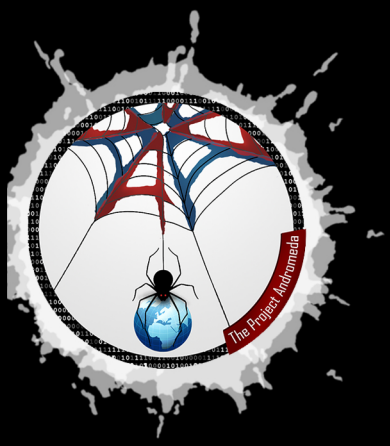


კიბერ უსაფრთხოება

კურსი დამწყებთათვის

თბილისი
2019

კიბერ უსაფრთხოების კურსი დამწყებთანთვის

წინასიტყვაობა

პირველად საქართველოში, კიბერ უსაფრთხოების კომპანია ,,პროექტი ანდრომედა" გთავაზობთ Cisco-ს კურსს კიბერ უსაფრთხოების საწყისებზე. ეს კურსი შედგენილია მსოფლიოს მოწინავე კიბერ უსაფრთხოების და ქსელური ტექნოლოგიების სპეციალისტების მიერ. ის მოიცავს აღნიშნული დისციპლინის ფუნდამენტებს, ტერმინთა განმარტებებს და ინფორმაციას საინტერესო მომავლის პერსპექტივებთან დაკავშირებით.

თარგმანი შესრულდა პროექტ ანდრომედას დირექტორის, ბატონი ალექსანდრე ღლონტის უშუალო ჩართულობით. გარკვეული ტერმინების თარგმნა იყო შეუძლებელი, არა იმიტომ, რომ ქართულ ენაში შესატყვისი ტერმინები არ არსებობს, არამედ იმიტომ, რომ შესაბამის სიტყვებს განსხვავებული აზრობრივი მნიშვნელობა აქვთ. ზოგი ტერმინის გადათარგმნა კი უბრალოდ შეუძლებელია.

იმედი გვაქვს, კურსი მოგეწონებათ და აღმოაჩენთ მრავალ საინტერესო და პრაქტიკულ სიახლეს.

შესავალი

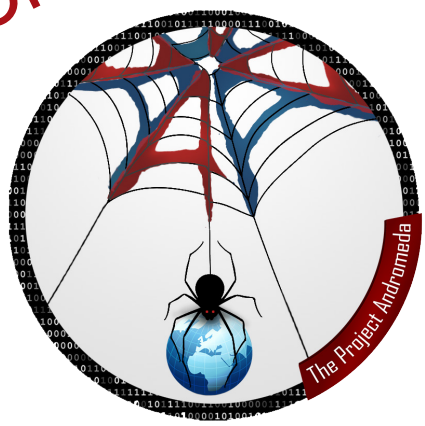
ბავშვობაში, დიდი ალბათობით, ოცნებობდით გამხდარიყავით სუპერ გმირი, რომელიც დაიცავდა მთელ სამყაროს ბოროტი ძალებისგან. გინდოდათ საფრთხის აღმოჩენა, უდანაშაულოთა დაცვა, ბოროტმოქმედების მოძებნა და მათი გადაცემა მართლმსაჯულებისთვის.

იცით, რომ არსებობს ასეთი პროფესია?

- კიბერ უსაფრთხოების გურუ;
- კიბერ უსაფრთხოების კრიმინალისტი;
- ინფორმაციული უსაფრთხოების ექსპერტი;
- ეთიკური ჰაკერი.

კიბერ უსაფრთხოების მოთხოვნად და მაღალანაზღაურებად საქმიანობაში შეძლებთ ზემოაღნიშნული როლების მორგებას.

WWW.THEPROJECTANDROMEDA.COM



სარჩევი

სარჩევი

ᲙᲣᲠᲡᲘᲡ ᲛᲘᲛᲝᲮᲘᲚᲕᲐ

კურსის სათაურიდან გამომდინარე, ალბათ მიხვდით, რომ ჩვენი ძირითადი მიმართულება იქნება კიბერ უსაფრთხოება. ამ კურსში თქვენ დაეუფლებით შემდეგ ცოდნას:

- *ონლაინ უსაფრთხოების საწყისებს;*

- *ინფორმაციას სხვადასხვა ტიპის მავნებელი პროგრამების და კიბერ შეტევების შესახებ. ასევე, საკუთარი თავის და დამსაქმებლის დაცვას აღნიშნული შეტევებისგან;*

- *კიბერ უსაფრთხოების კარიერულ შესაძლებლობებს.*

კურსის დასასრულს, თქვენი ონლაინ უსაფრთხოების, კიბერ თავდასხმების პოტენციური შედეგების და კიბერ უსაფრთხოების კარიერული შესაძლებლობების ცოდნა საგრძნობლად გაიზრდება.

თავი 1.

კიბერ უსაფრთხოების საჭიროება

ამ თავში განვიხილავთ კიბერ უსაფრთხოების მიმართულებას და მისთვის დამახასიათებელ ნიშნებს. აქვე ავხსნით, რატომ არის ამხელა მოთხოვნილება კიბერ უსაფრთხოების სპეციალისტებზე და რატომ აგრძელებს ეს მოთხოვნა დინამიურ ზრდას. ასევე, გავამახვილებთ ყურადღებას იმ გარემოებაზე, თუ რატომ არის თქვენი ონლაინ იდენტობა და ინფორმაცია დაუცველი კიბერ დამნაშავეებისგან. გარდა ამისა, ჩვენ მოგცემთ რჩევებს საკუთარი ონლაინ იდენტობის და ინფორმაციის დაცვისთვის.

პირველთავშიასევეშევეხებითორგანიზაციულ/კორპორაციულ ინფორმაციას და ავხსნით, თუ რატომ საჭიროებს ის დაცვას. აგრეთვე, მოვახდენთ კიბერ დამნაშავეების კატეგორიზაციას და ვისაუბრებთ მათი ქმედების მოტივებზე. კიბერ უსაფრთხოების პროფესიონალ სპეციალისტს უნდა გააჩნდეს იგივე ცოდნა, რაც კიბერ დამნაშავეს, მაგრამ ის უნდა მუშაობდეს ეროვნული და საერთაშორისო სამართლის ფარგლებში. ასევე, კიბერ უსაფრთხოების ექსპერტებმა უნდა გამოიყენონ თავიანთი შესაძლებლობები ეთიკის ნორმების დაცვით.

ამ თავში ზედაპირულად განვიხილავთ კიბერ ომის კონცეპტს და რისთვის სჭირდება სახელმწიფოებს კიბერ უსაფრთხოების სპეციალისტები თავიანთი მოქალაქეების და ინფრასტრუქტურის დასაცავად.

ჰა არის კიბერ უსაფრთხოება?

ერთმანეთთან შეერთებული ელექტრონული ინფორმაციის ქსელი გახდა ჩვენი ყოველდღიურობის განუყოფელი ნაწილი. ნებისმიერიორგანიზაცია,მაგალითადსამედიცინო,საფინანსოდა საგანმანათლებლო დაწესებულება, ეფექტიანი ფუნქციონირების უზრუნველსაყოფად იყენებს ქსელებს - ელექტრონული ინფორმაციის შეგროვებისთვის, დამუშავებისთვის, შენახვისთვის და გაზიარებისთვის.

რაც უფრო მეტად გროვდება და ზიარდება ელექტრონული ინფორმაცია, მით უფრო მეტად ხდება საჭირო ამ ინფორმაციის დაცვა, რათა არ იყოს ხელყოფილი ეროვნული უსაფრთხოება და ეკონომიკური სტაბილურობა.

კიბერ უსაფრთხოება არის მუდმივმოქმედი ძალისხმევა, რომელიც მიზნად ისახავს ქსელური სისტემების და ელექტრონული ინფორმაციის დაცვას არასანქცირებული ხელყოფისგან და დაზიანებისგან. პიროვნულ დონეზე, თქვენ უნდა დაიცვათ თქვენი იდენტობა, ინფორმაცია და კომპიუტერული მოწყობილობები. კორპორაციულ დონეზე, თითოეული თანამშრომლის ვალდებულებაა დაიცვას ორგანიზაციის რეპუტაცია, ინფორმაცია და კლიენტები. სახელმწიფო დონეზე - ეროვნული უსაფრთხოება, მოქალაქეთა უსაფრთხოება და კეთილდღეობა.

ონლაინ და ოფლაინ იდენტობა

რაც უფრო მეტ დროს ატარებთ ონლაინ, მით უფრო მეტი ზეგავლენა აქვს თქვენს ონლაინ და ოფლაინ იდენტობას თქვენს ცხოვრებაზე. ოფლაინ იდენტობა არის ის, რომელიც სახლში, სკოლაში, ან სამსახურში ურთიერთობს თქვენს მეგობრებთან და ოჯახის წევრებთან. მათ იციან თქვენი პერსონალური ინფორმაცია - სახელი, ასაკი, საცხოვრებელი მისამართი და ა.შ. ონლაინ იდენტობა არის ის - რაც წარმოგადგენთ თქვენ კიბერ სივრცეში. ეს იდენტობა არის თქვენ მიერ შექმნილი პროფილი, რომელსაც იყენებთ საკუთარი თავის წარსადგენად სხვა ონლაინ მომხმარებლებისთვის. ონლაინ იდენტობამ უნდა გასცეს თქვენი პერსონალური ინფორმაცია მხოლოდ ლიმიტირებულ საზღვრებში.

ინფორმაცია თქვენ შესახებ

ნებისმიერი ინფორმაცია თქვენ შესახებ არის პერსონალური ინფორმაცია. ამ ინფორმაციას შეუძლია თქვენი იდენტიფიცირება უნიკალურ ინდივიდად. ეს ინფორმაცია მოიცავს სურათებს, შეტყობინებებს, რომელსაც უგზავნით თქვენს ოჯახის წევრებს და მეგობრებს ინტერნეტის მეშვეობით. სხვა ინფორმაცია, როგორიცაა პირადი ნომერი, დაბადების თარიღი და ადგილი, დედის ქალიშვილობის გვარი, გეკუთვნით მხოლოდ თქვენ და ის გამოიყენება თქვენი იდენტიფიცირებისთვის. სამედიცინო, განათლების, ფინანსური და დასაქმების ისტორია ასევე გამოიყენება თქვენი ონლაინ იდენტიფიცირებისთვის.

სამედიცინო ისტორია

ყოველ ჯერზე, როდესაც სტუმრობთ ექიმს, მატულობს ინფორმაცია თქვენი ჯანმრთელობის მდგომარეობის შესახებ. როგორც წესი, ინფორმაცია ჯანმრთელობის შესახებ ინახება ციფრულ ფორმატში. ასევე, რეცეპტები, რომლებსაც ექიმი გამოგიწერთ ხვდება ელექტრონულ ანკეტაში. ანუ, თქვენი ანკეტა ინახავს ინფორმაციას ფიზიკური და ფსიქიკური ჯანმრთელობის შესახებ. მაგალითად, თუ ბავშვობაში ჩაგიტარდათ გამოკვლევა, ოჯახში სიტუაციის შეცვლის ფონზე, ეს ინფორმაცია მოექცევა თქვენს სამედიცინო ანკეტაში. გარდა სამედიცინო და პერსონალური ინფორმაციისა, შესაძლოა ანკეტა შეიცავდეს ინფორმაციას თქვენი ოჯახის წევრების შესახებაც.

სამედიცინო ელექტრონული გაჯეტები, როგორებიცაა ფიტნეს სამაჯურები, ინფორმაციის შესანახად იყენებენ „ღრუბლის“ მეხსიერებას და გადასცემენ ინფორმაციას უკაბელო კავშირგაბმულობის გამოყენებით. ეს გაჯეტები ზომავენ ისეთ კლინიკურ მონაცემებს, როგორც გულის ცემა, წნევა და სისხლში შაქრის შემცველობა. ამ გაჯეტებს შეუძლიათ აურაცხელი მოცულობის ინფორმაციის გენერირება, რომელიც ასევე მოექცევა თქვენს სამედიცინო ანკეტაში.

განათლების ისტორია

სასწავლო დაწესებულებებში ყოფნისას, ინფორმაცია ნიშნების, ტესტების შეფასებების, დასწრების, გავლილი კურსების, ჯილდოების და აკადემიური ხარისხის მოპოვების, დისციპლინარული ჩანაწერების შესახებ ეტაპობრივად გროვდება თქვენი განათლების ისტორიაში. შესაძლოა ის ასევე მოიცავდეს ინფორმაციას საკონტაქტო, ჯანმრთელობის იმუნიზაციის, სპეციალური განათლების და ინდივიდუალური განათლების შესახებ.

დასაქმების და ფინანსური ისტორია

ფინანსური ისტორია შეიცავს ინფორმაციას თქვენი შემოსავლების და გასავლების შესახებ. გადასახადების გადახდის მონაცემთა ბაზაში ასევე მოიძებნება ინფორმაცია თქვენი ჩეკების, სესხის მოთხოვნის, საკრედიტო ისტორიის, და სხვა საბანკო ოპერაციების შესახებ. დასაქმების ისტორიაში კი აუცილებლად იქნება ინფორმაცია თქვენი წარსული დასაქმების და შეფასების შესახებ.

სად ინახება თქვენი ინფორმაცია?

ყველა ზემოთხსენებული ინფორმაცია არის უშუალოდ თქვენ შესახებ. ქვეყანაში, სადაც თქვენ ცხოვრობთ, აუცილებლად იქნება შესაბამისი კანონი, რომელიც იცავს პერსონალურ ინფორმაციას, მაგრამ იცით სად ინახება ეს ინფორმაცია?

როდესაც იმყოფებით ექიმის კაბინეტში, თქვენსა და ექიმს შორის დისკუსია იწერება თქვენს სამედიცინო ანკეტაში. არსებობს იმის ალბათობა, რომ ამ ინფორმაციას საავადმყოფო გაუზიარებს სადაზღვეო კომპანიებს, რათა მოხდეს სამედიცინო მომსახურების დროული და სრული ანაზღაურება. როგორც ხედავთ, თქვენი სამედიცინო ანკეტის ნაწილი შესაძლოა მოხვდეს მესამე პირთან - სადაზღვეო კომპანიასთან.

ერთგულების ბარათები არის ფულის დაზოგვის ძალიან მომგებიანი მეთოდი, მაგრამ მაღაზიები, სადაც თქვენ იყენებთ ასეთ ბარათებს აგროვებენ ინფორმაციას თქვენი შენაძენების შესახებ. მაგალითად, ასეთმა ბარათმა შეიძლება გასცეს თქვენი რეგულარული ჩვევა შეიძინოთ ერთი და იგივე ბრენდის და გემოს მქონე კბილის პასტა.

ამ ინფორმაციას იყენებენ მაღაზიები, რათა გამოგიგზავნონ სპეციალური შემოთავაზებები, რომლებსაც უკვეთავენ მაღაზიის პარტნიორი კომპანიები. ერთგულების ბარათის გამოყენებისას, მაღაზიაც და მისი პარტნიორები ქმნიან თქვენი ჩვევების აღმრიცხველ პროფილს.

როდესაც ინტერნეტის მეშვეობით მეგობრებს უზიარებთ სურათებს, იცით ვისთან შეიძლება აღმოჩნდეს ეს სურათი? თქვენს მეგობრებს შეუძლიათ გადმოწერონ თქვენ მიერ გამოგზაცნილი სურათები და შეინახონ ისინი საკუთარ კომპიუტერულ მოწყობილობაზე. არის იმის ალბათობაც, რომ აღნიშნული სურათები მოხვდება ღია ცირკულაციაში. ეს ნიშნავს, რომ უცხო ადამიანებიც შეძლებენ მათ ნახვას. ამ ადამიანებს შეუძლიათ თქვენი სურათების გადმოწერა, ან „სქრინშოტების“ გადაღება. ვინაიდან ეს სურათები მიმოიცვლება ინტერნეტის მეშვეობით, ისინი ასევე ინახება სერვერებზე, რომლებიც მსოფლიოს სხვადასხვა წერტილში არიან განლაგებულნი. შესაბამისად, თქვენი კომპიუტერული მოწყობილობის გარდა, თქვენი სურათები ინახება მრავალ სხვა ადგილზეც.

კომპიუტერული მოწყობილობები

კომპიუტერული მოწყობილობა არამხოლოდ ინახავს თქვენს პირად ინფორმაციას, არამედ ის გახდა ერთგვარი პორტალი, რომელიც გამუდმებით აგენერირებს (ქმნის) ინფორმაციას თქვენ შესახებ.

გარდა იმ შემთხვევებისა, როდესაც თავად აირჩევთ (საბანკო) ანგარიშების ბეჭდური ვერსიის მიღებას, თქვენს კომპიუტერულ მოწყობილობებს თვითონ აქვთ წვდომა ამ ინფორმაციაზე.

თუ თქვენ გსურთ საკრედიტო ბარათის ამონაწერის ხილვა, თქვენ შედიხართ კრედიტის გამცემი დაწესებულების ვებ-საიტზე და უკვეთავთ ელექტრონულ ამონაწერს.

თუ გსურთ სესხის გადახდა, თქვენ თავად შედიხართ ბანკის ვებსაიტზედაასრულებთფულადტრანსფერებსკომპიუტერული მოწყობილობის გამოყენებით. გარდა იმისა, რომ კომპიუტერულ მოწყობილობას აძლევთ უფლებას მიიღოს წვდომა თქვენს პირად ინფორმაციაზე, უკანასკნელი პარალელურად აგენერირებს ამ ინფორმაციას თქვენ შესახებ.

იმის გათვალისწინებით, რომ თქვენ შესახებ არსებობს ამდენი ელექტრონული ინფორმაცია, თქვენ ხდებით ძალიან მომგებიანი სამიზნე ჰაკერებისთვის.

მათ თქვენი ფული უნდათ...

თუ თქვენს ქონებას აქვს რაიმე ღირებულება, დამნაშავეს ის უნდა თავისთვის.

საბანკო მონაცემებს აქვთ ღირებულება. ეს მონაცემები არის საბანკო ანგარიშთან წვდომის წინაპირობა. შესაძლოა მოგეჩვენოთ, რომ „საჰაერო მილები“ , რომლებსაც მოწიწებით აგროვებთ ხშირი ფრენების შედეგად არ არის ღირებული კიბერ დამნაშავეებისთვის. დაფიქრდით კიდევ ერთხელ. მას შემდეგ რაც American და United ავიახაზების დაახლოებით 10,000 მომხმარებლის ანგარიშები გატყდა, კიბერ დამნაშავეებმა დაჯავშნეს უფასო ფრენები სწორედ კეთილსინდისიერი კლიენტების „საჰაერო მილების“ ხარჯზე. მიუხედავად იმისა, რომ აღნიშნულმა ავიაკომპანიებმა დაუბრუნეს ეს „საჰაერო მილები“ კეთილსინდისიერ მფლობელებს, ეს მაგალითად ცალსახად აჩვენებს, თუ რამდენად მნიშვნელოვანია ჰაკერებისთვის ონლაინ ანგარიშების მომხმარებლის სახელებზე და პაროლებზე დაუფლება.

კიბერ დამნაშავეებს ასევე შეუძლიათ ბოროტად გამოიყენონ თქვენი ურთიერთობები სხვა ადამიანებთან. თუ მათ შეძლეს შესვლა თქვენი სოციალური ქსელების ანგარიშებში, ისინი გაუგზავნიან ფულადი დახმარების თხოვნას თქვენს მეგობრებს და ნათესავებს. ხშირად გამოიყენება ასეთი შეტყობინება: „საზღვარგარეთ დამაყაჩაღეს. სახლში დასაბრუნებლად მჭირდება თანხა. გთხოვთ ამ ანგარიშზე გადმომირიცხოთ.“ ზოგადად, ბოროტმოქმედები არ უჩივიან ფანტაზიას, როდესაც ცდილობენ ფულის გამოტყუებას. გარდა იმისა, რომ ისინი მოგაყენებენ ფინანსურ ზიანს, ისინი ასევე მოიპარავენ თქვენს იდენტობას, რითიც დაგინგრევენ ცხოვრებას.

მათ უნდათ დაუფლება თქვენს იდენტობაზე...

თუ სახსრების მოპარვით დამნაშავეები უზრუნველყოფენ მოკლევადიან შემოსავალს, თქვენი იდენტობის მოპარვის შედეგად, მათ გაუჩნდებათ გრძელვადიანი შემოსავლის მიღების პერსპექტივები.

ეპოქაში, როდესაც ჯანდაცვის ფასები ასე ინტენსიურად იზრდება, პარალელურად იზრდება სამედიცინო იდენტობის ღირებულებაც. იდენტობის ქურდებს შეუძლიათ მოიპარონ თქვენი სამედიცინო დაზღვევა და გამოიყენონ ის თავისთვის. შედეგად, მათი სამედიცინო პროცედურები მოხვდება თქვენს სამედიცინო ისტორიაში.

გადასახადების გადახდის პროცედურები ყველა ქვეყანაში განსხვავებულია, მაგრამ კიბერ დამნაშავეები უყურებენ ამ გადასახადებს, როგორც შემოსავლების მიღების შესაძლებლობას. მაგალითისთვის, შეერთებული შტატების მოქალაქეები იხდიან გადასახადებს ყოველი წლის 15 აპრილს. საშემოსავლო სამსახური არ ამოწმებს ამ გადასახადებს ივლისის თვემდე.

ამ დროს, ადამიანები, რომელთაც სინამდვილეში უნდა დაბრუნებოდათ გადასახადების ნაწილი, აღმოაჩენენ, რომ საგადასახადო სამსახურმა უკვე დაუბრუნა ეს თანხა იდენტობის ქურდს. ასევე, მოპარული იდენტობის საფუძველზე, კიბერ დამნაშავეებს შეუძლიათ გახსნან საკრედიტო ბარათები და მოაგროვონ ვალები თქვენ სახელზე. ეს გამოიწვევს საკრედიტო ისტორიის შელახვას და გაგირთულებთ სესხის მიღების პროცედურებს.

ასევე, პერსონალური ინფორმაციის გამოყენებით, ბოროტმოქმედებს შეუძლიათ მოიპარონ კორპორაციული ინფორმაცია და ინფორმაცია თქვენ შესახებ სახელმწიფო მონაცემთა ბაზებიდან.

ორგანიზაციული ინფორმაციის ნაირსახეობა

ტიპიური ინფორმაცია

კორპორაციული ინფორმაცია მოიცავს მონაცემებს თანამშრომლების შესახებ, ინტელექტუალურ საკუთრებას და ფინანსურ დოკუმენტებს. თანამშრომელთა მონაცემებში მოიაზრება ნებისმიერი ინფორმაცია, რომელიც საჭიროა პიროვნების დასაქმებისთვის. ინტელექტუალური საკუთრება არის პატენტები, „ტრეიდმარკები“, პროდუქციის გამოშვების გეგმები და ინფორმაცია, რომელიც გამოიყენება კონკურენტებთან მიმართებაში უპირატესობის მოსაპოვებლად. ასევე, ინტელექტუალური საკუთრება მოიაზრებს ვაჭრობის წარმოების საიდუმლოს. კომპანიის კეთილდღეობისთვის ამ ინფორმაციის დაკარგვა დამანგრეველი ხასიათისაა. ფინანსური დოკუმენტები მოიცავს შემოსავლის ანგარიშებს, მიმდინარე ბალანსის აღმრიცხველ ინფორმაციას, სახსრების დინების მიმართულებების ინფორმაციას და ანალიტიკოსების შეფასებებს კომპანიის პერსპექტივების შესახებ.

,,ყველაფრის ინტერნეტი'' და ,,დიდი ინფორმაცია''

ყველაფრის ინტერნეტის (IoT) აღმოცენებასთან ერთად, სულ უფრო მეტი ინფორმაცია საჭიროებს უსაფრთხოებას. IoT არის ფიზიკური საგნების დიდი ქსელი, რომელშიც მოიაზრება, მაგალითად სენსორები და მოწყობილობები, რომლებიც სცილდება ტრადიციული კომპიუტერული ქსელის მოთხოვნებს. ამ ელექტრონულმა კავშირებმა, დიდი მოცულობის მქონე მეხსიერების მატარებლებმა, „ღრუბლის“ ტიპის მეხსიერების მატარებლებმა და ვირტუალიზაციამ, გამოიწვის ელექტრონული ინფორმაციის განსაკუთრებული ზრდა. ამ ინფორმაციას გააჩნია ინტერესის ახალი სფერო, რომელსაც ასევე უწოდებენ „დიდ ინფორმაციას“. IoT-ის მიერ გენერირებული ინფორმაციის სიჩქარემ, ზომამ და ნაირსახეობამ ტექნოლოგიურად განვითარებულ კომპანიებისთვის წარმოშვა ახალი საფრთხეები.

კონფიდენციალურობა, სისხლე და ხელმისაწვდომობა

კონფიდენციალურობას,სისრულესადახელმისაწვდომობას ასევე უწოდებენ ამერიკის შეერთებული შტატების ცენტრალური დაზვერვის სააგენტოს (Central Intelligence Agency - CIA) ტრიადას. ეს არის ერთგვარი ინფორმაციული უსაფრთხოების გზამკვლევი ორგანიზაციებისთვის.

კონფიდენციალურობის უზრუნველყოფა შესაძლებელია ინფორმაციაზე წვდომის შეზღუდვით და მისი დაშიფვრით. სისრულე გულისხმობს, რომ ინფორმაცია სრულფასოვანი, ზუსტი და დამაჯერებელია. ხელმისაწვდომობაში მოიაზრება ავტორიზაციის მქონე პირებისთვის წვდომის მინიჭებაში.

ინფორმაციის კონფიდენციალურობა

ტერმინი კონფიდენციალურობის კიდევ ერთი შესატყვისია სიტყვაა - პრივატულობა. კომპანიის პოლიტიკა უნდა უზრუნველყოფდეს ინფორმაციაზე წვდომის შეზღუდვას არაავტორიზირებული პირებისთვის, მაშინ როდესაც ავტორიზირებულ პირებს უნდა გააჩნდეთ შეუფერხებელი წვდომა. შესაძლებელია ინფორმაციის დაყოფა სენსიტიურობის, ან უსაფრთხოების ხარისხის საფუძველზე. მაგალითისთვის, Java პროგრამის დეველოპერს არ უნდა ჰქონდეს წვდომა კომპანიის თანამშრომლების პერსონალურ მონაცემებზე. უფრო მეტიც, თანამშრომლებს უნდა ჩაუტარდეთ სპეციალიზებული ტრეინინგები, რათა მათ შეძლონ საკუთარი და კომპანიის სენსიტიური ინფორმაციის დაცვა. კონფიდენციალურობის უზრუნველყოფის ერთერთი მეთოდია ინფორმაციის დაშიფვრა - ავტორიზაცია მომხმარებლის სახელით, პაროლით და „ორ ნაბიჯიანი ავტორიზაციის გამოყენებით“. ეს უზრუნველყოფს სენსიტიურ ინფორმაციაზე არასანქცირებული წვდომის მინიმიზაციას.

ინფორმაციის სისხლე

ინფორმაციის სისრულე გულისხმობს მის სიზუსტეს, სრულფასოვნებას და სანდოობას. ინფორმაციის გადაცემისას, ის არ უნდა იცვლებოდეს. მიზანშეწონილია თითოეულ ფაილზე წვდომის ნებართვის განსაზღვრა, რათა არ მოხდეს ინფორმაციაზე არაავტორიზებული წვდომა. არანაკლებ მნიშვნელოვანია ფაილების ვერსიის კონტროლი, რათა ავტორიზებულმა მომხმარებლებმა შემთხვევით არ შეიტანონ ცვლილებები. კორუმპირებული ინფორმაციის აღსადგენად მიზანშეწონილია ინფორმაციის არქივების (Backup) გაკეთება. ინფორმაციის გაგზავნისას უნდა გაკეთდეს „Checksum Hashing“-ის მონიტორინგი, რათა შესაძლებელი იყოს მისი სისრულის დადგენა.

„Checksum“ გამოიყენება ფაილების სისრულის დადგენაში, მას შემდეგ რაც ეს ფაილები გაიგზავნება ლოკალური ქსელის ან ინტერნეტის მეშვეობით. „Checksum“-ები გამოითვლება ჰეშირების ფუნქციის საფუძველზე. „Checksum“-ის გავრცელებული ვარიაციებია MD5, SHA-1, SHA-256 და SHA-512. ჰეშ ფუნქცია გარდაქმნის ინფორმაციას ფიქსირებული სიგრძის მაჩვენებელში. ამისთვის ის იყენებს მათემატიკურ ალგორითმს. ჰეშირებული მაჩვენებელი გამოიყენება შედარებების გასაკეთებლად. ამ მონაცემიდან შეუძლებელია ინფორმაციის პირდაპირი ამოღება.

მას შემდეგ, რაც ფაილი გადმოიწერება, თქვენ შეგიძლიათ შეამოწმოთ მისი სისრულე ჰეშ მაჩვენებლის მეშვეობით, რომელიც მოცემულია გადმოწერის წყაროზე. ამის გაკეთება შესაძლებელია ნებისმიერი ჰეშის კალკულატორის გამოყენებით. ჰეშ მაჩვენებლის დადარებით, შეგიძლიათ დარწმუნდეთ, რომ ფაილი არის სრული და ჩამოტვირთვისას ის არ შეცვლილა.

ინფორმაციის ხელმისაწვდომობა

ელექტრონული ხელსაწყოების მომსახურებისას, მათი ნაწილების რემონტისას, ოპერაციული სისტემების და პროგრამული უზრუნველყოფის განახლებისას და არქივების შექმნისას, კომპანიამ უნდა უზრუნველყოს ინფორმაციაზე წვდომის შენარჩუნება ავტორიზებული მომხმარებლებისთვის. ასევე, კომპანიას უნდა გააჩნდეს გეგმა, რომლის მეშვეობით ის შეძლებს სწრაფ რეაბილიტაციას ბუნებრივი და ადამიანის მიერ გამოწვეული კატაკლიზმების შემთხვევაში. უსაფრთხოების განმაპირობებელმა ხელსაწყოებმა და შესაბამისმა პროგრამულმა უზრუნველყოფამ, მაგალითად „Firewall“-მა, უნდა დაიცვას კომპანიის კიბერ ინფრასტრუქტურა სერვისის მიწოდების შეფერხებისგან / გაჩერებისგან. შესაძლებელია ეს იყოს DoS შეტევა, რა დროსაც ჰაკერ(ებ)ი ცდილობენ გადატვირთონ სერვისის მომწოდებელი ან / და შეაჩერონ მისი მუშაობა.

ჯიბეი უსაფრთხოების ხელყოფის შედეგები

რიგი მიზეზების გამო, ორგანიზაციის დაცვა ყველა არსებული კიბერ შეტევისგან უბრალოდ შეუძლებელია. ქსელის მონტაჟის და ადმინისტრირებისთვის საჭიროა სათანადო ცოდნა, რომელიც კლიენტს საკმაოდ ძვირი დაუჯდება. კიბერ ბოროტმოქმედები კი ყოველთვის იპოვიან ქსელის ხელყოფის ახალ გზებს. როგორც წესი, დახვეწილი და გამიზნული კიბერ შეტევა ყოველთვის წარმატებით დასრულდება. აქ მთავარი ის არის, რაოდენ სწრაფად შეძლებს ორგანიზაციის უსაფრთხოების სამსახური ასეთი კიბერ შეტევის აღმოჩენას, ინფორმაციის დაკარგვის მინიმიზაციას და შეფერხებული / გაჩერებული სერვისის სწრაფ აღდგენას.

ამ დროისთვის, თქვენ უკვე უნდა იცოდეთ, რომ ყველაფერი რაც ხვდება ონლაინ, შესაძლოა უსასრულოდ დარჩეს ონლაინ, მიუხედავად იმისა, რომ წაშლით თქვენს წვდომაში არსებულ ყველა ასლს. თუ თქვენი სერვერი გატეხეს, მასზე შენახული კონფიდენციალური პერსონალური მონაცემები შესაძლოა გახდეს საჯარო. ჰაკერ(ებ)ს შეუძლია ვებსაიტის განადგურება, სახის შეცვლა, ან არასწორი ინფორმაციის დაწერა, რაც გამოიწვევს თქვენი კომპანიის რეპუტაციის მნიშვნელოვან ხელყოფას - იმ რეპუტაციის, რომელსაც თქვენ წლების მანძილზე ამყარებდით. ვებსაიტის მწყობრიდან გამოსვლისას, კომპანია იზარალებს ფინანსურადაც. თუ ვებსაიტი გაითიშება ხანგრძლივი დროის მონაკვეთით, შესაძლოა კომპანია ჩაითვალონ არასანდოდ. გარდა ამისა, ვებსაიტის ან ქსელის ხელყოფისას, არსებობს საკმაოდ მაღალი რისკი, რომ კონფიდენციალური დოკუმენტები, სავაჭრო საიდუმლო და ინტელექტუალური საკუთრება მოექცევა კიბერ ბოროტმოქმედის ხელში. ეს გამოიწვევს კომპანიის განვითარების და ექსპანსიის მნიშვნელოვან შეფერხებას, ან სრულ გაჩერებას.

როგორც წესი, წარმატებული კიბერ შეტევის შედეგად გამოწვეული ზარალი გაცილებით უფრო დიდია, ვიდრე

ფიზიკური ხელსაწყოების ღირებულება. ამიტომაც, აუცილებელია კიბერ და ფიზიკური უსაფრთხოების გაძლიერება, შესაძლო ნეგატიური შედეგების დადგომამდე.

ასევე, კომპანია არის ვალდებული დაუკავშირდეს საკუთარ კლიენტებს და აცნობოს მათ უსაფრთხოების ხელყოფის შესახებ. ამ დროს, კომპანია უნდა იყოს მზად, რომ მის წინააღმდეგ დაიწყება სასამართლო დავები. გაურკვევლობის დროს, ბევრი კვალიფიციური თანამშრომელი სამსახურს დატოვებს, რადგან მათ არ სურთ საკუთარი რეპუტაციის შელახვა. შედეგად, კომპანიას გახდება იძულებული დახარჯოს ენერგია რეპუტაციის აღდგენაზე და არა განვითარებაზე.

ᲙᲘᲑᲔᲠ ᲣᲡᲐᲤᲠᲗᲮᲝᲔᲑᲘᲡ ᲮᲔᲚᲧᲝᲤᲘᲡ ᲛᲐᲒᲐᲚᲘᲗᲘ 1

2015 წლის ივლისში, ონლაინ პაროლების მენეჯერმა, „LastPass“-მა საკუთარ ქსელში აღმოაჩნა ანომალიური აქტივობები. გაირკვა, რომ ჰაკერებმა შეძლეს „LastPass“-ის მომხმარებელთა ელ. ფოსტის მისამართების, პაროლების გამოცვლის „შემხსენებლების“ და აუთენტიფიკაციის ჰეშების მოპარვა. მომხმარებელთა საბედნიეროდ, ჰაკერებმა ვერ მოიპარეს მათი დაშიფრული პაროლები.

მიუხედავად იმისა, რომ ადგილი ჰქონდა კიბერ უსაფრთხოების ცალსახა ხელყოფას, „LastPass“-მა მოახერხა საკუთარი მომხმარებლების ანგარიშების დაცვა. როდესაც ანგარიშში შესვლის მცდელობა ხორციელდება უცნობი IP მისამართიდან, „LastPass“ მომხმარებლებისგან ითხოვდა ვერიფიკაციის გავლას ელ. ფოსტის მეშვეობით, ან ორ ნაბიჯიანი აუთენტიფიკაციის გამოყენებით. გარდა ამისა, ანგარიშებში შესასვლელად ჰაკერებს ასევე დასჭირდებოდათ ე.წ. „Master Password“.

რა თქმა უნდა, მომხმარებლებსაც ეკისრებათ საკუთარი ანგარიშების დაცვის პასუხისმგებლობა. მათ უნდა გამოიყენონ კომპლექსური „Master Password“ და პერიოდულად შეცვალონ ის. ასევე, მათ უნდა იცოდნენ ე.წ. „Phishing“ შეტევების შესახებ. ასეთი შეტევის ერთერთი მაგალითია, ბოროტმოქმედის მიერ ყალბი / „ფეიკ“ ელ. წერილის გაგზავნა „LastPass“-ის სახელით. ამ ელ. წერილში იქნება პაროლის გამოცვლის თხოვნა ყალბი „LastPass“-ის ადმინისტრაციისგან. ასეთ წერილში იქნება ბმული, რომელიც გადაიყვანს მომხმარებელს „LastPass“-ის მსგავს გვერდზე, სადაც უკანასკნელი მოსთხოვენ ძველი პაროლის შეყვანას, ხოლო შემდგომ ახლის. რა საკვირველია, ახალი პაროლი ჰაკერს სულ არ სჭირდება, მაგრამ ძველს ის გამოიყენებს ნამდვილ ანგარიშზე შესასვლელად. ასევე, მომხმარებლები უნდა იყონ ფრთხილად, როდესაც იყენებენ პაროლის შემხსენებლებს. უკანასკნელი არავითარ შემთხვევაში არ უნდა გასცემდეს თქვენს პაროლს. გარდა ამისა, მომხმარებლებმა აუცილებლად უნდა გამოიყენონ ორ ნაბიჯიანი აუთენტიფიკაცია ყველა ვებსაიტზე, რომელიც ამის საშუალებას იძლევა.

თუ მომხმარებლები და სერვისის მიმწოდებლები იყენებენ ეფექტიან უსაფრთხოების ინსტრუმენტებს, მაშინ უსაფრთხოების ნაწილობრივი ხელყოფის დროსაც კრიტიკული ინფორმაცია არ იქნება ხელყოფილი.

ჯიბერ უსაფრთხოების ხელყოფის მაგალითი 2

2015 წლის ნოემბერში, მაღალტექნოლოგიური საბავშვო სათამაშოების გამომშვები კომპანიის, „Vtech“-ის უსაფრთხოება იქნა ხელყოფილი. ამ ინციდენტმა შესაძლოა იქონიოს ცუდი შედეგები მილიონობით ადამიანისთვის მსოფლიოს მასშტაბით, მათ შორის ბავშვებისთვისაც. კიბერ თავდასხმის შედეგად ბოროტმოქმედებმა შეაღწიეს „Vtech“-ის მონაცემთა ბაზაში, რომელიც შეიცავს კლიენტების სახელებს, ელ. ფოსტის მისამართებს, პაროლებს, სურათებს და მათი „ჩატის“ ისტორიას.

საკუთარ სამიზნედ ჰაკერებმა აირჩიეს სათამაშო პლანშეტური კომპიუტერები. ამ სათამაშო პლანშეტების გამოყენებით მომხმარებლები აზიარებდნენ ფოტოებს. ინფორმაცია, რომელიც იგზავნებოდა ამ პლანშეტებიდან არ იყო სათანადოდ დაცული. კომპანიის ვებსაიტსაც არ გააჩნდა SSL ტიპის დაშიფრული კავშირის უზრუნველყოფის შესაძლებლობა. მიუხედავად იმისა, რომ ამ კიბერ შეტევის შედეგად მომხმარებელთა პერსონალური და საბანკო ბარათების ინფორმაცია არ გაჟონილა, უსაფრთხოების ხელყოფის გამო კომპანიის აქციები საფონდო ბირჟაზე აღარ დაშვებულა.

„Vtech“-მა ვერ შეძლო საკუთარი კლიენტების ინფორმაციის ნაწილის სათანადო დაცვა. კიბერ შეტევის შედეგად, ამ ინფორმაციის ნაწილმა გაჟონა. მიუხედავად იმისა, რომ კომპანიამ აცნობა თავის მომხმარებლებს, რომ მათი პაროლები იყო ჰეშირებული, მაინც არსებობს იმის ალბათობა, რომ ჰაკერები შეძლებდნენ ამ ჰეშების გატეხვას. კომპანიამ დაშიფრა პაროლები MD5 ჰეშ ფუნქციის გამოყენებით, მაგრამ მას არ დაუშიფრავს უსაფრთხოების კითხვები და პასუხები. სამწუხაროდ, MD5 ჰეშ ფუნქციას აქვს თავისი სისუსტეები. ჰაკერებს შეუძლიათ გაიგონ ორიგინალური პაროლები მილიონობით პრე-გამოთვლილი ჰეშების მაჩვენებლების ერთმანეთთან დადარებით.

ასევე, ინფორმაციის გაჟონვის შედეგად, ჰაკერებს შეუძლიათ შექმნან ყალბი ელ. ფოსტის ანგარიშები, მოითხოვონ სესხის დამტკიცება, ჩაიდინონ დანაშაული და ა.შ. ასევე, კიბერ დამნაშავეებს შეუძლიათ მოიპარონ მომხმარებელთა სხვა ანგარიშებიც, რადგან ადამიანები ხშირად იყენებენ ერთი და იგივე პაროლს ყველა ონლაინ სერვისზე რეგისტრირებისას.

ამ კიბერ შეტევამ ხელყო არამხოლოდ კლიენტების პრივატულობა, არამედ კომპანიის რეპუტაციაც. როგორც იცით, „Vtech“-ის აქციები არ იქნა დაშვებული საფონდო ბირჟაზე.

მშობლებისთვის ეს კიბერ შეტევა იყო საკუთარი შვილების ონლაინ პრივატულობის დაცვის აუცილებლობის ერთგვარი საგანგაშო ზარი. ასევე, მათ გაუჩნდათ მორალური უფლება მოითხოვონ კომპანიებისგან უსაფრთხოების უფრო მაღალი სტანდარტის უზრუნველყოფა. ქსელური მოწყობილობების გამომშვებთათვის, ეს კიბერ შეტევა იყო იმის მანიშნებელი, რომ კლიენტების მონაცემების დაცვის მხრივ, ისინი უნდა იყონ უფრო აგრესიულები. კიბერ შეტევების პოტენციალი განიცდის მუდმივ ევოლუციას.

ᲙᲘᲑᲔᲠ ᲣᲡᲐᲤᲠᲗᲮᲝᲔᲑᲘᲡ ᲮᲔᲚᲧᲝᲤᲘᲡ ᲛᲐᲒᲐᲚᲘᲗᲘ 3

„Equifax Inc.“ არის აშშ-ს საკრედიტო რეპუტაციის შემფასებელი ერთერთი კომპანია. ის აგროვებს ინფორმაციას მილიონობით კლიენტზე და ბიზნესზე მსოფლიოს მასშტაბით. ამ ინფორმაციაზე დაყრდნობით ის აფასებს კლიენტების საკრედიტო რეპუტაციას. კერძოდ, ეს ინფორმაცია გამოიყენება მაშინ, როდესაც კლიენტები ავსებენ განაცხადებს სესხის დამტკიცებაზე.

2017 წლის სექტემბერში, „Equifax Inc.“-მა საჯაროდ გამოაცხადა, რომ ადგილი ჰქონდა მათი კიბერ უსაფრთხოების ხელყოფას. ჰაკერებმა შეძლეს „Equifax Inc.“-ის „Apache Stratus“ ვებ აპლიკაციის გატეხვა. კომპანიას სწამს, რომ კიბერ ბოროტმოქმედებმა მოიპოვეს მილიონობით ამერიკელი მომხმარებლის სენსიტიური პერსონალური მონაცემები. ეს შეტევა მიმდინარეობდა 2017 წლის მაისიდან ივლისის ჩათვლით. პერსონალური ინფორმაცია, რომელსაც დაეუფლნენ ჰაკერები მოიცავს კლიენტების სახელებს და გვარებს, პირად ნომრებს, დაბადების თარიღებს, მისამართებს და სხვა ინფორმაციას, რომლის გამოყენება შეიძლება მათი იდენტიფიცირებისთვის. ასევე, არსებობს იმის მტკიცებულება, რომ მომხმარებელთა ნაწილი იყო გაერთიანებული სამეფოს და კანადის მოქალაქე.

„Equifax Inc.“-მა დაარსა სპეციალური ვებსაიტი, რომლის მეშვეობით მომხმარებლებს მიეცა საშუალება დაედგინათ, მოხდა თუ არა მათი პერსონალური მონაცემების ხელყოფა. იმის ნაცვლად, რომ კომპანიას ამ დანიშნულებით გამოეყენებინა საკუთარი „საბდომეინი“, მათ შექმნეს სრულიად ახალი დომეინი. მომხმარებელთა მოსატყუებლად, ჰაკერებმა მალევე შექმნეს სატყუარა დომეინები მსგავსი სახელწოდებით. უფრო მეტიც, „Equifax Inc.“-ის ერთერთ თანამშრომელს თავად აერია საკუთარი ახალი დომეინის სახელწოდება და კლიენტებს ის გაუმიზნებლად აძლევდა სატყუარა ვებსაიტის ბმულს. საბედნიეროდ, ეს ვებსაიტი გაქრა 24 საათის განმავლობაში. როგორც გაირკვა, საიტი შექმნა პიროვნებამ, რომელსაც უნდოდა ეჩვენებინა ხალხისთვის, თუ რა ტიპის სისუსტეები არსებობს „Equifax Inc.“-ის ვებსაიტზე.

როგორც დაინტერესებული მომხმარებელი, თქვენ დიდი ალბათობით გენდომებათ იმის დადგენა, მოხდა თუ არა თქვენი პერსონალური მონაცემების ხელყოფა. ასეთ კრიზისულ დროს, არაკეთილსინდისიერმა ადამიანებმა შესაძლოა შეგიტყუონ სატყუარა ვებსაიტებზე, რათა მოიპარონ თქვენი პირადი ინფორმაცია. თქვენ, როგორც მომხმარებელი, უნდა გაფრთხილდეთ და არ მისცეთ ბოროტმოქმედებს შესაძლებლობა, რომ ისინი დაეუფლონ თქვენს პირად ინფორმაციას. ეს არ ნიშნავს, რომ კომპანია არ არის ვალდებული დაიცვას კლიენტების პერსონალური მონაცემები. პირიქით, ეს პასუხისმგებლობა, პირველ რიგში, ეკისრება კომპანიას, რომელსაც გაანდეთ ინფორმაცია თქვენ შესახებ. ა.გ. კომპანიები არიან ვალდებულნი რეგულარულად განაახლონ საკუთარი უსაფრთხოების პოტენციალი და როგორც მინიმუმ, უზრუნველყონ საკუთარი კიბერ სივრცის დაცვა ცნობილი კიბერ შეტევების წინააღმდეგ. კომპანიის თანამშრომლებს უნდა გააჩნდეთ შესაბამისი ცოდნა, რომ მათ შეძლონ მომხმარებელთა სათანადო დაცვა და ხელყოფის შემთხვევაში, მოახდინონ სწრაფი რეაგირება.

სამწუხაროდ, ზემოაღნიშნული კიბერ შეტევის ნამდვილი მსხვერპლი არის ის ადამიანი, რომლის ინფორმაცია მოხვდა კიბერ ბოროტმოქმედების ხელში. ამ შემთხვევაში, სრული პასუხისმგებლობა ეკისრება „Equifax Inc.“-ს, რადგან მომხმარებლები არ იყენებდნენ მათ სერვისს ნებაყოფლობით. უფრო მეტიც, კიბერ დამნაშავეებს შეუძლიათ გამოიყენონ მოპარული ინფორმაცია მომხმარებელთა იდენტობის დასაუფლებლად და ნამდვილი კრედიტორების ვინაობის გარკვევა გახდება ძალიან რთული, რადგან კეთილსინდისიერმა მომხმარებელმაც და ბოროტმოქმედმაც იციან ერთი და იგივე ინფორმაცია. ასეთი სიტუაციის დადგომისას, მომხმარებელი უნდა იყოს ძალიან ფრთხილი, როდესაც გასცემს საკუთარ ინფორმაციას, რომელიც შესაძლოა გამოდგეს მისი იდენტიფიცირებისთვის. ასევე, მან გამუდმებით უნდა ამოწმოს საკუთარი კრედიტის ისტორიის მონიტორინგი, რათა დაუყოვნებლივ შეძლოს არასწორი ინფორმაციის შესახებ განცხადების დაწერა - მაგალითად, როდესაც მისი სახელის გამოყენებით ვიღაცა ავსებს საკრედიტო განაცხადს, ან არასანქცირებული შესყიდვები წარმოებს მისი საკრედიტო ბარათის გამოყენებით.

ჯიბეში თავდასხმელების ჯგუფობრივი

კიბერ თავდასხმების მწარმოებელი შესაძლოა იყოს ინდივიდი, ან დაჯგუფება, რომელიც ცდილობს სისუსტის ხელყოფას პირადი, ან მერკანტილური ინტერესებიდან გამომდინარე. ასეთ ბოროტმოქმედებს აინტერესებთ შემოსავლის ნებისმიერი წყარო, დაწყებული საკრედიტო ბარათებიდან, დამთავრებული ნებისმიერი ღირებული მატერიალური და არამატერიალური საგნებით.

დამწყებები

მათ ასევე უწოდებენ „Script Kiddies“. როგორც წესი, მათ ფაჩნიათ კიბერ შეტევების წარმოების მხოლოდ საბაზისო ცოდნა, ან საერთოდ არ აქვთ. ისინი იყენებენ ინტერნეტში ნაპოვნ ინსტრუქციებს, რათა აწარმოონ კიბერ შეტევები. ზოგი მათგანი უბრალოდ ცნობისმოყვარეა, ხოლო ზოგი ცდილობს მოახდინოს საკუთარი გამოცდილების დემონსტრირება. იმის მიუხედავად, რომ მათი ინსტრუმენტები საკმაოდ პრიმიტიულია, მათ შეუძლიათ გამოიწვიონ მნიშვნელოვანი ზიანი.

ჰაკერები

ამ კატეგორიის წარმომადგენლები ტეხავენ კომპიუტერულ სისტემებს და ქსელებს და იღებენ არასანქცირებულ წვდომას სხვადასხვა კიბერ სივრცეზე. გატეხვის მოტივიდან გამომდინარე, ეს ჰაკერები იყოფიან სამ ძირითად კატეგორიად - თეთრქუდიან, ნაცრისფერქუდიან და შავქუდიან ჰაკერებად. თეთრქუდიანი ჰაკერი ტეხავს ქსელებს და კომპიუტერულ სისტემებს, რათა გამოკვეთოს მათი სისუსტეები და დაეხმაროს სისტემების ადმინისტრატორებს ამ სისუსტეების აღმოფხვრაში. ასეთი ტიპის კიბერ თავდასხმები სრულდება წინასწარი ნებართვის საფუძველზე და შედეგად ინფორმაცია სისუსტეების შესახებ გადაეცემა ნებართვის გამცემს. შავქუდიან ჰაკერებს საერთოდ არ ადარდებთ მომხმარებლის უსაფრთხოება. ისინი ხელყოფენ კიბერ ინფრასტრუქტურას, პირადი, ფინანსური, ან პოლიტიკური ინტერესებიდან გამომდინარე. ნაცრისფერქუდიანი ჰაკერები ექცევიან თეთრქუდიან და შავქუდიან ჰაკერებს შორის. შესაძლოა მათ აღმოაჩინონ სისუსტეები კიბერ ინფრასტრუქტურაში. შესაძლოა მათ აცნობონ ამ სისუსტის შესახებ სისტემის ადმინისტრატორს (თუ ეს შედის მათ გეგმებში). ზოგი ნაცრისფერქუდიანი ჰაკერი დადებს ინფორმაციას სისუსტის შესახებ ინტერნეტში, რათა სხვა ჰაკერებმა შეძლონ ამ სისუსტის ხელყოფა.

ჰაკერების ორგანიზებული ჯგუფი

ეს კატეგორია გულისხმობს კიბერ დამნაშავეების გაერთიანებას - ასოციაციას, „ჰაკტივისტებს“, ტერორისტებს, სახელმწიფოების მიერ დაფინანსებულ ჰაკერთა ჯგუფებს. ხშირ შემთხვევაში, ამ კატეგორიის ჰაკერები წარმოადგენენ პროფესიონალებს, რომელთა მიზანია კონტროლის, ძალაუფლების და სიმდიდრის დაუფლება. ძირითადად, ასეთი დაჯგუფებები გამოირჩევიან კარგი ცოდნით და ორგანიზებულობით. ზოგჯერ, ისინი სთავაზობენ საკუთარ სერვისს სხვა კატეგორიის დამნაშავეებსაც. „ჰაკტივისტები“ არიან ჰაკერები, რომლებიც აკეთებენ პოლიტიკურ განცხადებებს, ამახვილებენ ყურადღებას სოციალურ პრობლემებზე და ა.შ. სახელმწიფოს მიერ დაფინანსებული ჰაკერები ასრულებენ სადაზვერვო ოპერაციებს, ეწევიან საბოტაჟს სხვა სახელმწიფოების წინააღმდეგ და ა.შ.. ასეთი ჰაკერებს აქვთ უმაღლესი დონის ცოდნა და მათ კარგად აფინანსებენ. მათი შეტევები არის ორიენტირებული სპეციალურად განსაზღვრულ სამიზნეებზე, რომლებიც შედის სახელმწიფო ინტერესებში.

შიდა და გარე საფრთხეები

შიდა საფრთხეები

შეტევები ორგანიზაციის წინააღმდეგ იწარმოება შიგნიდან, ან გარედან. ორგანიზაციის თანამშრომელს, ან კონტრაქტით დაქირავებულ პირს, შემთხვევით, ან გამიზნულად, შეუძლია:

- *დაუდევრად, ან გულგრილად მოეპყროს კონფიდენციალურ ინფორმაციას;*

- *შეუქმნას საფრთხე შიდა ქსელის ხელსაწყოებს ან/და სერვერებს;*

- *კიბერ შეტევის მიზნით, შეაერთოს მავნებელი პროგრამით ინფიცირებული USB მეხსიერების მატარებელი (ფლეშკა) კორპორაციულ კიბერ ინფრასტრუქტურაში;*

- *შეუშვას ქსელში მავნებელი პროგრამა, რომელსაც ის მიიღებს ელ. ფოსტის მეშვეობით, ან გადმოწერს ინტერნეტიდან.*

ზოგჯერ, შიდა საფრთხეების შედეგად გამოწვეული ზიანი აღემატება გარე საფრთხეების შედეგად გამოწვეულ ზიანს. ეს განპირობებულია იმით, რომ თანამშრომელს აქვს უშუალო წვდომა ორგანიზაციის შენობაზე და კიბერ ინფრასტრუქტურაზე. გარდა ამისა, თანამშრომლებმა უფრო კარგად იცნობენ კორპორაციულ ქსელს, ამ ქსელში არსებულ რესურსებს, კონფიდენციალურ ინფორმაციას და ა.შ. ხშირად, მათ აქვთ წვდომის უფრო მაღალი დონე, ან კიბერ ინფრასტრუქტურის ადმინისტრირების პრივილეგიებიც.

გარე საფრთხეები

გარე საფრთხეები მოიცავს დამწყები და პროფესიონალი ჰაკერების მიერ ორგანიზაციის ქსელური ან კომპიუტერული სისტემების სისუსტეების ხელყოფას, ან წვდომის მიღებას სოციალური ინჟინერიის გამოყენებით.

ჰა ჰრის ჯიბერ ომი?

კიბერ სივრცე ჩამოყალიბდა სამხედრო მოქმედებების კიდევ ერთი მნიშვნელოვანი განზომილებად, სადაც ქვეყნები აწარმოებენ სამხედრო ოპერაციებს ტრადიციული ჯარის და საბრძოლო ტექნიკის გამოყენების გარეშე. ეს მნიშვნელოვნად აძლიერებს სუსტი სამხედრო პოტენციალის მქონე ქვეყნების შესაძლებლობას აწარმოოს ომი უფრო ძლიერ მეტოქეებთან. კიბერ ომი არის ინტერნეტის პოტენციალზე დაყრდნობილი კონფლიქტი, რომელიც მოიცავს შეღწევას მოწინააღმდეგე ქვეყნის კომპიუტერულ სისტემებში და ქსელებში.

ჰაკერებს, რომლებიც მონაწილეობენ ამ ტიპის შეტევების განხორციელებაში, გააჩნიათ საჭირო რესურსები და გამოცდილება, რათა აწარმოონ მასობრივი ხასიათის ინტერნეტ შეტევები, რომლებიც გათვლილია ზიანის მიყენებაზე, მუნიციპალური სერვისების ხელყოფაზე, მაგალითად ელექტრო სადგურების გაჩერებაზე.

ერთერთ ასეთ, სახელმწიფოს მიერ დაფინანსებულ შეტევას, წარმოადგენს მავნებელი პროგრამა „Stuxnet“, რომელიც იყო გათვლილი ირანის ბირთვული საწვავის გამდიდრების სადგურის დაზიანებაზე. „Stuxnet“ არ იყო განკუთვნილი კომპიუტერული სისტემების დაუფლებაზე, ან ელექტრონული ინფორმაციის მოპარვაზე. ის იყო შექმნილი იმ ფიზიკური ხელსაწყოების დაზიანებისთვის, რომლებიც იმართებოდა კომპიუტერის მეშვეობით. „Stuxnet“ იყენებდა მოდულარულ პროგრამირების კოდს, რომელსაც უნდა შეესრულებინა მხოლოდ ცალკეული დავალება. მას ასევე გააჩნდა მოპარული ელექტრონული სერთიფიკატები, რომელთა მეშვეობით ის ნიღბავდა საკუთარ ქმედებებს და ასაღებდა მათ ლეგიტიმურად.

ᲙᲘᲑᲔᲠ ᲝᲛᲘᲡ ᲓᲐᲜᲘᲨᲜᲣᲚᲔᲑᲐ

კიბერ ომის ძირითადი დანიშნულება არის უპირატესობის მოპოვება მოწინააღმდეგესთან მიმართებაში. ამ შემთხვევაში, მოწინააღმდეგეებში მოიაზრებიან დაპირისპირებული სახელმწიფოები.
კიბერ შეტევების საფუძველზე, ქვეყანას შეუძლია აწარმოოს გამუდმებული შეტევები სხვა ქვეყნის ინფრასტრუქტურაზე, თავდაცვის საიდუმლოებების მოპარვა და სამხედრო ტექნოლოგიებზე დაუფლება. გარდა ინდუსტრიული და სამხედრო ჯაშუშობისა, კიბერ ომის ნიადაგზე წარმოებულ შეტევას შეუძლია გამოიწვის მოწინააღმდეგე ქვეყნის ინფრასტრუქტურის საბოტაჟი, რომელმაც, თავის მხრივ, შესაძლოა განაპირობოს სიცოცხლის მოსპობა. მაგალითად, კიბერ შეტევას შეუძლია გამოიყვანოს მწყობრიდან ელექტრო სადგურები.

ამას მოყვება საავტომობილო მოძრაობის შეფერხება. შედეგად, შეწყდება საქონლის და გარკვეული სერვისების მიწოდებაც. პაციენტებს ვერ ჩაუტარდება გადაუდებელი სამედიცინო დახმარება. ინტერნეტთან წვდომაც გაწყდება. როგორც ხედავთ, ელექტრო სადგურის მწყობრიდან გამოსვლა იქონიებს დიდ ზეგავლენას ჩვეულებრივი მოქალაქეების ცხოვრებაზე.

უფრო მეტიც, სენსიტიური ინფორმაციის გამოყენება შესაძლებელია ხელისუფლების წარმომადგენლების დასაშანტაჟებლადაც. ამ ინფორმაციას ასევე შეუძლია მისცეს არასანქცირებულ პირებს წვდომა სენსიტიურ მართვის მექანიზმებზე.

თუ სახელმწიფო ვერ უზრუნველყოფს საკუთარი თავის დაცვას კიბერ თავდასხმებისგან, ხელისუფლება დაკარგავს ამომრჩევლის ნდობას. ფიზიკური საომარი მოქმედებების გარეშეც, კიბერ ომს აქვს ქვეყნის დესტაბილიზაციის, ვაჭრობის შეჩერების და რევოლუციის მოწყობის პოტენციალი.

თავი 2.

კიბერ შეტევები

კონცეპტები და

ნაიმოების ტექნიკა

ეს თავი მოიცავს ინფორმაციას უსაფრთხოების ექსპერტების მიერ კიბერ შეტევის შედეგების გაანალიზებაზე. ყურადღება ასევე დაეთმობა უსაფრთხოების ფიზიკურ და პროგრამულ სისუსტეებს და მათ კატეგორიებს.

შემდგომ, ჩვენ განვიხილავთ სხვადასხვა ტიპის მავნებელი პროგრამებს (Malware) და მათ სიმპტომებს. გარდა ამისა, ყურადღება ასევე დაეთმობა კომპიუტერულ სისტემაში შეღწევის სხვადასხვა მეთოდებს. ამ თავში განვიხილავთ DoS შეტევებსაც.

თანამედროვე კიბერ შეტევების უმრავლესობა არის შერეული ხასიათის. ეს გულისხმობს, რომ თითოეული კიბერ თავდასხმა კომპიუტერულ ინფრასტრუქტურაზე შედგება რამდენიმე ტექნიკის ნაზავისგან. თუ ასეთი კიბერ შეტევის სრული აღკვეთა შეუძლებელია, ნამდვილად შესაძლებელია რისკების მინიმიზაცია.

უსაფრთხოების სისუსტეების აღმოჩენა

უსაფრთხოების სისუსტედ ჩაითვლება ფიზიკური მოწყობილობის ან / და პროგრამული უზრუნველყოფის დეფექტი. მას შემდეგ, რაც ბოროტმოქმედი აღმოაჩენს სისუსტეს, მისი შემდეგი ნაბიჯი იქნება ამ სისუსტის ხელყოფა. ამისთვის ჰაკერი იყენებს ე.წ. „ექსპლოიტს“ - ანუ, პროგრამულ უზრუნველყოფას, რომელიც გათვლილია ცნობილი სისუსტის ხელყოფისთვის. ამ „ექსპლოიტის“ გამოყენების პროცესს კი ეწოდება კიბერ შეტევა. „ექსპლოიტის“ გამოყენებისას, ჰაკერის მიზანია მიიღოს წვდომა მთლიან კომპიუტერულ სისტემაზე, ან რაიმე ინფორმაციაზე, რომელიც ინახება ამ სისტემაში.

პირობითი სისუსტეები

პროგრამულ სისუსტეებში ძირითადად იგულისხმება ოპერაციულ სისტემების, ან ცალკეული აპლიკაციების პროგრამული კოდის სინტაქსში დაშვებული შეცდომები. მიუხედავად დეველოპერების თავდაუზოგავი შრომისა, ეს შეცდომები მაინც იპარება. შედეგად, ეტაპობრივად ჩნდება ინფორმაცია სისუსტეების აღმოჩენის შესახებ. წარმოიდგინეთ, რომ ისეთ კომპანიებს, როგორიც Microsoft და Apple, ყოველდღე უწევთ სისუსტეების აღმოფხვრა. ამიტომაც, ჩვენ - მომხმარებლებს, ყოველდღიურად მოგვდის განახლებები, რომლებიც დიდ წილად გათვლილია კიბერ უსაფრთხოების მისაღები სტანდარტის უზრუნველყოფაზე. არანაკლებ იშვიათად მოგვდის ცალკეული აპლიკაციების განახლებები, რადგან ნებისმიერ აპლიკაციაში მოიძებნება უსაფრთხოების ღრიჭოები.

2015 წელს, „Cisco IOS“-ში იქნა აღმოჩენილი სისუსტე სახელწოდებით SYNful Knock. ამ უსაფრთხოების ღრიჭომ მისცა ბოროტმოქმედებს შესაძლებლობა შეეღწიათ

Cisco-ს მაღალი კლასის როუტერებში (Cisco 1841, 2811 და 3825 მოდელებს). შედეგად, ჰაკერებს შეეძლოთ აღნიშნულ როუტერებში ინტერნეტ ტრეფიკის მონიტორინგი და შეერთებული კომპიუტერული სისტემების ინფიცირებაც. ამ სისუსტემიჩინათავი,როდესაცCisco-საღნიშნულიროუტერების მოდელებზე დაყენდა ხელყოფილი ოპერაციული სისტემა. იმისათვის, რომ თავი აღნიშნულ სისუსტეებს აარიდოთ თავი, თქვენ უნდა შეადაროთ თქვენ მიერ გადმოწერილი ოპერაციული სისტემის საინსტალაციო ფაილის სისრულე (უცვლელობა) და უზრუნველყოთ მხოლოდ ავტორიზებული მომხმარებლების ფიზიკური წვდომა თქვენს როუტერებთან.

ზოგადად, განახლების მიზანია უსაფრთხოების პროტოკოლების აქტუალიზაცია და სისუსტეების აღმოფხვრა. მაშინ, როდესაც კომპანიებს ჰყავთ სპეციალიზებული შეღწევადობის ტესტირების ჯგუფები, რომლებიც ეძებენ და აღმოფხრავენ სისუსტეებს, დამოუკიდებელი მკვლევარი სპეციალისტები ასევე ეძებენ სისუსტეებს სხვის მიერ დაწერილ პროგრამულ უზრუნველყოფაში.
Google-ის Project Zero არის ზემოაღნიშნული პრაქტიკის კარგი მაგალითი. მას შემდეგ რაც სხვადასხვა აპლიკაციაში იქნა აღმოჩენილი მთელი რიგი სისუსტეები, Google-მა შექმნა მუდმივმოქმედი ჯგუფი, რომლის მიზანი გახდა ასეთი სისუსტეების აღმოჩენა.

ფიზიკური მოწყობილობების სისუსტეები

ფიზიკურიმოწყობილობებისსისუსტეებიხშირადგამოწვეულია დიზაინერული ჩანაფიქრის დეფექტებით. მაგალითისთვის, ცვალებადი მეხსიერება (RAM) წარმოადგენს ერთმანეთთან ახლოს განლაგებულ კონდენსატორებს. აღმოჩნდა რომ დაშორებას ამ კონდენსატორებს შორის შეუძლია გამოიწვიოს უწესივრობები მათ მუშაობაში.

ამ დიზაინერული დეფექტის აღმოჩენის შედეგად გაჩნდა „ექსპლოიტი - Rowhammer“. ეს „ექსპლოიტი“ რამოდენიმეჯერ გადაწერდა ინფორმაციას მეხსიერების ერთ სივრცეზე, რის შედეგადაც ის იპარავდა მეზობლად მყოფ სივრცეში არსებულ ინფორმაციასაც. ეს ხდებოდა იმის მიუხედავად, დაცული იყო მეზობლად მყოფი სივრცე, თუ არა.

როგორც წესი, ფიზიკური მოწყობილობების სისუსტეების ხელყოფა არ არის შემთხვევითი ხასიათის. ასეთი სისუსტეების ექპლოატაცია ხდება გამიზნული კომპლექსური შეტევების წარმოების დროს.

უსაფრთხოების სისუსტეების კატეგორიები

პრაქტიკულად ნებისმიერი პროგრამული სისუსტე ხვდება ამ კატეგორიებიდან ერთერთში:

ბუფერის გადავსება (Buffer overflow) – ეს სისუსტე იჩენს თავს მაშინ, როდესაც ხდება ინფორმაციის ოდენობა, გადააჭარბებს ბუფერის ლიმიტს. ბუფერები არის მეხსიერების სივრცე, რომელიც განკუთვნილია ცალკეული აპლიკაციისთვის. თუ ინფორმაცია გადააჭარბებს ბუფერის ლიმიტს, აპლიკაცია გამოიყენებს მეხსიერებას, რომელიც გამოყოფილია სხვა პროცესისთვის. შედეგად, შესაძლოა მოხდეს სისტემის ჩაშლა, ინფორმაციის გაჟონვა, ან პრივილეგიების გაფართოვება (ესკალაცია).

არა-ვალიდური ინფორმაციის შეყვანა (Non-validated input) – პროგრამები მუშაობენ იმ ინფორმაციაზე დაყრდნობით, რომელიც შეჰყავს მომხმარებელს. შესაძლოა, ეს ინფორმაცია იყოს მავნებელი ბუნების და აიძულოს პროგრამას იმუშაოს გაუთვალისწინებელი ფორმით. მაგალითისთვის წარმოიდგინეთ, რომ პროგრამა დასამუშავებლად იღებს გამოსახულებას. კიბერბოროტმოქმედს შეუძლია გარდაქმნას ეს გამოსახულება არასტანდარტულ განზომილებებში. შედეგად, პროგრამა დაიბნევა და გადატვირთავს ბუფერს.

ე.წ. „სარბოლო პირობები“ (Race conditions) – ეს სისუსტე იჩენს თავს, როდესაც ინფორმაცია უნდა დამუშავდეს შესაბამის დროში და კონკრეტული თანმიმდევრობით. სარბოლო პირობები ხდება სისუსტე, როდესაც პროცესი არ მიმდინარეობს საჭირო თანმიმდევრობით ამისთვის განსაზღვრულ დროში.

სისუსტეები უსაფრთხოების პრაქტიკაში – სისტემების და სენსიტიური ინფორმაციის დაცვა შესაძლებელია აუთენტიფიკაციის, ავტორიზაციის და დაშიფვრის მეშვეობით. დეველოპერები, რომლებიც ქმნიან საკუთარ უსაფრთხოების ალგორითმებს, მნიშვნელოვნად რისკავენ საკუთარი უსაფრთხოების ხელყოფას. უსაფრთხოების მისაღები სტანდარტის უზრუნველსაყოფად რეკომენდირებულია უკვე კარგად დაცდილი ალგორითმების გამოყენება.

წვდომის კონტროლის პრობლემები - წვდომის კონტროლი გულისხმობს პროცესს, რომლის დროსაც კონტროლდება ვის და რა დოზით აქვს ფიზიკური და ელექტრონული წვდომა კომპიუტერულ ინფრასტრუქტურასთან. ასევე, ვის აქვს კომპიუტერულ სისტემებზე ფაილების მოდერირების (გარდაქმნის / ცვლილების შეტანის) შესაძლებლობა. უსაფრთხოების მრავალი ღრიჭო ჩნდება მაშინ, როდესაც არ ხორციელდება წვდომის პრივილეგიების სათანადო განკარგვა. პრაქტიკულად ნებისმიერი ტიპის უსაფრთხოების ხელყოფა შესაძლებელია, როდესაც ჰაკერს აქვს უშუალო ფიზიკური კონტაქტი კომპიუტერულ მოწყობილობებთან. მაგალითისთვის, თუ ცალკეულ ფაილზე განსაზღვრულია შემზღუდველი პრივილეგიები, ჰაკერს მაინც შეეძლება ფაილის წაკითხვა ოპერაციული სისტემიდან, ან თავად მყარი დისკიდან. კომპიუტერული მოწყობილობების და მათზე ჩაწერილი ინფორმაციის დაცვა შესაძლებელია ფიზიკური წვდომის ლიმიტირებით და დაშიფვრის ტექნიკის გამოყენებით.

მავნებელი პროგრამების ტიპოლოგია

მავნებელი პროგრამა არის ნებისმიერი პროგრამული კოდი, რომელიც გამოიყენება ინფორმაციის მოსაპარად, ავტორიზაციის გვერდის შემოვლისთვის, სისტემის დაზიანებისთვის და მისი ფუნქციონირების შეჩერებისთვის. ქვემოთ არის მოცემული რამდენიმე ტიპის მავნებელი პროგრამის განმარტება.

ჯაშუში პროგრამები (Spyware) - ეს არის მავნებელი პროგრამის ნაირსახეობა, რომელიც გათვლილია სამიზნე ადამიანის გადაადგილების მონიტორინგზე და სხვა ჯაშუშური ოპერაციების ჩატარებაზე. როგორც წესი, ჯაშუშური აპლიკაციები აგროვებენ ინფორმაციას სამიზნე მომხმარებლის ყოველდღიურ აქტივობაზე, მის მიერ შეყვანილ ტექსტზე, მეხსიერებაში არსებულ ინფორმაციაზე და ა.შ. იმისათვის, რომ ჯაშუშურმა პროგრამამ მოიპოვოს მაქსიმალური წვდომა მოწყობილობაზე, ხშირად ის ცვლის უსაფრთხოებასთან დაკავშირებულ პარამეტრებს. როგორც წესი, ჯაშუშური პროგრამა გაერთიანებულია ლეგიტიმურ უვნებელ პროგრამასთან, ან ტროიანის ტიპის მავნებელ პროგრამასთან.

სარეკლამო მავნებელი პროგრამები (Adware) – არსებობს აპლიკაციები, რომლებიც გათვლილია სარეკლამო კონტენტის მიწოდებაზე. ზოგჯერ, ასეთ აპლიკაციებში ჩაშენებულია მავნებელი სარეკლამო პროგრამებიც. თანამედროვე სარეკლამო მავნებელი პროგრამები ინტეგრირებულია ჯაშუშურ პროგრამებთანაც.

ბოტი - ტერმინი ბოტი წარმოიშვა სიტყვიდან რობოტი. ეს არის მავნებელი პროგრამა, რომლის მიზანია გარკვეული ბრძანებების ავტომატიზირება. ბოტების უმრავლესობა უვნებელია, მაგრამ არსებობს მავნებელი ბოტებიც, მაგალითად ბოტნეტი. ბოტნეტით ინფიცირებული კომპიუტერები კი ასრულებენ ჰაკერის ბრძანებებს.

გამომძალველი პროგრამები (Ransomware) - პირდაპირი მნიშვნელობით, ასეთი ტიპის პროგრამები „მძევლად“ იყვანენ კომპიუტერზე არსებულ ინფორმაციას და არ აძლევენ ლეგიტიმურმფლობელსმათზეწვდომას,ვიდრეისარგადაიხდის გარკვეულ თანხას. როგორც წესი, გამომძალველი პროგრამები შიფრავენ კომპიუტერზე არსებულ ინფორმაციას უნიკალური გასაღების მეშვეობით, რომელიც, რა თქმა უნდა, უცნობია კომპიუტერის მფლობელისთვის. სხვა ტიპის გამომძალველი პროგრამები პოულობენ კომპიუტერულ სისტემაზე სისუსტეებს და უბრალოდ ბლოკავენ სისტემას. გამომძალველი პროგრამები ვრცელდებიან ინტერნეტიდან გადმოწერილი ფაილების სახით, ან სხვა პროგრამული უზრუნველყოფის სისუსტეების ხარჯზე.

დამაშინებელი პროგრამები (Scareware) – ასეთი ტიპის მავნებელი პროგრამები გათვლილია ადამიანის შიშზე. ისინი აიძულებენ ადამიანებს შეასრულონ გარკვეული ბრძანებები შიშის ფაქტორზე დაყრდნობით. როგორც წესი, კომპიუტერულ სისტემაზე ამოხტება ფანჯარა, სადაც წერია, რომ თუ არ ჩატარდება გარკვეული ოპერაცია, ან მომხმარებელი არ გახსნის მითითებულ ფაილს, მისი კომპიუტერი ვერ შეძლებს ნორმალურ ფუნქციონირებას. შედეგად, დაუდევარი მომხმარებელი ასრულებს დამაშინებელი პროგრამების მიერ მითითებულ რეკომენდაციებს და საკუთარი ხელით აინფიცირებს თავის კომპიუტერულ სისტემას.

Rootkit – ამ ტიპის მავნებელი პროგრამა შექმნილია ოპერაციულ სისტემაზე დისტანციური წვდომის / მართვის შესაძლებლობის გახსნაზე (Backdoor). „რუტქითების“ უმრავლესობა გათვლილია პროგრამული უზრუნველყოფის სისუსტეების ექსპლოატაციაზე, რათა მათ მოახდინონ ჰაკერის პრივილეგიების ესკალაცია და სისტემური ფაილების ხელყოფა. ხშირად, „რუტქითები“ ხელყოფენ სისტემის მონიტორინგის ხელსაწყოებსაც, რაც ხდის მათ პრაქტიკულად შეუმჩნეველს. ზოგი იმდენად დახვეწილია, რომ მათი მოშორების ერთადერთი გზა არის ოპერაციული სისტემის გადაწერა.

ვირუსი - ეს არის მავნებელი პროგრამული კოდი, რომელიც მიერთებულია „.exe“ ფაილებზე - ხშირად ლეგიტიმური პროგრამების გასაშვებ ფაილებზეც. ვირუსების დიდი ნაწილი დამოკიდებულია დაუდევარი მომხმარებლის მიერ მათ გაშვებაზე. შესაძლოა ისინი მომენტალურად არ გაეშვან და გააკეთონ ეს მოგვიანებით (ან განსაზღვრულ დროს). ვირუსების დესტრუქციულობის ხარისხი ვარირებს მათი დამწერის მოტივებიდან გამომდინარე. ზოგი უვნებელია - ის უბრალოდ ხსნის სურათს. ზოგიც, დამანგრეველია, იმ თვალსაზრისით, რომ მათ შეუძლიათ კომპიუტერულ სისტემაზე არსებული ინფორმაციის მოსპობა. ძირითადად, ვირუსები ვრცელდება USB მეხსიერების მატარებლებით, ოპტიკური დისკებით, ქსელის მეშვეობით, ან ელ. ფოსტით.

ტროიანის ცხენი (Trojan Horse) - ტროიანი არის ისეთი მავნებელი პროგრამის ნაირსახეობა, რომელიც ნიღბავს საკუთარ თავს. ის ახდენს პრივილეგიების ესკალირებას და აძლევს ჰაკერს წვდომას კომპიუტერულ სისტემაზე. ტროიანების აღმოჩენა შესაძლებელია „იმიჯ“ ფაილებში, აუდიო ფაილებში, ან თამაშებში. ტროიანი განსხვავდება ვირუსებისგან იმ თვალსაზრისით, რომ ის ასევე ებმება ფაილებს, რომელთა გაშვება შეუძლებელია.

კომპიუტერული ჭია (Worms) – ჭია არის მავნებელი კოდი, რომელიც ახორციელებს დამოუკიდებელ რეპლიკაციას და ახდენს ქსელის ინფიცირებას. ხშირად, ჭიები ანელებენ ქსელებს. თუ ვირუსებს გასაშვებად სჭირდებათ მასპინძელი პროგრამა, ჭია თავად არის დამოუკიდებელი პროგრამა, რომელიც არ საჭიროებს მასპინძელს. მას შემდეგ, რაც კომპიუტერული სისტემა ინფიცირდება, ჭია იწყებს ინტენსიურ გავრცელებას ქსელში. როგორც წესი, ყველა ჭია მსგავსია. ისინი მუშაობენ სისუსტეების ექსპლოატაციის საფუძველზე და ყველას გააჩნია „Payload“-ი.

სწორედ კომპიუტერულ ჭიებს აწერენ ყველაზე დესტრუქციულ შეტევებს ინტერნეტში. 2001 წელს, „Code Red“ ჭიამ დააინფიცირა 658 სერვერი. 19 საათის შემდეგ, „Red Code“-მა მოახერხა 300.000 სერვერის ინფიცირება.

Man-In-The-Middle (MitM) – MitM აძლევს ჰაკერს შესაძლებლობას დაეუფლოს სამიზნე მომხმარებლის კომპიუტერულ სისტემას ისე, რომ უკანასკნელს ეს არ ეცოდინება. საჭირო დონის წვდომის არსებობისას, ჰაკერს შეუძლია გადაიჭიროს ინფორმაცია, ვიდრე ის მიაღწევს დანიშნულების ადგილს. MitM შეტევა გამოიყენება ფინანსური ინფორმაციის მოსაპარადაც. თანამედროვე მავნებელი პროგრამების უმრავლესობას გააჩნია MitM შეტევის ფუნქციაც.

Man-In-The-Mobile (MitMo) – ეს არის MitM შეტევის ერთერთი ნაირსახეობა, რომელიც გამოიყენება მობილურ ხელსაწყოებზე დასაუფლებლად. როდესაც ხდება მობილური ხელსაწყოს ინფიცირება, MitMo აძლევს უკანასკნელს ინსტრუქციას გადაუგზავნოს საჭირო ინფორმაცია ჰაკერს. „Zeus“ არის ერთერთი „ექსპლოიტი“, რომელსაც გააჩნია MitMo შეტევის განხორციელების შესაძლებლობა. მისი გამოყენება შეიძლება 2 ნაბიჯიანი აუთენტიფიკაციისთვის საჭირო მოკლე ტექსტურ შეტყობინებაში არსებული კოდის მოსაპარად.

მავნებელი პროგრამების სიმპტომები

განურჩევლად მავნებელი პროგრამის ტიპისა, კომპიუტერულ სისტემაზე ჩნდება შემდეგი სიმპტომები:

- *იზრდება ცენტრალური პროცესორის დატვირთვა;*
- *ქვეითდება კომპიუტერული სისტემის მუშაობის სიჩქარე;*
- *კომპიუტერული სისტემა იწყებს ჭედვას და საჭირო ხდება მისი ხშირი გადატვირთვა;*
- *მნიშვნელოვნად ქვეითდება ვებ-ბრაუზერების მიერ ვებსაიტების გახსნის სიჩქარე;*

- *ჩნდება მოულოდნელი ქსელური კავშირის პრობლემები;*
- *ხდება ფაილების არასანქცირებული მოდიფიცირება;*
- *ხდება ფაილების არასანქცირებული წაშლა;*
- *დესქტოპზე ჩნდება გაურკვეველი ფაილები, პროგრამები და „შორთკატები“;*
- *გააქტიურებულია გაურკვეველი პროცესები;*
- *პროგრამები თავისით ითიშებიან, ან ასრულებენ გაურკვეველ ოპერაციებს;*
- *ელ. წერილები იგზავნება ავტომატურად.*

სოციალური ინჟინერია

სოციალური ინჟინერია არის წვდომის მოპოვებაზე გათვლილი შეტევა, რომელიც დაფუძნებულია სამიზნე მომხმარებლით მანიპულირებაზე. სოციალური ინჟინერიის მწარმოებლები აღწევენ შედეგებს კლასიკური ადამიანური სისუსტეებზე ზემოქმედებით, მაგალითად ადამიანის ბუნებრივი დახმარების სურვილის ექსპლოატაციით.

წარმოიდგინეთ მაგალითი, როდესაც სოციალური ინჟინერიის მწარმოებელი დაურეკავს კომპანიის რომელიმე თანამშრომელს და სთხოვს მას დახმარებას გადაუდებელი პრობლემის გადასაჭრელად. ასეთ დროს, კიბერ თაღლითს შეუძლია ისარგებლობს ადამიანის გულუბრყვილობით, გამოიყენოს მოჩვენებითი ავტორიტეტი, ან თანამშრომლის სიძუნწე.

გთავაზობთ სხვადასხვა ტიპის სოციალური ინჟინერიის შეტევის მიმოხილვას:

- *Pretexting - ამ ტიპის სოციალური ინჟინერიის შეტევის საწარმოებლად, კიბერ ბოროტმოქმედი ურეკავს ადამიანს და ატყუებს მას, რომ გარკვეული მიზეზების გამო მას სჭირდება გარკვეული ინფორმაცია. მაგალითისთვის, კიბერ ბოროტმოქმედს შეუძლია სთხოვოს მომხმარებელს პერსონალური ან ფინანსური ინფორმაციის მოწოდება, რათა შესაძლებელი გახდეს მისი იდენტიფიცირება.*

- *Tailgating - ამ დროს, არაავტორიზებული ადამიანი ფეხდაფეხ მიჰყვება ავტორიზებულ ადამიანს და შედეგად აღწევს მისთვის დახურულ სივრცეში.*

- *Something for Something (Quid pro quo) - კიბერ ბოროტმოქმედი ითხოვს პირისგან ინფორმაციას რაღაცის სანაცვლოდ, მაგალითად საჩუქრის.*

უკაბელო ინტერნეტის როუტერის პაროლის გატეხვა

უკაბელო როუტერის (Wi-Fi) პაროლის გასატეხად არსებობს სხვადასხვა მექანიზმები. ესენია:

სოციალრი ინჟინერია – აღნიშნული შეტევის მწარმოებელი მანიპულირებს ადამიანით, რომელმაც იცის უკაბელო ქსელის პაროლი, რათა მოტყუებით დაეუფლოს მას.

„ბრუტ-ფორს“ შეტევები – აღნიშნული შეტევის მწარმოებელი ცდილობს გამოიცნოს პაროლი. თუ პაროლი შედგება 4 ციფრისგან, საკმარისია 10000 კომბინაციის ცდა. როგორც წესი, „ბრუტ-ფორს“ შეტევებს აწარმოებენ სპეციალურ ლექსიკონებზე დაყრდნობით.

უკანასკნელი წარმოადგენს ტექსტურ დოკუმენტს, სადაც მოხვედრილია სიტყვები ჩვეულებრივი ლექსიკონიდან. შემდომ, პროგრამა ცდილობს თითოეული სიტყვის მორგებას, რათა საბოლოოდ გატეხოს პაროლი. ვინაიდან ასეთ შეტევას მიაქვს დიდი დრო, კომპლექსური პაროლების გატეხვა „ბრუტ-ფორსის“ მეშვეობით არ არის პრაქტიკული გამოსავალი. „ბრუტ-ფორს“ შეტევის საწარმოებლად შეგიძლიათ გამოიყენოთ შემდეგი პროგრამები:

- *Ophcrack;*
- *L0phtCrack;*
- *THC Hydra;*
- *RainbowCrack;*
- *Medusa.*

ქსელის „სნიფინგი“ – ეს შეტევა გულისხმობს ქსელში გაგზავნილი ინფორმაციული პაკეტების გადაჭერას და გაანალიზებას. ამ დროს, ჰაკერს შეუძლია დაეუფლოს პაროლს, თუ ის არ არის დაშიფრული (ანუ, Plain ტექსტშია). თუ პაროლი დაშიფრულია, შეტევის მწარმოებელს მაინც აქვს პაროლის ამოღების შესაძლებლობა - სპეციალური პროგრამული უზრუნველყოფის გამოყენებით.

ფიშინგი

ფიშინგი არის თაღლითური ელ. წერილი, რომელიც მაქსიმალურად მიმსგავსებულია ლეგიტიმურს და აჩენს ილუზიას, რომ ის წამოსულია ლეგიტიმური წყაროდან. ამ ელ. წერილის მიზანია ადრესატის მოტყუება - მისი დაყოლიება მავნებელი პროგრამის გამოწერაზე / გაშვებაზე, პერსონალური ინფორმაციის ან / და ფინანსური ინფორმაციის გაზიარებაზე.

ფიშინგის კლასიკური მაგალითია საცალო ვაჭრობის ობიექტისგან შემოსული ელ. წერილი, სადაც წერია, რომ ადრესატმა მოიგო რაღაც პრიზი და ამ პრიზის მისაღებად ის უნდა გადავიდეს მითითებულ ბმულზე. დიდი ალბათობით, ეს ბმული გადაგიყვანთ ყალბ, ანუ „ფეიკ“ ვებსაიტზე, რომელიც ეცდება თქვენი პირადი ინფორმაციის მოპარვას, ან თქვენს დაყოლიებას ვირუსის გაშვებაზე.

ფიშინგის ერთერთი ნაირსახეობაა „ფიშინგი შუბით“. ამ ტიპის ფიშინგი გათვლილია კონკრეტულ სამიზნეზე. მიუხედავად იმისა, რომ ორივე ტიპის ფიშინგი ხორციელდება ელ. წერილის გამოყენებით, „ფიშინგი შუბით“ არის პერსონალიზებული და გათვლილია კონკრეტულ ადამიანზე. ვიდრე კიბერ ბოროტმოქმედი დაიწყებს „ფიშინგს შუბით“, ის ჯერ შეისწავლის თავის სამიზნეს. მაგალითისთვის, რა ავტომობილი მოსწონს სამიზნეს. შემდგომ, ჰაკერი უერთდება სადისკუსიო ფორუმს გადის უშუალო კონტაქტზე თავის სამიზნესთან, ქმნის ყალბ ფასდაკლების შეთავაზებას და უგზავნის მას თავის მსხვერპლს. როდესაც, სამიზნე მომხმარებელი აწკაპუნებს მითითებულ ბმულზე, მის კომპიუტერულ სისტემაზე იწერება მავნებელი პროგრამა.

სისუსტეების ხელყოფა

სისუსტეების ხელყოფა არის შეღწევის კიდევ ერთი გავრცელებული მეთოდი. შეტევის მწარმოებელი ასკანირებს კომპიუტერს და მაქსიმალურად აგროვებს ინფორმაციას მის შესახებ. გთავაზობთ სისუსტეების ხელყოფის გავრცელებული მეთოდების მიმოხილვას:

ნაბიჯი 1. სამიზნე კომპიუტერულ სისტემაზე ინფორმაციის შეგროვება. ამის გაკეთება შესაძლებელია მრავალი სხვადასხვა მეთოდით, მათ შორის პორტების სკანირებით და სოციალური ინჟინერიის გამოყენებით. ძირითადი მიზანია სამიზნე კომპიუტერულ ინფორმაციაზე მაქსიმალური ინფორმაციის შეგროვება.

ნაბიჯი 2. პირველი ნაბიჯში აღწერილი ქმედების შესრულების შედეგად მოპოვებული ინფორმაცია მოიცავს ოპერაციულ სისტემას, მის ვერსიას და სერვისებს, რომლებიც მუშაობენ ამჟამად. მეორე ნაბიჯზე ხდება ამ ინფორმაციის გაანალიზება.

ნაბიჯი 3. როდესაც შეტევის მწარმოებელმა იცის, თუ რომელი ოპერაციული სისტემის რა ვერსია აყენია მის სამიზნე კომპიუტერზე, ის იწყებს აღმოჩენილი სისუსტეების „ექსპლოიტების“ მოძებნას.

ნაბიჯი 4. როდესაც სისუსტე მოიძებნება, ჰაკერი იწყებს „ექსპლოიტების“ ძებნას. თუ „ექსპლოიტი“ არ არსებობს, მას თავად შეუძლია დაწეროს ის.

აღწერილი შეტევის საწარმოებლად გამოიყენება პროგრამა Nmap.

დახვეწილი „ჯიუტი“ საფრთხეები
ADVANCED PERSISTENT THREATS

შეღწევის ერთერთი მეთოდია დახვეწილი „ჯიუტი“ საფრთხეების გამოყენება (APT-ები). ისინი შედგება მულტი-ფაზური, გრძელვადიანი, აღმოსაჩენად რთული და კომპლექსური ოპერაციებისგან, რომლებიც გამიზნულია კონკრეტულ სამიზნეზე. ვინაიდან, ასეთი ტიპის შეტევა საჭიროებს საკმაოდ მაღალ ცოდნას და გამოცდილებას, APT-ს ტიპის შეტევებს ძირითადად კარგად აფინანსებენ. ეს შეტევები გამოიყენება ორგანიზაციების, სახელმწიფოების და პოლიტიკური მოღვაწეების წინააღმდეგ.

ძირითად, APT შეტევა დაყრდნობილია ქსელურ ჯაშუშობაზე, რა დროსაც, შეტევის მწარმოებელი სამიზნე ქსელში ნერგავს სპეცლიზებულ მავნებელ პროგრამას / პროგრამებს. ასეთი მავნებელი პროგრამების აღმოჩენა ძალიან რთული გამოწვევაა.

ზოგჯერ, გამოიყენებასხვადასხვატიპისმავნებელიპროგრამების ერთობლიობა, რათა მოხდეს, ქსელში არსებული ყველა მოწყობილობის, ინფიცირება. APT შეტევის საწარმოებლად საჭიროა ჯგუფი, ვინაიდან ცალკეულ ჰაკერს გაუჭირდება ყველა ოპერაციის შესრულება და მოპოვებული ინფორმაციის გაანალიზება.

DENIAL OF SERVICE

უარი სერვისის მიწოდებაზე „Denial-of-Service“ (DoS) - ეს არის ქსელური შეტევის ერთერთი გავრცელებული ნაირსახეობა. DoS შეტევის შედეგად, ქსელური სერვისი წყვეტს მუშაობას, რა დროსაც წყდება სერვისის მიწოდება მომხმარებლებისთვის, ელექტრონული მოწყობილობებისთვის და აპლიკაციებისთვის. არსებობს DoS შეტევის ორი ვარიანტი:

ჭარბი ინტერნეტ ტრეფიკის მიწოდება - ამ დროს, DoS შეტევის სამიზნეს ეგზავნება აურაცხელი ოდენობის ინტერნეტ ტრეფიკი, რომლის მომსახურებასაც ის ვერ ახერხებს. ეს იწვევს მოთხოვნების და პასუხების შენელებას, ან სერვისის სრულ შეჩერებას.

ბოროტი განზრახვით ფორმატირებული საინფორმაციო პაკეტები (Maliciously Formatted Packets) - ასეთი DoS შეტევის საწარმოებლად, ჰაკერი უგზავნის „ჰოსტს“, ან აპლიკაციას ისეთ ინტერნეტ პაკეტებს, რომლებთანაც გამკლავება უკანასკნელს არ შეუძლია. ეს იწვევს მიმღები მოწყობილობის შენელებას, ან დროებით გათიშვას.

DoS შეტევა წარმოადგენს მნიშვნელოვან რისკს, რადგან მას შეუძლია კავშირგაბმულობის შეფერხება; დროის და სახსრების მნიშვნელოვანი დანაკარგის გამოწვევა. სხვა კიბერ შეტევებთან შედარებით, DoS შეტევა საკმაოდ ადვილი საწარმოებელია და მის წარმოებას გამოცდილების არმქონე ადამიანიც გაუმკლავდება.

DISTRIBUTED DENIAL OF SERVICE

DDoS არის DoS-ის მსგავსი შეტევა, იმ განსხვავებით, რომ პირველი ერთდროულად წარმოებს რამდენიმე წყაროდან. თვალსაჩინოებისთვის, წარმოიდგინეთ DDoS შეტევის შემდეგი მაგალითი:

შეტევის მწარმოებელი ქმნის ინფიცირებული „ჰოსტების“ (ბოტნეტების) ქსელს. მათ ასევე უწოდებენ ზომბებს. ეს ზომბები იმართება ჰაკერის კომპიუტერიდან.

ზომბი კომპიუტერები გამუდმებით ასკანირებენ და აინფიცირებენ სხვა ჰოსტებს. როდესაც ჰაკერი განსაზღვრავს მიზანს, ზომბები ერთდროულად განახორციელებენ DDoS შეტევას.

SEO POISONING

Google და მისი ანალოგი საძიებო სისტემები მუშაობენ ვებსაიტების შეფასების სისტემაზე დაყრდნობით. ვებსაიტის კონტენტიდან გამომდინარე, საძიებო სისტემა ძიების შედეგებში ათავსებს მას შესაბამის ადგილზე. SEO შეტევა გამოყენება საძიებო სისტემების მიერ ვებ-საიტების შეფასების გასაუმჯობესებლად. მაშინ, როდესაც კეთილსინდისიერი მომხმარებელი იბრძვის უფრო მაღალი შეფასებისთვის, არაკეთილსინდისიერ ადამიანს შეუძლია მოაქციოს საკუთარი უფრო დაბალი ხარისხის ვებ-საიტი უფრო მაღალ პოზიციაზე. სწორედ ამ ტექნიკას ეწოდება საძიებო სისტემების მოწამვლა.

მითითებულ ვებ-საიტზე ტრეფიკის გაზრდა არის SEO შეტევის ძირითადი მიზანი. შესაძლოა ასეთ ვებსაიტებზე იყოს მავნებელი პროგრამები ან/და სოციალური ინჟინერიის ელემენტები. ძიების შედეგებში მოწინავე ადგილის დასაკავებლად, არაკეთილსინდისიერი ადამიანები იყენებენ პოპულარულ საძიებო ტერმინებს.

ჰა არის შეხვედრი შეტევა?
BLENDED ATTACK

შეტევა შერეულია, როდესაც თავდასხმის საწარმოებლად ერთდროულად გამოიყენება რამდენიმე სხვადასხვა ტექნიკა. როგორც წესი, ასეთი შეტევის მწარმოებლებს აქვთ სპეციალური მავნებელი პროგრამა, რომელიც კომპიუტერული ჭიის, ტროიანის, ჯაშუშური პროგრამის, „Keylogger"-ის, სპამის და ფიშინგ სქემის ჰიბრიდია. როგორც ხედავთ, შერეული შეტევების საწარმოებლად გამოიყენება კომპლექსური მავნებელი პროგრამები, რომლებიც მნიშვნელოვნად ზრდიან სამიზნე მომხმარებლის ინფორმაციის ხელყოფის რისკებს.

შერეული შეტევის ერთერთი ყველაზე გავრცელებული ფორმაა მავნებელი საიტების ბმულების გავრცელება „სპამის" შემცველ ელ. წერილებში, ტექსტური შეტყობინებებში, ან ლეგიტიმურ ვებსაიტებზეც კი. შედეგად, დაუდევარი მომხმარებელი იწერს მავნებელ პროგრამას საკუთარ კომპიუტერზე. შერეული შეტევის წარმოების კიდევ ერთი გავრცელებული მეთოდია ერთდროული DDoS შეტევა ვებსაიტზე და ამ ვებსაიტის მომხმარებლებისთვის ფიშინგ წერილების გაგზავნა. დასაწყისისთვის, კიბერ ბოროტმოქმედი აწარმოებს DDoS შეტევას, მაგალითად ბანკის ვებსაიტზე. შემდგომ, ის ბანკის სახელით უგზავნის მომხმარებლებს მობოდიშების წერილს, სადაც უთითებს ბანკის ყალბ სარეზერვო ვებსაიტს. დაუდევარი მომხმარებელი ამ ყალბ ვებსაიტზე შეიყვანს თავის ანგარიშზე შესვლისთვის საჭირო მონაცემებს, რომლებიც მოხვდება ჰაკერის ხელში.

ყველაზე დამანგრეველი კომპიუტერული ჭიები, როგორებიცაა Nimbda, CodeRed, BugBear, Klez და Slammer ექცევა ნაზავი კიბერ თავდასხმების კატეგორიაში.

- *Nimbda-ს ზოგიერთი ვარიანტი გამოიყენება, როგორც ელ. წერილის თანდართული ფაილი. ეს ფაილი ჩამოიტვირთება ხელყოფილი სერვერიდან, ან Microsoft-ის „File Sharing"-იდან;*

- *Nimbda-ს სხვა ვარიაციებს შეუძლიათ კომპიუტერული სისტემის სტუმრის ანგარიშების ხელყოფა და შემდგომ პრივილეგიების ესკალაცია ადმინისტრატორის დონემდე.*

შედარებით ახალი Conficker და ZeuS/LICAT ჭიები ასევე წარმოადგენენ ნაზავი შეტევის ნაირსახეობებს. Conficker იყენებდა გავრცელების ყველა სტანდარტულ მეთოდს.

ᲠᲐᲡ ᲜᲘᲨᲜᲐᲕᲡ ᲖᲘᲐᲜᲘᲡ ᲛᲘᲜᲘᲛᲘᲖᲐᲪᲘᲐ?

იმის მიუხედავად, რომ წარმატებული კომპანიების უმეტესობამ იცის კიბერ რისკების შესახებ და მათ შეაქვთ დიდი ძალისხმევა ამ საფრთხეების განეიტრალებაში, არ არსებობს 100%-იანად უსაფრთხო კიბერ გარემო. რაც უფრო დიდი ნადავლი ელის ჰაკერს წარმატების შემთხვევაში, მით უფრო დიდია რისკი, რომ ის არ დაზოგავს კრეატიულობას და ენერგიას, რათა მიაღწიოს თავის მიზანს. შესაბამისად, კომპანიები და ორგანიზაციები უნდა იყონ მზად ზიანის მინიმიზაციისთვის.

ნიშანდობლივია, რომ შეღწევის შედეგად გამოწვეული ზიანი მდგომარეობს არამხოლოდ ტექნიკური საკუთრების გამოსწორებაში, არამედ კომპანიას ასევე მოუწევს გამკლავება მოპარული ინფორმაციის, დაზიანებული მონაცემთა ბაზების, ინტელექტუალური საკუთრების მოპარვის და რეპუტაციასთან დაკავშირებული ზიანის შედეგებთან. ამ გამოწვევებთან გამკლავება არის ძალზე დინამიური პროცესი.

გთავაზობთ რეკომენდაციებს ზიანის მინიმიზაციის უზრუნველსაყოფად:

- *კომპანიის თანამშრომლებმა უნდა იცოდნენ მომხდარი შეღწევის შესახებ და შეიტანონ თავიანთი წვლილი რისკების მინიმიზაციაში. კომპანიის კლიენტებმაც უნდა გაიგონ ამის შესახებ. კომუნიკაცია ქმნის გამჭვირვალობას და ასეთი სიტუაციაში ის აუცილებელია;*

- *იყავით გულწრფელი და აღიარეთ პასუხისმგებლობა (რა თქმა უნდა, თუ შეღწევა მოხდა თქვენი ბრალეულობით);*

- *არ დამალოთ დეტალები. აუხსენით დაინტერესებულ საზოგადოებას, რის გამო მოხდა სისტემაში შეღწევა და რა ინფორმაცია იქნა ხელყოფილი. მოემზადეთ იმისთვის, რომ თქვენ კომპანიას შესაძლოა მოუწიოს გარკვეული ხარჯების ანაზღაურება;*

- *გაიაზრეთ, რამ გამოიწვია და შეუწყო ხელი მომხდარ შეღწევას. თუ საჭიროა, დაიქირავეთ კიბერ კრიმინალისტები;*

- *გაანალიზეთ კიბერ კრიმინალისტების რეკომენდაციები, რათა ასეთი ტიპის შეღწევა აღარ გამეორდეს;*

- *დარწმუნდით, რომ ყველა სისტემა გასუფთავებულია, ის არ შეიცავს „Backdoor“-ებს და სხვა ინფორმაციის / სივრცის ხელყოფა არ მომხდარა. როგორც წესი, კიბერ ბოროტმოქმედები ეცდებიან „Backdoor“-ის დატოვებას თქვენს სისტემაზე, რათა მოგვიანებით შეძლონ განმეორებითი შეტევის განხორციელება. დარწმუნდით, რომ ეს არ მოხდება;*

- *დაატრეინინგეთ თქვენი თანამშრომლები, პარტნიორები და კლიენტები კიბერ უსაფრთხოების ფუნდამენტალურ საკითხებში.*

თავი 3.

საკუთარი პირადულობის და ინფორმაციის დაცვა

ამ თავში განვიხილავთ საკუთარი კომპიუტერული ტექნიკის და პერსონალური ინფორმაციის დაცვას, ძლიერი პაროლების შექმნას და უკაბელო ქსელების უსაფრთხო გამოყენებას.

თქვენი ონლაინ ინფორმაცია ღირებულია კიბერ დამნაშავეებისთვის. ამ თავში აღმოაჩენთ უსაფრთხო აუთენტიფიკაციის ხერხების მოკლე მიმოხილვას და რჩევებს საკუთარი ონლაინ უსაფრთხოების სტანდარტის ამაღლებისთვის. ჩვენ შემოგთავაზებთ რეკომენდაციებს იმის თაობაზე, თუ რა უნდა გააკეთოთ და რა არა - ონლაინ ყოფნისას.

კომპიუტერული მოწყობილობების დაცვა

კომპიუტერული მოწყობილობები ინახავენ თქვენს ინფორმაციას და ამავდროულად წარმოადგენენ ერთგვარ პორტალს ონლაინ სამყაროში. გთავაზობთ რეკომენდაციების მოკლე სიას, თუ როგორ უნდა დაიცვათ თქვენი კომპიუტერული მოწყობილობები შეღწევისგან:

- *თქვენი „Firewall“ უნდა იყოს მუდმივად ჩართული – არ აქვს მნიშვნელობა, ეს ფიზიკური, თუ პროგრამული „Firewall“-ია, ის უნდა იყოს განახლებული ბოლო ვერსიამდე და იყოს ჩართული.*

- *გამოიყენეთ ანტივირუსული და ანტიჯაშუშური პროგრამული უზრუნველყოფა – ისეთი მავნებელი პროგრამები, როგორებიცაა ტროიანი, ჭია, გამომძალველი და ჯაშუშური აპლიკაციები, ყენდება კომპიუტერულ სისტემაზე თქვენი ნებართვის გარეშე. ვირუსებს შეუძლიათ თქვენი ინფორმაციის განადგურება, კომპიუტერის შენელება ან / და წვდომის გახსნა არასანქცირებული პირებისთვის. ჯაშუშური აპლიკაციები გაუმჟღავნებენ ჰაკერს თქვენს ონლაინ მოქმედებებს, პერსონალურ ინფორმაციას, შეგაწუხებენ „პოპ-აპებით“, რეკლამებით და ა.შ. დაიმახსოვრეთ ერთი წესი, რომელიც გამოგადგებათ ნებისმიერ შემთხვევაში - გადმოწერეთ პროგრამები მხოლოდ სანდო ვებსაიტებიდან. ანტივირუსული პროგრამები შექმნილია თქვენი კომპიუტერული სისტემის და შემოსული ელექტრონული კორესპოდენციის სკანირებისთვის. ზოგჯერ, ანტივირუსში ჩაშენებულია ანტიჯაშუშური პროგრამების აღმომჩენი აპლიკაციაც. არ დაგავიწყდეთ თქვენი პროგრამული უზრუნველყოფის რეგულარული განახლება, რათა აარიდოთ თავი ახალ მავნებელ პროგრამებს.*

- *განახორციელეთ თქვენი ოპერაციული სისტემის და ინტერნეტ ბრაუზერის რეგულარული მენეჯმენტი - ჰაკერები*

ყოველთვის ცდილობენ ოპერაციულ სისტემაში ვებ ბრაუზერში არსებული სისუსტეების ხელყოფას. თქვენი კომპიუტერული სისტემის და ინფორმაციის დასაცავად, დააყენეთ უსაფრთხოების პარამეტრები საშუალოზე, ან მაღალზე. განაახლეთ თქვენი ოპერაციული სისტემა და ინტერნეტ ბრაუზერები რეგულარულად - გადმოტვირთეთ და დააინსტალირეთ პროგრამული „პაჩები“ და უსაფრთხოების განახლებები უშუალოდ დეველოპერი კომპანიებისგან.

- *დაიცავით ყველა კომპიუტერული ხელსაწყო – თქვენი კომპიუტერულ მოწყობილობებში შედის „დესქტოპ“ კომპიუტერი, „ლეპტოპ“ კომპიუტერ, პლანშეტი, სმარტფონი და ა.შ. ყველა ხელსაწყოზე უნდა გეყენოთ ძლიერი პაროლი, რათა აარიდოთ საკუთარი მოწყობილობები არაავტორიზებულ შეღწევას. ამ მოწყობილობებზე შენახული ინფორმაცია უნდა იყოს დაშიფრული - განსაკუთრებით სენსიტიური ხასიათის ინფორმაცია. გაითვალისწინეთ, რომ შესაძლოა ვიღაცამ მოიპაროს თქვენი მობილური ხელსაწყოები. ასეთ შემთხვევაში, ქურდს არ უნდა ერგოს თქვენი ინფორმაციაც. თუ თქვენი რომელიმე მოწყობილობა იქნა ხელყოფილი, ჰაკერებს შეუძლიათ დაეუფლონ „ღრუბელზე“ განთავსებულ ინფორმაციასაც.*

შედარებით პრიმიტიული „IoT“ მოწყობილობებისგან გამომდინარეობს კიდევ უფრო მაღალი რისკები. მაშინ როდესაც, „დესქტოპ“ კომპიუტერების, „ლეპტოპ“ კომპიუტერების და მობილური პლატფორმების პროგრამული უზრუნველყოფა რეგულარულად ახლდება, „IoT“ მოწყობილობები ძირითადად რჩებიან თავიანთი თავდაპირველი ოპერაციული სისტემის ვერსიებზე. თუ ამ ოპერაციულ სისტემაზე აღმოჩნდება სისუსტე, ისინი, დიდი ალბათობით, იქნება მუდმივი ხასიათის. უარესია ის გარემოება, რომ „IoT“ მოწყობილობების დიდ ნაწილს გააჩნიათ ინტერნეტთან წვდომის შესაძლებლობა. შედეგად, ეს მოწყობილობები ქმნიან ერთგვარ შეტევის გვირაბს, რომლის გამოყენებითაც ჰაკერებს შეულიათ დაეუფლონ სამიზნე მომხმარებლის ქსელს და შემდგომ ამ ქსელში

არსებულ ინფორმაციას. ასეთი სისუსტეების აღმოსაფხვრელად, მიზანშეწონილია „IoT“ მოწყობილობების შეერთება იზოლირებულ ქსელებთან.

უკაბელო ქსელების უსაფრთხო გამოყენება

უკაბელო ქსელები აძლევს უკაბელო ინტერნეტის მხარდამჭერ მოწყობილობებს შესაძლებლობას იქონიონ კავშირი ინტერნეტთან, კაბელების გამოუყენებლად. „ლეპტოპები“ და პლანშეტები უერთდება ასეთ ქსელებს უნიკალური ამომცნობი სახელწოდების (SSID) მითითებით / ამორჩევით და სტანდარტული პაროლის შეყვანის საფუძველზე. იმისთვის, რომ დაიცვათ თქვენი ქსელი არაავტორიზებული პირებისგან, დაუყოვნებლივ გამოცვალეთ სტანდარტული SSID და პაროლი. გაითვალისწინეთ, რომ ხშირად ჰაკერები ფლობენ ქსელური მოწყობილობების სტანდარტულ პაროლებს, ან მათ ნიმუშებს. არსებობს SSID-ის დამალვის შესაძლებლობაც, რომელიც წარმოქმნის დაცვის დამატებით ბარიერს. მიუხედავად ამ პრევენციული ღონისძიებებისა, არ იფიქროთ, რომ თქვენი უკაბელო ქსელი სათანადოდაა დაცული. აუცილებლად გამოიყენეთ WPA2 ტიპის უსაფრთხოების ალგორითმი. ესეც არ არის უსაფრთხოების გარანტია, მაგრამ ის ჰაკერებს საქმეს მნიშვნელოვნად გაურთულებს.

2017 წლის ოქტომბერში, WPA2 პროტოკოლში აღმოაჩინეს უსაფრთხოების ღრიჭო. ეს სისუსტე აძლევდა არაავტორიზებულ მომხმარებელს შესაძლებლობას „ჩადგომოდა“ უკაბელო როუტერის და ავტორიზებულ მომხმარებლის კავშირს შორის. შედეგად, არაავტორიზებულ მომხმარებელი მანიპულირებდა ქსელის ტრეფიკით. ამ სისუსტის ექსპლოატაცია შესაძლებელია „Key Reinstallation Attacks“ (KRACK)-ის გამოყენებით. ყველა თანამედროვე ქსელს აქვს ეს სისუსტე.

იმისათვის, რომ აღნიშნულ შეტევასთან დაკავშირებული რისკები შემცირდეს, აუცილებლად განაახლოთ როუტერის ოპერაციული სისტემა და თქვენი მოწყობილობის უკაბელო ადაპტერის „დრაივერი“. თუ თქვენს კომპიუტერულ ტექნიკას გააჩნია Ethernet კაბელის შესაერთებელი, ჯობს გამოიყენოთ კაბელი. ასევე, გირჩევთ სანდო VPN მომსახურების გამოყენებას, რათა შეამციროთ არაავტორიზებული წვდომის ალბათობა.

როდესაც სახლში არ იმყოფებით, საჯარო უკაბელო ინტერნეტი გაძლევთ შესაძლებლობას შეინარჩუნოთ წვდომა ინტერნეტთან. ეს მოსახერხებელია, მაგრამ სენსიტიური ინფორმაციის შეყვანა ასეთი ქსელის გამოყენებით არ არის რეკომენდებული. ასევე, დარწმუნდით, რომ თქვენს კომპიუტერზე არ არის გახსნილი საჯარო საქაღალდეები, ან დისტანციური წვდომის მისაღებად ისინი საჭიროებენ პაროლის შეყვანას. გამოიყენეთ VPN სერვისები, რათა კიბერ ბოროტმოქმედებმა ვერ შეძლონ თქვენი ინფორმაციის გადაჭერა. VPN სერვისი არის ინტერნეტთან უსაფრთხო წვდომის ერთერთი შესაძლებლობა, რომელიც შიფრავს თქვენს კავშირს. ჰაკერმა რომც მოახერხოს ინფორმაციის გადაჭერა, ის ვერ შეძლებს მის გაშიფვრას - შესაბამისად ის ვერ ხელყოფს თქვენს ინფორმაციულ უსაფრთხოებას.

ბევრ მობილურ მოწყობილობას (სმარტფონებს და პლანშეტებს) გააჩნიათ Bluetooth-ის მხარდაჭერა. ამ უკაბელო პროტოკოლის გამოყენებით შეძლებთ თქვენი ელექტრონული მოწყობილობების დაკავშირებას და ინფორმაციის გაზიარებას. სამწუხაროდ, Bluetooth-ს აქვს თავისი სისუსტეები და ჰაკერებს შეუძლიათ ამ სისუსტეების ხელყოფა - ხელსაწყოს დისტანციური მართვა, მავნებელი პროგრამების გავრცელება და აკუმულატორის სწრაფი დასმა. ამ პრობლემების თავიდან ასარიდებლად, გათიშეთ Bluetooth კავშირი, როდესაც მას არ იყენებთ.

ონლაინ ანგარიშების პაროლები

დიდი ალბათობით, თქვენ გაქვთ გახსნილი ერთზე მეტი ონლაინ ანგარიში. თითოეულს უნდა ჰქონდეს უნიკალური, ანუ განსხვავებული, პაროლი. დიახ, ყველა პაროლის დამახსოვრების თვალსაზრისით ეს რთულია, მაგრამ სუსტი პაროლის გამოყენება ონლაინ სერვისებზე წარმოშობს მნიშვნელოვან უსაფრთხოების რისკებს. ეს იგივეა, რაც ყველა კარის საკეტზე ერთი და იგივე გასაღები გამოიყენოთ. თუ ბოროტმოქმედი დაეუფლება ერთ გასაღებს, ის შეძლებს ყველა კარის გახსნას. ჰაკერს შეუძლია დაეუფლოს თქვენს პაროლს ფიშინგის მეშვეობით. შედეგად, ის მიიღებს წვდომას თქვენს ყველა ონლაინ ანგარიშზე. როგორც წესი, ამას მოყვება ინფორმაციის ან იდენტობის მოპარვა.
თანამედროვე ადამიანი იყენებს უამრავ ონლაინ ანგარიშს და ყველა პაროლის დამახსოვრება ხდება საკმაოდ რთული გამოწვევა. გამოიყენეთ პაროლების მენეჯერი პროგრამები, რათა არ მოგიწიოთ ყველა პაროლის დამახსოვრება. ასეთი პროგრამა ინახავს ყველა პაროლს დაშიფრული სახით. თუმცა, პაროლების მენეჯერის გასახსნელად უნდა გამოიყენოთ რთული პაროლი, რომელსაც ასევე უწოდებენ „მასტერ პაროლს“.

ძლიერი პაროლის შერჩევის რეკომენდაციები:

- *არ გამოიყენოთ ლექსიკონში არსებული სიტყვები (არცერთი ენის);*

- *არ გამოიყენოთ პაროლები, რომლებიც წარმოადგენენ ლექსიკონში არსებული სიტყვების ხშირად დაშვებულ შეცდომებს;*

- *არ გამოიყენოთ კომპიუტერის სახელწოდებები და ანგარიშების სახელები;*

- *თუ შესაძლებელია, გამოიყენეთ შემდეგი სპეციალური სიმბოლოები ! @ # $ % ^ & * ( )*

- *გამოიყენეთ პაროლი, რომელიც შედგება 10-ზე მეტი ასოსგან / ციფრისგან / სიმბოლოსგან.*

პაროლის ნაცვლად გამოიყენეთ საიდუმლო წინადადება

არაავტორიზებული წვდომის რისკის მინიმიზაციისთვის, პაროლის ნაცვლად გამოიყენეთ საიდუმლო წინადადებები. გრძელი საიდუმლო წინადადების დამახსოვრება გაცილებით უფრო ადვილია, ვიდრე გრძელი პაროლის, რადგან პირველი შედგება რამდენიმე სიტყვისგან. რაც უფრო გრძელი იქნება თქვენი საიდუმლო წინადადება, მით ნაკლებია იმის შანი, რომ ჰაკერი შეძლებს „ბრუტ-ფორს“, ან ლექსიკონის შეტევის წარმატებულ განხორციელებას. საიდუმლო წინადადების შერჩევისას გამოიყენეთ შემდეგი რეკომენდაციები:

- *აირჩიეთ წინადადება, რომელსაც თქვენთვის აქვს ლოგიკური მნიშვნელობა;*

- *თუ შესაძლებელია, გამოიყენეთ შემდეგი სპეციალური სიმბოლოები ! @ # $ % ^ & * ( )*

- *რაც უფრო გრძელია საიდუმლო წინადადება, მით უკეთესი;*

- *არ გამოიყენოთ ცნობილი გამოთქმები და სიმღერების ტექსტებიდან ამოღებული წინადადებები;*

ცოტა ხნის წინ, შეერთებული შტატების ტექნოლოგიური სტანდარტების ეროვნულმა ინსტიტუტმა (NIST) გამოსცა გაუმჯობესებული პაროლების მოთხოვნები. NIST-ის სტანდარტები გამიზნულია სახელმწიფო ორგანიზაციებისთვის, თუმცა მათი გამოყენება შესაძლებელია სტანდარტული საჭიროებებისთვისაც. ახალი რეკომენდაციები გათვლილია მომხმარებლის მოქმედებების გასამარტივებლად, რა დროსაც საკმაოდ მძიმე ტვირთი ეკისრება პროვაიდერებს.

ეს რეკომენდაციებია:

- *მინიმუმ 8 სიმბოლოს შემცველი პაროლი, მაგრამ არაუმეტეს 64 სიმბოლოსა;*

- *პაროლები, როგორიცაა abc123 და მისი ანალოგების გამოყენება დაუშვებელია;*

- *არ არის საჭირო პაროლის კომპოზიციის დადგენა. ანუ, სერვისებმა მომხმარებელი არ უნდა აიძულონ გამოიყენოს დიდი და პატარა ასოების და ციფრების კომბინაცია;*

- *მომხმარებლებს უნდა მიეცეს საშუალება დაინახონ პაროლი თავდაპირველი შეყვანისას;*

- *ნებისმიერი სიმბოლო და ადგილის გამოტოვება უნდა იყოს დასაშვები;*

- *დაუშვებელია პაროლის მიმანიშნებელი ფრაზების გამოყენება (Password Hints);*

- *პაროლის პერიოდული და იძულებით გამოცვლა არ უნდა იყოს სავალდებულო;*

- *აუთენტიფიკაცია არ უნდა მოხდეს ე.წ. „ცოდნის“ ფაქტორზე. ანუ, დაუშვებელია საიდუმლო კითხვებში, მარკეტინგული ინფორმაციის და ტრანზაქციების ისტორიის გამოყენება.*

ინფორმაციის დაშიფვრა

თქვენი ინფორმაცია ყოველთვის უნდა იყოს დაშიფრული. შესაძლოა დაგებადოთ კითხვა: „თუ მე დასამალი არაფერი მაქვს, რისთვის მჭირდება ინფორმაციის დაშიფვრა?“ შესაძლოა, თქვენ ფიქრობთ, რომ არავის სჭირდება თქვენი ინფორმაცია. დიდი ალბათობით, თქვენ ფიქრობთ არასწორად.

მზად ხართ, აჩვენოთ ყველა თქვენი ფოტოგრაფიის და დოკუმენტის უცხო ადამიანს? აჩვენებდით საკუთარ ფინანსებთან დაკავშირებულ ინფორმაციას თქვენს მეგობრებს? გამოაქვეყნებდით თქვენი ელ. ფოსტის და სხვა ონლაინ სერვისების „ლოგინებს“ და პაროლებს საჯაროდ?

თუ კომპიუტერი, ან მობილური ელექტრონული ხელსაწყო დაინფიცირდება მავნებელი პროგრამით, ჰაკერს ექნება საშუალება მოიპაროს თქვენი ანგარიშის ნომრები, პაროლები და სხვა დოკუმენტაცია. აღნიშნული ინფორმაციის გამოყენება შესაძლებელია თქვენი იდენტობის მოსაპარად, თაღლითური სქემების გასატარებლად და გამოძალვისთვის. ჰაკერს შეუძლია დაშიფროს თქვენი ინფორმაცია და მოგთხოვთ ფული მისი გაშიფვრისთვის.

რა არის დაშიფვრა? დაშიფვრა ეწოდება პროცესს, რომლის დროსაც ხდება ინფორმაციის ტრანსფორმაცია ისეთ ფორმაში, რომელსაც ვერ ამოიკითხავს არაავტორიზებული პირი. მხოლოდ ავტორიზებულ ადამიანს, რომელსაც გააჩნია შიფრის გასაღები, შეძლებს ამ ინფორმაციის დაბრუნებას ორიგინალურ ფორმაში. თავად დაშიფვრის პროცესი ვერ უზრუნველყოფს ინფორმაციის დაცვას გადაჭერისგან, მაგრამ ჰაკერისთვის ის იქნება უსარგებლო, რადგან ის ვერ წაიკითხავს / დაინახავს მის შიგთავსს.

ფაილების, ან მთლიანი მყარი დისკის სექტორის დასაშიფრად გამოიყენება სპეციალური პროგრამული უზრუნველყოფა.

„Encrypting File System“ (EFS) არის MS Windows-ის დასაშიფრი ფუნქცია. EFS მიმაგრებულია უშუალო მომხმარებლის ანგარიშთან. EFS-ით დაშიფვრის შედეგად, მხოლოდ დამშიფვრელ მომხმარებელს შეეძლება გაშიფვრის გაკეთება. ინფორმაციის დასაშიფრად Windows-ზე:

ნაბიჯი 1. აირჩიეთ ერთი, ან რამდენიმე საქაღალდე;

ნაბიჯი 2. დააწკაპუნეთ მაუსის მარჯვენა ღილაკით და აირჩიეთ > Properties.

ნაბიჯი 3. დააწკაპუნეთ > Advanced…

ნაბიჯი 4. მონიშნეთ > Encrypt contents to secure data;

ნაბიჯი 5. ფაილები და საქაღალდეები, რომლებიც იქნა დაშიფრული გამოჩნდება მწვანე ფრად.

ინფორმაციის ჰეზეჰვიჰება BACKUPS

არსებობს იმის ალბათობა, რომ თქვენი მყარი დისკი გაფუჭდება, ლეპტოპს ან/და მობილურ სმარტფონს მოიპარავენ. შესაძლოა თქვენ შემთხვევით წაშალოთ მნიშვნელოვანი დოკუმენტის დედანი. არქივების წარმოება მოგცემთ იმის გარანტიას, რომ მნიშვნელოვანი (აღუდგენადი) ინფორმაცია არ გაქრება. იმისათვის, რომ შეძლოთ ინფორმაციის არქივირება, დაგჭირდებათ დამატებითი მეხსიერების მატარებელი, რომელზეც რეგულარულად შექმნით ინფორმაციის სარეზერვო ასლებს. შესაძლებელია ამ პროცესის ავტომატიზაციაც.

არქივების სარეზერვო სივრცედ შეგიძლიათ გამოიყენოთ სახლის ქსელი, დამატებითი მეხსიერების მატარებელი, ან „ღრუბელი“. თუ თქვენი ინფორმაცია არქივირებულია ლოკალურად, მაშინ თქვენ მასზე გაქვთ განუსაზღვრელი წვდომა. სარეზერვო ასლების შენახვა შეგიძლიათ ქსელურ მეხსიერების მატარებლებზე (NAS), ჩვეულებრივ გარე მეხსიერების მატარებლებზე, USB ფლეშკებზე, ან ოპტიკურ დისკებზე. თუ აირჩევთ ამ ვარიანტს, მაშინ არქივირებული ინფორმაციის მოწყობილობების შეძენა და მოვლა იქცევა თქვენს უშუალო პასუხისმგებლობად.

ასევე, შეგიძლიათ გამოიყენოთ „ღრუბლის“ ტიპის ინფორმაციის სათავსო, რომლისთვისაც მოგიწევთ გარკვეული თანხის გადახდა. მაგალითისთვის, Amazon Web Services (AWS) ტიპის „ღრუბლის“ სერვისზე არქივირებულიინფორმაციაშეინახებაიქამდე,ვიდრეთქვენ გექნებათ გახსნილი მომხმარებლის ანგარიში. როდესაც ირჩევთ ამ ტიპის სარეზერვო ასლების გაკეთებას, თქვენ ასევე უნდა შეარჩიოთ ინფორმაცია, რომლის არქივირებაც გსურთ. დიდი მოცულობის „ღრუბლის“ ტიპის მეხსიერება შესაძლოა დაგიჯდეთ საკმაოდ ძვირი. არქივირებას „ღრუბელზე“ აქვს მნიშვნელოვანი დადებითი მხარე. ცეცხლის გაჩენის, ან სხვა (არამასშტაბური) კატასტროფის შედეგად, თქვენი ინფორმაცია შენარჩუნდება.

ინფორმაციის სამუდამო ნაშიერა

როდესაც ფაილებს ყრით თქვენი კომპიუტერის სანაგვე ურნაში და შემდგომ შლით, ისინი სინამდვილეში სამუდამოდ არ იშლება. სპეციალური კიბერ კრიმინალისტიკური ინსტრუმენტების გამოყენებით შესაძლებელია მათი აღდგენა, რადგან ასეთი მეთოდით წაშლილი ფაილები მაინც ტოვებენ მაგნიტურ კვალს თქვენს მყარ დისკზე.

იმისათვის, რომ ინფორმაცია მართლაც წაიშალოს სამუდამოდ, საჭიროა მყარი დისკის შესაბამისი სივრცის გადაწერა 0-ებით და 1-იანებით. თანაც, რამდენიმეჯერ. იმისათვის, რომ წაშლილი ფაილების აღდგენა გახდეს შეუძლებელი, თქვენ დაგჭირდებათ სპეციალური პროგრამული ინსტრუმენტების გამოყენება. მაგალითისთვის, MS Windows-ის ოპერაციული სისტემის (Vista, ან უფრო ახალი) პროგრამა „SDelete“ ირწმუნება, რომ მას შეუძლია ფაილების სამუდამო წაშლა. Linux-ის ოპერაციულ სისტემებზე ასეთი პროგრამაა „Shred“, ხოლო Mac OS-ებისთვის „Secure Empty Trash“.

ერთადერთი 100%-იანი გარანტია, რომ ფაილი მართლაც წაიშალა არის მეხსიერების მატარებლის ფიზიკური განადგურება. ბევრმა კიბერ დამნაშავემ არ იცოდა იმის შესახებ, რომ შესაძლებელია ფაილების აღდგენა. სწორედ ამან დაღუპა ისინი.

გარდა ლოკალური მეხსიერების მატარებლებისა, ინფორმაციის შენახვა შესაძლებელია „ღრუბელზეც“. ინფორმაციის გასანადგურებლად საჭიროა „ღრუბელზე“ არსებული ფაილების სამუდამო წაშლაც. აბა დაფიქრდით, სად ინახება თქვენი ინფორმაცია? არსებობს, თუ არა, ამ ინფორმაციის სარეზერვო ასლები? დაშიფრულია, თუ არა, ეს ინფორმაცია? არსებობს იმის გარანტია, რომ ინფორმაცია არაავტორიზებული ადამიანის ხელში არ მოხვდება?

ორი ნაბიჯიანი აუთენტიფიკაცია

პოპულარული ონლაინ სერვისები, როგორიცაა Google, Facebook, Twitter, LinkedIn, Apple და Mircosoft, იყენებენ ორ ნაბიჯიან აუთენტიფიკაციას, რათა დაამატონ უსაფრთხოების კიდევ ერთი შრე. გარდა მომხმარებლის სახელებისა, პაროლებისა, ან პერსონალური იდენტიფიკაციის ნომრისა (PIN), ისინი იყენებენ ორ ნაბიჯიან აუთენტიფიკაციას, რა დროსაც საჭიროა დამატებითი ობიექტის გამოყენება, მაგალითად:

- *ფიზიკური ობიექტი - საკრედიტო ბარათი, სადებიტო ბარათი, ტელეფონი, ან ელექტრონული „ბრელოკი“;*

- *ბიომეტრული ინფორმაცია - თითის ანაბეჭდი, ხელის გულის ანაბეჭდი, სახის, ან ხმის ამომცნობი.*

ორ ნაბიჯიანი აუთენტიფიკაცია არ არის უსაფრთხოების 100%-იანი გარანტია. ჰაკერებს მაინც შეეძლებათ თქვენი მოტყუება ფიშინგის და სოციალური ინჟინერიის ტიპის შეტევების შედეგად, ან მავნებელი პროგრამული უზრუნველყოფის გამოყენებით.

OAUTH 2.0

ღია ავტორიზაცია (OAuth) არის სტანდარტული ღია პროტოკოლი, რომელიც იძლევა საშუალებას გადასცეს მესამე პირს თქვენი აუთენტიფიკაციის ინფორმაცია - მოხმარებლის პაროლის გაუცემლად. „OAuth“ ითავებს შუამავალის როლს და წყვეტს, მიანიჭოს, თუ არა, მესამე პირის აპლიკაციას წვდომა თქვენს აუთენტიფიკაციის ინფორმაციაზე. მაგალითისთვის, თუ უკავშირდებით ვებ აპლიკაციას XYZ, მაგრამ თქვენ არ გაქვთ ანგარიში ამ ვებ აპლიკაციაზე, XYZ გაძლევთ შესაძლებლობას შეხვიდეთ სისტემაში თქვენი სოციალური მედიის ABC აუთენტიფიკაციის გამოყენებით.

იმისათვის, რომ ამ მეთოდმა იმუშაოს, XYZ აპლიკაცია უნდა იყოს დარეგისტრირებული ABC-ზე. უკანასკნელმა უნდა მისცეს მას შესაბამისი უფლება. შედეგად, XYZ საიტზე შესვლისას გამოყენებული იქნება თქვენი ABC ანგარიშის მონაცემები. XYZ არ მიიღებს წვდომას ABC-ს მიერ შენახულ პაროლზე. ა.გ, თქვენი პერსონალური ინფორმაცია იქნება დაცული.

ინფორმაციის გაზიარება სოციალურ ქსელებზე

თუ თქვენთვის მნიშვნელოვანია პრივატულობა (ანონიმურობა), მაშინ დაიყვანეთ მინიმუმამდე ის ინფორმაცია, რომელსაც თქვენ აზიარებთ სოციალურ ქსელებზე. არ გააზიაროთ თქვენი დაბადების წელი და თარიღი, ელ. ფოსტის მისამართი, ტელეფონის ნომერი და ა.შ. თქვენს ნაცნობებს, რომლებსაც სჭირდებათ ეს ინფორმაცია, დიდი ალბათობით, ის უკვე აქვთ. ასევე, რეგისტრაციისას არ შეავსოთ სოციალური მედიის ყველა ველი. ზოგი რეგისტრაციისთვის საჭირო სულაც არ არის. კარგად შეისწავლეთ სოციალური მედიის პრივატულობის ფუნქციები - არ მისცეთ უცნობ ხალხს შესაძლებლობა ჩაერთონ თქვენს დისკუსიაში და გაიგონ თქვენი აქტივობების შესახებ.

რაც უფრო მეტ ინფორმაციას აზიარებთ ონლაინ, მით უფრო ადვილია კიბერ დამნაშავისთვის თქვენი პროფილის შექმნა. ამ პროფილს ის გამოიყენებს თქვენ წინააღმდეგ ოფლაინ.

ოდესმე დაგვიწყებიათ რომელიმე ონლაინ სერვისის მომხმარებლის სახელი ან / და პაროლი? ამ დორს გამოიყენება უსაფრთხოების კითხვები, მაგალითად „დედათქვენის ქალწულობის გვარი“, ან „რომელ ქალაქში დაიბადეთ“ და ა.შ. ასეთი კითხვების გამოყენებით პაროლის აღდგენა არის უსაფრთხოების პრინციპების მნიშვნელოვანი უგულვებელყოფა, რადგან ამ კითხვებზე პასუხები ადვილად მოიძებნება ინტერნეტში. რა თქმა უნდა, შეგიძლიათ ამ კითხვების პასუხად განსაზღვროთ მცდარი ინფორმაციაც, მაგრამ ეცადეთ ის არ დაგავიწყდეთ.

ელექტრონული ფოსტის და ვებ ბრაუზერის პრივატულობა

ყოველდღიურად, ინტერნეტ სივრცეში მიმოიცვლება მილიონობით ელ. წერილი. ეს წერილები პირადი, ან ბიზნეს ხასიათისაა. ელ. ფოსტა არის სწრაფი კომუნიკაციის ძალიან მოსახერხებელი საშუალება. ელ. წერილები იგზავნება ჩვეულებრივი plain text-ის სახით და მათ ხედავს ყველა, ვისაც გააჩნია განსაზღვრული წვდომა. ვიდრე წერილი მიაღწევს ადრესატს, ის მიედინება არაერთი სერვერის გავლით. რომც წაშალოთ ელ. წერილი, რაღაც პერიოდის განმავლობაში, ის მაინც დარჩება არქივირებული სხვადასხვა სერვერზე.

ყველას, ვისაც აქვს ფიზიკური წვდომა თქვენს კომპიუტერთან, ან როუტერთან, ასევე აქვს შესაძლებლობა ნახოს, თუ რომელ ვებსაიტებს სტუმრობდით. ამის გაკეთება შესაძლებელია ვებ ბრაუზერის ისტორიის, „ქეშის“, ან „ლოგ“ ფაილების ნახვით. ამ პრობლემის თავიდან ასაცილებლად, ვებ-ბრაუზერში გააქტიურეთ ე.წ. „პრივატული“ (ზოგი ეძახის ინკოგნიტო) რეჟიმი.

თანამედროვე ვებ ბრაუზერების უმრავლესობას აქვს ეს ფუნქცია.

- *Microsoft Internet Explorer: InPrivate*
- *Google Chrome: Incognito*
- *Mozilla Firefox: Private tab / private window*
- *Safari: Private: Private browsing*

როდესაც პრივატული რეჟიმი გააქტიურებულია, თქვენს კომპიუტერზე აღარ შეინახება ე.წ. „Cookie“ ფაილები, დროებითი ინტერნეტ ფაილები და წაიშლება ვებსაიტებზე სტუმრობების ისტორია, როგორც კი დახურავთ ვებ ბრაუზერს.

თუ ბრაუზერი იმუშავებს პრივატულ რეჟიმში, არაავტორიზებულ პირებს გაუჭირდებათ ინფორმაციის მოგროვება თქვენ შესახებ. გარდა ამისა, აღარ მოგივათ გამიზნული სარეკლამო კამპანიები. ამის საპასუხოდ, კომპანიები ცდილობენ ჩამოაყალიბონ სხვადასხვა მექანიზმი, რათა მათ შეძლონ თქვენი ონლაინ ჩვევების მონიტორინგი. მაგალითად, ზოგი როუტერი ინახავს ვებსაიტების სტუმრობების ისტორიას.
გაითვალისწინეთ, რომ საკუთარი პირადი ინფორმაციის დაცვა არის თქვენი პასუხისმგებლობა. შემდეგ ელ. წერილს რომ გააგზავნით, ნუთუ კვლავ დაურთავთ მას ისეთ სენსიტიურ დოკუმენტებს, როგორიცაა, მაგალითად თქვენი სამედიცინო ანკეტა?! როდესაც ეწვევით სხვადასხვა ვებსაიტებს, არ შეამოწმებთ - დაშიფრულია, თუ არა, კავშირი?! სულ რამდენიმე მარტივი პრევენციული ზომის გამოყენებით, თქვენ აარიდებთ თავს მნიშვნელოვან პრობლემებს.

თავი 4.

ორგანიზაციის დაცვა

ამ თავში ჩვენ განვიხილავთ ტექნოლოგიას და პროცესებს, რომლებსაც იყენებენ კიბერ უსაფრთხოების დარგის პროფესიონალები, რათა დაიცვან ორგანიზაციის ქსელი, მოწყობილობები და ინფორმაცია. ასევე, მოკლედ მიმოვიხილავთ სხვადასხვა „Firewall“-ს, უსაფრთხოების ურუნველმყოფელ მოწყობილობებს, აპლიკაციებს და საუკეთესო გამოცდილებას.

ზემოაღნიშნულის გარდა, ჩვენ შევეხებით ბოტნეტებს, „Kill Chain“-ს, ქმედებებზე დამოკიდებულ უსაფრთხოებას და „Net-Flows“, რომელიც დაგვეხმარება ქსელზე დაკვირვებაზე.

მესამე სექციაში შემოგთავაზებთ Cisco-ს მიდგომას კიბერ უსაფრთხოებისადმი, რომელშიც შესულია CSIRT ჯგუფის მიმოხილვა და უსაფრთხოების გზამკვლევი. აგრეთვე, ზედაპირულად განვიხილავთ ინსტრუმენტებს, რომელთაც იყენებენ კიბერ უსაფრთხოების პროფესიონალები, რათა აღმოაჩინონ ქსელური ტიპის შეტევები.

FIREWALL-ის ნაირსახეობები

ტერმინი „Firewall“ ნიშნავს კედელს, რომელიც იცავს შენობებს ცეცხლის გავრცელებისგან. კომპიუტერული „Firewall“ არის შემუსული და გასული კომუნიკაციების ერთგვარი ფილტრი „Firewall“-ის დაყენება შესაძლებელია ცალკეულ კომპიუტერზე (ინდივიდუალური თაცვისთვის), ან ცალკეულ ხელსაწყოზე, რომელიც დაიცავს მთლიან ქსელს. უკანასკნელს ეწოდება ქსელური „Firewall“.

წლებთან ერთად, კომპიუტერული და ქსელური შეტევები ხდება სულ უფრო და უფრო დახვეწილი. ამის საპასუხოდ, საჭიროა ახალი ტიპის „Firewall“-ების განვითარება. გთავაზობთ გავრცელებული „Firewall“-ების ნაირსახეობებს:

- *ქსელური (Network Layer) Firewall – ფილტრავს კომუნიკაციას IP მისამართების მიხედვით;*

- *სატრანსპორტო (Transport Layer) Firewall – ფილტრავს კომუნიკაციას ადგილობრივი და ადრესატი პორტების მიხედვით;*

- *აპლიკაციების (Application Layer) Firewall – ფილტრავს კომუნიკაციას აპლიკაციების და სერვისების დონეზე;*

- *Context Aware Application Firewall – ფილტრავს მომხმარებლის, ცალკეული კომპიუტერული ხელსაწყოს, როლების და აპლიკაციის ტიპის მიხედვით;*

- *Proxy Server – ფილტრავს დომეინის, URL მოთხოვნის, მედიის და სხვა ანალოგიური კომუნიკაციების დონეზე;*

- *Reverse Proxy Server – ფილტრავს კავშირს ვებ-სერვერთან. ძირითადად ის ყენდება ვებ-სერვერამდე;*

• *Network Address Translation (NAT) Firewall – მალავს, ან შეგნებულად ურევს, ქსელში არსებული ჰოსტების მისამართებს;*

• *Host-based Firewall – ფილტრავს პორტებს და სისტემურ სერვისებს.*

პორტების სკანირება

პორტის სკანირებას ასევე უწოდებენ კომპიუტერული სისტემის, სერვერის, ან სხვა ქსელის შემოწმებას ღია პორტების არსებობაზე. ქსელში მყოფ კომპიუტერულ მოწყობილობებზე მომუშავე სერვისებს აქვთ მინიჭებული პორტები - პორტის ნომრები. ეს პორტი გამოიყენება კომუნიკაციის ორივე ბოლოში, რაც უზრუნველყოფს იმას, რომ განსაზღვრული ინფორმაცია მიეწოდება მხოლოდ განსაზღვრულ აპლიკაციას. პორტების სკანირება გამოიყენება სადაზვერვო დანიშნულებით - ოპერაციული სისტემის და სერვისების გასარკვევად, ან მას იყენებენ ქსელის ადმინისტრატორები, რათა დარწმუნდნენ ქსელის უსაფრთხოებაში.

იმისათვის, რომ შეაფასოთ თქვენი ქსელის „Firewall“-ის და პორტების დაცულობის ხარისხი, გამოიყენეთ პროგრამული ინსტრუმენტი - Nmap. უკანასკნელი იპოვის ყველა ღია პორტს თქვენს ქსელში. თუ სკანირებას თავად არ აწარმოებთ, პორტების სკანირება შეგიძლიათ ჩათვალოთ პოტენციური კიბერ შეტევის პრეკურსორად. ნებართვის გარეშე ქსელის სკანირება არ გააკეთოთ!

Nmap-ის მეშვეობით ქსელის სკანირებისთვის, გადმოწერეთ პროგრამა Zenmap, მიუთითეთ სამიზნე IP მისამართი, აირჩიეთ სტანდარტული სკანირების პროფილი (Default Scanning Profile) და დააწკაპუნეთ „Scan“.

Nmap დაასკანირებს ყველა გააქტიურებულ სერვისს (მაგალითად, ვებ სერვისები, ელ. ფოსტის სერვისები და ა.შ.) და პორტებს. პორტის სკანირებამ შესაძლოა გაჩვენოთ მომდევნო სამი შედეგიდან ერთერთი:

- *Open or Accepted – ჰოსტის ერთერთი სერვისი უსმენს მოცემულ პორტ(ებ)ს;*

- *Closed, Denied, or Not Listening – მოცემულ პორტ(ებ) ზე კავშირი დახურულია;*

- *Filtered, Dropped, or Blocked – ჰოსტისგან პასუხი არ დაბრუნებულა;*

პორტების სკანირება შესაძლებელია ქსელის გარედანაც. ასეთი ტიპის Nmap სკანირება იქნება მიმართული თქვენი როუტერის გარე IP მისამართზე. საკუთარი გარე IP მისამართის დასადგენად, ნებისმიერ ონლაინ საძიებო სერვისში ჩაწერეთ: „what is my ip address“. შედეგად, საძიებო სისტემა გიჩვენებთ თქვენს გარე IP მისამართს.
ასევე შეგიძლიათ გამოიყენოთ Nmap-ის ონლაინ სკანერი, რათა დაასკანიროთ 6 ძირითადი პორტი.

1) გადადით ბმულზე:

https://hackertarget.com/nmap-online-port-scanner/

2) შეიყვანეთ თქვენი გარე IP მისამართი;

3) დააჭკაპუნეთ „Quick Nmap Scan“-ზე.

თუ პასუხად მიიღებთ, რომ 21, 22, 25, 80, 443, or 3389 პორტებიდან რომელიღაცა არის ღია, ე.ი. თქვენს როუტერს, ან „Firewall“-ს აქვს გააქტიურებული პორტების გადამისამართება. დიდი ალბათობით, თქვენს პირად ქსელში ასევე მუშაობს სერვერი.

უსაფრთხოების მოწყობილობები

თანამედროვე პირობებში, ვერცერთი მოწყობილობა ინდივიდუალურად ვერ უზრუნველყოფს თქვენი ქსელის 100%-იან უსაფრთხოებას. აუცილებელია, რომ თქვენს ქსელს იცავდეს სხვადასხვა ტიპის უსაფრთხოების მოწყობილობა, რა დროსაც ისინი ერთმანეთთან ჰარმონიულად იმუშავებენ. უსაფრთხოების ხელსაწყოები ყველაზე ეფექტურია მაშინ, როდესაც ისინი წარმოადგენენ ერთიანი სისტემის კომპონენტებს.

უსაფრთხოების მოწყობილობა შეიძლება იყოს ცალკე ხელსაწყო, მაგალითად როუტერი, ან „Firewall“, პლატა, რომელიც ყენდება თქვენს ქსელურ მოწყობილობაში, ან საკუთარი პროცესორის და მეხსიერების მქონე მოდული. უსაფრთხოების მოწყობილობად შესაძლოა ჩაითვალოს პროგრამული უზრუნველყოფა, რომელიც მუშაობს ქსელურ მოწყობილობაზე. როგორც წესი, ყველა უსაფრთხოების ხელსაწყო ექცევა ამ კატეგორიაში:

- *როუტერები - Cisco Integrated Services Router (ISR) როუტერებს აქვთ ტრეფიკის ფილტრაციის უამრავი შესაძლებლობა, შეღწევის პრევენციის სისტემა (IPS), დაშიფვრა, VPN-ის ფუნქცია უსაფრთხო ინფორმაციული ნაკადის შესაქმნელად;*

- *„Firewall“-ები - Cisco მომავლი თაობის „Firewall“-ებს აქვთ ყველა შესაძლებლობა, რაც ISR როუტერებს. ასევე, მათ აქვთ გაუმჯობესებული ქსელის მენეჯმენტის და ანალიტიკის ხელსაწყოები;*

- *VPN - Cisco-ს უსაფრთხოების მოწყობილობებს აქვთ ვირტუალური პრივატული ქსელის (VPN) სერვერის და კლიენტის ტექნოლოგიის მხარდაჭერა. ეს საჭიროა დაშიფრული ინფორმაციული „გვირაბების“ შესაქმნელად;*

• *მავნებელი პროგრამები / ანტივირუსი - Cisco-ს როუტერებში, „Firewall“-ებში და IPS მოწყობილობებში ჩაშენებულია გაუმჯობესებული დაცვა მავნებელი პროგრამების წინააღმდეგ (AMP). ასევე, თქვენ შეძლებთ შესაბამისი პროგრამული უზრუნველყოფის დაინსტალირებას ჰოსტ კომპიუტერებზე;*

• *სხვა უსაფრთხოების მოწყობილობები – ეს კატეგორია მოიცავს ვებ და ელ. ფოსტის უსაფრთხოების მოწყობილობებს, გაშიფვრის მოწყობილობებს, კლიენტის მიერ კონტროლირებად სერვერებს და უსაფრთხოების მენეჯმენტის სისტემებს.*

მიმდინარე კიბერ შეტევების აღმოჩენა

არ არსებობს იდეალური პროგრამული უზრუნველყოფა. შეტევას, როდესაც ჰაკერი ხელყოფს პროგრამულ უზრუნველყოფას იქამდე, ვიდრე პროგრამის გამომშვები თავად აღმოფხვრავს არსებულ სისუსტეს, ეწოდება „Zero-Day“ შეტევა. დღეს, ასეთი ტიპის შეტევები გვხვდება სწრაფად მზარდი ინტენსივობით და დიდი ოდენობით. ა.გ. წარმატებულ დაცვად მიიჩნევა ის სისწრაფე, რომლითაც ქსელი მოასწრებს წარმატებულ კიბერ შეტევაზე რეაგირების მოხდენას. იდეალურ შედეგად ითვლება, თუ უსაფრთხოების სისტემა დაუყოვნებლივ აღმოაჩენს და აღკვეთს მიმდინარე კიბერ შეტევას, ან რამდენიმე წუთის განმავლობაში. სამწუხაროდ, ბევრი კომპანია და ორგანიზაცია ამას ვერ ახერხებს და ისინი გებულობენ მომხდარი შეღწევის შესახებ დღეების, ან თვეების მერე.

• მიმდინარე სკანირება Edge-დან to Endpoint-მდე - რეალურ დროში შეტევების აღმოჩენა საჭიროებს აქტიური სკანირების წარმოებას „Firewall“-ების და IDS / IPS ქსელური მოწყობილობების მეშვეობით. ასევე, უნდა გამოიყენოთ

მომავალი თაობის კლიენტ / სერვერის ტიპის მავნებელი პროგრამების აღმომჩენი ხელსაწყოები, რომელთაც აქვთ წვდომა საფრთხეების აღმრიცხველ გლობალურ ცენტრებთან. თანამედროვე სკანირების ინსტრუმენტებს უნდა შეეძლოთ ქსელური ანომალიების აღმოჩენა კონტექსტზე დაყრდნობილი ანალიზის და მოქმედებების შემფასებლით.

- *DDoS შეტევა და რეაგირება რეალურ დროში - DDoS წარმოადგენს ერთერთ ყველაზე დიდ საფრთხეს, რომელიც საჭიროებს გადაუდებელ რეაგირებას. DDoS შეტევებისგან დაცვა ძალიან რთულია, ვინაიდან შეტევა მიმდინარეობს ასობით, ან ათასობით ზომბი ჰოსტისგან. გარდა ამისა, ეს შეტევა გამოიყურება, როგორც ლეგიტიმური ინტერნეტ ტრეფიკი. ბევრი კომპანიისთვის და ორგანიზაციისთვის DDoS შეტევები დამღუპველია, რადგან ეს შეტევები ხელყოფენ მათ სერვერებს და ქსელურ შესაძლებლობებს. კომპანიის შესაძლებლობა, მოახდინოს დაუყოვნებლივი რეაგირება DDoS შეტევაზე არის მისი სიცოცხლისუნარიანობის ერთერთი ძირითადი განმაპირობებელი ფაქტორი.*

დაცვა მავნებელი პროგრამებისგან

როგორ ფიქრობთ, შესაძლებელია, თუ არა საკუთარი თავის დაცვა გამუდმებული „ZeroDay“, ან APT-ს ტიპის შეტევებისგან? ერთერთი გამოსავალი არის პროფესიონალური დონის მავნებელი პროგრამების აღმომჩენი აპლიკაციების გამოყენება. ასეთი, დიდი ალბათობით, აღმოაჩენს მიმდინარე საფრთხეებს. ქსელის ადმინისტრატორებმა გამუდმებით უნდა აწარმოონ ქსელის მონიტორინგი, რათა დროულად აღმოაჩინონ მავნებელი პროგრამები და ქმედებები, რომლებიც მიუთითებენ APT შეტევის არსებობაზე. Cisco-ს განკარგულებაშია გაუმჯობესებული მავნებელი პროგრამებისგან დაცვის (AMP) საფრთხეების ქსელი, რომელიც აანალიზებს მილიონობით ფაილს და

ახდენს მათ შედარებას მილიონობით აღმოჩენილ მავნებელ პროგრამასთან. ეს იძლევა მავნებელი პროგრამების, კამპანიების და მათი გავრცელების გლობალური დანახვის შესაძლებლობას.

AMP არის კლიენტ / სერვერის ტიპის პროგრამული უზრუნველყოფა, რომელიც ყენდება „end-point“ ჰოსტებზე, როგორც ცალკე სერვერი სახით, ან ნებისმიერ ქსელური უსაფრთხოების მოწყობილობაზე.

უსაფრთხოების საუკეთესო პრაქტიკა

მრავალმა ეროვნულმა და პროფესიონალურმა ორგანიზაციამ გამოაქვეყნა საკუთარი საუკეთესო გამოცდილების პრაქტიკა. გთავაზობთ სიას, რომელშიც მოვახვედრეთ უსაფრთხოების საუკეთესო პრაქტიკების ნაზავი:

- *შეაფასეთ რისკები – იმის ღირებულების დადგენა, რის დაცვასაც აპირებთ, მოგცემთ საშუალებას ადეკვატურად განსაზღვროთ ხარჯები უსაფრთხოებაზე;*

- *შექმენით თქვენი საკუთარი უსაფრთხოების პოლიტიკა – შექმენით პოლიტიკა, სადაც გარკვევით წერია კომპანიის წესების, თანამშრომლების მოვალეობების და მოლოდინების შესახებ;*

- *ფიზიკური უსაფრთხოების ზომები – შეზღუდეთ წვდომა ქსელურ მოწყობილობებთან, სასერვერო ოთახებთან და ხანძარსაწინააღმდეგო სისტემის სამართავ მექანიზმთან;*

- *ადამიანური რესურსის შემოწმება – კარგად შეისწავლეთ თანამშრომელთა პირადი საქმეები;*

- *შეასრულეთ ინფორმაციის არქივის (Backup) სატესტო აღდგენა – მას შემდეგ, რაც შეასრულებთ სტანდარტული არქივირების პროცესს, სცადეთ ინფორმაციის აღდგენა;*

- *აწარმოეთ რეგულარული განახლებები – გამუდმებით განაახლეთ სერვერი, კლიენტები, ქსელური მოწყობილობების ოპერაციული სისტემები და პროგრამები;*

- *განსაზღვრეთ წვდომის დონეები – განსაზღვრეთ მომხმარებელთა როლები და პრივილეგიები. ასევე, განსაზღვრეთ მომხმარებელთა ავტორიზაციის ძლიერი და სანდო მექანიზმები;*

- *ინციდენტების ინსცინირება – მოახდინეთ კიბერ ინციდენტების ინსცინირება და შეაფასეთ, თუ რამდენად ეფექტიანად გაუმკლავდება მათ თქვენი გუნდი;*

- *გამოიყენეთ ქსელის მონიტორინგის, ანალიტიკის და მენეჯმენტის ხელსაწყოები - აირჩიეთ ისეთი უზრუნველყოფა, რომელიც შეძლებს ინტეგრირებას თქვენს დანარჩენ ტექნოლოგიებთან;*

- *გამოიყენეთ ქსელის უსაფრთხოების მოწყობილობები - მომავალი თაობის როუტერები, „Firewall“-ები და სხვა უსაფრთხოების მოწყობილობები;*
- *გამოიყენეთ ყოვლისმომცველი end-point უსაფრთხოების უზრუნველყოფა – გამოიყენეთ პროფესიონალური (Enterprise დონის) ანტივირუსები;*

- *ჩაუტარეთ თქვენს თანამშრომლებს ტრეინინგები კიბერ უსაფრთხოებაზე;*

- *დაშიფრეთ ინფორმაცია – კომპანიის სენსიტიური ინფორმაცია და ელ. ფოსტა უნდა იყოს დაშიფრული.*

ყველაზე სასარგებლო გზამკვლევები იძებნება ორგანიზაციულ რეპოზიტორიებში, მაგალითად შეერთებული შტატების ტექნოლოგიური სტანდარტების ეროვნული ინსტიტუტის (NIST) ინფორმაციულ ბაზებში. მსოფლიოში ერთერთი ყველაზე დიდი რეპუტაციის მქონე კიბერ უსაფრთხოების ინსტიტუტი არის SANS. აუცილებლად ნახეთ მათი ტრეინინგები და სერთიფიკაციის კურსები.

ბოტნეტი

ბოტნეტი არის ადამიანის, ან დაჯგუფების კონტროლის ქვეშ მყოფი ბოტების ჯგუფი, რომელიც ერთმანეთთან შეერთებულია ინტერნეტის მეშვეობით. როგორც წესი, ბოტი კომპიუტერი ინფიცირდება ვებსაიტიდან, ელ. წერილთან თანდართული ფაილიდან, ან მავნებელი პროგრამის შემცველი მედია ფაილის გახსნის შედეგად.

ბოტნეტი შესაძლოა შეიცავდეს ასობით, ან ათასობით ბოტს. ბოტნეტის ოპერატორს შეუძლია დაავალოს ბოტებს მავნებელი პროგრამების გავრცელება, DDoS შტევის წარმოება, სპამის შემცველი ელ. წერილების გაგზავნა, ან „ბრუტ-ფორს“ შეტევებების განხორციელება. ბოტნეტი კონტროლდება ბრძანებით, ან სერვერის მეშვეობით.

ხშირად, კიბერ ბოროტმოქმედები აქირავებენ საკუთარ ბოტნეტებს. ალბათ ლოგიკურია, რომ დამქირავებელი იყენებს მათ დანაშაულებრივი ქვენა გრძნობით.

THE KILL CHAIN

კიბერ უსაფრთხოების ტერმინოლოგიაში, „Kill Chain“ გულისხმობს სისტემური შეტევების წარმოების სხვადასხვა სტადიას. „Kill Chain“-ის ავტორი არის ლოკჰიდ მარტინი, რომელმაც განსაზღვრა უსაფრთხოების ინციდენტთა აღმოჩენის და რეაგირების სტრუქტურული სტადიები.

ესენია:

სტადია 1. დაზვერვა - შეტევის მწარმოებელი აგროვებს ინფორმაციას სამიზნის შესახებ;

სტადია 2. შეიარაღება - შეტევის მწარმოებელი ქმნის „ექსპლოიტს“ და მავნებელ „payload-ს“, რომელსაც ის მოგვიანებით გაუგზავნის საკუთარ სამიზნეს;

სტადია 3. მიწოდება - შეტევის მწარმოებელი, ელ. ფოსტით, ან სხვა მეთოდის გამოყენებით, უგზავნის „ექსპლოიტს“ და „payloads“ საკუთარ სამიზნეს.

სტადია 4. ხელყოფა / ექსპლოატაცია - „ექსპლოიტი“ გაიშვება;

სტადია 5. ინსტალირება - მავნებელი პროგრამა და „Backdoor“ დაყენდება სამიზნე სისტემაზე;

სტადია 6. კონტროლის დამყარება - სამიზნე სისტემაზე მყარდება დისტანციური კონტროლი;

სტადია 8. მოქმედება - შემტევი იწყებს მავნებელი ქმედებების შესრულებას. ასევე, სამიზნე მომხმარებლის ქსელიდან ასრულებს დამატებით შეტევებს სხვა მოწყობილობებზე და ასრულებს „Kill Chain“-ის სტადიებს ხელმეორედ - სხვა ქსელის წინააღმდეგ.

საკუთარი თავის დასაცავად, ქსელური უსაფრთხოების პროტოკოლები გათვლილია „Kill Chain“-ში აღწერილ თითოეულ სტადიასთან საბრძოლველად:

• რა არის შეტევის ინდიკატორები „Kill Chain“-ის თითოეულ სტადიაზე?

• რა უსაფრთხოების ინსტრუმენტებია საჭირო შეტევის აღმოსაჩენად „Kill Chain“-ის თითოეულ სტადიაზე?

• რამ შეიძლება ხელყოს კომპანიის შესაძლებლობა აღმოაჩინოს შეტევები?

ლოკჰიდ მარტინის სიტყვებით, „Kill Chain“-ის თითოულის სტადიის სწორმა აღქმამ მისცა მის გუნდს შესაძლებლობა შეემუშავებინათ უსაფრთხოების ბარიერები, რომლებიც შეანელებდნენ კიბერ შეტევას და უკეთეს შემთხვევაში, საერთოდ არ დაუშვებდნენ ინფორმაციის დაკარგვას.

იმის გარკვევა / გათავისება, თუ რა ხდება „Kill Chain“-ის თითოეულ სტადიაზე დაეხმარება კიბერ უსაფრთხოების სპეციალისტს კიბერ შეტევებთან გასამკლავებლად.

მოქმედების შესწავლაზე დაყრდნობილი უსაფრთხოება

მავნებელი პროგრამების აღმოსაჩენად აღნიშნული ფორმის უსაფრთხოება არ იყენებს ბინარულ ანაბეჭდებს. ამის ნაცვლად, ის შეისწავლის მათ მოქმედებებს და აკვირდება ქსელში ანომალიების გაჩენას. მოქმედების შესწავლაზე დაყრდნობილი უწესივრობების აღმოჩენის სპეციფიკა მოიცავს ლოკალური ქსელის შიგნით კომუნიკაციის ანალიზს. თავის მხრივ, კომუნიკაციების ანალიზი ავლენს მავნებელი პროგრამების კონტექსტს და მოქმედებების თავისებურებებს, რომლებიც საჭიროა ანომალიების გამოვლენაში. ანუ, მოქმედებების შესწავლაზე დაყრდნობილი უსაფრთხოება ამჩნევს გადახვევებს ნორმალური მუშაობის ციკლიდან.

- სათაფლეები (Honeypots) - სათაფლე არის მოქმედების შესწავლაზე დაყრდნობილი უწესივრობის აღმომჩენი ინსტრუმენტი, რომელიც თავად იტყუებს შეტევის მწარმოებელს. უკანასკნელის მოქმედების მოდელი უკვე ცნობილია. შესაბამისად, შეტევის მწარმოებელი ხვდება „სათაფლეში“, სადაც ქსელის ადმინისტრატორს შეეძლება მისი ქმედებების გამოკვეთა, „ლოგირება“ და გაანალიზება. შედეგად, ადმინისტრატორს მიეცემა საკუთარი დაცვის მექანიზმების გაძლიერების შესაძლებლობა.

- Cisco-ს კიბერ საფრთხეებისგან დასაცავი არქიტექტურა - ეს უსაფრთხოების არქიტექტურა მორგებულია უწესივრობების მოქმედების შესწავლაზე. ის უზრუნველყოფს უფრო მაღალ აღმოჩენადობის ხარისხს, კონტექსტს და კონტროლს.

ამ არქიტექტურის ძირითადი მიზანია იმის დადგენა, თუ ვინ, სად, როდის და როგორ აწარმოა კიბერ თავდასხმა. ამ მიზნის მისაღწევად, გამოიყენება მრავალი სხვადასხვა ტექნოლოგია.

NETFLOW

ტექნოლოგია NetFlow გამოიყენება ქსელში მონაცემთა დინების შესახებ ინფორმაციის შესაგროვებლად. შესაძლოა NetFlow-ის ინფორმაცია გააიგივოთ სატელეფონო ანგარიშის ამონაწერთან, ოღონდ ქსელისთვის. NetFlow არის მოქმედებების შესწავლაზე დაყრდნობილი ანალიტიკის მნიშვნელოვანი ინსტრუმენტი. „სვიჩებს“, როუტერებს და „Firewall“-ებს, რომლებსაც გააჩნიათ NetFlow, შეუძლიათ ინფორმაციის მოგროვება შემოსული, გასული, და მიმდინარე ინტერნეტ პაკეტების შესახებ. შემდგომ, ეს ინფორმაცია ეგზავნება Netflow კოლექტორს, რომელიც აგროვებს, ინახავს და აანალიზებს ამ ჩანაწერებს.

CSIRT

ბევრ დიდ ორგანიზაციას ჰყავს საკუთარი ჯგუფი, რომელიც ახდენს რეაგირებას კომპიუტერული უსაფრთხოების ინციდენტებზე (CSIRT). ისინი ღებულობენ და განიხილავენ მომხდარ ინციდენტებთან დაკავშირებულ ინფორმაციას და შემდგომ ამზადებენ ანგარიშს ამის თაობაზე. CSIRT-ის ძირითადი დანიშნულება არის კომპიუტერული ინციდენტების დეტალური გამოძიება. კომპიუტერული ინციდენტების თავიდან ასარიდებლად, Cisco-ს CSIRT-ი პროაქტიურად აფასებს საფრთხეებს, რისკების შემცირების გეგმებს, ახორციელებს ინციდენტთა ტრენდის ანალიზს და განიხილავს უსაფრთხოების არქიტექტურას.

Cisco-ს CSIRT-ი თანამშრომლობს Forum of Incident Response and Security Teams (FIRST)-თან, National Safety Information Exchange (NSIE)-თან, the Defense Security Information Exchange (DSIE)-თან და the DNS Operations Analysis and Research Center (DNS-OARC)-თან.

არსებოს ეროვნული და საჯარო CSIRT ორგანიზაციები, მაგალითად Carnegie Mellon-ის უნივერსიტეტის პროგრამირების ინსტიტუტის CERT განყოფილება. მათ შეუძლიათ დაეხმარონ სხვადასხვა ორგანიზაციებს, ეროვნულ CSIRT-ებს ინციდენტის მენეჯმენტის შესაძლებლობების განვითარებაში, მართვასა და გაუმჯობესებაში.

უსაფრთხოების გზამკვლევი

ტექნოლოგია მუდამ იცვლება. ეს ნიშნავს, რომ კიბერ შეტევებიც განიცდიან ევოლუციას. ჩნდება ახალი უსაფრთხოების სისუსტეები და შეტევის მეთოდები. ბიზნესებისთვის უსაფრთხოება ხდება მნიშვნელოვანი საფიქრალი, რადგან უსაფრთხოების ხელყოფის შედეგად შესაძლოა დაზიანდეს მათი რეპუტაცია და ფინანსური მდგომარეობა. ძირითადად, კიბერ შეტევების სამიზნე ხდება კრიტიკული მნიშვნელობის ქსელები და სენსიტიური ინფორმაცია. ყველა ორგანიზაციას უნდა გააჩნდეს საკუთარი გეგმა, ამ საფრთხეების შედეგად გამოწვეული ზიანის აღდგენაზე.

რა თქმა უნდა, საუკეთესო ვარიანტია უსაფრთხოების ხელყოფის თავიდან არიდება. კომპანიებს უნდა გაჩნდეთ საკუთარი კიბერ უსაფრთხოების რისკების აღმოჩენის, სისტემის დაცვის და უსაფრთხოების მექანიზმების ოპერირების ინსტრუქციები. გარდა ამისა, შტატი უნდა იყოს დატრეინინგებული აღნიშნული საფრთხეების თავიდან ასარიდებლად. როდესაც (თუ) დადგინდება უსაფრთხოების ხელყოფის ინციდენტი, კომპანიას უნდა შეეძლოს ზიანის მინიმიზაცია. მიზანშეწონილია მოქნილი გეგმის შემუშავება, რომელიც ამოქმედდება სისტემაში შეღწევისას. მას შემდეგ, რაც კომპანიის კიბერ სივრცე გაანეიტრალებს საფრთხეს, მან უნდა გაანალიზოს მიღებული გამოცდილება და ეცადოს ანალოგიური შემთხვევის პრევენცია.

ზემოაღნიშნული ინფორმაცია უნდა მოექცეს კომპანიის უსაფრთხოების გზამკვლევში. ის იქნება თქვენი ანგარიშების კრებული, რომელიც გამოდგება არასასურველი კიბერ ინციდენტის დადგომის და სათანადო რეაგირების შესაძლებლობის უზრუნველსაყოფად. იდეალურ შემთხვევაში, უსაფრთხოების გზამკვლევი უნდა მოიცავდეს შემდეგ ინფორმაციას:

- *მავნებელი პროგრამებით ინფიცირებული კომპიუტერების დადგენის შესახებ;*
- *საეჭვო ქსელური აქტივობის დადგენის შესახებ;*
- *წარუმატებელი აუთენტიფიკაციის მცდელობების დადგენის შესახებ;*
- *ინფორმაციას შემოსული და გასული ტრეფიქის შესახებ;*
- *დაკავშირებული ტრენდების და სტატისტიკის შესახებ;*

ინციდენტთა დადგენის და პრევენციის ინსტრუმენტები

არსებობს უსაფრთხოების ინციდენტთა აღმოჩენის ფიზიკური და პროგრამული უზრუნველყოფა. ესენია:

- *SIEM – პროგრამული უზრუნველყოფა „Security Information and Event Management (SIEM)“, რომელიც აგროვებს და აანალიზებს უსაფრთხოების საგანგაშო მომენტებს და ლოგებს. ასევე ინახავს მიმდინარე და შენახულ ინფორმაციას ქსელში არსებული უსაფრთხოების ხელსაწყოებიდან.*

• *DLP – Data Loss Prevention Software (DLP) არის პროგრამული უზრუნველყოფა, ან ფიზიკური მოწყობილობა, რომლის დანიშნულებაა სენსიტიური ინფორმაციის დაცვა ქურდობისგან, ან ქსელისდატოვებისგან.DLPსისტემაფოკუსირდებაავტორიზაციაზე, ინფორმაციის მიმოცვლაზე, ინფორმაციის კოპირებაზე, მომხმარებელთა აქტივობის მონიტორინგზე და სხვა. ის აკვირდება და იცავს სამ სხვადასხვა მდგომარეობაში მყოფ ინფორმაციას - data in-use, data in-motion და data at-rest. Data in-use ფოკუსირდება კლიენტზე, Data in-motion გულისხმობს ინფორმაციას, რომელიც მიედინება ქსელში და Data at-rest გულისხმობს დამახსოვრებულ ინფორმაციას.*

• *Cisco ISE და TrustSec – Cisco Identity Services Engine (Cisco ISE) და Cisco TrustSec აკონტროლებენ წვდომას ქსელურ რესურსებზე როლების განაწილების პრინციპით - მაგალითად, სტუმრები, მობილური პლატფორმების მომხმარებლები, თანამშრომლები და ა.შ. მოწყობილობებიდან გამომავალი ტრეფიკის კლასიფიკაცია გამომდინარეობს უშუალოდ მომხმარებლის, ან თავად ხელსაწყოს იდენტობიდან.*

IDS და IPS

შეღწევის აღმოჩენის სისტემა (IDS) არის სპეციალური ქსელური მოწყობილობა; სერვერზე, ან „Firewall“-ში არსებული ინსტრუმენტი, რომელიც მავნებელი ტრეფიკის აღმოჩენის მიზნით, ასკანირებს ინფორმაციას. ეს მონიტორინგი ასევე დაფუძნებულია სხვადასხვა შეტევის „კვალის“ აღმოჩენაზე, რომელიც მოცემულია სპეციალურ მონაცემთა ბაზაში. თუ აქტივობა ემთხვევა მონაცემთა ბაზაში არსებულ „კვალს“, მაშინ IDS ინახავს აღმოჩენის ლოგს და ატყობინებს ამის შესახებ ქსელის ადმინისტრატორს. თავად IDS არ რეაგირებს, თუ ის დაადგენს შეღწევის ფაქტს. შესაბამისად, ის ვერ დაგიცავთ შეტევებისგან. მისი დანიშნულებაა შეტევის აღმოჩენა, ლოგის გაკეთება და ამის შესახებ ანგარიშის მომზადება.

IDS-ის მიერ წარმოებული სკანირება ანელებს ქსელს. იმისათვის, რომ არ მოხდეს ქსელის შენელება, მას ათავსებენ ოფლაინ რეჟიმში, ძირითადი ქსელის გარეთ. ინფორმაცია ქსელიდან კოპირდება

„სვიჩზე“ და შემდგომ ეგზავნება IDS-ს. არსებობს IDS ინსტრუმენტები,რომელთადაყენებასშეძლებთკომპიუტერულ სისტემებზეც.

შეღწევის პრევენციის სისტემას (IPS) შეუძლია დაბლოკოს ტრეფიკი, რომელიც შეიცავს სპეციალურ მონაცემთა ბაზაში მოქცეულ საეჭვო ტრეფიკის ნიშნებს. ერთერთი ყველაზე ცნობადი IPS/IDS სისტემა არის „Snort“. ეს არის Cisco-ს „Sourcefire“-ის კომერციული ვერსია. „Sourcefire“-ს შეუძლია რეალურ დროში აწარმოოს ტრეფიკის და პორტების ანალიზი, მოახდინოს ლოგიერება, მოძებნოს განსაზღვრული კონტენტი და დამთხვევები სპეციალურ მონაცემთა ბაზაში; დაადგინოს სისტემის მიმდინარე „პროუბინგი“, შეტევები და პორტების სკანირება. გარდა ამისა, მას აქვს შესაძლებლობა იმუშაოს სხვა პროგრამებთან ერთადაც.

თავი 5.

ჰა იქნება

კიბერ უსაფრთხოების მომავალი?

ეს თავი მიმოიხილავს კიბერ უსაფრთხოებასთან დაკავშირებულ სამართლებრივ და ეთიკურ პრობლემებს. ასევე, ყურადღება დაეთმობა კიბერ უსაფრთხოების საგანმანათლებლო და კარიერულ მიმართულებებს. Cisco-ს ქსელურ აკადემიას გააჩნია არაერთი საგანმანათლებლო მიმართულება, რომლმაც შესაძლოა დაგაინტერესოთ. ამ მიმართულებებს შორის ასევე არის სერთიფიცირებული პროგრამები ქსელის სხვადასხვა სპეციალობებზე, მათ შორის კიბერ უსაფრთხოებაზე.

ეწვიეთ ქსელური აკადემიის „Talent Bridge“-ის ვებსაიტს

https:\\www.netacad.com

სადაც იპოვით საინტერესო ინფორმაციას კარგი რეზიუმეს მოსამზადებლად, ან წარმატებული გასაუბრების გასავლელად. იქვე აღმოაჩენთ Cisco-ს და Cisco-ს პარტნიორების მიერ შემოთავაზებულ ვაკანსიებს. ასევე, ვაკანსიების საპოვნელად, თქვენს განკარგულებაში იქნება სამი საძიებო სისტემა.

ჯიბეი უსაფრთხოების სამართლებრივი პრობლემები

კიბერ უსაფრთხოების პროფესიონალებს უნდა გააჩნდეს იგივე ცოდნა, რაც ჰაკერებს - განსაკუთრებით შავქუდიან ჰაკერებს. ეს საჭიროა საკუთარი და დამკვეთი კომპანიის კიბერ სივრცის სათანადო დაცვის უზრუნველსაყოფად. ერთადერთი განსხვავება კიბერ უსაფრთხოების პროფესიონალსა და ჰაკერს შორის არის მისი ქმედებების ლეგალურობა. კიბერ უსაფრთხოების პროფესიონალი უნდა მოქმედებდეს კანონით დადგენილ ჩარჩოებში.

პერსონალური სამართლებრივი პრობლემები

კანონი ერთია ყველასთვის. რომც არ იყოთ რომელიმე კიბერ უსაფრთხოების კომპანიის თანამშრომელი, კანონი თქვენზეც იმოქმედებს. შესაძლოა თქვენ გქონდეთ ჰაკინგის უნიკალური შესაძლებლობა და ცოდნა, მაგრამ ეს არ ნიშნავს, რომ თქვენ ის უნდა გამოიყენოთ კანონსაწინააღმდეგოდ. არსებობს ძველი ბრძნული გამონათქვამი: „ის რომ თქვენ იცით, არ ნიშნავს, რომ უნდა გააკეთოთ“. დაიმახსოვრეთ ეს სიბრძნე. ჰაკერების უმრავლესობა ცნობიერად, ან გაუცნობიერებლად, ტოვებს კვალს, რომელიც მიიყვანს მსურველს მათ ადგილმდებარეობამდე.

კიბერ უსაფრთხოების პროფესიონალები ავითარებენ ოსტატობას, რომლის გამოყენება შესაძლებელია კეთილი და ბოროტი განზრახვებით. მათზე, ვინც იყენებს ცოდნას კანონის ფარგლებში, იცავს კიბერ ინფრასტრუქტურას, ყოველთვის იქნება დიდი მოთხოვნა.

ჯოჰოჰასიული სამართლებრივი პრობლემები

პრაქტიკულად ყველა ქვეყანას გააჩნია საკუთარი კიბერ უსაფრთხოების მარეგულირებელი კანონმდებლობა. ეს ნორმატიული აქტები ეხება კრიტიკულ ინფრასტრუქტურას, ქსელებს და კორპორაციულ და პერსონალურ პრივატულობას. ყველა ბიზნესმა უნდა დაიცვას ეს კანონები.

ზოგ შემთხვევაში, მუშაობისას, თანამშრომლის მიერ კიბერ უსაფრთხოების მარეგულირებელი კანონების უგულვებელყოფისთვის, ისჯება კომპანია და შესაძლოა გულგრილი თანამშრომელიც დარჩეს სამსახურის გარეშე. სხვა შემთხვევაში, მას დაგაპატიმრებენ, დააკისრებენ ჯარიმას, ან საერთოდაც მიუსჯიან თავისუფლების აღკვეთას.

ჯობს მიჰყვეთ შემდეგ პრინციპს: თუ არ იცით ლეგალურია თქვენი ქმედება, თუ არა, ჯობს ეს ქმედება არ ჩაიდინოთ. შესაძლოა თქვენს კომპანიაში იყოს იურიდიული დეპარტამენტი, ან იქნებ ვინმე ადამიანის რესურსების დეპარტამენტიდან დაგეხმაროთ.

საერთაშორისო კანონმდებლობა და კიბერ უსაფრთხოება

სამართლის ეს დარგი გაცილებით ახალგაზრდაა ვიდრე თავად კიბერ უსაფრთხოება. როგორც აქამდე აღვნიშნეთ, ყველა ქვეყანას აქვს საკუთარი კანონმდებლობა და გვერწმუნეთ, ეტაპობრივად კანონების რაოდენობა აუცილებლად მოიმატებს.

ეთიკის საკითხები

პერსონალური ეთიკის საკითხები

გარდა იმისა, რომ თქვენი ქმედება უნდა იყოს კანონიერი, ის ასევე უნდა ჯდებოდეს ეთიკის ნორმებში.

შესაძლოა ადამიანი იქცეოდეს არაეთიკურად, მაგრამ ეს არ გამოიწვევს მის სამართლებრივ დევნას. ეს ხდება იმიტომ, რომ მისი ქმედება შესაძლოა არ იყოს დასჯადი. მაგრამ ეს იმას არ ნიშნავს, რომ ეს ქმედება იყო სოციალურად მისაღები. ეთიკის საზღვრების დადგენა საკმაოდ მარტივია. კიბერ უსაფრთხოების მცოდნეს აქვს არაეთიკური მოქცევის მთელი რიგი შესაძლებლობები - მათი ჩამოთვლა უბრალოდ შეუძლებელია. ჩვენ გთავაზობთ ორ კითხვას, რომელიც დაგეხმარებათ ქმედების ეთიკურობის შეფასებაში:

- *მინდა, რომ ვიღაცამ შეაღწიოს ჩემს კომპიუტერში და ჩემ სოციალურ ქსელზე ჩემი სურათები შეცვალოს?*

- *მინდა, რომ IT ტექნიკოსმა, რომელსაც მე ვანდე ჩემი ქსელის სისუსტეების გამოსწორება, გაანდოს ჩემი საიდუმლო ინფორმაცია საკუთარ კოლეგებს?*

თუ ზემოაღნიშნულ კითხვებზე თქვენი პასუხია „არა“, მაშინ თქვენც არ გაუკეთოთ ეს სხვას.

პროფესიული ეთიკის საკითხები

ეთიკა არის მოქცევის სოციალურ ნორმათა კოდექსი, რომელსაც ზოგჯერ ამლევენ კანონის ძალას. კიბერ უსაფრთხოების დარგში არის უამრავი სივრცე, რომელიც არ რეგულირდება კანონით. მიუხედავად იმისა, რომ თქვენი ქმედება შესაძლოა იყოს თანხვედრაში კანონთან, ეს არ ნიშნავს, რომ ის ჯდება ეთიკის ნორმებში. რადგან კიბერ უსაფრთხოების ბევრი სივრცე (ჯერ) არ რეგულირდება კანონით, ბევრმა IT ორგანიზაციამ შექმნა საკუთარი ეთიკის კოდექსი თავიანთი თანამშრომლებისთვის.

გთავაზობთ სამ ორგანიზაციას, რომელსაც გააჩნია საკუთარი ეთიკის კოდექსი:

- *The CyberSecurity Institute (CSI)*
- *The Information Systems Security Association (ISSA)*
- *The Association of Information Technology Professionals (AITP)*

Cisco-ს გუნდის მუშაობს საკუთარი ეთიკის კოდექსის ნორმების შესაბამისად. იხილეთ ისინი ცისკოს ვებსაიტზე. უფრო მეტიც, ჩვენ გაქვს ელექტრონული სახელმძღვანელო, სადაც აღწერილია Cisco-ს ბიზნესის წარმოების კოდექსი. მისი მოძიება შესაძლებელია "Ethics Decision Tree"-ში. შესაძლოა თქვენ არ მუშაობდეთ Cisco-ში, მაგრამ ჩვენ მიერ მომზადებული საქმის წარმოების სახელმძღვანელო დაგეხმარებათ ნებისმიერ სამუშაო ადგილზე. რაც შეეხება სამართლებრივ საკითხებს, თუ თვლით, რომ თქვენი ქმედება შესაძლოა იყოს არაეთიკური, მაშინ არსებობს იმის ალბათობა, რომ ის ასევე არალეგალურია. შესაძლოა თქვენი კომპანიების ადამიანის რესურსების მართვის, ან იურიდიული დეპარტამენტის თანამშრომელმა გაგარკვიოთ ამ საკითხებში.

ასევე, შეგიძლიათ მოიძიოთ სხვადასხვა ორგანიზაციის ეთიკის კოდექსები ონლაინ. ეცადეთ დაადგინოთ, რა პუნქტები აკავშირებს ამ კოდექსებს ერთმანეთთან.

დასაქმება კიბერ უსაფრთხოების სფეროში

გარდა კიბერ უსაფრთხოებაზე ორიენტირებული სამსახურებისა, მრავალი სხვა ბიზნესი და ინდუსტრია ასაქმებს კიბერ უსაფრთხოების პროფესიონალებს. ონლაინ ძიება დაგეხმარებათ თქვენთვის მისაღები სამუშაო ადგილის პოვნაში.

ამისათვის შეგიძლიათ გამოიყენოთ ეს ვებსაიტები:

- ITJobMatch – სამსახურის გლობალური საძიებო პორტალი IT სპეციალისტებისთვის;

- Monster – სამსახურის საძიებო პორტალი, სადაც შეგიძლიათ გამოჰყოთ კიბერ უსაფრთხოება;

- CareerBuilder – სამსახურის საძიებო პორტალი, სადაც შეგიძლიათ გამოჰყოთ კიბერ უსაფრთხოება.

თუ ხართ დამწყები IT სპეციალისტი, მაინც ნახეთ შემოთავაზებული სამსახურები. შესაძლოა ეს დაგეხმაროთ თქვენი მომავალი მიმართულების განსაზღვრაში.

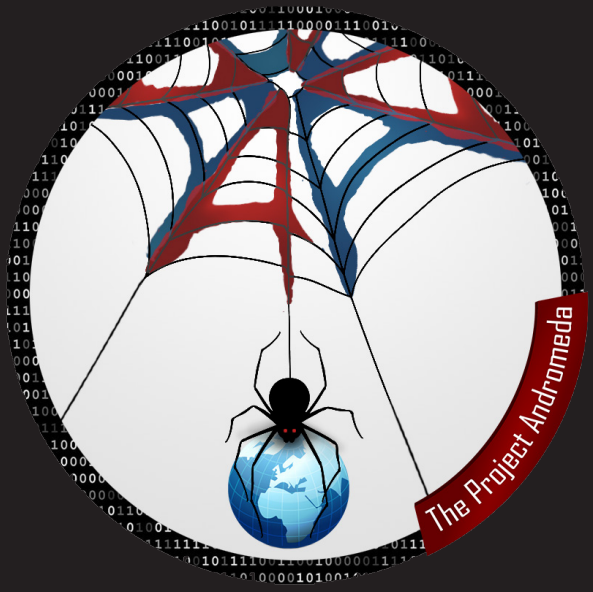
იქიდან გამომდინარე, თუ რომელი კიბერ უსაფრთხოების სფეროთი ინტერესდებით, თქვენ ადვილად იპოვით ვაკანტურ სამუშაო ადგილებს მსოფლიო მასშტაბით. შესაძლოა, სამსახურებმა მოგთხოვოთ ცოდნის დამადასტურებელი სერთიფიკატი. მაგალითისთვის, პენტესტერი, რომელსაც ასევე უწოდებენ ეთიკურ ჰაკერს, ეძებს უსაფრთხოების სისუსტეებს აპლიკაციებში, ქსელებში და სისტემებში. იმისათვის, რომ გახდეთ პენტესტერი, თქვენ უნდა გქონდეთ სამუშაო გამოცდილება სხვა IT სფეროებშიც, მაგალითად უსაფრთხოების ადმინისტრატორის, ქსელის ადმინისტრატორის, ან სისტემური ადმინისტრატორის გამოცდილება. უნარჩვევები, რომელსაც მიიღებთ აღნიშნულ სამსახურებში (სპეციალიზაციებში) დაგეხმარებათ ცოდნის კარგი ფუნდამენტის ჩამოყალიბებაში, რაც თავის მხრივ, გაქცევთ სასურველ კადრად ნებისმიერი კომპანიისთვის.

ბოლოს...

ვიმედოვნებთ, რომ ამ კურსმა აღძრა თქვენში ინტერესი და შესაძლოა გადაგაწყვეტინათ განათლების მიღება IT და კიბერ უსაფრთხოების დისციპლინებში. ცისკო-ს ქსელური აკადემია გთავაზობთ უამრავ კურსს, რომელიც დაგეხმარებათ კიბერ უსაფრთხოების დარგის შესწავლის გაგრძელებაში. გირჩევთ, დაიწყოთ კიბერ უსაფრთხოების საწყისებით, რათა შეიქმნათ ცოდნის მყარი ფუნდამენტი. ეწვიეთ ცისკოს ქსელურ აკადემიას და ნახეთ კურსების ჩამონათვალი, რომელთაც ჩვენ გთავაზობთ.

სახელმძღვანელოს შექმნაში იქონიეთ მონაწილეობა მოიწვიეთ...

Aleksandre Glonti | ალექსანდრე ღლონტი



ეს სახელმძღვანელო თქვენთვის შეიმუშავა და თარგმნა ყიბერ უსაფრთხოების ყომპანიამ

ჰრიექცი ანდრომედა

ჩვენი ძირითადი მიზანია ყომპიუტერული მეცნიერებების და ყიბერ უსაფრთხოების დარგების განვითარება საქართველოში. იქიდან გამომდინარე, რომ ჰრიექცი დიდ წილად საქველმოქმედოა, ეს სახელმძღვანელო გადაეცემა ყველა მსურველს უსასყიდლოდ!

დარგის სპეციალისტებს მივუწოდებთ შემოგვიერთდნენ ამ ყეთილშობილურ საქმეში, რათა გავაძლიერით ჩვენი საქართველო!