ინფორმაციულ სისტემებში კონფიდენციალური ინფორმაციის დაცვის პროგრამული და არატექნიკური საშუალებები

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

რეზიუმე

ინფორმაციის დასაცავად ინფორმაციული სისტემების შიდა რისკებისგან, სა-ჭიროა ელექტრონულ ფორმატში მოცემულ კონფიდენციალურ ინფორმაციასთან მუშაობის რეგლამენტირების, ამ ინფორმაციის კლასიფიკაციის და შენახვის თავისებურებების გაცნობა. არასანქცირებული დაშვებისაგან კონფიდენციალური ინფორმაციის დასაცავად გამოიყენება, როგორც არატექნიკური, ფსიქოლოგიური და ორგანიზაციული, ასევე ტექნიკური ღონისძიებები. განხილულია ტექნიკური ღონისძიებების ფარგლებში Infowatch გადაწყვეტილებების მუშაობის პრინციპები და მახასიათებლები.

საკვანძო სიტყვები: ჟურნალირება, ინტერნეტი, ინსაიდერი, აქტიური მომხმარებელი, გაჟონვის არხი, RFID, კონსოლი.

Program and nontechnical means of protection of confidential information in information systems

Associate Professor
Ekaterine Rochikashvili,

Associate Professor
Gulnara Kotrikadze,

Head teacher
Laura Shaverdashvili

Summary

To protect information from internal risks of information systems, it is necessary to get acquainted with the regulation of work with confidential information, the peculiarities of classification and storage of this information. for protection of confidential information against nesanktsirovanny access are trampled down as nontechnical - psychological and organizatsionny, also tekhnichesly measures. Rassmotreni the principles of work the solved InfoWatch within technical measures.

Keywords: Logging, intranet, insider, active user, information leakage channel, RFID, console.

ძირითადი ნაწილი

კონფიდენციალური ინფორმაციის შენახვის მეთოდები. კორპორატიულ საინფორმაციო ქსელში შენახული კონფიდენციალური ინფორმაციის დასაცავად უნდა განისაზღვროს კონკრეტულად რას ვიცავთ და რატომ ვიცავთ. უნდა განი-საზღვროს რა არის კონფიდენციალური და დაინერგოს მომხმარებელთა სხვადასხვა ჯგუფისათვის მასზე დაშვების წესები. ყველა კომპანიაში უნდა არსებობდეს კონფიდენციალურ ბეჭდურ მონაცემთან მუშაობის წესები. დაცვის პირველი ამოცანაა ამ მეთოდების ადაპტირება ელექტრონული დოკუმენტებისათვის, რაც ფაქტიურად დაიყვანება შემდეგი მოქმედებების (რომელიც არ გვაქვს ქაღალდზე არსებულ დოკუმენტებთან მიმართებაში) — დოკუმენტის ასლი, დოკუმენტის ნაწილი და ა.შ. რეგლამენტირებამდე. განისაზღვრება დოკუმენტის სასიცოცხლო ციკლი – სად იქმნება, ვინ და როგორ მოიხმარს, ვინ და რა პირობებში აკორექტირებს, რახნით ინახება და როგორ ნადგურდება.

აქ არის ნიუანსები, რომელიც ეხება ელ-ფოსტით მიმოწერას. რეგლამენტი მკაცრად არეგულირებს კონფიდენციალური ინფორმაციის შემცველი დოკუმენტების გადაგზავნას. კომპანიაში აუცილებლად უნდა განისაზღვროს ინფორმაციის ტიპები, რომლის გადაგზავნა ელ-ფოსტით იკრძალება. თითქმის ყველა კომპანიაში არის ინფორმაციის სტანდარტული ნაკრები, რომლის კორპორატიული ფოსტით გაგზავნაც ერთ განყოფილებას შეუძლია და მეორეს არა. კონფიდენციალური ინფორმაციის შემცველი დოკუმენტების გამოყენების რეგლამენტი უნდა ასახავდეს მისი შენახვის და მასზე დაშვების ორგანიზაციის სისტემის აღწერას. მაგალითად, წასაკითხად ან კორექტირებისათვის დოკუმენტზე დაშვების მიღებამდე თანამშრომელმა უნდა მიუთითოს რის საფუძველზე და რა მიზნით აპირებს დოკუმენტზე მიმართვას, რა მოქმედება უნდა შეასრულოს მასზე, როდის დაასრულებს დოკუმენტზე მუშაობას და ა.შ. ელექტრონული მონაცემების შემთხვევაში დოკუმენტებთან მუშაობის “ჟურნალი”-ს წარმოება გაცილებით იოლია, რადგან ოპერაციების უმეტესობა (მაგალითად, დაშვების და კორექტირების უფლებების შემოწმება, მუშაობის დროის ათვლა და შესწორებების კონტროლი) შესაძლებელია განხორციელდეს ავტომატურად. ტერმინი ჟურნალირების პარალელურად, შეიძლება შეგვხვდეს ტერმინი ლოგირება.

უნდა განისაზღვროს რომელი დოკუმენტია კონფიდენციალური და რომელ თანამშრომელს რა

დონის დაშვება აქვს მათზე — იქმნება კონფიდენციალური დოკუმენტების ე.წ. რეესტრი, რომელიც აგრეთვე განსაზღვრავს დაშვების, რეესტრში დოკუმენტების შეტანის და შეცვლის (ან განადგურების) წესებს. ვინაიდან ყოველდღიურად იზრდება დოკუმენტების რაოდენობა მათი ავტომატური კლასიფიკაციის მექანიზმის გარეშე რეესტრი დაკარგავს აქტუალობას.

თითოეული კონფიდენციალური დოკუმენტი უნდა შეიცავდეს ჭდეს, რომლის მიხედვითაც მაკონტროლებელი პროგრამა განსაზღვრავს კონფიდენციალობის ხარისხს და მომხმარებლის კატეგორიას, რომელსაც შეუძლია პოტენციურად საშიში ოპერაციის განხორციელება — ინტერნეტში გამოქვეყნება, კოპირება სხვადასხვა მატარებლებზე, სახელის შეცვლა, ელ-ფოსტით გადაგზავნა და ა.შ. თუ დაცული დოკუმენტები ინახება MS Office ფორმატში, ჭდის როლში შეიძლება გამოყენებული იქნეს დოკუმენტის თვისებების შესაბამის ველში არსებული ჩანაწერი "კონფიდენციალურია". შეიძლება გამოყენებულ იქნას პროგრამული ჭდეები და ფაილების სპეციალური ფორმატები. დაჭდევების ყველაზე გავრცელებული და მარტივი მეთოდია ფაილებზე სახელების მინიჭება სპეციალური ნიღბით. ამ პროცედურის დანერგვის ყველაზე მარტივი გზაა დოკუმენტის ფაილის ფაილურ სერვერზე განთავსების, კორპორატიულ საცავში შენახვის ან ინტრანეტში გამოქვეყნების საშუალება მიეცეს მხოლოდ წინასწარ განსაზღვრული შაბლონის მიხედვით სახელის დარქმევის შემდეგ. დროთა განმავლობაში ყველა ფაილს, რომელმაც გაიარა ელ-ფოსტა, ფაილური სერვერი, მონაცემთა საცავი ან ინტრანეტი, სწორად ექნება მინიჭებული სახელი. ასეთი დოკუმენტი მასზე დაუშვებელი მოქმედების შესრულების შემდეგ ავტომატურად ხვდება მაკონტროლებელი სისტემების ხედვის არეში არა კონტენტური ფილტრაციის გზით არამედ უსაფრთხოების პოლიტიკის საფუძველზე მოქმედი მონიტორების დახმარებით. კონტენტური ფილტრაციისგან განსხვავებით ეს მოთოდი იძლევა 100%-იან გარანტიას. ეს მოსახერხებელია ვიზუალური კონტროლისთვისაც — ბეჭდვის რიგშიც შესაძლებელია კონფიდენციალური დოკუმენტების დანახვა.

რეესტრის შექმნის შემდეგ ხდება ინფორმაციის შენახვის ორგანიზება. მსხვილ კომპანიებში აკრძალულია კონფიდენციალური ინფორმაციის შენახვა ლოკალურად, სამუშაო ადგილებზე. ჩვეულებრივ ასეთი მონაცემები ინახება სპეციალურ კლიენტ-სერვერულ ან web-დანართებზე (კორპორატიულ ინტრანეტ-პორტალებზე, დოკუმენტურ საცავებში, ბიზნეს-დანართებზე, საცნობარო-ნორმატიულ ბაზებში, დოკუმენტბრუნვის სისტემებში და ა.შ.) რომლებიც განასხვავებენ მომხმარებელთა დაშვების უფლებებს და იცავენ ინფორმაციას არასანქცირებულ ადგილზე შენახვისგან. შერვერზე ასეთი მონაცემების დაცვა მრავალდონიანია (აპარატული პლატფორმის, ოპერაციული სისტემის, მონაცემთა ბაზების მართვის სისტემის და დანართის დონეზე). მაგრამ სამუშაო ადგილებიდან ინფორმაციის გაჟონვის ალბათობა მაინც არსებობს.

დაცვის ძირითადი მიმართულებები. რადგან ყველა თანამშრომელი, რომელსაც აქვს ინფორმაციაზე წვდომის უფლება, პოტენციური დამტაცებელია, მეთოდები იგეგმება იმის გათვალისწინებით, რომ დაცული იყოს ბალანსი ინფორმაციის ლეგალური გამოყენებისათვის ხელმისაწვდომობასა და გაჟონვისგან მის დაცვას შორის.

ელექტრონული დოკუმენტაციის დაცვის ბიზნეს-პროცესის მაგალითად, აღებულია ბეჭდვით დოკუმენტებთან მუშაობის მეთოდები. ელ-დოკუმენტის სასიცოცხლო ციკლის კონტროლის ფუნქციის ნაწილი ავტომატიზებულია. ამ ნაწილში აქტიურად გამოიყენება დოკუმენტების შიფრაცია და ფაილის სპეციალური ფორმატები, რომელიც კრძალავს დოკუმენტის სხვა ფორმატში შენახვას, რედაქტირებას ან შიგთავსის კოპირებას Windows ბუფერში, მაგალითად unsearchable PDF ან MS Office ახალ ფორმატში.

ეფექტურია კომპანიის ტერიტორიაზე ინფორმაციის ფიზიკური მატარებლების კონტროლი. მაგრამ მატარებლების ზომის სულ უფრო შემცირების გამო ეს მეთოდი ნაკლებეფექტური ხდება. ამიტომ უფრო მისაღებია დოკუმენტების დაცვა კოპირებამდე.

მნიშვნელოვანია არამარტო ის თუ ვის აქვს დაშვების უფლება დოკუმენტზე, არამედ ისიც თუ რა მოქმედებების შესრულებას აპირებს ეს მომხმარებელი. სხვადასხვა მომხმარებელმა ერთიდაიგივე დოკუმენტი სხვადასხვაგვარად შეიძლება გამოიყენოს (წაკითხვა, რედაქტირება და ა.შ.) მნიშვნელოვანია იმ მოქმედებების კონტროლი, რომელმაც შეიძლება ინფორმაციის გაჟონვამდე მიგვიყვანოს. ეს არის მოქმედებების სამი ჯგუფი: პირველია ფაილების კოპირება გარე მატარებლებზე, ფოსტით გაგზავნა, ინტერნეტში გამოქვეყნება, ბეჭდვა. მეორეა — დოკუმენტებიდან ინფორმაციის კოპირება Windows — ის ბუფერში, დროებითი ფაილის კოპირება და ა.შ. მესამე ჯგუფს განეკუთვნება ფაილის სახელის ან გაფართოების შეცვლა, შენახვა სხვა ფორმატში, არქივირება, კოდირება, დაშიფვრა. კონტროლის მეთოდის მიხედვით კონფიდენციალურ ფაილზე კონკრეტული მომხმარებლისათვის დაუშვებელი ოპერაცია ან იბლოკება, ან მასზე ინფორმაცია გადაეცემა უსაფრთხოების ოფიცერს.

კონფიდენციალური ინფორმაციის გაჟონვაში მონაწილე თანამშრომლები კლასიფიცირდებიან რამოდენიმე კრიტერიუმით — წინასწარგანზრახული ან დაუდევარი, საკუთარი მიზნებით ან სხვისი დაკვეთით მოქმედი, კონკრეტულ ინფორმაციაზე მონადირე ან დაინტერესებული სრული ინფორმაციით. სწორი კლასიფიკაციის შემთხვევაში შესაძლებელია მოქმედებების პროგნოზირება. გარდა ამისა დაცვის საშუალებების შერჩევისას გათვალისწინებული უნდა იქნას კონკრეტული დამრღვევის ტიპი.

შიდა საფრთხეებისაგან დაცვის არატექნიკური

ღონისძიებები. თუ დაცვის სისტემის დანერგვის ძირითადი მიზანია გაჟონვის არსებული არხების, მისი ყველა რგოლის, კომპანიის შიგნით არსებული შემსრულებლებისა და შემკვეთების გამოვლენა, მაშინ მიზანშეწონილია პირველ რიგში მომხმარებელთა აქტივობის მონიტორების და ფოსტის კონტენტური ფილტრაციის გამოყენება. ამ შემთხვევაში მისაღებია სამუშაო ადგილებზე პროგრამული აგენტების დაყენება და მათი შენიღბვა სხვა პროგრამების სახით, მაგალითად ანტივირუსი ან პროგრამული უზრუნველყოფის აუდიტის მონიტორი. თუ დაცვის სისტემა აშკარად დაინერგება (მაგალითად ვიდეოკამერები) ფსიქოლოგიური ფაქტორის გავლენით შესაძლებელია საკმაოდ დიდი ეკონომიის მიღება.

უსაფრთხოების სისტემის მუდმივი ტესტირების გარდა აუცილებელია პოტენ-ციური დამრღვევების შესაძლებლობების შეზღუდვა, პირველ რიგში მომხმარებელს არ უნდა ქონდეს ლოკალური ადმინისტრატორის უფლება თავის სამუშაო ადგილზე, ამ შემთხვევაში აუცილებელია პროგრამული უზრუნველყოფა, რომელსაც შეეძლება იმ ოპერაციულ სისტემებთან მუშაობა, რომლებსაც აქვთ დაშორებული მართვის მხარდაჭერა.

დასაშვები პროგრამული უზრუნველყოფის ჩამონათვალის შედგენის შემდეგ, აუცილებელია ყველა სამუშაო ადგილზე მათი დაყენება და სხვა ნებისმიერი პროგრამის გაშვების აკრძალვა ადმინისტრატორის ნებართვის გარეშე (მაგალითად ოპერაციულ სისტემაში ჩაშენებული Windows Explorer ნაკლებად მოხერხებულია, მაგრამ იგი ჭინდოწს დროებითი ფაილების კოპირების საშუალებას არ იძლევა).

მცირე ორგანიზაციული ღონისძიებებით შესაძლებელია დიდი პრობლემების გადაწყვეტა — თუ მონაცემთა ბაზიდან ყოველდღიური მოთხოვნების მოცულობის ლიმიტი შემცირდება ისე, რომ მის გადმოსაქაჩად (ბაზის მოცულობიდან გამომ-დინარე) საჭირო იქნება არაერთი სამუშაო დღე. ამ შემთხვევაში ნაწილ-ნაწილ, სხვა და სხვა დღეს გადმოწერილი ინფორმაცია, ბაზის ყოველდღიური განახლების ფონზე კარგავს აქტუალობას.

თანამშრომლების სწავლებები და ინსტრუქტაჟი ეხმარება ინფორმაციის დაცვის საკითხს. ამასთან ერთად თანამშრომლის მაღალი კომპიუტერული კვალიფიკაცია ზოგჯერ უფრო სერიოზული ნაკლია ვიდრე არასაკმარისი კვალიფიკაცია (ნამდვილად არასაჭიროა ბუღალტერიის თანამშრომელი ფლობდეს სისტემური ადმინისტრატორის უნარებს).

სარეზერვო ასლების ფიზიკური მატარებლებით გატანა არის ინფორმაციის გაჟონვის კიდევ ერთი არხი. ამ არხის დასაცავად გამოიყენება მატარებლების ანონიმიზაცია — ინფორმაციაზე წვდომის მქონე თანამშრომლებისათვის უცნობია, რომელ მატარებელზე რომელი ინფორმაციაა ჩაწერილი, მიმართვა ხდება მხოლოდ ანონიმური ნომრებით. იმ თანამშრომლებს კი, რომლებმაც იციან სად რა ინფორმაციაა ჩაწერილი არ აქვთ მატარებლების საცავთან დაშვება. დაცვის მეორე ვარიანტია, სარეზერვო ასლების შექნისას ინფორმაციის შიფრაცია.

InfoWatch-ის პროგრამული გადაწყვეტები: ეს გადაწყვეტები ემყარება ორ ძირითად ტექნოლოგიას — კონტენტის ფილტრაცია და სამუშაო ადგილებზე მომხმარებლის ან ადმინისტრატორის მოქმედებების აუდიტი. აგრეთვე Iნფოჭატცჰ-ის კომპლექსური გადაწყვეტების შემადგენელი ნაწილია ინფორმაციული სისტემიდან გამოსული ინფორმაციის საცავი და შიდა უსაფრთხოების მართვის ერთიანი კონსოლი.

InfoWatch კონტენტური ფილტრაციის ძირითადი განსხვავებაა მორფოლოგიური ბირთვის გამოყენება. ტრადიციული სიგნატურული ფილტრაციისაგან განსხვავებით ამ ტექნოლოგიას აქვს ორი უპირატესობა — ელემენტარული კოდირებისადმი (ერთი სიმბოლოების მეორეთი შეცვლა) არამგრძნობიარობა და უფრო მაღალი ქმედუნარიანობა. რადგან ბირთვი სიტყვების ნაცვლად მუშაობს ფუძის ფორმებზე, იგი ავტომატურად პოულობს ფუძეებს, რომლებიც შერეულ კოდირებას შეიცავენ. ასევე ფუძესთან მუშაობა, რომლებიც ნებისმიერ ენაში ათი ათასს არ აჭარბებს, სიტყვის ფორმებთან მუშაობასთან შედარებით, რომელთა რაოდენობაც მილიონს აღწევს, მნიშვ-ნელოვანი შედეგების მიღების საშუალებას იძლევა საკმაოდ დაბალი ქმედუნა-რიანობის მქონე ტექნიკის გამოყენების დროსაც.

მომხმარებლის მოქმედებების მონიტორინგისათვის InfoWatch გვთავაზობს რამოდენიმე ინტერცეპტორს (დამჭერს) — ფაილური ოპერაციების, ბეჭდვის ოპერაციების, დანართების შიგნით ოპერაციების, მიერთებულ მოწყობილობებთან ოპერაციების ინტერცეპტორები სამუშაო ადგილზე ერთ აგენტში.

ყველა დოკუმენტი, რომელმაც გაიარა ინფორმაციული სისტემიდან გამავალი რომელიმე არხი — ელ-ფოსტა, ინტერნეტი, ბეჭდვა, გარე მატარებლები, ინახება *storage დანართში ყველა ატრიბუტის მითითებით — მომხმარებლის სახელი, გვარი, თანამდებობა, ელ-პროექციები (სააღრიცხვო ჩანაწერის და ელ-ფოსტის IP —მისამართები) ოპერაციის შესრულების თარიღი და დრო, დოკუმენტის სახელი და ატრიბუტები.

კონფიდენციალური ინფორმაციის დაცვის ტექნიკური საშუალებების დანერგვა ნაკლებეფექტური იქნება სხვა მეთოდების, პირველ რიგში ორგანიზაციულის, გამოყენების გარეშე. შიდა და გარე დამრღვევებს შორის არსებობს როლების განაწილება და, გარე და შიდა საფრთხეების მონიტორინგის სისტემებიდან მიღებული ინფორმაციის გაერთიანებით შესაძლებელია კომბინირებული შეტევების ფაქტების აღმოჩენა. შიდა და გარე უსაფრთხოების შეხების ერთერთი წერტილია დაშვების უფლებების მართვა. ნებისმიერი განაცხადი რესურსებზე წვდომის უფლებაზე, რომელიც არ არის განპირობებული სამსახურეობრივი აუცილებლობით, სიგნალია ამ ინფორმაციაზე აუდიტის მოქმედებების მექანიზმის ჩართვისათვის.

შიდა ინციდენტების მონიტორინგის სისტემის განვითარების მეორე მიმართულებაა — გაჟონვის აღკვეთის სისტემის აგება. ასეთი სისტემის მუშაობის ალგორითმი იგივეა, რაც შეჭრის აღკვეთის გადაწყვეტილებებში. იგება დამრღვევის მოდელი და მისი მიხედვით "დამრღვევის სიგნატურა" - დამრღვევის მოქმედებების თანმიმდევრობა. თუ რამოდენიმე მოქმედება დაემთხვა დამრღვევის სიგნატურას, ხდება შემდეგი ნაბიჯის პროგნოზირება, თუ ისიც დაემთხვა სიგნატურას, მაშინ მიიცემა განგაშის სიგნალი. დამრღვევის მოქმედებების მოდელის (პროფილის) გამოყენება შესაძლებელია არამარტო პროგრამული აგენტებიდან ინფორმაციის მოგროვებით. თუ გაანალიზდება მონაცემთა ბაზაზე

მოთხოვნების ხასიათი, ყოველთვის არის შესაძლებელი იმ თანამშრომლის გამოვლენა, რომელიც მთელი რიგი თანმიმდევრული მოთხოვნების საფუძველზე ცდილობს ბაზიდან ინფორმაციის ფრაგმენტის მიღებას.

მონაცემთა შიფრაციის და ანონიმიზაციის პრინციპები აუცილებელი შენახვისა და დამუშავების ორგანიზაციისათვის. დაშორებული დაშვების ორგანიზება კი ტერმინალური პროტოკოლით შესაძლებელია ისე, რომ მოთხოვნის გამცემ კომპიუტერზე არ დარჩეს არანაირი ინფორმაცია.

მონიტორინგის სისტემას შეუძლია მოგვცეს მხოლოდ დამრღვევის IP მისამართი, სააღრიცხვო ჩანაწერი, ელ-ფოსტის მისამართი და ა.შ. იმისათვის, რომ დადანაშაულდეს თანამშრომელი იდენტიფიკატორი უნდა მიებას პიროვნებას. აქ ინერგება აუტენტიფიკაციის სისტემებები — მარტივი სიმბოლებიდან ბიომეტრიამდე და RFID იდენტიფიკატორები.

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