

R1(config)#**login block-for 60 attempts 2 within 30**

SSH-ის კონფიგურაცია

R1(config)#**username Admin01 privilege 15 secret Admin01pas01**
R1(config)#**ip domain-name samagistro.com**
R1(config)#**crypto key generate rsa general-keys modulus 1024**
R1(config)#**line vty 0 4**
R1(config-line)#**privilege level 15**
R1(config-line)#**login local**
R1(config-line)#**transport input ssh**
R1(config-line)#**exit**

აუტენთიფიკაციის კონფიგურაციაა AAA და RADIUS სერვერის მეშვეობით

R1(config)#**aaa new-model**
R1(config)#**aaa authentication login default group radius local**
R1(config)#**radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 key WinRadius**

აუტენთიფიკაციის კონფიგურაციაა AAA და RADIUS სერვერის მეშვეობით
R1(config)#**aaa new-model**
R1(config)#**aaa authentication login default group radius local**
R1(config)#**radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 key WinRadius**

CBAC Firewall-ის კონფიგურაცია

R1#**auto secure firewall**

```
--- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of the router, but
it will not make it absolutely resistant to all security attacks ***
AutoSecure will modify the configuration of your device. All
configuration changes will be shown. For a detailed explanation of
how the configuration changes enhance security and any possible side
effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
Gathering information about the router for AutoSecure
Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 unassigned YES unset administratively down down
FastEthernet0/1 192.168.1.1 YES manual up up
Serial0/0/0 10.1.1.1 YES SLARP up up
Serial0/0/1 unassigned YES unset administratively down down
Enter the interface name that is facing the internet: serial0/0/0
Configure CBAC Firewall feature? [yes/no]: yes
This is the configuration generated:
ip inspect audit-trail
ip inspect dns-timeout 7
```

```
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip access-list extended autosec_firewall_acl
permit udp any any eq bootpc
deny ip any any
interface Serial0/0/0
ip inspect autosec_inspect out
ip access-group autosec_firewall_acl in
!
end
Apply this configuration to running-config? [yes]: yes
Applying the config generated to running-config
```

R1(config)#**ip inspect name autosec_inspect icmp timeout 60**
R1(config)#**ip access-list extended autosec_firewall_acl**
R1(config-ext-nacl)#**13 permit tcp 192.168.3.0 0.0.0.255 any eq 22**
R1(config-ext-nacl)#**15 permit udp host 10.1.1.2 host 10.1.1.1 eq ntp**
R1(config-ext-nacl)#**18 permit esp any any**
R1(config-ext-nacl)#**exit**

შემოჭრისგან პრევენციის სისტემის კონფიგურაცია (IPS)

R1#**mkdir ipsdir**
Create directory filename [ipsdir]?
Created dir flash:ipsdir

R1(config)#**ip ips signature-category**
R1(config-ips-category)#**category all**
R1(config-ips-category-action)#**retired true**
R1(config-ips-category-action)#**exit**
R1(config-ips-category)#**category ios_ips basic**
R1(config-ips-category-action)#**retired false**
R1(config-ips-category-action)#**exit**
R1(config-ips-category)#**exit**
Do you want to accept these changes? [confirm] **<Enter>**
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned
R1(config)#**interface serial0/0/0**
R1(config-if)#**ip ips iosips in**

%IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

%IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

R1(config)#**interface fa0/1**
R1(config-if)#**ip ips iosips in**

R1#**copy tftp://192.168.1.3/IOS-S364-CLI.pkg idconf**
R1#**dir flash:ipsdir**
Directory of flash:/ipsdir/
16 -rw- 230621 Jan 6 2008 03:19:42 +00:00 R1-sigdef-default.xml
15 -rw- 255 Jan 6 2008 01:35:26 +00:00 R1-sigdef-delta.xml
14 -rw- 6632 Jan 6 2008 03:17:48 +00:00 R1-sigdef-typedef.xml
13 -rw- 28282 Jan 6 2008 03:17:52 +00:00 R1-sigdef-category.xml
10 -rw- 304 Jan 6 2008 01:35:28 +00:00 R1-seap-delta.xml
18 -rw- 491 Jan 6 2008 01:35:28 +00:00 R1-seap-typedef.xml

VPN-ის კონფიგურაცია

R1(config)#**interface tunnel 0**
R1(config-if)#**ip address 192.168.5.5 255.255.255.0**
R1(config-if)#**tunnel source serial 0/0/0**
R1(config-if)#**tunnel destination 10.2.2.1**
R1(config-if)#**tunnel mode gre ip**
R1(config-if)#**no shutdown**

R1(config)# **access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**

R1(config)# **crypto isakmp policy 10**
R1(config-isakmp)# **encryption aes**
R1(config-isakmp)# **authentication pre-share**
R1(config-isakmp)# **group 2**
R1(config-isakmp)# **exit**
R1(config)# **crypto isakmp key cisco address 10.2.2.1**

R1(config)# **crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac**
R1(config)# **crypto map VPN-MAP 10 ipsec-isakmp**
R1(config-crypto-map)# **set peer 10.2.2.1**
R1(config-crypto-map)# **set transform-set VPN-SET**
R1(config-crypto-map)# **match address 110**
R1(config-crypto-map)# **exit**

R1(config)# **interface S0/0/0**
R1(config-if)# **crypto map VPN-MAP**
R1(config-if)# **exit**

კონფიგურაციის ფაილის ასლის შენახვა

R1#**copy startup-config tftp**
Address or name of remote host []? **192.168.1.3**
Destination filename [R1-confg]? **Configuration**

Writing startup-config....!!
[OK - 1227 bytes]

1227 bytes copied in 3.033 secs (404 bytes/sec)

პაროლის და გამფრთხილებელი ბანერის კონფიგურაცია სვიჩზე

S1(config)#**banner motd $არასანქცირებული წვდომა აკრძალულია და ისჯება კანონით $**
S1(config)#**enable secret samag12345**
S1(config)#**service password-encryption**

S1(config)#**line console 0**
S1(config-line)#**password samagistro01**
S1(config-line)#**exec-timeout 5 0**
S1(config-line)#**login**
S1(config-line)#**logging synchronous**

SSH-ის კონფიგურაცია

S1(config)#**ip domain-name ccnasecurity.com**
S1(config)# **username Admin01 privilege 15 secret Admin01pas01**
S1(config)#**crypto key generate rsa general-keys modulus 1024**
S1(config)#**line vty 0 4**
S1(config-line)#**privilege level 15**
S1(config-line)#**exec-timeout 5 0**
S1(config-line)#**login local**
S1(config-line)#**transport input ssh**
S1(config-line)#**exit**

აუტენთიფიკაციის კონფიგურაციაა AAA და RADIUS სერვერის მეშვეობით

S1(config)#**aaa new-model**
S1(config)#**aaa authentication login default group radius local**
S1(config)#**radius-server host 192.168.1.3 auth-port 1812 acct-port 1813 key WinRadius**

Trunk პორეტის უსაფრთხოება

S1(config)#**interface FastEthernet 0/1**

S1(config-if)#**switchport mode trunk**
S1(config-if)#**switchport trunk native vlan 99**
S1(config-if)#**switchport nonegotiate**
S1(config-if)#**storm-control broadcast level 50**
S1(config-if)#**exit**

Access პორტის უსაფრთხოება

S1(config)#**interface FastEthernet 0/5**
S1(config-if)#**switchport mode access**
S1(config-if)#**spanning-tree portfast**
S1(config-if)#**spanning-tree bpduguard enable**
S1(config-if)#**shutdown**
S1(config-if)#**switchport port-security**
S1(config-if)#**switchport port-security mac-address sticky**
S1(config-if)#**no shutdown**

S1(config)#**interface FastEthernet 0/6**
S1(config-if)#**switchport mode access**
S1(config-if)#**spanning-tree portfast**
S1(config-if)#**spanning-tree bpduguard enable**
S1(config-if)#**shutdown**
S1(config-if)#**switchport port-security**
S1(config-if)#**switchport port-security mac-address sticky**
S1(config-if)#**no shutdown**

გამოუყენებელი პორტების გათიშვა

S1(config)#**interface range Fa0/2 - 4**
S1(config-if-range)#**shutdown**
S1(config-if-range)#**interface range Fa0/7 - 24**
S1(config-if-range)#**shutdown**
S1(config-if-range)#**interface range gigabitethernet0/1 - 2**
S1(config-if-range)#**shutdown**

დასკვნა

ინფორმაციული უსაფრთხოების უზურნველყოფა მოიცავს ისეთ ცნებებს, როგორიცაა ინფორმაციის კონფიდენციალობა, დაცულობა, არასანქცირებული დაშვებისაგან და სისტემის ფუნქციონირების საიმედოობის უზრნველყოფა. ჩვენ უდა განვსაზღვროთ თუ რისი დაცვა გსურს, რა ტიპის საფრთხისგან ვიცავთ და რა საშუალებით ვაპირებთ უსაფრთხოების მიღწევას. ინფორმაციული უსაფრთხოება არ არის უცვლელი მდგომარეობა, რომელიც მიიღწევა ერთხელ და შემდეგ არასდროს იცვლება, არამედ უწყვეტი პროცესი, რომელიც მდგომარეობს დაცვის სისტემის სრულყოფისა და განვითარებისათვის უფრო რაციონალური მეთოდების, ხერხებისა და გზების დაფუძნებასა და რეალიზაციაში, დაცვის სისტემის მდგომარეობის განუწყვეტელ კონტროლში, სისტემის სუსტი ადგილების გამოვლენაში. მნიშვნელოვანი ეფექტი მიიღწევა მაშინ, როცა გამოყენებული მეთოდი, საშუალება და მიღებული ზომები ერთიანდება მთლიან ორგანიზმად – ინფორმაციული უსაფრთხოების სისტემად. ამავე დროს სისტემის ფუნქციონირება უნდა იყოს კონტროლირებადი, განახლებადი და შევსებადი, გარე და შიდა პირობების ცვლილების მიხედვით. უნდა აკმაყოფილებდეს ინფორმაციის უსაფრთხოების მოთხოვნილ დონეს, რისთვისაც საჭიროა მომხმარებელთა მომზადება და მათ მიერ ინფორმაციის დაცვისათვის გამიზნული ყველა წესის დაცვა. აქედან გამომდინარე, შესაძლოა ჩამოვაყალიბოთ მიმართულებები, რომელსაც აუცილებლად ხაზი უნდა გაესვას ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავებისას:

- რისკების შეფასება და ჯგუფებად დაყოფა;
- ინფორმაციაზე წვდომის დაშვება-აკრძალვის პოლიტიკა;
- პაროლების მართვა;
- მომხმარებლის მართვა;
- ინფორმაციული სისტემების ფიზიკური უსაფრთხოება;
- სახიფათო და დავირუსებული პროგრამების დაცვა;
- გარე ინფორმაციული მოწყობილობებისგან დაცვა;
- მონიტორინგი და კონტროლი;
- ინციდენტების მართვა;

აუცილებელია აღინიშნოს, რომ ინფორმაციული უსაფრთხოების მიიღწევა მხოლოდ კონტროლის მექანიზმების დანერგვით არ არის შესაძლებელი და აუცილებელია

დამატებითი მმართველობითი ქმედებები: მონიტორინგი, განხილვა, ინფორმაციული უსაფრთხოების კონტროლის მექნიზმების ეფექტიანობის გაუმჯობესება ორგანიზაციის მიზნების მიღწევის მხარდასაჭერად.

გამოყენებული ლიტერატურა

1. Celia Paulsen, Patricia Toth. Small Business Information Security: The Fundamentals (2016) http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
2. Chaiw Kok Kee. Security Policy Roadmap - Process for CreatingSecurity Policies (2001) https://www.sans.org/reading-room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies-494
3. Frederick M. Avolio, Steve Fallin. PRODUCING YOUR NETWORK SECURITY POLICY (2007) https://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf
4. Jonathan Gana KOLO, Umar Suleiman DAUDA. Network Security: Policies and Guidelines for Effective Network Management. (2008). Leonardo Journal of Sciences, http://ljs.academicdirect.org/A13/007_021.pdf
5. Richard Kissel, Small Business Information Security: The Fundamentals (2009) http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
6. A practical guide to IT : security Ideal for the small business https://ico.org.uk/media/fororganisations/documents/1575/it_security_practical_guide.pdf
7. Cyber Security Planning Guide. Federal Communications Commission https://transition.fcc.gov/cyber/cyberplanner.pdf
8. Network Security Policy: Best Practices White Paper http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html
9. The Complete Guide to Securing Your Small Business (2007) Network Security Journal http://www.networksecurityjournal.com http://www.networksecurityjournal.com/whitepaper/pdf/NSJcompleteguideitsecurity.pdf
10. How to develop a Network Security Policy http://www.windowsecurity.com/whitepapers/policy_and_standards/How_to_develop_a_Network_Security_Policy_.html