კომპანიებში ინსაიდერებისგან მომდინარე საფრთხეები, მათგან დაცვის პრობლემატიკა და Log-მენეჯმენტი

დავით გომელაური
საქართველოს ტექნიკური უნივერსიტეტი

რეზუმე

ნაშრომში მოყვანილია ინსაიდარებისგან და გარე საფრთხეებისგან ინფორმაციის დაკარგვა, დაზიანების მაგალითები და მათგან თავდაცვის თანამედროვე საშუალებები. საფთხის თავიდან აცილების მიზნით განხილულია კორპორაციულ ქსელში ინფორმაციის დაცვის თანამედროვე მეთოდების ერთ-ერთი სქემა. ასევე ნაშრომში განხილულია ლოგ მენეჯმენტის კრიტიკულობა.

საკვანძო სიტყვები: ინსაიდერი. ინსაიდერებისგან დაცვის პრობლემატიკა. ინფორმაციის დაცვის მეთოდები.

1. შესავალი

იმისათვის, რომ გავერკვეთ და შევაფასოთ ის მუქარები, რომელთა მატარებლებიც არიან ინსაიდერები ნებისმიერი საწარმოს მიმართ და შერჩეული იქნას ნამდვილად ადეკვატური დაცვის ზომები, აუცილებელია განვმარტოთ ცნება ტერმინისა ,,ინსაიდერი''.

არსებობს აღნიშნული ტერმინის მრავალნაირი განმარტება, მაგრამ ჩვენი თემატიკიდან გამომდინარე შემოგვაქვს შემდეგი განმარტება: ინსადერი – პიროვნება, რომელსაც თავისი სამსახურეობრივი ან ოჯახური მდგომარეობიდან გამომდინარე აქვს დაშვება კომპანიის საქმიანობის კონფიდენციალურ და სხვა სასიცოცხლო მნიშვნელობის ინფორმაციასთან. საუბარია თანამდებობის პირზე, დირექტორზე, ზოგადად თანამშრომლებზე, რომლებიც მუშაობენ კომპანიის ავტომატიზებულ საინფორმაციო სისტემასთან. ამ კატეგორიას ვაკუთვნებთ ასევე, კორპორაციის ძირითად აქციონერებს და მათ ახლო ნათესავებს.

აქვე უნდა აღვნიშნოთ ის გარემოება, რომ ყველა განმარტებაში, ჩვენი განმარტების ჩათვლით, საყრდენი სიტყვებია: ,,აქვთ დაშვება ინფორმციასთან''. ეს კი საშუალებას იძლევა კიდევ უფრო დავაკონკრეტოთ ,,ინსაიდერების'' პრობლემა, გავაცნობიეროთ, რომ არსებობს შიდა ბოროტგანმზრახველის პრობლემა, და ის გავყოთ ორ ნაწილად: ინსაიდერად, რომელსაც აქვს დაშვება ინფორმაციასთან და თანამშრომლად, რომელიც ცდილობს მიიღოს ასეთი დაშვება;

ინსაიდერებისგან და გარე საფრთხეებიდან გამომდინარე ,ინფორმაციის გაჟონვის მინიმიზაციისთვის კომპანიამ უნდა უზრუნველყოს ყოველდღიური მონიტორინგი- კერძოდ დანერგოს ლოგების მონიტორინგის სისტემა.

2. ძირითადი ნაწილი

ინფორმაცია – ესაა განმარტება, რაღაც ცნობა.

მონაცემები – ესაა წარმოდგენა ფაქტების და იდეების ფორმალიზებულ სახეში, რომელიც გამოსადეგია გადაცემისა და დამუშავებისათვის რომელიღაც საინფორმაციო პროცესში.

ამ ცნებებში კიდევ უფრო უკეთ გასარკვევად მოვიყვანოთ მაგალითები (ცხრ.1).

ინსაიდერები ასოცირდებიან იმასთან, რომ მათ გამოაქვთ კლიენტების სია, დოკუმენტები, მონაცემთა ბაზები და ინფორმაცია.

როგორც ანალიზმა გვიჩვენა ამოცანები, რომლებიც უნდა გადაწყდეს ინსაიდერებთან ბრძოლისას ასეთია: ნორმატიული აქტების და სტანდარტების მოთხოვნებთან შესატყვისობა; ინფორმაციული დაცულობა (უვნებლობა); მონაცემების დაცულობა; გაჟონვის არსების გამოვლენა; უთანაზიარობის დამამტკიცებელი საბუთი.

ფაქტების, მონაცემების და ინფორმაციის ცხრილი ცხრ.1.

ფაქტი	მონაცემები	ინფორმაცია
კომპანია ემზადება გამოუშვას ახალი პროდუქტი	ტექნიკური დოკუმენტაცია, სარეკლამო მასალა, დისტრიბუტიკი, პროდუქტის საწყისი კოდი.	პროდუქტი ჯერ კიდევ არაა მზად/არაა ატესტირებული, გამოშვების ვადები იქნება დარღვეული/დაცული
კომპანია ცდილობს გაზარდოს თავისი აქციების ღირებულება	ღონისძიებების გეგმას, რომლებიც მიმართულია-------, პროგნოზები აქციების ღირებულებაზე და ა.შ.	კომპანიას უბრალოდ ამზადებენ გასაყიდად
კომპანია აგროვებს ახალ თანამშრომლებს	განცხადებები სერვერებზე მაძიებლებისათვის	კომპანია ემზადება ახალი მომსახურების გამოსაშვებად მალე გახსნის ახალ ფილიალს

შეიძლება გამოვყოთ ინფორმაციის გაჟონვის აღკვეთის შემდეგი ძირითადი გზები:

ინსაიდერების თვითკონტროლი, რათა არ მოხდეს ამ ინფორმაციის უნებლიე გაჟონვა; ხელმძღვანელ თანამდებობაზე დანიშვნა პასუხისმგებელი, შემოწმებული, მორალურად მდგრადი ადამიანების; ამ ადამიანების ყურადღების აქცენტირება იმაზე, რომ არა ყველა ინფორმაციაა განკუთვნილი ფართო პუბლიკაში გასავრცელებლად.

ეს პრობლემა, როგორც ჩანს მთლიანად ძევს ადამიანის ფაქტორის სფეროში. სამწუხაროდ, მასთან გამკლავება უჭირთ საუკეთესო სპეცსამსახურებსაც კი.

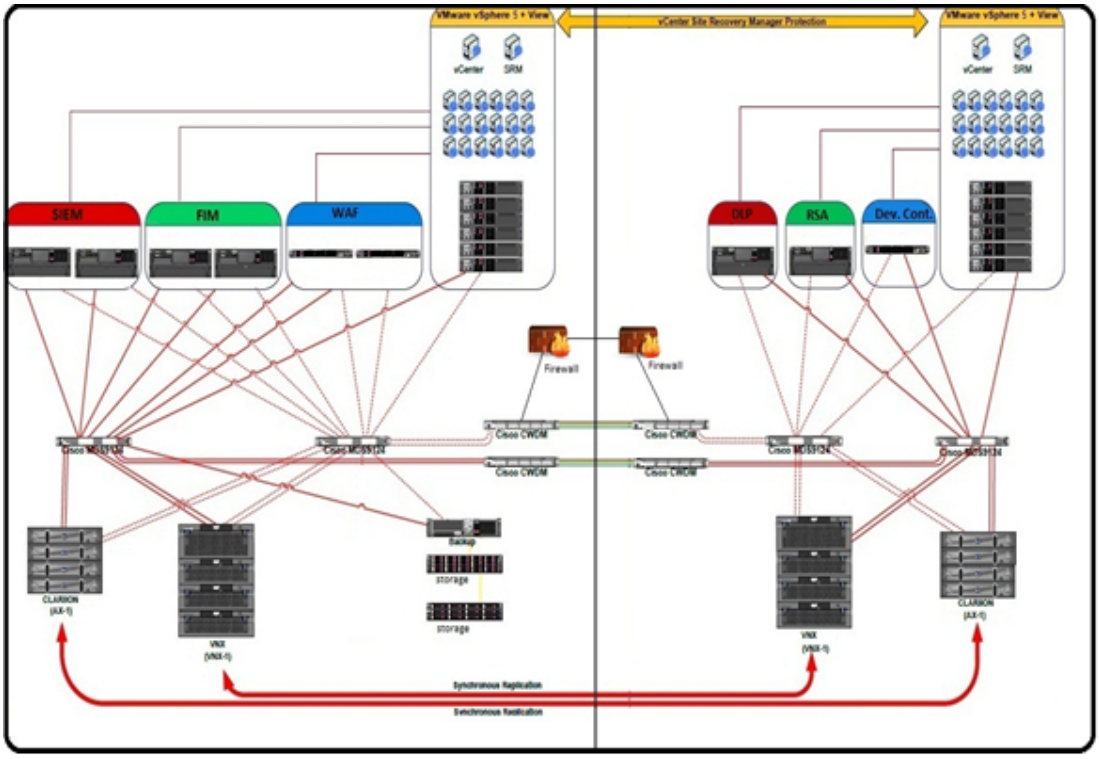
მონაცემთა გაჟონვის პრობლემის წინააღმდეგ ბრძოლა შესაძლებელია. დიახ სწორედ ბრძოლაა შესაძლებელი და არა ამ პრობლემის დამარცხება და აი რატომ , როგორც არ უნდა შევზღუდოთ ადამიანების დაშვება ინფორმაციასთან:

- ადამიანს შეუძლია აჩვენოს დოკუმენტი კოლეგას მონიტორზე/ნაბეჭდი, რომლისთვისაც ის არაა განკუთვნილი;
- ადამიანს შეიძლება დაავიწყდეს დოკუმენტი პრინტერში, სასადილოში, დატოვოს უმეთვალყუროდ კაბინეტი ან კეისი ან სეიფი;
- ადამიანს შეუძლია ეკრანიდან ფურცელზე ამოწეროს;
- ადამიანს შეუძლია წაიკითხოს ტელეფონში ან ბევრი რამ თქვას დიქტოფონზე;
- შეიძლება მონიტორის ეკრანის ფოტოგრაფირება ფიჭური ტელეფონის ფოტოკამერით;
- ადამიანს ბოლოს და ბოლოს შეუძლია უბრალოდ დაიმახსოვროს დოკუმენტის შიგთავსი სხვა რამესთან ერთად, იგივე ნოუთბუკი მონაცემებით შეიძლება დაიკარგოს ან მოპარულ იქნას.

დაცვის ნებისმიერი საშუალება ქმნის მოუხერხებლობას და დაკავშირებულია დამატებით ხარჯებთან – ეს აქსიომაა. ნებისმიერი დასანერგი (დანერგილი) დაცვის საშუალება საჭიროებს მომსახურებას – ეს ცხოვრების კანონია.

თანამედროვე კომპანიებს რომლის IT-ინფრასტრუქტურაში ათეულობით სერვერი, ქსელური მოწყობილობები, აპლიკაცები და ბაზებია, ხოლო ინფორმაცია სენსიტიური, ძალზედ მნიშვნელოვანია ყოველდღიურად ლოგების მონიტორინგი და ანალიზი.

შესაბამისად, საჭიროა ფიზიკური მოწყობილობა ან ისეთი პროგრამული უზრუნველყოფა, როგორიცაა Security information and event management. იგი უზრუნველყოფს სხვადასხვა სისტემებიდან, ბაზებიდან, მოწყობილობებიდან და აპლიკაციებიდან ლოგების გაგზავნას ერთ ცენტრალიზირებულ სერვერზე, შემდგომ მათ კორელაციასა და ანალიზს, ასევე სტატისტიკური მონაცემების ნახვასა და შეტყობინებების გაგზავნას.



ნახ.1. კორპორაციული ქსელი - ინფორმაციული უსაფრთხოების თანამედროვე დამცავი მექანიზმები

ლოგების ანალიზი ამცირებს ინფორმაციის დაკარგვის, დამახინჯება-დაზიანების რისკებს. ინფორმაციული უსაფრთხოების თანამშრომელი ყოველდღიურად უნდა ამოწმებდეს სხვადასხვა IT-ინფრასტრუქტურის (ნახ.1), როგორიცაა სისტემები (Windows, Linux), მონაცემთა ბაზების, სერვერების, RSA, FireWall, Router, FIM, Switch, DLP, აპლიკაციების და ა.შ. ლოგებს, რათა მაგალითისათვის არ მოხდეს ან დროულად განხორციელდეს რეაგირება შემდეგ ქმედებებზე: არასანქცირებული წვდომის გახსნა, ინფორმაციის გატანა, მომხმარებლისთვის ზედმეტი უფლებების მინიჭება, პაროლის შეცვლა და შემდგომ მისი არასანქცინირებულად გამოყენება, ეგრეთ წოდებული "brute force" შეტევა, SQL Injection , DDOSშეტევები და ა.შ.

3. დასკვნა

მიუხედევად იმისა , რომ ინფორმაციის დაცვის 100% გარანტი არ არსებობს, "კომპანიამ" ხარჯების გათვალისწინებით უნდა დანერგოს ინფორმაციის დაცვის სხვადასხვა მექანიზმები და ინფორმაციის გატანა-დამახინჯების მინიმიზაციისთვის უზრუნველყოს ყოველდღიური ჩანაწერების (ლოგების) მონიტორინგი.

ლიტერატურა:

1. Исследование CheckPoint: рост количества удаленных сотрудников приведет к усломнению инфраструктуры безопасности в 2011 году. www. ms-security.ru.

2. Взлом и защита 1с: Предприятия. Анализ проблемы цисайдерского взлома для меподтлеров. – Оригинал статьи находится на сайте компании «Поликом Про».

3. Утечки корпоративной информации и персональных данных в 2010 году. www.stcurity.ru.

4. Зарубежный опыт защиты информации в процессе организации работы с кадрами (на примере США) – http://security.meganet.md .

THREATS COMING FROM INSIDERS TO AN ORGANIZATION AND LOG MANAGEMENT

Gomelauri David
Georgian Technical University

Summary

The article discusses issues related to the protection of computer networks from insiders. The article deals developed scheme of information security including newest information security methods. Also in the article is shown criticality of log management.

УГРОЗЫ, ИСХОДЯЩИЕ ОТ ИНСАЙДЕРОВ И ЛОГ МЕНЕДЖМЕНТ

Давид Гомелаури
Грузинский Технический Университет

Резюме

Рассматриваются вопросы, связанные с защитой компьютерных сетей от инсайдеров. Разработана схема информационной безопасности, включая новейшие методы защиты информации, а также показано критичность управления лог журналами.