Transactions. Georgian Technical University. AUTOMATED CONTROL SYSTEMS - No 1(6), 2009

კომპანიის ვებ-სერვერის დაცვის იერარქია

დავით კაპანაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

სტატიაში განხილულია კომპანიის ქსელის დაცვის სხვადასხვა საშუალებების ოპტიმალური მორგების ამოცანა მისი ინფორმაციული უსაფრთხოების მოთხოვნების შესაბამისად. აღნიშნულია, რომ ამ ამოცანის გადასაწყვეტად საჭიროა ინფორმაციული უსაფრთხოების თეორიულ საფუძვლებში კარგად გარკვევა და მის საფუძველზე დაცვის ღონისძიებების მომზადება. აღწერილია ვებ-სერვერების დაცვის ახალი მიდგომა და რისკების ანალიზის მეთოდიკა. მოცემულია სირთულის მიხედვით ექვს დონედ დაყოფილი ქსელის დაცვის იერარქია. ჩამოყალიბებულია კომპანიის ვებ-სერვერების უსაფრთხოების დონის შერჩევის რეკომენდაციები.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება. დაცვის დონეები. რისკების ანალიზი.

1. შესავალი

ნებისმიერ კომპანიაში ინფორმაცის დაცვის აუცილებლობა დღეისათვის ყველასათვის ცხადია. მომხმარებელთა უმრავლესობამ იცის, რა არის პროგრამული ვირუსები, Firewall და ქსელის დაცვის სხვადასხვა საშუალებები, მაგრამ ამ საშუალებების კომპანიის დაცვის მოთხოვნებისადმი ოპტიმალური მორგება მაინც მთავარ ამოცანად რჩება [1]. მით უმეტეს, რომ ხშირად ამაზე დამოკიდებულია არამარტო მონაცემების დაცულობა, არამედ თვით საწარმოს არსებობაც.

ინფორმაციის დაცვის ამოცანის გადასაწყვეტად საჭიროა ინფორმაციული უსაფრთხოების თეორიულ საფუძვლებში კარგად გარკვევა და მის საფუძველზე დაცვის ღონისძიებების მომზადება.

2. ძირითადი ნაწილი

თანამედროვე კომპანიებში ხშირად ასეთი სცენარით მიმდინარეობს მონაცემთა დაცვის საკითხი: კომპანიას, რომლის ლოკალურ ქსელს ინტერნეტში მუდმივი გასასვლელი აქვს, თავისი მონაცემების დაცვის უზრუნველყოფა სურს. ამისათვის სპეციალისტი აყენებს Firewall-ს, რითაც გადაკეტავს (მისი აზრით) გარე, გლობალური ქსელიდან პირდაპირი შეტევის საფრთხეებს. შემდეგ ვირუსებისა და ტროიანების შემოღწევის აღსაკვეთად აყენებს ანტივირუსულ პროგრამულ უზრუნველყოფას.

შედეგად აღმოჩნდება, რომ ზოგიერთი სამომხმარებლო პროგრამა მუშაობს ქსელთან, მაგრამ ამას ვერ აკეთებს უსაფრთხოების საკმარის დონეზე, ამიტომ სპეციალისტს ამ კავშირის აკრძალვაც უწევს. თანდათანობით იზრდება პოტენციური საფრთხეები და შესაბამისად იზრდება გამოყენებული დაცვის საშუალებების რიცხვიც. ასეთი მიდგომის დროს, როგორც წესი, გამოყენებული საშუალებები სხვადასხვაა, არაა საკმარისი უსაფრთხოების უზრუნველყოფისათვის და სამწუხაროდ, სისტემის მუშაობა

კრახით მთავრდება. აუცილებელი ხდება სისტემის ხელახლა დაყენება (ინსტალაცია), რაც ძვირადღირებული სამუშაო დროისა და რესურსების ფლანგვას იწვევს.

ამ მაგალითიდან გამომდინარე, შეიძლება დავასკვნათ, რომ ასეთი მიდგომა მოძველებულია. თანამედროვე საწარმოებში საფრთხეები ძალიან ბევრია და ამიტომ აუცილებელია დაცვის იერარქია საიმედო საფუძველზე აიგოს.

ინფორმაციული უსაფრთხოების თეორიული და პრაქტიკული კვლევების შედეგად დადგენილია, რომ დაცვის გასარღვევად საჭიროა სამი ფაქტორის დამთხვევა: პროგრამულ უზრუნველყოფაში, პროტოკოლებში ან პროცესებში **სუსტი ადგილის** არსებობა, რომლის გამოყენებაც შეუძლია ბოროტმზრახველს; **საფრთხე**, რომელსაც შეუძლია ამ სუსტი ადგილის გამოყენება თავდასხმისათვის; **მოქმედება**, რომელიც იყენებს არსებული სუსტი ადგილისადმი საფრთხეს [2].

კომპიუტერული უსაფრთხოების არსი მარტო მის აგებაში კი არ მდგომარეობს, არამედ სუსტი ადგილების მუდმივად ძებნაში და მის მანამდე აღმოფხვრაში, სანამ ბოროტმზრახველი შეძლებს საფრთხის წარმოქმნას და მის განხორციელებას. შესაბამისად, უსაფრთხოება დინამიკური პროცესია და არა სტატიკური. შესაძლო რისკების ანალიზი და აღმოფხვრა მისი ძირითადი შემადგენელია, რომლის უგულვებელყოფა არ შეიძლება.

განვაზოგადოთ და ჩამოვთვალოთ ვებ-სერვერების სუსტი ადგილების წარმოქმნის მიზეზები:

- მზარდი საწარმოების უმრავლესობა რეგულარულად ცვლის თავისი ქსელის კონფიგურაციას, ამატებს ახალ სამუშაო ადგილებს (ზოგჯერ სერვერებსაც), მაგრამ არ ახდენს ამ დროს ლოკალური ქსელის ტესტირებას უსაფრთხოების კუთხით. ცხადია, ახალი მომხმარებლების დამატების აკრძალვა შეუძლებელია, მაგრამ საჭიროა ქსელის გაფართოების გააზრება თავიდანვე. უნდა მოინიშნოს ის სეგმენტები, რომლებიც შესაძლოა გაფართოვდეს და მოხდეს მათი წინასწარი ტესტირება უსაფრთხოებაზე;
- ყოველი მომხმარებლისათვის უნდა განისაზღვროს წვდომის (მიმართვის) უფლებების პოლიტიკა, რომელიც მის უფლებებს შეზღუდავს მის მოვალეობებამდე;
- კომპიუტერზე განთავსებული ლიცენზირებული, shareware, freeware და ზოგჯერ არალიცენზირებული (პირატული) პროგრამული უზრუნველყოფის ერთობლიობა სისტემას სახიფათოს ხდის. რეკომენდებულია და შედარებით ყველაზე უფრო უხიფათო მიდგომაა ერთი მწარმოებლის მიერ გამოშვებული და თავსებადი პროგრამების შერჩევა.

ვებ-სერვერების უსაფრთხოება დადის რისკების მართვაზე. ყველა კომპანია არ საჭიროებს თავისი ინფორმაციის უმაღლეს დონეზე დაცვას. უსაფრთხოების დონის საკითხი – ესაა ქსელის რესურსების გამოყენების საკითხი. მაგალითად, თუ ვებ-სერვერი მხოლოდ მარკეტინგისთვის გამოიყენება, განსაკუთრებით რთული დაცვის დაყენება საჭირო არაა. ელექტრონული კომერციის სისტემებისათვის, ელექტრონული გადარიცხვის სისტემები მოითხოვს დაცვის მაღალ დონეს. ამიტომ მიღებულია ვებ-სერვერების დაცვის დაყოფა დონეებად.

ქსელის დაცვა დაყოფილია სირთულის ექვს დონედ:

პირველი დონე – ყველაზე ელემენტარული და აუცილებელია. აქ დაცვის მთავარ ინსტრუმენტს წარმოადგენს Firewall. იგი ლიმიტს უწესებს მომხმარებლისადმი სერვისების გამოყენებას. ასევე Firewall თვალყურს ადევნებს კავშირებს ორივე მხრიდან. აქ ყოველთვის ჯობია ცნობილი ფირმების ლიცენზირებული პროდუქტის გამოყენება, ვინაიდან იგი ფაქტობრივად დაცვის პირველი ზღუდეა;

მეორე დონე გულისხმობს იმ ოპერაციული სისტემის კონფიგურირებას, რომელიც მართავს სერვერის მუშაობას. ყოველი ოპერაციული სისტემა საშუალებას იძლევა შეიქმნას უსაფრთხოების

საკონტროლო სიები (security checklist). მნიშვნელოვანია, რომ ახალი სამომხმარებლო პროგრამების შეტანა ამ სიებში დროულად მოხდეს;

მესამე დონე ორიენტირებულია ქსელზე. უნდა მოხდეს ჰოსტინგის უზრუნველმყოფი პროვაიდერის ქსელური მოწყობილობების შეტევის აღმომჩენი გადამწოდებით აღჭურვა. მთავარია საშიშროების შესახებ მიღებული სიგნალი სწორად იქნას დამუშავებული და საფრთხე ნეიტრალიზებული;

უსაფრთხოების **მეოთხე დონეზე** ხდება ჰოსტინგზე სპეციალური პროგრამული უზრუნველყოფის დაყენება. ეს გაცილებით რთული ამოცანაა. ჯერ ერთი, ასეთი პროგრამების წინააღმდეგი შეიძლება წავიდეს თვით ჰოსტინგ-კომპანია. მეორე – ასეთი პროგრამები გაცილებით რთულია ვიდრე მარტივი გადამწოდები;

მეხუთე დონეს აქვს ორი ქვედონე - A და B. 5A დონე – ესაა სპეციალური პროგრამული უზრუნველყოფის დაყენება, რომელიც ასრულებს ფენის როლს ვებ-სერვერის ოპერაციულ სისტემასა და ყველა გამოყენებით პროგრამას შორის. ასეთი ბუფერის საშუალებით შესაძლებელია იმ სუსტი ადგილის მქონე პროგრამებზე ჰაკერების შემოტევისაგან დაცვა, რომლებიც თავისი შესრულების დროს მთელ ოპერაციულ სისტემას უწევენ კონტროლს;

5B დონე წარმოადგენს კონკრეტულ პროგრამებზე ორიენტირებულ firewall-ს ან პროქსი-სერვერს. ისინი ორიენტირებულია HTTP-პროტოკოლზე და შემოტევებს იგერიებს მანამ, სანამ პოტენციური ბოროტმზრახველი შეძლებს ვებ-სერვერზე დაყენებული პროგრამის გაშვებას. თუმცა, პროქსი-სერვერი მნიშვნელოვნად ზღუდავს მუშაობას და მისი სათანადო კონფიგურირებაც საკმაოდ რთულია.

მეექვსე დონე უსაფრთხოების მწვერვალია. აქ დასაშვებია მხოლოდ ნდობის მექანიზმების მქონე ოპერაციული სისტემების და მათი მმართველობით მომუშავე პროგრამების გამოყენება. ოპერაციული სისტემა და ყველა მომუშავე პროგრამა ან მაქსიმალურად უნდა იყოს ადაპტირებული, ან სპეციალურად, კომპანიის სპეციფიური მოთხოვნების მიხედვით უნდა იყოს დამუშავებული. ეს დაცვის ყველაზე ძვირი, მაგრამ ყველაზე ეფექტური გზაა. ამ დროს ქსელის ადმინისტრატორს და მომხმარებელს სპეციალური მომზადება მოეთხოვებათ, რაც დამატებით დანახარჯებს მოითხოვს. რომელიმე პროგრამის განახლება, ამ შემთხვევაში მოითხოვს მის წინასწარ ინტეგრირებას ნდობის მექანიზმებიან სისტემაში.

ბოლოს დგება მთავარი კითხვა – რომელი დონის დაცვა იქნეს არჩეული ? აქ მთავარი გადამწყვეტი ფაქტორია ფასისა და ხარისხის შეფარდება. ყველა კომპანიას უნდა ჰქონდეს მინიმუმ პირველი ორი დონის დაცვა. ნებისმიერმა კომპანიამ, რომლისთვისაც ინფორმაციის დაზიანება კრიტიკულია და შეიძლება ზეგავლენა მოახდინოს საწარმოს ფუნქციონირებაზე, თავისი ვებ-სერვერი უნდა აღჭურვოს უსაფრთხოების მესამე დონით.

კომპანიებს, რომლებიც იყენებს ვებ-სერვერზე გარედან პროგრამების გაშვების სერვისს, მეოთხეზე მაღალი დაცვის დონე უნდა ჰქონდეს (4, 5A ან 5B). თუ მომხმარებლებს შეუძლიათ ქსელური პროგრამების პარამეტრების კონტროლირება და მართვა, საჭიროა მეხუთე დონის დაცვა (როგორც 5A ისე 5B). ეს სამართლიანია რთული სისტემებისათვის, როდესაც კომპიუტერები ქსელის საშუალებით უერთდება სერვერს და უფლება აქვს არა მარტო პროგრამების გაშვებისა, არამედ ამ პროგრამების პარამეტრების შეცვლისაც. მეექვსე დონე – პრაქტიკულად უსაფრთხოების სრულ გარანტიას იძლევა.

ყოველი კომპანიისათვის მნიშვნელოვანია მოგება, ამიტომ საინტერესოა იმ ეკონომიკური ეფექ-ტიანობის შეფასება, რაც მოჰყვება კომპიუტერულ ინფორმაციულ სისტემაში უსაფრთხოების ღონისძი-ებების დანერგვას. არსებობს სერვერზე ჰაკერების შეტევისადმი მდგრადობის შემოწმების მეთოდიკა ანუ რისკების არსებობის შეფასება. ამისათვის გამოიყენება ე.წ. ROI (Return of Investment) – ესაა მოგების რაოდენობრივი შეფასება უსაფრთხოების სისტემის დანერგვისათვის ინვესტირებულ კაპიტალზე. რისკების არსებობის რაოდენობრივი შეფასების დადგენის სერვისს დღეისათვის მრავალი უსაფრთხოების სფეროში მომუშავე თანამედროვე კომპანია სთავაზობს საწარმოებს. ეს შეფასებები ხდება მარტივი ონლაინ ფორმის შევსებით.

ამ ფორმებში უკვე გათვალისწინებულია ციფრები, რომლებიც საწარმოსათვის ეტალონურად ითვლება. შეფასებები მოიცემა საკმაოდ დეტალურად. გამოითვლება შემდეგი მაჩვენებლები: Net Present Value (NPV) Savings, Internal Rate of Return (IRR), Return on Investment (ROI).

3. დასკვნა

ამრიგად, უსაფრთხოება – ესაა ადამიანები, პროცესები, პროგრამები. უსაფრთხოების უზრუნველყოფა გულისხმობს სისტემაში სუსტი ადგილების გამოვლენის უწყვეტ პროცესს, საფრთხეების ლიკვიდაციის გამართულ სტრუქტურას და გამოყენებითი პროგრამების მიმართ კონტროლს. კომპანიების ცხოვრებაში შემოსული ინტერნეტ-ტექნოლოგიები გვაიძულებს მუდმივად მოვახდინოთ ინფორმაციული უსაფრთხოების მეთოდიკის სრულყოფა და ახალი მიდგომების ძიება.

ლიტერატურა

1. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003
2. Маккарти Л. IT-безопасность: стоит ли рисковать корпорацией? Пер. с англ. - М.: КУДИЦ-ОБРАЗ, 2004.

HIERARCHY OF PROTECTION A WEB-SERVERS OF THE COMPANY

Kapanadze David
Georgian Technical University

Summary

The problem of optimum adjustment of company protection systems according to requirements of information safety is considered in this article. It is noted, that for the decision of this problem it is necessary to generate the approach and to prepare protection according to it. There are described a new approach for protection of web-servers and a technique analysis of risks. The hierarchy of protection of the network divided on six levels of complexity is given. Recommendations for a choice of a level of protection a web-servers of the company are generated.

ИЕРАРХИЯ ЗАЩИТЫ WEB-СЕРВЕРОВ КОМПАНИИ

Капанадзе Д.
Грузинский Технический Университет

Резюме

Рассмотрена задача оптимальной настройки системы защиты компании в соответствии с требованиями информационной безопасности. Отмечено, что для решения этой задачи необходимо сформировать подход и подготовить защиту в соответствии с ним. Описаны новый подход для защиты веб-серверов и методика анализа рисков. Дана иерархия защиты сети, разделенная на шесть уровней сложности. Сформированы рекомендации для выбора уровня защиты веб-серверов компании.