კიბერუსაფრთხება და მავნე პროგრამები

ოხანაშვილი სვიმონ
იაკობ გოგებაშვილის სახელობის სახელმწიფო უნივერსიტეტი, თელავი
DOI: https://doi.org/10.52340/idw.2023.72

აბსტრაქტი. *თანამედროვე ტექნოლოგიების განვითარებამ ხელი შეუწყო ვიტუალური სამყაროს - ინტერნეტ სივრცის განვითარებას, სადაც სამუშაო ვიზიტით გადავიდა როგორც კერძო წარმოების და მომსახურების სამსახურები, ასევე სახელმწიფო დაწესებულებები. ამან კი გამოიწვია ინტერნეტ სამყაროში უზარმაზარი ინფორმაციის გავრცელება და გაცვლა, რამაც თავის მხრივ საჭირო გახადა კიბერუსაფრთხოების დონის ამაღლება და განმტკიცება, რაც დღეისათვის იგი წარმოადგენს აუცილებელ და მოთხოვნად თემას.*

ნაშრომი - კიბერუსაფრთხოება და მავნე პროგრამები დღეისათვის ერთ-ერთი ყველაზე აქტუალური თემაა და მოითხოს სხვადასხვა სახის კიბერდანაშაულის საფრთხეების აღმოჩენას, მათი ტიპების განსაზღვრას და საჭირო ღონისძიებების ჩატარებას.

რეალურად ყოველდღე ინტერნეტში არსებობს მაღალი დონის საფრთხეები, რომელთა უდიდესი ნაწილი უკავშირდება კიბერუსაფრთხოებას, რაც თავისმხრივ იგი არის ერთ-ერთი ძირითადი ღონისძიება ასე ვთქვათ ინტერნეტ უსაფრთხოების პოლიტიკა, რომელიც გულისხმობს: სწრაფ აქტიურ რეაგირებას და ქმედებას ინფორმაცის დაცვას სხვადასხვა მავნე პროგრამებისა და ბოროტი ქმედებისაგან.

ინფორმაციული საფრთხეები შეიძლება გამოწვეული იყოს, როგორც ადამიანური ფაქტორებით, როგორიცაა სხვადსხვა სახი მუქარ (უნებლიე, შემთხვევი, გამიზნული), ასევე ბუნებრივი ფაქტორებით: ქარიშხალი, ელვა, მიწისძვრა, წყალდიდობა და ა.შ.

საერთოდ კიბერდანაშაულის დროს ყურადღება მახვილდება: ტექნიკურ, პროგრამულ და ორგანიზაციულ ნაწილზე. პროგრამულ ნაწილში იგულისხმება ოპერაციული სისტემები და გამოყენებითი პროგრამული გარსები, რომლეთა დიდი ნაწილი დამზადებულია სხვადასხვა კომპანიების მიერ და მათი დაისტალირება მოითხოვს საკმაოდ დიდ ყურადღებას თავსებადობის და შესაბამისობის მიმართულებით. ტექნიკურში იგულისხმება ციფრული მოწყობილობები და მათი შესაძლებლობები, ხოლო ორგანიზაციულ დაცვაში იგულისხმება: თანამშრომელთა შერჩევა, განათლება, განაწილება, განთავსება სპეციალურ პოზიციებზე, მათ შორის თანამშრომლობის და ჯგუფური მუშაობის ჩამოყალიბება და ამაღლება, სამსახურეობლივი ეთიკის, იფორმაციის და ქცევის მოთხოვნათა დაცვის გაზრდა.

საკვანძო სიტყვები *– კიბერდანაშაული, კიბერთავდაცვა, კიბერუსაფრთხოება, ინფორმაციული უსაფრთხოება, ქსელური უსაფრთხოება, პროგრამული უსაფრთხოება .*

კიბერუსაფრთხოება ნიშნავს დაცვას ისეთი მოწყობილობებისას როგორიცაა: კომპიუტერები, მობილური ტექნოლოგიები, ელექტრონული სისტემები, სერვერები, ქსელები და ინფორმაციული მონაცემები ბოროტი და მავნე შეტევებისგან.

ტერმინი უსაფრთხოება ხშირად გამოიყენება სხვადასხვა კონტექსტში და ზოგჯერ მას კატეგორიებად ყოფენ, როგორიცაა: კიბერუსაფრთხოება, ინფორმაციული უსაფრთხოება , ქსელური უსაფრთხოება, პროგრამული უსაფრთხოება და სხვა.

დღეისათვის ყველაზე არაპროგნოზირებად და ვირტუალურ სამყაროში ფართოდ გავრცელებულ პრობლემას წარმოადგენს კიბერდანაშაული, რომელიც არის კიბერ უსაფრთხოების საწინააღმდეგო ქმედება და გულისხმობს დანაშაულების სხვადასხვა ტიპს.

ცნობილია, რომ კიბერუსაფრთხოება არის ღონისძიებათა მთელი კომპლექსის ერთობლიობა, რომელიც განკუთვნილია პირადი და სამსახურეობლივი ინფორმაციული სივრცის დასაცავად.

აქ შეიძლება დაისვას კითხვა, თუ ვისგან უნდა დავიცათ ინფორმაცია. ესენი შეიძლება იყვნენ: ჰაკერები, ინსაიდერები და მავნე პროგრამები (ვირუსები).

ჰაკერები არიან (14 – 35 წწ.) პირები - რომლებმაც კარგად იციან თანამედროვე საინფორმაციო ტექნოლოგიები, კომპიუტერები და მათი ოპერაციულ სისტემები, ასევე იციან რამდენიმე მაღალი დონის დაპროგრამირების ენა და შეუძლიათ: ვირუსების და მავნე პროგრამების შექმნა, ქსელებში თვალთვალის დევნება, ინფორმაციის მოპარვა და შეტაევაზე გადასვლა.

ინსაიდერები არიან - პირები, რომლებიც სამსახურებრივი მოვალეობის გამო დაშვებულინი არიან - წვდომა აქვთ საიდუმლო ინფორმაციასთან. ხშირია შემთხვევები, როდესაც ორგანიზაციის გამოუცდელ ახალ ან ყოფილ თანამშრომელ(ებ)ს უფრო დიდი ზარალი და ზიანი მომტანიათ ფირმისთვის - სამსახურისთვის, ვიდრე ნებისმიერ ჰაკერს ან მავნე პროგრამას.

ასეთ მაგალითს წარმოადგენს ცნობილი ინსაიდერი აშშ - NSA - ნაციონალური უსაფრთხოების სააგენტოს თანამშრომელი ედუარდ სნოუდენი, რომელმაც მოიპარა უზარმაზარი საიდუმლო ინფორმაცია და გასაჯაროვა.

მავნე პროგრამები არის - **Malware** ინგლისური სიტყვების **Mal**icious Soft**ware** აბრევატურა და წარმოადგენს ისეთ კომპიუტერულ ბოროტ პროგრამებს, რომლებიც ასრულებენ მავნე ქმედებებს: კომპიუტერული სისტემების ბლოკირებას, წაშლას, ფაილ(ებ)ის მოპარვას, გადაადგილებას, შიგთავსების სხვა ინფორმაციით შეცვლას, ვირუსების გავრცელებას, ინფორვაციის მოპარვას, თვალთვალის დევნება და კიდევ მრავალ სხვა მავნე ქმედებას.

ცნობილი მავნე პროგრამებს ტიპებია:

ა) **Spyware - ჯაშუში** – აკონტროლებს მომხმარებლის აქტივობას, რას აკეთებს სად შედის, რომელ პროგრამას იყენებს, ვის ესაუბრება და კიდევ სხვა მრავალ ინფორმაციას იხსომებს და შემდეგ გადასცემს წინასწარ მიცემულ მისამართებზე.

ბ) **Adware - არის** იძულებითი რეკლამის გამავრცელებელი, რომელიც მომხმარებლის სურვილის საწინააღმდეგოდ აწვდის მოსაბეზრებელ და არასასურველ რეკლამებს.

გ) **Phishing - ფიშინგი** – არის თევზაობა, რომელიც მოტყუებით მომხმარებელს გადაიყვანს სხვა ვებგვერდებზე და ახდენს მის სხვადსხვა სახის პირად ინფორმაციის მოპარვას (CV, პაროლი, პლასტიკური ბარათის ნომერი და სხვა.)

დ) **Spam - სპამი** არის არასასურველი და არაფრის მომცემი ელექტრონული წერილი, რომლებიც მოხმარებელს ნების საწინაღმდეგოდ ეგზავნება საკმაოდ დიდი რაოდენოვით. წერილი შეიძლება შეიცავდეს, რაიმის პროპაგანდას, რეკლამას ან ტყულს რაიმე საგნის ან თანხის მოგების შესახებ. პროგრამა-სპამ(ერ)ი ნიშნავს, რომ მომხმარებლის კომპიუტერი წარმოადგენს სპამის გავრცელების ნაწილს ანუ ბოტნეტს.

ე) **Ransomware - გამომძალველი** – პროგრამის ძირითადი მიზანია მომხმარებლის კომპიუტერს შეუქმნას ტექნიკური პრობლემები, რაც შეიძლება იყოს ფაილების დაშიფრვა, მოპარვა, წაშლა და შემდეგ მათი აღდგენისათვის - დაბრუნებისათვის თანხის მოთხოვნა. ასევე ახდენს ქსელში ცრუ ინფორმაციის გავრცელებას, მუქარას, ფსიქოლოგიური ზეწოლას და

დაშინებას.

ვ) **Cyber Bullying - კიბერბულინგი** - არის ადამიან(ებ)ის მიერ, ციფრული ტექნოლოგიების დახმარებით რომელიმე ორგანიზაციის, ადამიანთა ჯგუფის ან რომელიმე კონკრეტული ადამიანის შეურაცყოფა და დამცირება ინტერნეტ სივრცეში.

ზ) კიბეროომი - არის რეალური ომის პარალელურად ან მანამე მიმდინარე კიბერთავდასხმები ქვეყანაზე. 2008 წელს რუსეთი ომს აწარმოებდა საქართველოზე და მის პარალელურად ახორციელებდა კიბერშეტევებს.

კიბერ შეტევის რამდნიმე ათეული სახე არსებობს, თუმცა ჩვენ განვიხილავთ ყველაზე ხშირად გამოყენებულ შეტევებს, როგორიცაა:

- პასიური შეტევა - Passive Attack
- აქტიური შეტევა - Active Attack
- განაწილებული შეტევა - Distributed Attack
- ჰაკერით შეტევა - Close-in Attack
- სნიფინგი შეტევა - Sniffing -
- სპამით შეტევა - Spoof spoofing
- DDoS შეტევა - Distributed-Denial-of-Service
- ბუფერის გადავსებით შეტევა - Buffer overflow (Smurf)
- სინქროზული შეტევა - SYN floods
- ტროიანები შეტევა - Trojan . . .

- Passive Attack - პასიური შეტევის დროს დგინდება დაუცველი ტრაფიკი, საიდანაც ხდება ინფორმაციის და პაროლების გაგება.
- Active Attack - ესა არის აქტიური შეტევა, როცა ჰაკერი დაცულ სისტემეზე ახდენს შეტევას, აქ შეიძლება გამოიყენოს ვირუსები და სხვადასხვა შესაძლებლობები.
- Distributed Attack - ეს არის განაწილებული შეტევა, რომლის დროსაც ჰაკერი სისტემას თავაზობს რაიმე კოდს, რომელსაც სისტემა ჩათვლის დაცულ კოდად და შემდეგ იწყება შეტევა როელსაც გარკვეული ზიანი მოაქვს.
- Close-in Attack - აქ თუ ჰაკერი ქსელს მიახლოვდება და მოიპივებს ინფორმაციას ქსელის შესახებ მაშინ შეტევას ადვილად განახოეციელებს.
- Social Engineer - აქ ჰაკერი იღებს პირად ინფორმაციას სხვადასხვა სოციალური ქსელების გამოყენებით რომელსაც მომხმარებელი ხშირად ავრცელებს.
- Sniffing - აქ ხდება ქსელში გამავალი მონაცემების მოსმენა - მოპარვა პასიურად და შემდეგ შეგროვილი ინფორმაციის საფუძველზე ხდება შეტევები.
- Distributed-Denial-of-Service (DDoS) ეს ის შემთევა, როდესაც გატეხილ რამდენიმე საიტზე ხდება შეტევა ერთდროულად ძალიან ბევრ მოთხოვნებზე.
- Buffer overflow – აქ მსხვერპლს ეგზავნება აპლიკაცია ბევრ მონაცემებზე ხდება გადავსება ბუფერის, რაც ახდენს სიტუაცის შეცვლას და თავდამსხმელი ადმინისტრაციულ უფლებებს იძენს.
- ელექტრონული წერილი Spoofing წარმოშობილია spoof ინგლისური სიტყვისგან და ქართულად **გაყალბებას**ს ნიშნავს. მისი გამომგზავნი ცდილობს წერილი დაამგზავსოს ლეგიტიმურ წყაროებიდან გამოგზავნილს, როგორიც შეიძლება იყოს ცნობილი კომპანია, ბანკი, სახელმწიფო დაწესებულება ან სხვა რომელიმე კერძო ორგანიზაცია.
- Trojan - ეს აის მავნე პროგრამა, რომელიც ტროიან ვირუსის გამოყენებით ახდენს მომხმარების ბლოკირებას და გარკვეული ინფორმაციის მოპარვას.

მსოფლიოში ყველა ქვეყანა ცდილობს შექმნას ისეთი კიბერ თავდაცვა, რომელიც

აამაღლებს ქვეყნის იმიჯს, საერთაშორისო ურთიერთობებს, კავშირებს, ეკონომიკას და ქვეყნის ბედს.

კიბერ თავდაცვაა, ეს ის შემთხვევაა, როდესაც მაღალ დონეზე ხდება კიბერ შეტევების აღმოჩენა, ანალიზი, კონტროლი და მისი და აღმოფხვრა.

დღეს კიბერ თავდასხმები და შეტევები გახდა უფრო რთული და კომპლექსური რაც დიდ საფრთხეს უქმნის ქვეყნის ეკონომიკას და საეთოდ უსაფრთხოებას ყველა მიმართულებით.

კიბერ შეტევები დღეს არის ობიექტური რეალობა, რომელიც საკმაოდ რთული დასაცავია. თუმცა მასშტაბური შეტევის დროს შესაძლებელია წინასწარ მოვემზადოთ გარკვეული უკვე არსებული მსოფლიო გამოცდილების მასალებით (სპეციალური პროგრამები, მოწყობილობები და ალგორითმები) და მათ გამოყენებით გარკვეული წინააღმდეგობა გაუწიოთ.

კიბერ თავდაცვის დროს ძირითადად იხილავენ ორ სახეს: პასიურს და აქტიურს.

პასიური თავდაცვის დროს აუცილებელია ქვეყანას მაღალ დონეზე ჰქონდეს დამუშავებული ის სტრატეგიები, რომელიც შესაძლებელია კიბერ შეტევის დროს იქნეს გამოყენებული

აქტიური კიბერ-თავდაცვის დროს აუცილებელია თავდასხმის დაწყებამდე უფრო ზუსტად ყოველდღიურად წინასწარ ხდებოდეს ანალიზის ჩატარება, ხოლო თავდასხმის დროს აუცილებელია სწარაფი რეაგირება და სათანადო პრაქტიკული და თეორიული მასალების გამოყენება. შეტყობინება ქვეყნის მაშტაბით შესაბამის სამსახურებში, პროგრამების ბლოკირება, დაცვითი სისტემების გააქტიურება და ტექნიკასთან წვდომის გამორთვა.

კიბერ თავდაცვა გულისხმობს ყოველთვის მზადყოფნას.

ქვეყნის კიბერთავდაცვა მაღალ დონეს ვერცერთმა სახელმწიფომ ვერ შეძლო. თუმცა ამ მიმართულებით ქვეყნები ერთმანეთთან თანამშრომლობენ და დღეისათვის შექმნილია კიბერუსაფრთხოების საერთაშორისო გაერთიანება.

ამერიკის შეერთებული შტატები იყო პირველი ქვეყანა, რომელმაც შეიმუშავა კიბერუსაფრთხოების სტრატეგია 2000 წელს, მას სამი წელი დასჭირდა იმისათვის, რომ დაეხვეწნა და სრულყოფილად გამოექვეყნებინა ქვეყნის კიბერ-სივრცის უსაფრთხოების ეროვნული სტრატეგია (NSSC), სადაც ფართოდ არის განხილული ეროვნული უსაფრთხოების სხვადასხვა ტიპის სტრატეგიები (NSHS).

საქართველოში ინტერნეტ ქსელში ჩართულია მილიონზე მეტი მომხმარებელი, თუმცა ზოგიერთ რეგიონებში არსებობს ინტერნეტთან წვდომის პრობლემა და გარკვეული რაოდენობის სოფელები ჯერ კიდევა არ არის ჩართული ინტენეტში.

საქართველოში ინფორმაციული და კიბერ უსაფრთხოებაზე პასუხის მგებელია საქართველოს ეროვნული უშიშროების საბჭო (სეუს - NSC) რომლის მიზანია ქვეყანაში უსაფრთხოების პოლიტიკის განსაზღვრა და სპეციალური კონცეფციების შემუშავება.

კიბერუსაფრთხოების სტრატეგია საქართველოში შემუშავრბული იქნა 2008 წელს რუსეთ - საქართველოს ომის დროს, როდესაც რუსეთმა განხორციელა სხვადსხვა ტიპის მასიური შეტევები, მათ შორის კიბერშეტევაც ინტერნეტ სივრცეზე, რის გამოც დროის გარკვეულ პერიოდში პარალიზებული იყო კერძო და სამთავრობო ვებ - გვერდები.

ქვეყანაში კიბერუსაფრთხოების განვითარების აღმა სვლა დაიწყო 2010 წელს ეტაპობრივად და ჩამოყალიბდა საქართველოს იუსტიციის მმართველობაში შემავალი მონაცემთა გაცვლის სააგენტო.

2012 წელს შეიქმნა კიბერდანაშაულთან ბრძოლის ცენტრალური სამმართველო;

2014 წელს კიბერუსაფრთხოების ბიურო;

2013-2016 წელს შეიმუშავებული იქნა საქართველოს თავდაცვის სამინისტროს მიერ კიბერ-უსაფრთხოების პოლიტიკა.

2017-2018 წლებში მეორედ გამოაქვეყნა საქართველომ კიბერუსაფრთხოების სტრატეგიები.

დღეისთვის საკმაოდ მოწესრიგებული და სათანადოდ მომზადებული სპეციალისტებით არის შევსებული აღნიშნული სამსახურები და გამართულად მუშაობენ.

კიბერდანაშაული ყოველდღიურად იცვლება და იგი უფრო საშიში და სერიოზული პრობლემა ხდება მთელ მსოფლიოში განსაკუთრებით ბიზნესისთვის.

ცნობილია, რომ ბოლო 20 წლის განმავლობაში კიბერ დანაშაულის ყოველ წლიურმა ღირებულებამ 2026 ტრილიონ დოლარს გადააჭარბა. სტატისტიკოსებმა დაადგინეს, რომ ყოველდღე 2244 კიბერშეტევა ხორციელდება, ანუ წელიწადში ეს არის 800 000 -სზე მეტი შეტევა, რაც იმას ნიშნავს, რომ ყოველ ორ წუთში სამი შეტევა ხორციელდება. ასევე გამოთვლილია 2023 წლის კიბერდანაშაულის გლობალური ზიანის მოტანის პროგნოზირება: წელიწადში, თვეში, კვირაში, დღე-ღამეში, საათში, წუთში და წამში.

წელიწადში	8	ტრილიონი დოლარი
თვეში	666	მილიარდი დოლარი
კვირაში	153.84	მილიარდი დოლარი
დღე-ღამეში	21.9	მილიარდი დოლარი
საათში	913.24	მილიონი დოლარი
წუთში	15.2	მილიონი დოლარი
წამში	253 679	დოლარი

ცხრილი N1

საკმაოდ შრომატევადი და აღმოსაჩენათ ძალიან ძნელია კიბერ შეტევის აღმოჩენა და შემდეგ შეჩერება ამას თვეები, კვირები, დღეები და საათები ჭირდება. მაგალითად: კიბერ-შეტევის აღმოსაჩენად და შესაჩერებლად სჭირდება 287 დღე (პატარა ორგანიზაციისთვის 212 დღე, შესაკავებლად 75 დღე)

დასკვნა

კიბერდანაშაული ყველზე გავრცელებული დანაშაულია და არის მართლსაწინააღმდეგო ქმედება და ყველა დამნაშავე ისჯება. კიბერდამნაშავეები ინფორმაციის მოსაპარად იყენებენ სხვადასხვა ტიპის მავნე ქმედებებს, როგორიცაა: სპამისა და ვირუსის გავრცელება, ინტერნეტ თაღლითობა, ფიშინგი, ქურდობა, სხვისი კომპიუტერის უნებართვო გამოყენება და წვდომა, დაშინება და ა.შ.

კიბერუსაფრთხობისათვის და დანაშაულის თავიდან აცილების მიზნით აუცილებელია:

ა) კომპიუტერს და საჭირო პროგრამებს დაედოს რვა ან მეტ სიმბოლოიანი პაროლები და მათი განახლება - შეცვლა მოხდეს ყოველ თვე.

ბ) მუდმივად განახლდეს სერთიფიცირებული ანტივირუსული პროგრამები ახალი ვარიანტებით.

გ) არავის ანდოთ ან გადაუგზავნოთ საკუთარი პირადი ინფორმაცია, პაროლები, საკუთარი მიმოწერის მისამართები და მასალები.

დ) მინიმუმ კვირაში ერთხელ მაინც წაშალეთ ზედმეტი ფაილები კომპიუტერიდან სპეციალური პროგრამების ან/და ბრძანებების („temp%") გამოყენებით.

ე) თუ გახდით კიბერთავდასხმის მსხვერპლი ან იცით მგზავსი ინფორმაცია დაუკავშირდით სპეციალურ ორგანიზციებს ცხელი ხაზზე (112, 2 41 12 96, cybercrime@mia.gov.g)

გახსოვდეთ, საქართველოში მიღებულია კანონი ინფორმაციული უსაფრთხოებისა და კიბერდანაშაულის შესახებ და მისი ჩამდენი ისჯება მიღებული კანონის მიხედვით.

ლიტერატურა:

1. https://ge.itstep.org/blog/a-wide-range-of-cyber-security-a-new-generation-of-non-mobile-viruses-and-the-principle-of-their-operation კიბერუსაფრთხოების ფართო სპექტრი - ახალი თაობის არაფაილური ვირუსები და მათი მუშაობის პრინციპი
2. https://eufordigital.eu/geo/discover-eu/cybereast-action-on-cybercrime-for-cyber-resilience-in-the-eastern-partnership-region/ CyberEast – კიბერდანაშაულზე ქმედება
3. https://police.ge/files/pdf/kiber_danashauli/Convention%20on%20Cybercrime%20GEO.pdf კონვენცია კომპიუტერული დანაშაულის შესახებ
4. https://www.websiterating.com/ka/research/cybersecurity-statistics-facts/#sources კიბერუსაფრთხოების სტატისტიკა, ფაქტები და ტენდენციები 2023 წლისთვის

Cyber security and malware

Okhanashvili Svimon

Iakob Gogebashvili State University, Telavi

Abstract

The development of modern technologies contributed to the development of the virtual world - the Internet space, where both private production and service departments, as well as state institutions, went on a work visit. This led to the spread and exchange of huge information in the Internet world, which in turn made it necessary to raise and strengthen the level of cyber security, which today is a necessary and demanding topic.

Thesis - Cyber security and malware is one of the most relevant topics today and calls for the detection of various types of cybercrime threats, their types and the implementation of necessary measures.

In fact, every day there are high-level threats on the Internet, most of which are related to cyber security, which in turn is one of the main measures, so to speak, of the Internet security policy, which implies: quick active response and action to protect information from various malicious programs and malicious actions.

Information threats can be caused both by human factors, such as various types of threats (unintentional, accidental, targeted), and by natural factors: storms, lightning, earthquakes, floods, etc.

In general, during cybercrime, attention is focused on: technical, software and organizational part. The software part refers to operating systems and application software shells, most of which are made by different companies and their installation requires a lot of attention in the direction of compatibility and compliance. Technical refers to digital devices and their capabilities, while organizational protection refers to: employee selection, education, distribution,

placement in special positions, including the formation and enhancement of cooperation and teamwork, increasing the protection of work ethic, information and behavior requirements.

Keywords: cyber crime, cyber defense, cyber security, information security, network security, software security