კიბერდანაშაული

თანამედროვე ტექნოლოგიების განვითარებამ ბიზნესის წარმოება უფრო ეფექტიანი და ხელმისაწვდომი გახადა. კომპანიებს გაუადვილდათ მომხმარებლისთვის პროდუქციისა და მომსახურების შეთავაზება, თუმცა, კიბერსივრცეზე მზარდ დამოკიდებულებასთან ერთად, გაიზარდა კიბერდანაშაულის საფრთხეც. ინტელექტუალური საკუთრება და კომერციულად სენსიტიური ინფორმაცია ორგანიზებული დანაშაულებრივი ჯგუფებისთვის მიმზიდველი სამიზნეებია. აქედან გამომდინარე, კიბერდანაშაულმა დიდი ზიანი შეიძლება მიაყენოს ბიზნესს.

თანამედროვე პერიოდში კიბერდანაშაულის საკმაოდ გავრცელებული შემთხვევებია: ონლაინ თაღლითობა, კომპიუტერულ სისტემასთან უნებართვო წვდომა, კომპიუტერული სისტემისა და მონაცემის უნებართვოდ გამოყენება და ა.შ. კიბერდანაშაულის ერთ-ერთ ხელშემწყობ ფაქტორს კერძო სექტორის დაბალი ცნობიერება წარმოადგენს.

კიბერ სივრცეს არ გააჩნია საზღვრები. კიბერდანაშაულთან ბრძოლის ერთ-ერთი მიზანია, ხელი შეუწყოს საქართველოში კერძო სექტორის კიბერსივრცეში გამართულ ფუნქციონირებას, ელექტრონული ტრანზაქციების უსაფრთხო განხორციელებასა და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებელ განვითარებას.

დასაცავი ინფრასტრუქტურის უდიდეს ნაწილს ფლობს და ოპერირებს კერძო სექტორი. აუცილებელია კერძო სექტორმა დაიცვას კომერციულად სენსიტიური ინფორმაცია, ინტელექტუალური საკუთრება, მომხმარებელთა მონაცემები და სხვ.

განხორციელებული ღონისძიებები

2008 წლიდან მოყოლებული, დაიწყო კონკრეტული ნაბიჯების გადადგმა კიბერდანაშაულის წინააღმდეგ ბრძოლის კუთხით:

- საქართველოს კიბერ უსაფრთხოების სტრატეგია 2013-2015 წარმოადგენს კიბერ უსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ მთავარ დოკუმენტს.
- 2012 წლიდან მოქმედებს „საქართველოს კანონი ინფორმაციული უსაფრთხოების შესახებ“, რომელიც აწესებს ინფორმაციული უსაფრთხოების ზოგად სტანდარტებს საჯარო და კერძო სექტორისთვის.
- საქართველოს მიერ რატიფიცირებულია ევროპის საბჭოს კონვენცია „კიბერდანაშაულის შესახებ“.
- სრულად განახლდა სისხლის სამართლის კოდექსის XXXV თავი. ცვლილებები შეეხო საპროცესო კანონმდებლობასაც. დაემატა სპეციფიური საგამოძიებო მოქმედებები, ტერმინთა განმარტება და სხვა. შემოღებულ იქნა იურიდიული პირის სისხლის სამართლებრივი პასუხისმგებლობა კიბერდანაშაულის ჩადენისათვის.
- დაიხვეწა ინტელექტუალური საკუთრების შესახებ მუხლი (საავტორო, მომიჯნავე უფლების მფლობელისა და მონაცემთა ბაზის დამამზადებლის უფლების ხელყოფა).
- ცვლილებები შევიდა ასევე საქართველოს კანონებში „ოპერატიულ-სამძებრო საქმიანობის შესახებ“ და „ელექტრონული კომუნიკაციების შესახებ.“
- ასევე შეიქმნა კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი რომელიც უფლებამოსილია, განახორციელოს კიბერსივრცის მონიტორინგი კომპიუტერული ინციდენტების გამოვლენისა და მართვის მიზნით, განსაზღვროს და გაატაროს კიბერ უსაფრთხოების პოლიტიკა, ასევე განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებები.
- კიბერდანაშაულის წინააღმდეგ ბრძოლა შინაგან საქმეთა სამინისტროს კომპეტენციას წარმოადგენს.
  - შინაგან საქმეთა სამინისტრომ შეიმუშავა ორგანიზებული დანაშაულის სტრატეგია, რომელშიც ცალკე თავად არის წარმოდგენილი კიბერ დანაშაულის წინააღმდეგ ბრძოლის საკითხები. აღნიშნულ სტრატეგიას ასევე გააჩნია საკუთარი სამოქმედო

გეგმა, სადაც დაზუსტებულია გასატარებელი ღონისძიებები და პასუხისმგებელი უწყებები.

- ცენტრალური კრიმინალური პოლიციის დეპარტამენტში შექმნილია კიბერდანაშაულის წინააღმდეგ ბრძოლის სამმართველო, რომელიც მოიცავს კიბერდანაშაულის საერთაშორისო საკონტაქტო პუნქტს 24/7.
- შსს-ში ასევე ფუნქციონირებს საექსპერტო-კრიმინალისტიკური მთავარი სამმართველოს ჰაბიტოსკოპიური და კომპიუტერულ - ტექნიკური ექსპერტიზის განყოფილება, რომელიც ახორციელებს საგამოძიებო მოქმედებების შედეგად მიღებული ციფრული მტკიცებულებების ექსპერტიზას.

ყველაფერი, რაც უნდა იცოდეთ კიბერდანაშაულის შესახებ!

კიბერ დამნაშავეები ძირითადად იყენებენ ფიშინგის, სპამის მეთოდებსა და სხვადასხვა მავნე პროგრამებს. აღნიშნულიდან გამომდინარე **სსიპ – მონაცემთა გაცვლის სააგენტომ** შეიმუშავა ზოგადი ინსტრუქციები, რომლებიც წარმოადგენს პრაქტიკული წესების ერთობლიობას ინტერნეტ რესურსებით უსაფრთხო სარგებლობის შესახებ. აღნიშნული ინსტრუქციები მოიცავს შემდეგ საკითხებს:

SPAM- სპამი

სპამი არის ელექტრონული წერილის ტიპი, რომელიც იგზავნება პიროვნების ან კომპანიის მიერ, მიმღების დაუკითხავად და სურვილის გარეშე. მსგავსი წერილები უმეტესწილად სარეკლამო ხასიათისაა. პიროვნებას, რომელიც მსგავს წერილებს გზავნის ეწოდება სპამერი. მათი ძირითადი მიზანია ამა თუ იმ პროდუქტის პოპულარიზაცია.

სპამერები რამდენიმე ხერხს მიმართავენ: 1) ცნობილი კომპანიის მომხმარებლის ბაზის გატეხვა; 2) კომპანიის თანამშრომლისგან არაოფიციალური გზით მომხმარებლის მონაცემების შეძენა; 3) სხვადასხვა, ყველასათვის ნაცნობი და პოპულარული საიტებიდან მონაცემების ამოღება სპეციალური პროგრამებით (მაგ: Harvester); 4) კომპიუტერიდან, რომელიც დაინფიცირებულია trojan-ით, შესაძლებელია მოიპოვო ყველა მეილი, რომელზეც მოხდა მიმოწერა დაინფიცირებული კომპიუტერით.

<u>დაიცავით თქვენი ბიზნესი შემდეგი მეთოდებით</u>

- ✓ არ უპასუხოთ სპამ წერილებს - პასუხის გაცემით თქვენ ადასტურებთ, რომ თქვენი ელ-ფოსტის მისამართი არის აქტიური და ამის შემდეგ შესაძლებელია მოგივიდეთ უფრო მეტი არასასურველი წერილი;
- ✓ არ გახსნათ სპამ წერილში მითითებული არცერთი ლინკი (ბმული) რა შინაარსისაც არ უნდა იყოს ის, ლინკზე დაჭერით შესაძლოა გადახვიდეთ სახიფათო ვებ-გვერდზე;
- ✓ არ გახსნათ სპამ წერილში თანდართული ფაილი, რადგან შეიძლება შეიცავდეს ვირუსს ან მავნე პროგრამას;
- ✓ გამოიყენეთ ანტივირუსი - ბევრ თანამედროვე ანტივირუსულ პროგრამას აქვს ანტი-სპამ ფუნქცია.

Phishing - ფიშინგი

ფიშინგი (ინგლისურად phishing : fishing - თევზაობა) — ინტერნეტ თაღლითობის დანაშაულებრივი ფორმა, რომლის მიზანია თაღლითური გზით მომხმარებელს გამოსძალოს პირადი საიდენტიფიკაციო მონაცემები, მაგალითად პაროლი, საკრედიტო ბარათის ან საბანკო ანაგარიშის ნომერი და სხვა კონფიდენციალური ინფორმაცია.

დაიცავით თქვენი ბიზნესი შემდეგი მეთოდებით

- ✓ **ფიშინგთან ბრძოლა** - რამდენიმე წლის წინ ფიშინგთან საბრძოლველად შეიქმნა ანტი-ფიშინგის სამუშაო ჯგუფი (Anti-Phishing Working Group - APWG), რომელშიც გაერთიანებულები არიან ფიშინგის სამიზნე კომპანიები, ასევე უსაფრთხოების პროგრამული უზრუნველყოფის მწარმოებლები და კიბერდანაშაულთან მებრძოლი კომპანიები, ჯამში 2500 კომპანიაზე მეტი. APWG-ს წევრები ატყობინებენ ერთმანეთს ახალი ფიშერული შეტევების შესახებ და ერთად ზრუნავენ ამ საკითხთან დაკავშირებით საზოგადოების განათლებაზე.

MALWARE- ზიანის მომტანი პროგრამა

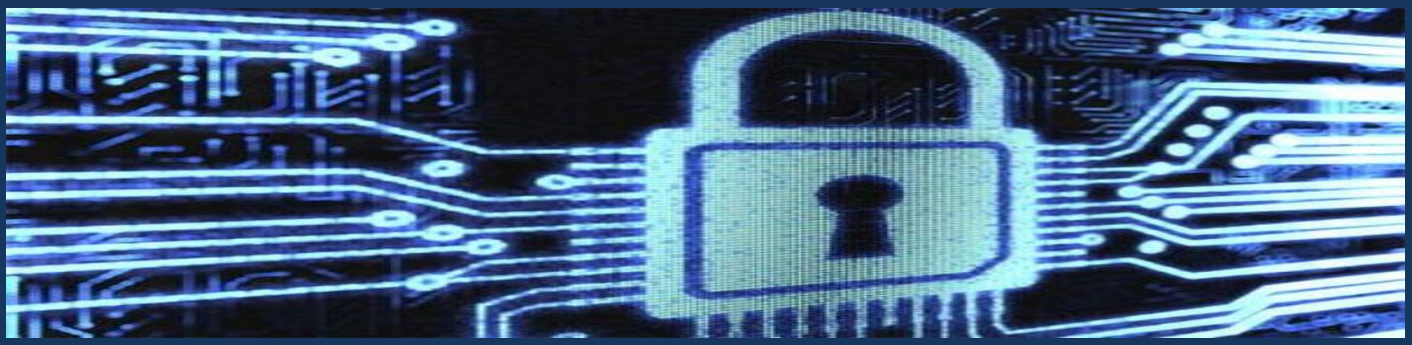
Malware - „ბოროტი“ პროგრამა - ეს არის კრებსითი სახელწოდება ყველა ტიპის მავნე ფუნქციის მქონე პროგრამისთვის. მავნე ფუნქციების მქონე პროგრამა შეიცავს ვირუსებს, ე.წ. „Trojans“, „Worms“ და „Spyware“, თუმცა უნდა ითქვას, რომ მხოლოდ ამით არ შემოიფარგლება მისი მავნე ფუნქცია. მავნე ფუნქციის მქონე პროგრამის მიზანი, უპირველეს ყოვლისა, არის სისტემებში შეღწევა და ამდენად, იქ შენახული ინფორმაციის კრიმინალური, კომერციული ან გამანადგურებელი მიზნებისთვის გამოყენება.

დაიცავით თქვენი ბიზნესი შემდეგი მეთოდებით

- ✓ გამოიყენეთ ანტი-ვირუსული პროგრამული უზრუნველყოფა
- ✓ **გამოიყნებეთ დამცავი ბარიერი (Firewall)**
- ✓ **გააქტიურეთ „სპამის“ და „ფიშინგის“ ფილტრები**
- ✓ **გააქტიურეთ „მოციმციმე“ სარეკლამო ფანჯრების (Pop-Up) ბლოკირება**

ელექტრონული ფოსტა და უსაფრთხოება

ელექტრონული ფოსტა დღეისათვის კომუნიკაციის ერთ-ერთ ყველაზე პოპულარულ მეთოდს წარმოადგენს. რადგანაც ელექტრონული ფოსტა ინტერნეტ-ტექნოლოგიებს ეფუძნება, მისი გამოყენება დაკავშირებულია ისეთ საფრთხეებთან, როგორიცაა **მავნე კოდი და ფიშინგი** (ინტერნეტ-თაღლითობის სახეობა, რომელიც მიზნად ისახავს პირადი მონაცემების ხელში ჩაგდებას).



<u>დაიცავით თქვენი ბიზნესი შემდეგი მეთოდებით</u>

- ✓ **ელექტრონული ფოსტა** - ერთი შეხედვით კომუნიკაციის არაკონტროლირებადი საშუალებაა, მაგრამ მომხმარებელმა უნდა იცოდეს, რომ ელექტრონული გზავნილები შეიძლება ისევე დაექვემდებაროს იურიდიულ ნორმებს, როგორც ჩვეულებრივი წერილები და ისინი გამოყენებული იქნან სამხილის ან ნივთმტკიცების სახით. კარგად დაფიქრდით, რას აგზავნით ელექტრონული ფოსტის საშუალებით და წერილი გულდასმით წაიკითხეთ, სანამ გაგზავნის ღილაკს დააჭერთ.
- ✓ **დაშიფრეთ მნიშვნელოვანი გზავნილები** - დაუშიფრავად გაგზავნილი ელექტრონული წერილი ღია ბარათივითაა, ის შეიძლება წაიკითხოს **ნებისმიერმა** იმ გზაზე, რასაც წერილი ადრესატამდე გაივლის. დაშიფრული ელექტრონული გზავნილი კონვერტში ჩადებულ წერილს ჰგავს. მნიშვნელოვანი ინფორმაციის შემცველი ელ. ფოსტის გაგზავნისას აუცილებლად გამოიყენეთ დაშიფრვის მეთოდები, ამისთვის ყველაზე ხშირად გამოიყენება **PGP** და **S/MIME** მეთოდები. თუ ვერ ახერხებთ მნიშვნელოვანი წერილის დაშიფრვას, მაშინ მისი შიგთავსი მოათავსეთ ფაილში, დაშიფრეთ ფაილი, მიაბით წერილს და ისე გაგზავნეთ.
- ✓ **გამოიყენეთ ძლიერი და უნიკალური პაროლები** - პაროლი საშუალებას გვაძლევს დავიცვათ ელექტრონული ფოსტა შემოტევისა და არასანქცირებული წვდომისგან. შესაბამისად, რამდენიმე ინტერნეტ ანგარიშზე (ექაუნთზე) ერთი და იმავე პაროლის გამოყენება ყველა ამ ექაუნთზე წვდომის შესაძლებლობას იძლევა, იმ შემთხვევაში, თუ ერთი მაინც გატყდა. გამოიყენეთ პაროლი, რომელიც შეიცავს არანაკლებ 8 სიმბოლოს, მათ შორის დაბალი და მაღალი რეგისტრის სიმბოლოებს, რიცხვებს და სპეციალურ სიმბოლოებს. პაროლი ხშირად ცვალეთ და სხვა ექაუნთზე არ გამოიყენოთ.
- ✓ **წაშალეთ ან დააარქივეთ ძველი ელექტრონული წერილები** - თუ ელექტრონული ფოსტის ერთ ექაუნთს დიდი ხნის განმავლობაში ხმარობთ, დიდი შანსია, რომ მასზე დაგროვილია დიდი რაოდენობით მნიშვნელოვანი ინფორმაცია თქვენს შესახებ და თქვენი ორგანიზაციის შესახებ. ამის გამო მუდმივად იზრდება მნიშნელოვან ინფორმაციაზე არასანქცირებული წვდომის რისკი; ნუ შეინახავთ ელექტრონულ წერილებს წლების მანძილზე. წაშალეთ ან უსაფრთხოდ დააარქივეთ ყველა ის წერილი, რომელიც აღარ გჭირდებათ.
- ✓ ხშირია შემთხვევები, როდესაც რაიმე პროდუქტის ან სერვისის შეძენით დაინტერესებული ფიზიკური პირი თუ კომპანია მოლაპარაკებებს აწარმოებს ელექტრონული ფოსტის მეშვეობით როგორც ქვეყნის შიგნით ისე ქვეყნის საზღვრებს

მიღმა. ამ დროს ელექტრონული ინვოისისა და გადასარიცხი თანხის ადრესატი საბანკო ანგარიშებიც დაინტერესებულ მხარეებს შორის იგზავნება ელექტრონული ფოსტით. ზოგადად ინტერნეტ სივრცის არასათანადო დაცულობის გათვალისწინებით, კონკრეტულად კი ცალკეულ ელექტრონულ ფოსტაზე არასანქცირებული წვდომის მაღალი რისკის პირობებში მიზნაშეწონილია ფულადი ტრანზაქციის განხორციელებამდე გადამოწმებულ იქნას (სატელეფონო ან სხვა საშუალებით) ელექტრონული ფოსტით მიღებული ინვოისისა და საბანკო ანგარიშის რეკვიზიტების უტყუარობა. მით უფრო, თუკი ფულადი გადარიცხვის მიმღები მხარე მოულოდნელად ცვლის წინასწარ შეთანხმებულ საბანკო რეკვიზიტებს.

მიმართეთ ზემოთ ჩამოთვლილ ზომებს რათა გააუმჯობესოთ თქვენი ბიზნესის უსაფრთხოება!

კიბერ დანაშაულზე დამატებითი ინფორმაციის მისაღებად ეწვიეთ: http://police.ge/ge/projects/kiberdanashauli

თუ თქვენ გახდით კიბერ თავდასხმის მსხვერპლი ან ფლობთ ინფორმაციას კიბერდანაშაულის თაობაზე, გთხოვთ დაგვიკავშირდეთ შემდეგ საკონტაქტო მონაცემებზე:

24 საათიანი უფასო ცხელი ხაზი - 112

ტელ: 2 41 12 96, 2 41 17 67;

ელ–ფოსტა: cybercrime@mia.gov.ge