# ქსელური საინფორმაციო უსაფრთხოების სისტემის ფუნქციონირების პრინციპები

*მიხეილ დვალიშვილი,* დოქტორანტი

**რეზიუმე**

განხილულია საინფორმაციო და სატელეკომუნიკაციო ქსელებში ინფორმაციის დაცვის სისტემების მოწყობის პრინციპები და პრობლემები, ქსელის მრავალდონიანი დაცვის უზრუნველყოფის მექანიზმები. ჩამოთვლილია ინფორმაციის დაცვის სისტემის ნაკლოვანებები. მოცემულია IDS (Intrusion Detection Systems) და IPS (Intrusion Prevention Systems) სისტემების შედარება და მათი ფუნქციონირების ანალიზი. აგრეთვე აღწერილია ქსელური IDS (NIDS), რომელიც არა მარტო იძიებს ქსელში არანორმალურ და არასტანდარტულ პროტოკოლის გამოყენებას, არამედ ბლოკირებას უკეთებს მათ.

**საკვანძო სიტყვები**: არასანქცირებული შეღწევა, ქსელური .

The principles of operation of the network information security systems

M. Dvalishvili , Phd student

**Summary**

The main principles and problems of the information security system structure in the information and telecommunication networks, as well as provision of multi-level safety network mechanisms are discussed.

There are listed the drawbacks of information network security systems. The comparison of IDS systems (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) are given, along with the analysis of their functionality. In addition are offered the description of Network IDS System (NIDS), which is capable of detecting the use of non-standard and abnormal protocols in the network, as well as block these protocols.

**Keywords:** IDS (Intrusion Detection Systems), IPS(Intrusion Prevention Systems),

* * * * *

დაცვის სისტემის მოწყობისას, ტიპიურ შეცდომად ითვლება დავიცვად ყველაფერი ყველაფრისგან უცბად. პირველი ნაბიჯი ინფორმაციული უსაფრთხოების სისტემის მოწყობაშია. საშიშროების სათავის განსაზღვრა, როგორც წესი, რამდენიმეა. გამოვყოთ საშიშროების სათავე - ნიშნავს შევაფასოთ მისი მიზნები (თუ სათავე წინასწარ განსაზღვრულია), ან შესაძლო ზემოქმედება (წინასწარ არ არის განსაზღრული), ალბათობა (ან ინტენსივობა) მისი გამოჩენის. თუ ლაპარაკია პირების ბოროტგანზრახულ მოქმედებაზე, მაშინ საჭიროა შეფასდეს მისი ორგანიზაციული და ტექნიკური შესაძლებლობები ინფორმაციასთან დასაშვებად. მუქარის წყაროს განსაზღვრის შემდეგ შეიძლება ინფორმაციის უსაფრთხოების ფორმირება, ანუ რა შეიძლება მოუვიდეს ინფორმაციას. როგორც წესი შეიძლება განვასხვაოთ მუქარის შემდეგი ჯგუფები:

- ინფორმაციაში არასანქცირებული შეღწევა, კითხვა, კოპირება, ინფორმაციის შეცვლა
- კომპიუტერების და გამოყენებადი პროგრამების მუშაობის შეზღუდვა
- ინფორმაციის განადგურება

სამივე ჯგუფიდან შეიძლება გამოვყოთ ათობით კონკრეტული მუქარები. მუქარები შეიძლება იყოს წინასწარგანსაზღრული ან შემთხვევითი, ხოლო შემთხვევითები, თავის მხრივ, შეიძლება იყოს ბუნებრივი (სტიქიური უბედურება) და ხელოვნური (პერსონალის შეცდომით მოქმედება). შემთხვევითი მუქარები, რომელშიც არ არის ბოროტი ზრახვები, აღწერილია როგორც ინფორმაციის დაკარგვა და სისტემის მუშაობის უნარიანობის დარღვევა, ამისგან შეიძლება ადვილად დავიცვათ თავი. წინასწარგანსაზღრული მუქარები უფრო სერიოზულია ბიზნესის დაკარგვასთან დაკავშირებით, ანუ აქ გვიწევს ბრძოლა არა ბრმა შემთხვევასთან, არამედ მოაზროვნე მოწინააღმდეგესთან.

დაცვის სისტემის მოწყობა, შეიძლება გავატაროთ დაცვის პრინციპებით, რომლებიც საკმარისად უნივერსალურია ყველაზე განსხვავებული არეებისთვის.

**ადეკვატურობა**. დაცვის ერთობლიობის ღირებულება (დრო, ადამიანები და ფულადი რესურსები) უნდა იყოს დასაცავი რესურსების ღირებულებაზე დაბალი. თუ კომპანიის ბრუნვა არის ათიათასი დოლარი თვეში, საეჭვოა სისტემის გაფართოება 1 მილიონ დოლარამდე.

**სისტემურობა**. ამ სისტემის სერიოზულობა განსაკუთრებით გამოისახება მსხვილი დაცვების აგებისას. დაცვის სისტემა უნდა შედგებოდეს არა აბსტრაქტულ, არამედ რეალური მუქარის ანალიზზე, ამ მუქარების დაცვის საშუალებაზე, ამ საშუალებების ოპტიმალური ნაკრების მოძებნაზე და სისტემის მოწყობაზე.

**გამჭირვალობა ლეგალური მომხმარებლებისთვის**. უსაფრთხოების მექანიზმების შეყვანას აუცილებლად მივყავართ მისი მოქმედების გართულებასთან. ამის მიუხედავად არცერთმა მექანიზმა არ უნდა მოითხოვოს შეუსრულებელი მოქმედებები (მაგალითად, ყოველკვირეულად მოვიგონოთ 10 ციფრიანი პაროლი და არსად ჩავიწეროთ ის) ან გააჭიანუროს ინფორმაციასთან დაშვების პროცედურა.

**თანაბარმდგრადი რგოლები**. რგოლები - ეს არის დაცვის ელემენტები, მათი ნებისმიერის გადალახვა ნიშნავს მთელი დაცვის გადალახვას. გასაგებია, რომ არ შეიძლება ერთი რგოლის კონპესირებით გავაძლიეროთ მეორე. ყველა შემთხვევაში, დაცვის სიმყარე განისაზღვრება ყველაზე სუსტი რგოლის სიმყარით. თუ არალოიალური თანამშრომელი მზად არის თანხის საფასურად „ჩააგდოს დისკზე“ მნიშვნელოვანი ინფორმაცია, მაშინ არ მგონია ბოროტმზრახველმა გამოამზეუროს რთული ჰაკერული შეტევა, რათა მიაღწიოს იგივე მიზანს.

**უწყვეტობა**. იგივე თანაბარმდგრადობაა დროის არეში. თუ ჩვენ გადავწყვიტავთ რამეს დაცვას, მაშინ საჭიროა დავიცვათ ისე, როგორც დროის ნებისმიერ მომენტში. არ შეიძლება, მაგალითად გადავწყვიტოთ პარასკევობით გავაკეთოთ სარეზერვო ინფორმაციის კოპირება, ხოლო თვის ბოლო პარასკევს მივაწყოთ „სანიტარული დღე“.

**მრავალდონიანობა**. მრავალდონიანი დაცვა გვხვდება ყველგან. რატომ იწყება დაცვა რამდენიმე დონით, რომელიც უნდა გადალახოს როგორც ბოროტმზრახველმა ასევე ლეგალურმა მომხმარებელმა? სამწუხაროდ, ყოველთვის არსებობს იმის ალბათობა, რომ რომელიმე დონე შეიძლება იყოს გადალახული ან გაუთვალისწინებელი შემთხვევის ძალით ან არანულოვანი ალბათობით. უბრალო მათემატიკა გვკარნახობს: თუ ერთი დონე გვაძლევს დაცვის 90% გარანტიას, მაშინ სამი დონე (არავითარ შემთხვევაში არ იმეორებენ ერთმანეთს) მოგვცემს 99,9%.

ამ პრინციპების გათვალისწინებით, შეიძლება თავიდან ავიცილოთ ზედმეტი ხარჯები დაცვის სისტემის აგების და ამავე დროს მივაღწიოთ ბიზნესის ინფორმაციის უსაფრთხოების მაღალ დონეს. აშკარაა, რომ კორპორაციულ სისტემებზე თავდასხმა გახდა უფრო რეალური. ასეთი საშიშროების დროს დაცვა მოითხოვს „წინმსწრებ ტექნოლოგიებს“, რომელიც გამოიცნობს ვირუსების პროგრამას მათი „ანომალიური“ მოქცევით. დღესდღეობით კომპიუტერული უსაფრთხოების სფეროში არსებობს ორი პრინციპიალურად განსხვავებული მიდგომა კორპორატიულ ქსელში შეღწევის დაცვაზე. პირველი და შედარებით მოძველებულია IDS (Intrusion Detection Systems). IDS-ეს არის სისტემა, რომელიც მოწოდებულია აღმოაჩინოს კერძო ქსელში შეღწევა და გააფრთხილოს სისტემის ადმინისტრატორი შეხწევის ფაქტზე. ინფორმაციის დაცვის ეს ტექნოლოგია გამოიყენებოდა უფრო ადრე და დამკვეთებს შორის მოიპოვა დიდი პოპულარობა. ბევრი ანალიტიკოსი თვლის, რომ დღეს არსებობს უფრო ეფექტური და მოსახერხებელი საშვალებები ჰაკერებთან საბრძოლველად. ეს არის სისტემა IPS. (Intrusion Prevention Systems). IPS-ის აბრევიატურა ინფორმაციულობის დაცულობის სფეროში მიმაგრებულია სისტემებზე და გადაწყვერტილებებზე, რომელიც ემსახურება თავდასხმის აცილებას. მის ქვეშ იგულისხმება ტექნოლოგიების ნაკრები, რომლებიც გამოჩნდნენ ეკრანებს შორის შეერთების ადგილზე და IDS-ზე თავდასხმის აღმოჩენის სისტემაზე. ქსელებს შორისი ეკრანებიდან IDS-ში აღებულია ქსელების შორის ურთიერთქმედებაში აქტიური ჩარევის პრინციპი, ხოლო IDS-დან მომხდარი მოვლენების ინტელექტუალური მეთოდი. ასე, რომ IPS არა მარტო აღმოაჩენს თავდასხმას, არამედ ცდილობს შეაფასოს ის. დღევენდელ ბაზარზე არის სპეციალიზირებული პროდუქტებიც, ისეთები, როგორიცაა IPS აპარატების ოჯახი. (კომპანია Net Screen). IPS პროდუქტებს შორის ანალიტიკოსები გამოყოფენ ხუთი ტიპის კომპონენტებს, რომელთაგან თვითეული ასრულებს თავის ფუნქციას და შეუძლია კომბინირება სხვებთან. მოწყობილობა, რომელიც ანალიზზს უკეთებს მასში გამავალ IP პაკეტს, რომელიც ცდილობს იპოვოს მასში შეტევის ნიშნები, არის ქსელური IDS (NIDS). ტრადიციული IDS-დან ასეთი პროდუქტები განსხვავდებიან იმით, რომ ისინი არა მარტო იძიებენ ქსელურ არანორმალურ და არასტანდარტულ პროტოკოლის გამოყენებას, არამედ ცდილობენ ბლოკირება გაუკეთონ ყველა შეუსაბამობას.

NIDS იყენებს ცნობილი შეტევის სიგნალების ბაზას, მას ასევე შეუძლია თავიდან აიცილოს მისთვის უცნობი შეტევა, განსაკუთრებით მაშინ, როცა ის აგებულია პროტოკოლების ანომალურ გამოყენებაზე. ქსელურ მოწყობილობას, რომელიც განსაზღვრავს IP პაკეტების მარშრუტს, რომელიც დამოკიდებულია დანართის ტიპზე, ეწოდება მეშვიდე დონის კომუტატორი. მისი გამოყენება შეიძლება სხვადასხვა მიზნებისთვის: კლასტერების შექმნა, დატვირთვის ბალანსირება, მონაცემების ტიპების ცალ-ცალკე შენახვა, ასევე დაცვისთვის. მექანიზმს, რომელიც კონტროლს უწევს ქსელური პროგრამების სისტემურ გამოძახებებს, ეწოდება დანართის ეკრანი (Application Firewall / IDS). ის ყურადღებას აქცევს არა ქსელურ ურთიერთმოქმედებას, არამედ პროგრამის მოქცევას და ბიბლიოთეკას, რომელიც მუშაობს ქსელთან. ასეთ ეკრანს შეუძლია იმუშაოს წესების ფიქსირებულ ნაკრებთანაც. IPS კატეგორიას ასევე მიეკუთვნება დანართი - ხაფანგები, რომლებიც ცდილობენ ჩაერიონ შეტევების პროცესში. ასეთი პროდუქტები პროვოცირებას უკეთებენ შემტევს, ხოლო შემდეგ აკონტროლებენ მას. ყველაზე კარგია ხაფანგების კონბინირება კომუტატორებთან - ჰიბრიდებით ან მეშვიდე დონით, რათა რეაგირება მოხდეს არა ძირითადი ინფორმაციის ნაკადზე, არამედ მხოლოდ საეჭვო შეერთებაზე. ხაფანგებს იყენებენ უფრო შესაშინებლად და კონტრშეტევისთვის. აღსანიშნავია, რომ IPS-ს განსხვავებული ტიპები კარგად ინტეგრირდებიან საკმარისად ინტელექტუალურ დაცვის სისტემასთან. ამასთან ისინი კონკურენციას არ უწევენ უკვე არსე-

ბულ ინფორმაციული უსაფრთხოების საშუალებებს: ქსელებსშორისი ეკრანები, IDS, ანტივირუსები და სხვა.

შეძლებენ თუ არა სისტემები თავიდან აიცილონ არასანქცირებული შეღწევები კორპორაციულ ქსელებში. ამ საკითხით არიან შეწუხებული არა მარტო IPS-ის შემკვეთები, უკვე არსებული და პოტენციალური, ასევე შეღწევის აღმოჩენის სისტემის მწარმოებლები, რომლებიც ცდილობენ გაიგონ, როგორ გაუმკლავდნენ ტექნოლოგიას, რომლებიც საფრთხეს უქმნის მათ ბიზნესს. IPS-ის უპირატესობა IDS -თან შედარებით ნათლად გამოისახება კლიენტების ზრდის ფონზე. მაგრამ, რადგან ტექნოლოგიები უფრო რთულდება, კორპორაციული კლიენტები ხშირად განიცდიან სირთულეებს „ჭეშმარიტ“ IPS და მათი გამარტივებული ვერსიების გამოვლინების დროს, ასევე IPS-ს ინტეგრაციის დროს ქსელის ინფრასტრუქტურის განსხვავებულ ელემენტებთან.

შეღწევადობის აცილების სისტემის მუშაობის გადაფასება ძნელია, ბევრი IT სპეციალისტი აგრძელებს მუშაობას შეტევის სისტემის პროფილაქტიკაზე, რომლებსაც შეუძლიათ კომპანიებს მიაყენოს ძალიან დიდი ზარალი. ექსპერტები უშიშროების სფეროში ვარაუდობენ, რომ IPS ტექნოლოგიების დახვეწისას IPS შეერწყმება IDS სისტემას და ქსელთაშორის ეკრანებს, IPS მექანიზმების რიცხვი საგრძნობლად გაიზრდება. IDS-ის კონცეფციამ თავის თავი ამოწურა. ის დღეს პრაქტიკულად არ წარმოადგენს არავითარ ფასეულობას კორპორაციულ მომხმარებლისთვის. არსებობისთვის საჭიროა იმოქმედო სწრაფად, თითქმის იმ სიჩქარით, როგორც ინფორმაცია გადის კაბელში და აუცილებელია მცდარი ამოქმედების საკითხების გადაჭრა. მცდარი ამოქმედება - IDS -ს ერთ-ერთი ყველაზე სერიოზული ნაკლია. IPS-ის ტექნოლოგია საშუალებას იძლევა თავიდან ავიცილოთ ფალსიფიცირებული პოზიტური შედეგების მიღება განსხვავებული მექანიზმების წყალობით. მათ შორის ნაწილობრივ არის სიგნალის ანალიზი, რომელიც იცვლება სესიის შემოწმების დროს. ვირუსების ხშირი გავრცელება ძალიან მოქმედებს ბევრ კლიენტზე. ერთ-ერთ უნივერსიტეტში დააყენეს ქსელის კონსული Unit One -200 Tiping Point Technologis-ის ფირმის, რომელიც საშუალებას იძლევა განვახორციელოთ საშიშროების წყაროს ძიება. შედეგები აღმოჩნდა იმედის მომცემი. Microsoft Sol Server-დან სერვერების სიმრავლის მიუხედავად ქსელში, ჭია Slammer-მა ვერ შეძლო შეღწევა უნივერსიტეტის ვერც ერთ სისტემაში.

დღესდღეობით IPS-ის აბრევიატურა შეიძლება ვნახოთ ბევრ პოპულარულ გამოცემების სათაურებში, ნაწილობრივ Internet Security Systems (ISS) კომპანიის წარმომადგენლებს ეჭვი ეპარებათ პროგნოზებში, რის გამოც IDS უახლოეს პერიოდში უსარგებლო გახდება, ხოლო კლიენტებს დასჭირდებათ უფრო ეფექტური დაცვის საშვალება. სირთულე მდგომარეობს იმაში, რომ მოცემულ მომენტში ეს დარგი არ გვთავაზობს ინტეგრირებულ კორპორაციულ გადაწყვეტილებებს. არის ცალკეული წარმატებული მოდულები, რომლებიც განკუთვნილია კერძო დავალებების შესასრულებლად. ყველა ისინი ღირს ფული. რათქმაუნდა ეს სვავს კითხვებს. ჩვენ არ შეგვიძლია გავიაროთ გრძელი გზა არასრულფასოვანი პროდუქტებით.

საჭიროა ალგორითმების, სიგნალების, პროტოკოლების ანალიზის მყარი საშუალებების გულდასმით შერჩევის შეხამება მეთოდოლოგიებთან, და ყველა ამ მექანიზმების კორელაციით სხვა ტექნოლოგიებთან, რომლებიც უზრუნველყოფენ ქსელის მართვას. ვთქვათ, კომპანიების სინათლეზე გამოდიან IPS-ით, მაგრამ იქნება ეს ქსელებში რისი ეკრანის შემცვლელი? ქსელებსშორისი ეკრანი პროექტირდება, იქმნება და ეწყობა იმისთვის, რომ ვუზრუნველყოთ ფილტრაცია, ეკრანირება და დაშვების კონტროლი. IPS-ის მომავალი დევს არა იზოლირებულ, არამედ ინტეგრირებულ გადაწყვეტილებაში.

## დასკვნა

საინფორმაციო და სატელეკომუნიკაციო ქსელები წარმოადგენს მსხვილმაშტაბიან ქსელებს, რომლებშიც მუდმივად იზრდება აბონენტების რიცხვი. საინფორმაციო და სატელეკომუნიკაციო ქსელების მომხმარებელთა სწრაფი ზრდა წარმოშობს ინფორმაციის დაცვის და უსაფრთხოების პრობლემებს. ინფორმაციული უსაფრთხოების პრობლემების ანალიზმა გამოავლინა, რომ იმ პრობლემების გარდა, რომელიც დაკავშირებულია გლობალური ქსელის გამოყენებასთან, ინტერნეტში, როგორც ინფორმაციულ-ტელეკომუნიკაციურ სისტემაში, რომელიც საკმარისად ნაცნობია და ამოხსნადი, არსებობს აკრძალული კონტენტის ნაკლებად შესწავლილი პრობლემა. აკრძალული ინფორმაციის გავრცელების მოდელების და ალგორითმების შექმნა - ეს არის ერთ-ერთი ძირითადი მიდგომა მოცემული ამოცანის გადასაჭრელად.

**გამოყენებული ლიტერატურა:**


1. Larry L. Peterson, Bruce S. Davie “Computer Networks_a system approach”, 5th edition, 2011. http://booksite.mkp.com/9780123850591/
2. Richardson R. 2009 CSI Computer Crime and Security Survey *II* Computer Security Institute, 2009.
3. Яциковская У.О., Карпинский Н.П. Моделирование сетевого трафика компьютерной сети при реализации атак. http://www.nbuv.gov.ua/portal/natural/Ibez/2011_1/25.pdf
4. http://www.secure.com.ru