ქსელებში ინფორმაციის დაცვის კონცეფცია

ოთარ შონია, დავით შონია, ირაკლი გოგოხია, ნინო ფოლადაშვილი
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

ნაშრომში დეტალურადაა გაანალიზებული კომპიუტერულ დანაშაულებათა და მათ წინააღმდეგ ბრძოლის საკითხები. განხილულია საინფორმეციო სისტემების ინფორმაციული უსაფრთხოების პრობლემები და ჩამოყალიბებულია ასეთ ქსელებში ინფორმაციის დაცვის საერთო კონცეფცია.

საკვანძო სიტყვები: ქსელები, ინფორმაციული უსაფრთხოება, ბოროტგანმზრახველი, ელ.ფოსტა.

1. შესავალი

ისევე როგორც საქართველოში მსოფლიოს უმეტეს ქვეყნებში (მათ შორის რუსეთში) არსებობს ძალზე მცირე რაოდენობით საკანონმდებლო აქტებისა, რომლებიც ადექვატურად განიხილავენ კომპიუტერული დანაშაულებათა და მათ წინააღმდეგ ბრძოლის საკითხებს. ინფორმაციული ტექნოლოგიები ჯერ ისევ არაა სტანდარტიზებული, რომ შესაძლებელი იყოს ამ კანონების არაწინააღმდეგობრივი გამოყენება პრაქტიკაში. ამასთან ერთად, გასათვალისწინებელია ისიც, რომ ე.წ. კიბერნეტიკული სივრცე (კიბერსივრცე) არსებობს საზღვრებსა და კანონიერების გარეშეც. ეს ფაქტიურად უხილავია, შეუძლებელია მისი ხელით მოსინჯვა.

კიბერსივრცეში ბოროტგანმზრახველებს შეუძლიათ შეაღწიონ ორგანიზაციის უმნიშვნელოვანეს რესურსებში, წიაკითხონ წერილები ელ. ფოსტაში, შეუძლია არასანქცირებულად მიიღონ დაშვება სახელმწიფო დოკუმენტებთან სახელმწიფო საიდუმლოებასთან, შეცვალონ მონაცემები ოპერატიულ მდგომარეობაზე და ა.შ. დაამ დროს ისინი რჩებიან უხილავნი და სასამართლო დევნისათვის ძნელად ხელმისაწვდომნი. ყველაფერი ეს კი ისეთი სისწრაფით კეთდება, რომ ქსელის ადმინისტრატორს ამ პერიოდში შესაძლებლობა ეძლევა ყოველდღიური რეგისტრაციის ჟურნალი (log) ამოიბეჭდოს ამასობაში ბოროტგანმრახველს კვლავაც კი წაშლილი აქვს ქსელში.

როგორი პარადოქსალურიც არ უნდა იყოს კითხვაზე თუ რაა საინფორმაციო ქსელურ სისტემებში მოწყვლადი. პასიური ერთია - ფაქტიურად ყველაფერი პირველ რიგში თვითონ ქსელი - ქსელური ოქმები (TCP/IP, IPX/SPX, NetBOIS/SMB) და მოწყობილობების (მარშუტიზატორები, კომუტატორები), რომლებიც ქმნიან ქსელს. მეორე მხრივ ესაა ოპერატიული სისტემები (Win NT, UNIX, Netware). აგრეთვე მონაცემთა ბაზები (Oracle, Sybase, MS SQL Server) და გამოყენებითი პროგრამები CSAP, ელ. ფოსტა, web-სივრცეები და ა.შ.

უამრავი მიზეზი და ფაქტორი არსებობს, რომლებიც აფერხებენ ქსელების უსაფრთხოების საკითხებს. პრობლემების მოგვარებას პირველ რიგში ეს ეხება ორგანიზაციების ხელმძღვანელობს, რომელთა დარწმუნება ისეთი სახსრების გამოყოფის აუცილებლობაში, რომლებიც პირდაპირ არ არიან დაკავშირებული ორგანიზაციის მუშაობის ეფექტურობის ამაღლებასთან ან მოგების მიღებასთან. ამასთან ერთად საკმაოდ დიდი დროა საჭირო დამრღვევის იდენტიფიკაციისათვის, მაშინ როც ბოროტგანმრახველს სჭირდება სისტემაში მიგნოს ერთ სუსტ ადგილს მაინც, ხოლო სისტემის დამცველები იძულებული არიან აკონტროლო 200-300-ზე მეტი სუსტი ადგილია.

ორგანიზაციათა უმეტესობა დაცვაში აშმორჩენილი პრობელმების გადაწყვეტას ცდილობს ცალმხრივი მიდგომებით. ეს მიდგომები ემყარება მათ მიერ უსაფრთხოების რისკების აღქმას. კერძოდ, უსაფრთხოების ადმინისტრატორებს ახასიათებთ ტენდენცია რეაგირება მოახდინონ მხოლოდ იმ რისკებზე, რაც მათთვის გასაგებია. რეალურად კი რისკების რაოდენობა ბევრად მეტია, მათ კერძოდ ესმით, რომ სისტემის დაცვის დონე შეიძლება ამაღლდეს ისეთი ტექნიკური საშუალებების გამოყენებით, როგორებიცაა ასელთაშორისი ეკრანები. კრიპტოგრაფიული სისტემები. აუტენტიფიკაციის ან დაშვების გამიჯვნის საშუალებები. მაგრამ ხშირად მათ არ იციან თავიანთი ქსელური მოწყობილობების ტექნიკური მახასიათ ბლები, რომლებიც შეიძლება არასწორედ იქნეს გამოყენებული კრიტიკული მონაცემების შეყვანის, მოპარვის, განადგურების ან შეცვლისათვის. ასეთი მიდგომა საფრთხეების 20-30%-ისაგან დაცვის საშუალებას იძლევა. აღნიშნული ვარინატი შეიძლება გამოვსახოთ ფორმულით:

უსაფრთოხება = დაცვის ტრადიციული საშუალებები

ეს ფორმულა კარგად ასახავს უსაფრთოხებისადმი ცალმხრივ მიდგომას, რომლის დროსაც შესაძლებელია ზოგიერთი რისკის შემცირება, მაგრამ მოსალოდნელია სხვები სრულად გამოგვრჩეს.

ყოველმხრივი მიდგომის გარეშე, რომლის დროსაც გამომუშავებული იქნება უსაფრთოხების უზრუველყოფისადმი ერთიანი მიდგომა და მკაცრი მიმდინარე კონტროლი. ინფორმაციული ტექნოლოგიების განვითარება წარმოშობს ახალ პრობლემებს. ამ ცოტა ხნის წინ ჩატარებულმა გამოკვლევებზე გამოააშკარავეს სხვადასხვა გეოგრაფიული წერტილებიდან კოორდინირებული შეტევების ფაქტები. ამის სამაგალითოდ გამოდგება ხაკერების შეტევები იუგოლავიის ომის დროს. ეს შეტევები განხორციელდა ნატო-ს პოლიტიკით უკმაყოფილო ქვეყნებისა და პიროვნებების მიერ. ერთად მუშაობისას კიბერდამნაშავეებს შეუძლიათ „გააუმჯობესონ“ თავიანთი შედეგები, უფრო ეფექტურად დამალონ თავიანთი მოქმედებები და შეტევები განახორიცელონ დიდი სისწრაფით.

დაცვის კარგი სისტემა აუცილებლად გულისხმობს კარგად ნავარჯიშები პერსონალის ყოლას, რომელსაც შეუძლია:

ა) მკაცრად დაიცვას უსაფრთოხების უზრუნველყოფის სტანდარტული მიდგომები;

ბ) დანერგონ დაცვის პროცედურები და ტექნიკური საშუალებები;

გ) განახორციელოს აუდიტის ქვესისტემის უწყვეტი კონტროლი, რომელიც უზრუნველყოფს პოტენციური შეტევებისა და ბოროტმოქმედების ანალიზს.

თუ ქსელის განვითარებასთან ერთად არ ხდება მისი უსაფრთოხების უწყვეტი კონტროლი და ანალიზი, მაშინ დროთა განმავლობაში ქსელის დაცულობა ეცემა, ვინაიდან წარმოიშობიან ახალი გაუნალიზებელი მუქარები და სისტემაში სუსტი ადგილები, რომელთა თავიდან აცილება ასეთ ვითარებაში შეუძლებელი ხდება. ქსელური უსაფრთოხების საიმედო სისტემის შექმნა უნდა ემყარებოდეს შემდეგ ფორმულას:

უსაფრთოხება = უსაფრთოხების პოლიტიკა + დაცვის ტრადიციული საშუალებები + რისკის ანალიზი + კონტრლონისძიებების გატარება.

ამ შემთხვევასში დაცვის სისტემი ეფექტურობამ შეიძლება მიაღწიოს 40-60%-ს.

ამ ვარიანტში დაცვის სისტემის შექმნა უნდა იწყებოდეს რისკის (საფრთხეთა შეფასებით), რომელიც ფაქტიურად მთლიანად ყველა სამუშაოების ფუნდამენტია. რისკის შეფასება ნიშნავს: გამოვლინდე ქსელის სუსტი ადგილები, შესაძლო მუქარები და ა.შ. მაგრამ ვინაიდან ქსელი განუწყვეტლივ იცვლება, ასევე უწყვეტი უნდა იყოს რისკის შეფასებაც. დაცვის ეფექტურობა დამოკიდებული იქნება სწორი გადაწყვეტილებების მიღებაზე, რომლებიც უზრუნველყოფენ დაცვის ადაპტირებას ქსელის გარემოცვაში არსებული ცვლილებებისადმი.

აღნიშნულ მიდგომაში არაა გათვალისწინებული ის ფაქტი, რიგ ადმინისტრატორებმა და მომხმარებლემბა შეიძლება შეცვალონ სისტემის ადგილები, რომლებიც დაკავშირებული არიან ოპერატიულ სისტემებთან და გმაყენებით პროგრამებებთან.

ინფორმაციული ურთიერთოდაპირისპირებულობის პირობებში დამნაშავეები და მომხმარებლები ხდებიან უფრო კვალიფიცირებუნი. ასეთი სწრაფი განვითარება იზრდება ინტერნეტის ფართოდ გამოყენებისას და დაცვისათვის რესურსების უკმარისობას სახელმწიფო შეიარაღებული ძალები იძულებული არიან მიმართონ ინფორმაციული უსაფრთხოების უზრუნველყოფი სხვა მიდგომას, რომლის დროსაც უზრუნველყოფილი იქნება. უსართხოების საჭირო დონე ინფორმაციული ტექნოლოგიების ნებისმიერი ტემპით განვითარებისას. ამიტომ წამყვანმა ორგანიზაციებმა, რომლებიც მოღვაწეობენ ქსელური უსაფრთოხების სფეროში, ისეთებმა როგორებიცაა Britich Teleco/Syntegra, აშშ სამხედრო საჰაერო ძალების ინფორმაციებული ომის წამროების ცენტრი DISA და DRA (დიდი ბრიტანეთი). ქსელური მართვის მეთოდების საფუძველზე გამოიმუშავეს მიდგომა, რომელიც საშუალებას იძლევა ამოცანობილი იქნას დანარჩენი 40-60% სუსტი ადგილებისა და შეტაკებისა, არამედ გამოვალინონ, სახეცვლილი ძველი ან ახალი სისუსტეები. შემოთავაზებული იქნა დაცვის შესაბამისი საშუალებები. კომპანიამ Internet Systems, Inc. დააზუსტა და განავითარა ეს მიდგომა და შექმნა <u>უსაფრთოხების ადაპტიური მართვის მოდელი</u> (Adaptiro Network Security - ANS). აღნიშნული მიდგომა ქსელების უსაფრთოების უზრულვეყოფის უახლოები კონცეფციაა და ის შეიძელება გამოვსახოთ შემდეგი ფორმულით:

უსაფრთოხება = რისკის ანალიზი + უსაფრთოხების პოლიტიკა + დაცვის ტრადიციული პოლიტიკა + კონტრლონისძიებების განხორციელება + აუდიტი + მონიტორინგი + რეაგირება.

დავახასიათოთ ეს კონცენფია. ადაპტური უსაფრთხოება ისეთი მიდგომაა, რომელიც საშუალებას იძლევა რეალურ დროში განხორციელდეს უსაფრთხოების რისკის კონტროლი. Yankee Group-ის 1998 წლის ანგარიშში ANS აღწერილია როგორც პროცესი რომელიც მოიცავს:

1) დაცულობის (Security assestment) ანალიზის და სისუსტეების ძებნის ტექნოლოგიას;

2) შეტევათა აღმოჩენის ტექნოლოგიას (intrusion detection);

3) ადაპტურ კომპონენტს, რომელიც აერთიანებს პირველ ორ ტექნოლოგიას და აფართოებს მათ შესაძლებლობებს;

4) მართვის კომპონენტს.

დაცულობის ანალიზი – ესაა ქსელში მოწყვლადი ადგილების ძებნა და გამოყენება. თუ სისტემა, რომელიც ახდენს ამ ტექნოლოგიის რეალიზებას, შეიცავს ადაპტურ კომპონენტსაც, მაშინ ის ავტომატურად უზრუნველყოფს გამოვლენილი სუსტი ადგილების აღმოფხვრას (განმტკიცებას - დაცვის გაძლიერებას). შეიძლება გამოვყოთ ის პრობლემები, რომელთა იდენტიფიცერებაც ხდება აღნიშნული ტექნოლოგიით. ესენია:

ა) „სარქველი“ სისტემაში (back door) და „ტროას ცხენის“ სახის პროგრამები;

ბ) სუსტი პაროლები;

გ) დაუცველი სისტემებიდან შემოღწევის შესაძლებლობა და „უარი მომსახურებაზე“ ტიპის შეტევები;

დ) ოპერაციული სისტემების აუცილებელი განახლებათა არ არსებობის აღმოჩენა;

ე) ქსელთაშორისი ეკრანების, Web-სერვერების, მონაცემთა ბაზებისა და სხვ. არასწორი ორგანიზაცია.

შეტევათა აღმოჩენა გულისხმობს ქსელში საეჭვო ქმედებათა გამოვლენას. შეტევათა აღმომჩენი ტექნოლოგიის კომპონენტები, რომლებიც განლაგებულია ქსელის სეგმენტებსა ან კვანძებზე, აფასებს სხვადასხვა მოქმედებებს. მათ შორის იმ ქმედებებს, რომლებიც იყენებს ცნობილ სუსტ ადგილებს.

ადაპტური კომპონენტი ANS პასუხს აგებს დაცულობის ანალიზის პროცესის მოდიფიკაციაზე, რისთვისაც მას აწვდის უახლეს ინფორმაციას გამოვლენილი ახალი სუსტი ადგილების შესახებ. ის ასევე ახორციელებს შეტევათა აღმომჩენი კომპონენტის მოდიფიკაციას, აწვდის მას ახალ ინფორმაციას შეტევათა შესახებ. ადაპტური კომპონენტის მაგალითად გამოდგება ანტივირუსული პროგრამების ბაზების განახლების მექანიზმი, რის მეშვეობითაც შესაძლებელი ხდება ახალი ვირუსების აღმოჩენა.

მართვის კომპონენტს უნდა შეეძლოს ორგანიზაციის მიერ ქსელების უსაფრთხოების უზრუნველყოფის ძალისხმევასთან დაკავშირებული ანგარეშების და ანალიზების გენერაცია.

Yankee Group-is ანგარიშში მითითებულია, რომ ადაპტაცია შეიძლება გამოიხატოს რეაგირების სხვადასხვა ფორმით, რომლებიც შეიძლება მოიცავდეს:

- ქსელური მართვის სისტემებს შეტყობინებები შეიძლება დაეგზავნოთ SNMP ოქმით, ელ. ფოსტით ან ადმინისტრატორს პეიჯერზე;
- ავტომატური დასრულება სესიისა შეტევის ქვეშ მყოფ კვანძთან ან მომხმარებელთან, ქსელთაშორისი ეკრანის ან სხვა ქსელური მოწყობილობების რეკომენდაცია;
- ადმინისტრატორისათვის რეკომენდაციების გამომუშავება, რაც საშუალებას იძლევა გამოსწორდეს ქსელში აღმოჩენილი სუსტი ადგილები.

ამჟამად მიმდინარეობს საინფორმაციო-საძიებო სისტემის დასრულება, რომელშიც დაგროვდება სხვადასხვა არხებით მოპოვებული ინფორმაცია, როგორც კომპიუტერულ დანაშაულობებზე, ასევე საერთოდ ინფორმაციულ უსაფრთხოებაზე, ინფორმაციული ტექნოლოგიების პერსპექტივებზე და ა.შ., რაც საშუალებას მოგვცემს უფრო სრულად ჩავატაროთ აქ მოყვანილი პრობლემების ანალიზი, გამოვიმუშაოთ რეკომენდაციები, ნორმატიული დოკუმენტები, რაც აუცილებელია საქართველოში ამ მიმართულებით სამუშაოთა გააქტიურებისათვის.

3. დასკვნა

მრიგად, თუ ქსელის განვითარებასთან ერთად არ ხდება მისი უსაფრთხოების უწყვეტი კონტროლი და ანალიზი, მაშინდგოთა განმავლობაში ქსელის დაცულობა ეცემა, ვინაიდან წარმოიშობიან ახალი გაუანალიზებალი მუქარები და სისტემაში სუსტი ადგილები, რომელთა თავიდან აცილება ასეთ ვითარებაში შეუძლებელი ხდება.

4. გამოყენებული ლიტერატურა

1. Волеводз А. Г. Проект Европейской конвенции о киберпреступности. Конфидент, N5, 2001.
2. Трубачев А.П., Егоркин И.В., и др. Общие критерии оценки безопасности информационных технологии. Конфидент,N 2, 2002.
3. გ. ჩოგოვაძე, გ. გოგიჩაიშვილი, გ. სურგულაძე, თ. შეროზია, ო. შონია. მართვის ავტომატიზებული სისტემების დაპროექტება და აგება. თბილისი, სტუ, 2001.

КОНЦЕПЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ

Шония О., Шония Д., Гогохия И., Поладашвили Н.
Грузинский Технический Университет

Резюме

В работе детально проанализированны компьютерные преступления и вопросы борьбы против них. Рассмотрены проблемы информационной безопасности для информационных систем и установлена общая информационная защитная концепция в таких сетях.

SAFETY CONCEPTION OF INFORMATION IN NETS

Shonia Otar, Shonia David, Gogokhia Irakli, Poladashvili Nino
Georgian Technical University

Summary

There are given detailed analyze of computer crimes and questions of struggle against them in the work. Also are considered the problems of informational safety for informational systems and is set the general informational safety conception in such nets.