ინფორმაციის დაცვა ინფორმაციული ტექნოლოგიების შიდა რისკებისგან

ეკატერინე როჭიკაშვილი, *სტუ-ს პროფესორი*
გულნარა კოტრიკაძე, *სტუ-ს პროფესორი*
ლაურა შავერდაშვილი, *უფროსი მასწავლებელი*

რეზიუმე

შიდა ინფორმაციული ტექნოლოგიების საფრთხეებისაგან თავის დასაცავად პროგრამული და ტექნიკური პროდუქტების შერჩევამდე აუცილებელია ვუპასუხოთ საბაზო კითხვებს - რატომ უნდა დავიცვათ თავი, როგორია შესაძლო დამრღვევის - ინსაიდერის პორტრეტი, და რა თანხების დასახარჯადაა მზად კომპანია დაცვის უზრუნველსაყოფად. ქვემოთ განხილულია ამ კითხვებზე შესაძლო პასუხები და აგრეთვე მოცემულია დასახული მიზნის რეალიზაციის შესაძლო გზები. განხილულია ისეთი ცნება, როგორიცაა სისტემური ლანდშაფტი.

Summary

Information security from internal information threats

Associate Professor
Ekaterine Rochikashvili,

Associate Professor
Gulnara Kotrikadze,

Head teacher
Laura Shaverdashvili

Before to determine by what products it is necessary to be protected from internal IT threats, it is necessary to answer basic questions – why to be protected from them what portrait of the violator and what resources the company is ready to spend for protection against internal threats. In article answers to these questions are given, and also effective ways of implementation of the chosen purpose are offered. such concept as a system landscape is considered.

ძირითადი ნაწილი

შიდა რისკებისაგან თავის დასაცავად პროდუქტების არჩევამდე, ისევე როგორც ნებისმიერი სისტემის დანერგვამდე, აუცილებელია ბაზური საკითხების გარკვევა - რატომ არის საჭირო ამ რისკებისგან თავდაცვა, ვინ არის შესაძლო დამრღვევი და რა რესურსების დახარჯვას აპირებს კომპანია დაცვაზე.

რატომ არის საჭირო დანერგვა და როგორ დავნერგოთ?:

ნორმატიულ სტანდარტებთან შესაბამისობა - აუდიტის პროცესში შემოწმებადი კონტროლის დანერგვა;

ინფორმაციის დაცულობა - ღია დანერგვა საკადრო მუშაობასთან შეთანხმებით;

გადინების არხების გამოვლენა - ფარული დანერგვა;

შიდა საფრთხეების უარყოფა - ქსელური ოპერაციების და მონაცემთა მოძრაობის არქივაცია, იმის დასასაბუთებლად, რომ გადინების სათავე არ არის ფირმის შიგნით.

რეალურად ბევრ ქვეყანაში საბანკო და სადაზღვევო სფეროებში, ბირჟებზე და სხვა ფინანსურ ინსტიტუტებში არსებობს მკაცრი კანონმდებლობა, რომლის შეუსრულებლობაც გამოიწვევს ლიცენზიის ჩამორთმევას ძირითად საქმიანობაზე. ფინანსური ინფორმაციის შემნახავ სისტემებზე წაყენებული მოთხოვნების უმრავლესობას საფუძვლად უდევს ISO სტანდარტების მოთხოვნები და ბაზელის შეთანხმებები. კომპანიები, რომლებიც თავიანთი აქციებით ვაჭრობენ საერთაშორისო ბირჟებზე აქვთ საკუთარი მოთხოვნები. მაგალითად ნიუ-იორკის საფონდო ბირჟა მოქმედებს სანეინს-ოქსლის 2002 წლის აქტის შეთანხმების საფუძველზე, რომელიც აწესებს რეგლამენტს იმ კომპანიის ინფორმაციული სისტემების მართვაში, რომელსაც გამოაქვს სავაჭროდ საკუთარი ფასიანი ქაღალდები. ბოლო წლებში აქტუალური გახდა პერსონალური ინფორმაციის დაცვის საკითხები - მოქალაქეთა პირადი ინფორმაციის კონფიდენციალურობის დარღვევა.

სხვადასხვა ქვეყნებში მოქმედებს სხვადასხვა აქტები: GLBA, HIPAA - პერსონალური ინფორმაციის დაცვის სხვადასხვა ლოკალური აქტები.

ამრიგად შიდა იტ-ის თავდასხმებისგან დაცვის სისტემის მოდელი სტანდარტებშია ჩადებული და მისი დანერგვა პირველ რიგში აუცილებელია იმ პირობით, რომ გაიაროს აუდიტი აღწერილ სტანდარტებთან. ამ დროს სისტემის ფუნქციონირებისას წარმოქმნილი კონფლიქტი ეფექტურობასა და სტანდარტთან შესაბამისობას შორის ყოველთვის მთავრდება სტანდარტების სასარგებლოდ. ამავდროულად არცერთი მარეგულირებელი ორგანო არ იძლევა რეკომენდაციას იმ პროდუქტების შესახებ, რომლითაც ხდება დაცვის ორგანიზება და ზარალის ანაზღაურებაც ხდება ორგანიზაციის თანხებით.

ინფორმაციის დაცულობა - ეს საკითხი აქტუალური ხდება კონფიდენციალური ინფორმაციის გაჟონვის რეალური ინციდენტის შემდეგ. ამ შემთხვევაში შემკვეთი არ არის შეზღუდული სტანდარტებით და თავისუფლად შეუძლია დაეყრდნოს საკუთარ აზრს და არსებულ საშუალებებს ინფორმაციული სისტემის დაცვის აგების საკითხში. ამ შემთხვევაში დაცვის ეფექტურობის ამაღლების მიზნით ტექნიკური საშუალებების დანერგვას თან ახლავს მუშაობა პერსონალთან. ამ პროცესში შედის, როგორც

ინსტრუქტაჟი და ტრენინგი, ასევე ახალ პირობებთან ადაპტაცია, თანამდებობრივი ინსტრუქციების და ინფორმაციული სისტემის გამოყენების რეგლამენტის შეცვლა.

ფსიქოლოგიური ფაქტორი მუშაობს ინფორმაციის დაცვაზე. იციან რა, რომ მათი მოქმედება კონტროლდება, ბევრი პოტენციური დამრღვევი უარს ამბობს უსაფრთხოების პოლიტიკის დარღვევის განზრახვაზე. ამიტომ ასეთი სისტემის დანერგვას თან უნდა სდევდეს გახმოვანებული ღონისძიებები, შიდა უსაფრთხოების პოლიტიკა კი ბრძანებით უნდა იყოს დანერგილი. მაგრამ კონკრეტული ტექნოლოგიური გადაწყვეტილება უნდა იყოს დაცული გახმოვანებისაგან, რათა არ მოხდეს მუშაობა სისტემის წინააღმდეგ.

ინფორმაციის გაჟონვის არხების და წყაროების გამოვლენა - ეს მიზანი დგება შემკვეთის წინაშე თუ ინფორმაციული სისტემიდან რეგულარულად ხდება ინფორმაციის გაჟონვა. დანერგვის ეს ტიპი რადიკალურად განსხვავდება წინა განხილულისგან. პირველ რიგში აქცენტი აღებულია ფარულ დანერგვასა და მტკიცებულებების შეგროვებაზე. ხშირად ფარული დანერგვის დროს შესაბამისი პროგრამული უზრუნველყოფის დაყენების შეფუთვა (მასკირება) ხდება უსაფრთხოების არსებული სისტემის განახლების სახით, მაგალითად ანტივირუსის დაყენება.

მონაცემების შეგროვება - ასეთი დანერგვის არანაკლებ წონიანი ნაწილია, რათა არამარტო ამოვლინდეს გაჟონვის წყარო, არამედ დაისაჯოს დამრღვევი არსებული კანონმდებლობით. მონაცემთა შეგროვების იურიდიული ბაზა ყველა ქვეყანაში განსაზღვრულია კანონმდებლობით. მთლიანობაში სიტუაცია ასე გამოიყურება: ციფრული მტკიცებულებების შეგროვება (დაშვების ჟურნალები, წერილების ასლები და სხვა) მკაცრად რეგლამენტირდება კანონმდებლობის მიერ. ხშირად მტკიცებულებების აღიარებისათვის საჭიროა სპეციალური წესით სპეცსამსახურების მიერ დაღადაღებული სერვერი, რომელზეც სპეცსამსახურის გარდა არავის აქვს დაშვება. ამ შემთხვევაშიც მითითება შეიძლება მხოლოდ საფოსტო ყუთზე, სააღრიცხვო ჩანაწერზე, IŞ მისამართზე და სხვა. იმის მტკიცება, რომ დარღვევის დროს კომპიუტერთან იმყოფებოდა კონკრეტული ადამიანი ძალიან რთულია. უდანაშაულობის პრეზუმპციიდან გამომდინარე დანაშაულზე პასუხისმგებელია ხელმძღვანელი. ასეთ დროს შეიძლება გამოყენებული იქნას ისეთი ტექნიკური საშუალებები, როგორიცაა ბიომეტრიული გასაღებები და ვიდეოდაკვირვება.

კონკურენტული უპირატესობის შექმნა - ამ მიზანს უფრო ხშირად ისახავენ ინფორმაციის შემკრები საწარმოები - მონაცემთა ცენტრები, აუდიტორული კომპანიები, გამოძახებების მართვის ცენტრები (ცალლ - ცენტრები) და ა.შ. ამ შემთხვევაშიც დანერგვა ხდება ღიად, იმ განსხვავებით, რომ კომპანიას შეეძლოს კლიენტს მიაწოდოს ნებისმიერი ინფორმაცია მის მონაცემებზე წარმოებულ მოქმედებებზე.

სისტემური ლანდშაფტი - მას შემდეგ, რაც მომხმარებელი ჩამოყალიბდება პროექტის მიზანზე, ხდება სისტემური ლანდშაფტის - ტექნიკური საშუალებების და წესების, რომლებიც შეიძლება არსებობდნენ კომპანიაში, კომპლექსის აღწერა.

მომხმარებლების უფლებები - არ არსებობს მომხმარებლების სამუშაო ადგილებზე მიმდინარე პროცესების სტანდარტიზაციის ერთიანი პოლიტიკა. ეს ნიშნავს, რომ მომხმარებლების ნაწილი სარგებლობენ ლოკალური ადმინისტრატორის უფლებებით. ასეთი მომხმარებლები ძირითადად ერთიანდებიან მომხმარებელთა ორ ჯგუფში - მოძველებული ოპარაციული სისტემის მომხმარებლები (MS Windows 98) და ნოუთბუქების მომხმარებლები. ეს აგრეთვე ნიშნავს, რომ კონფიდენციალური დოკუმენტების ასლები ინახება სამუშაო ადგილებზე. ამას გარდა სამუშაო ადგილებზე მოქმედებს პოტენციურად საშიში პროგრამული უზრუნველყოფა - ფაილური მენეჯერები, რომლებმაც შეიძლება ჩაატარონ ოპერაციები ჭინდოწს-ის დროებით ფაილებზე, სინქრონიზაციის პროგრამები, შიფრაციის პროგრამები და ა.შ.

მოხმარებლების კვალიფიკაცია - მომხმარებლების კვალიფიკაცია ყოველწლიურად მატულობს. ისინი იძენენ უნარებს, რომელიც შეიძლება სახიფათო აღმოჩნდეს კომპანიის ინფორმაციული უსაფრთხოებისათვის. დღეს რიგით მომხმარებელს შეუძლია პროგრამების დაყენება, პროცესების მოხსნა, მობილური ინტერნეტით სარგებლობა, ინფორმაციის გადაცემა დაშიფრული სახით და ა.შ.

დაცვის საშუალებები - ძირითადი დაცვის საშუალებებია: რესურსებზე (ინტერნეტი, კორპორატიული ფოსტა, USB) დაშვების/წვდომის კონტროლის ტექნიკური გადაწყვეტილებები, კონტენტური სიგნატირული ფილტრაცია (ძირითადად სპეციალური წესით აწყობილი ანტისპამ-ფილტრი). მაგრამ ეს მეთოდები ქმედუნარიანია ძირითადად მხოლოდ ნაკლებკვალიფიცირებული ან არაფრთხილი დამრღვევების წინააღმდეგ. სიგნატურული კონტენტური ფილტრაციის თავიდან აცილება შესაძლებელია „საშიში“ სიტყვების პრიმიტიული ამოშლით ან ელემენტარული კოდირებით, რომელიც არ მოითხოვს შიფრაციის სპეციალური პროგრამების გაშვებას - მაგალითად, კოდირების ერთი ნაწილის სიმბოლოების (მაგ.: დასავლეთევროპული) სხვა ნაწილის მსგავსი სიმბოლოებით შეცვლა (მაგ.:კირილიცა), ასო-ბგერების შეცვლა ციფრებით, ტრანსლიტერირება და ა.შ. აკრძალული დაშვება ჩვეულებრივ ხორციელდება სამუშაო აუცილებლობის იმიტაციით - ჩვენ ხომ იტის შიდა უსაფრთხოებაზე ვსაუბრობთ. ე.ი. მეთოდი „ავკრძალოთ ყველაფერი“ მიუღებელია, ეს ყველა პროცესის შეჩერებას გამოიწვევს.

დასკვნა

ამრიგად კომპანიებს აქვთ აუცილებლობა ერთის მხრივ მოაწესრიგონ კონფიდენციალური ინფორმაციის შენახვა, ხოლო მეორეს მხრივ დანერგონ დაცვის მეტად დახვეწილი სისტემა.

გამოყენებული ლიტერატურა:

1. https://www.infowatch.ru/products
2. https://infowatch.com/
3. http://www.cnews.ru/reviews/free/insiders2006/articles/organizational.shtml
4. http://www.iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov/kak-zaschischatsya-ot-insaidera