Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 62-65 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

ATTACKS ON WIRELESS NETWORKS AND THEIR PREVENTIONS

უსადენო ქსელზე ორიენტირებული თავდასხმები და მათი პრევენცია

გიორგი იაშვილი -კავკასიის უნივერსიტეტი

Giorgi Iashvili – Caucasus University

გიორგი მელაძე - კომაროვი

Giorgi Meladze - Komarovi

გეგი ჩაჩიბაია -კომაროვი

Gegi Chachibaia-Komarovi

ლაშა ჯანჯალაშვილი - 1 კლასიკური გიმნაზია

Lasha Janjalashvili – 1 Classic Gymnasium

გეგა შავდათუაშვილი - აია -Gess

Gega Shavdatuashvili Gess

ABSTRACT. This article distinguishes between wireless (wifi) and wired networks, in particular, discusses the pros and cons of wireless and wired networks, and provides recommendations for their relatively more secure use.

აბსტრაქტი. მოცემული სტატია განასხვავებს უსადენო (wireless-wifi) და სადენიან (wired) ქსელებს, კერძოდ განიხილავს უსადენო და სადენიანი ქსელების უსაფრთხოების მინუსებს და პლიუსებს, ასევე მოცემულია რეკომენდაციები მათ შედარებით მეტად უსაფრთხოდ გამოყენებისთვის

საკვანძო სიტყვები: *Wireless-Wifi(უსადენო), Wired(სადენიანი).*

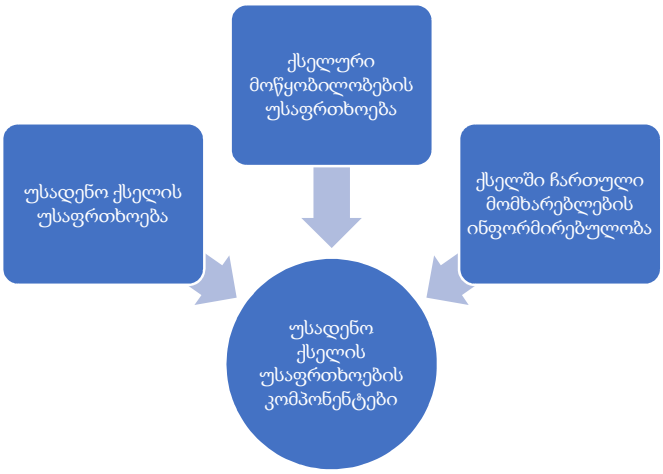
KEYWORDS: *Wireless-Wifi, Wired.*

შესავალი

XXI საუკუნე ტექნოლოგიების საუკუნეა, ტექნოლოგიის დაკავშირება სამყაროსთან კი სწორედ ქსელის გავლით ხდება. გამოყოფენ ქსელის 2 ძირითად კატეგორიას სადენიან (Wired) და უსადენო (Wireless) ქსელებს. ორივეს გააჩნია თავისი დადებითი და უარყოფითი მხარეები, რაც მომხმარებლის კომფორტულ ინტერესებზეა დამოკიდებული.

უსადენო ქსელის უსაფრთხოების კომპონენტები

უსადენო ქსელი იმდენად დაცულია, რამდენადაც უსაფრთხოა ქსელური მოწყობილობები და კომპიუტერები, ამასთან გათვითცნობიერებულია ამ ქსელში ჩართული ყველა მომხმარებელი. აქ საუბარი არ არის თუ რომელი უფრო მეტად მნიშვნელოვანია – საერთო ჯამში ზემოთქმული სამივე კომპონენტი ადგენს უსადენო ქსელის დაცულობის დონეს.



“wireless “ ქსელის მოწყვლადობის მთავარი კომპონენტია ქსელში ჩაბმული მოწყობილობების დაცულობა. მაგალითად შეგვიძლია ავიღოთ სისუსტეების შემცველი როუტერი, რომელსაც შეუძლია მთლიან ქსელს შეუქმნას საფრთხე, თუნდაც მოწყობილობაში არსებობდეს ძლიერი ფაიერვოლი და ამასთან უსაფრთხოების განახლებები.

ქსელური უსაფრთხოების კომპონენტებია ასევე კომპიუტერები და ის მოწყობილობები რომლებითაც ვუკავშირდებით ამა თუ იმ ქსელს. არსებობს უამრავი ქეისი სადაც დაუცველმა მოწყობილობამ დიდი რაოდენობის ზარალი მიაყენა ამა თუ იმ კომპანიას. მაგალითისთვის:

https://www.nytimes.com/2005/08/17/technology/virus-attacks-windows-computers-at-companies.html

ბოლო და ერთ-ერთი მნიშვნელოვანი კომპონენტია – მომხმარებელი – მოხმარებელმა საჭიროა ზუსტად იცოდეს, თუ როგორ გამოიყენოს wifi ქსელი უსაფრთხოდ, რადგან რისკი იმდენად მაღალია, რომ wifi-ს პაროლის გაზიარების შემთხვევაში შეუძლებელი ხდება ქსელი დაიცვა თუნდაც უახლესი ფაიერვოლით და როუტერით.

Wireless ქსელის უსაფრთხოების მთავარი გამოწვევები

უსადენო ქსელის ძირითადი შიდა და გარე გამოწვევები მოიცავს შემდეგს:

- უცხო პირები რომლებიც უსადენო ქსელის „გატეხვას“ ცდილობენ:
- Brute-Force შეტევა პაროლის ამოსაცნობად როგორც მოწყობილობაზე ისე WiFi-ზე
- შიფრაციის სისუსტეების გამოყენება
- მოწყობილობის სისუსტეების გამოყენება
- არასწორი კონფიგურაცია

- ფიშინგ შეტევა (მაგალითად, ზარი საფორთთან ასეთი შინაარსის ტექსტით, საკონფერენციო ოთახში ვარ და პაროლი დამავიწყდა. შემახსენეთ პაროლი თუ შეიძლება)

სტუმარი, რომელსაც WiFi სჭირდება

კომპანიის თანამშრომლები:

- ფიშინგ შეტევის ვერ გამოცნობა და მონაცემების გაცემა
- დავირუსებული ბარათების შეერთება კომპიუტერში და ვირუსების ქსელში გავრცელება
- მიღებული „ლეგიტიმური“, რეალურად ვირუსული ფაილების გახსნა
- ქსელში ჩართული მოწყობილობის ღიად დატოვება
- ქსელთან დაკავშირებული პორტატული (მობილური, ლეპტოპი) მოწყობილობის დაკარგვა

ქსელის დაცვა თანამედროვე მიდგომებით

ცხადია , რომ სადენიანი ქსელების შემთხვევაში, რისკი ფიზიკური კონტაქტისა უნდა იყოს მინიმუმამდე დაყვანილი. სადენიან ქსელზე წვდომის მოპოვება მხოლოდ ფიზიკურად დაკავშირებით შეიძლება და აშკარაა რომ ეს მისი უსაფრთხოების აუცილებელი და ყველაზე მთავარი შემადგენელი ნაწილია. მოწყვლად ადგილებში კი საჭიროა დაყენდეს სათვალთვალო სისტემები (კამერები).

სხვადასხვა რეკომენდაციებიდან გამომდინარე, რომ შევაჯამოთ რეკომენდირებულია რომ ერთ ცალკეულ კომპანიაში არსებობდეს ორი ან ორზე მეტი უსადენო ქსელი. ვინაიდან აუცილებელია თანამშრომლები, სხვა მომხმარებლებისგან იზოლირებულ ქსელში იყვენენ ჩაბმულნი.

ცალკეულ შემთხვევებში, ქსელების იზოლირებისთვის კომპანიები იყენებენ რამდენიმე უსადენო ქსელს, რომლებზეც მხოლოდ ადამიანთა კონკრეტულ ჯგუფებს აქვთ წვდომა.

თანამედროვე წვდომის წერტილებს გააჩნიათ - თაღლითი წვდომის წერტილების (rogue AP) აღმოჩენის, დაბლოკვისა და გათიშვის საშუალება. მაგალითისათვის კი მათ აქვთ საშუალება აღმოაჩინონ აუტორიზებული უსადენო ქსელის მსგავსი სახელის მქონე ჰაკერის მიერ ჩართული არააუტორიზებული უსადენო ქსელი და დაბლოკონ ის. რისკების შესამცირებლად, რეკომენდებულია ძველი Access Point-ების ახლით ჩანაცვლება.

ქსელური თავდასხმების პრევენცია

ქსელს უნდა იცავდეს თანამედროვე შესაძლებლობების მქონე ფაიერვოლი, ქსელური მოწყობილობები და კომპიუტერები დაცული იყოს, თანამშრომლები კი – ინფორმირებულნი. უფრო დეტალურად:

- ქსელური მოწყობილობები ფიზიკურად უნდა იყვნენ დაცული (რთულად ხელმისაწვდომ ადგილას);
- ქსელურ მოწყობილობებს უნდა გააჩნდეთ ძლიერი პაროლი, რომელიც არავითარ შემთხვევაში არ იქნება "Default";
- წვდომის წერტილები ისე უნდა იყოს განაწილებული რომ ტალღების გავრცელება რაღაც საზღვრებს მიღმა იზღუდებოდეს;
- WiFi იმდენად არის დაცული, რამდენადაც ძლიერია მისი შიფრაცია, პაროლი კი – გრძელი. ამიტომ WiFi-ს უნდა ჰქონდეს 10 ან მეტი სიმბოლოსგან შემდგარი რთული პაროლი, რომელიც დაცულია WPA2 (ან თუ მხარდაჭერა აქვს უახლესი WPA3) პროტოკოლით;
- დისტანციური კავშირის დროს, საჭიროა კომპანიის კუთვნილი, ან მის მიერ დაშვებული მომწოდებლის VPN-ის გამოყენება;
- ქსელურ მოწყობილობებზე განახლებები და პატჩები უნდა დაყენდეს დროულად;
- აუცილებელია შეღწევადობის ტესტირების ჩატარება წელიწადში ერთხელ მაინც;
- კომპანია დაცული უნდა იყოს ოფიციალურად შეძენილი ანტივირუსით;
- აუცილებელია თანამშრომლების ინფორმირებულობა და ტრენინგები ;
- მიუხედავად იმისა, რომ დიდ შრომას და ადამიანურ რესურს მოითხოვს მნიშვნელოვანია MAC მისამართის ფილტრაცია და ე.წ White List-ის შექმნა.

დასკვნა

მიმოვიხილეთ სადენიანი და უსადენო ქსელები, მათი დადებითი და უარყოფითი მხარეები, შევაჯამეთ მათი მნიშვნელობა დღევანდელობაში და მათი უსაფრთხოების აუცილებლობა, მათ შორის თუ რა ზომები უნდა გატარდეს თავდასხმების პრევენციისთვის.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

ბიბლიოგრაფია

1. Computer Networking: A Top-Down Approach (6th Edition) – Kurose and Ross
2. Wireless Networks by Clint Smith and Daniel Collins (2014)
3. Wireless Networking Absolute Beginner's Guide by Michael Miller (2013)
4. S Gnatyuk, V Kinzeryavyy, M Iavich, D Prysiazhnyi, K Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, ICTERI Workshops, 657-668