Превод
УДК: 343.326:004.738.5
DOI: 10.7251/BPG1701147M

САЈБЕР КРИМИНАЛИТЕТ – УПЕЦАНИ У МРЕЖУ НАПАДА ВИРУСА

Назив оргиналног наслова: Cyberterrorismus: Bedrohungen aus dem Internet, *доступно путем интернет сајта:* http://www.anwalt.org/cyberterrorismus/, *приступљено 20.03.2017.*

Сајбер криминалитет (енгл. *cyber crime*; њем. *Cyberkriminalität*) обухвата кривична дјела почињена против интернета или уз помоћ интернета. Било да се ради о наруџбама на он-лајн продаји, резервацији одмора, одржавању социјалних контаката или управљању личним финансијама, могућности интернета су бескрајне.

Почеци сајбер криминалитета сежу још од 1969. године и то у Сједињеним Америчким Државама, када је настао такозвани Арпанет, претеча данашњег интернета.

Током година, овај облик информационе технике стално се усавршавао и постао техничко помагало које не само што је постало омиљена приватна занимација и иновација за предузећа већ и као конститутивни саставни дио многобројних друштава представља есенцијални државни инструмент.

Управо у коришћењу брзог, некомпликованог преноса података и обављању важних организационо-структуралних послова, лежи и опасност интернета. Јер, моћ са собом увијек носи и злоупотребу, тако да је сајбер криминал постао озбиљна пријетња по државу, односно државно право и њене грађане.

Како дефинисати појам сајбер криминал?

Са терминологијом преплављеном појмовима из енглеског језика, њемачки језик кориснике ставља пред мучне изазове. Појмови који се користе не могу се баш тачно и прецизно појаснити.

Шта је на примјер сајбер криминал?

Најближи превод значења овог појма могао би да буде интернетски криминал. Ради се, дакле, о кривичним криминалним радњама у простору информационих структура који је доступан путем интернета, такозваном сајбер простору.

Како год га назвали: сајбер криминал, интернетски криминал или компјутерски криминал, сви ови појмови су синоним за кривична дјела усмјерена потив интернета, мреже података, ИТ система или њихових података, која се врше уз помоћ информационих одн. комуникационих технологија.

Појавни облици сајбер криминалитета

Појавни облици и елементи кривичног дјела сајбер криминалитета су многоструки. Сајбер криминал се јавља у најразличитијим облицима и са различитим елементима кривичног дјела. У Конвенцији о сајбер криминалу Вијећа Европе, као примјери за интернетски криминал наводи се злоупотреба података или повреде ауторских права. У припучнику за превенцију и контролу компјутерског криминала (енгл.: Manual on the Prevention and Control of Computer Related Crime), као компјутерски криминал Уједињене Нације наводе сљедеће примјере:

- превара
- фалсификовање и
- недозвољен приступ подацима.

Сви ови деликти могу се починити на најразличитије начине, тако да су случајеви у којима полиција врши истраге интернетског криминалитета крајње разнолики.

Са новим достигнућима и развојем технике расте и већа уносност криминалаца. Управо су платформе као што је тамна мрежа (darknet) хранљива подлога за криминалне мреже.

Као darknet (тамна мрежа) означавају се анонимне везе, које, за разлику од интернета који користимо, нису јавно доступне. Претраживачи као што је гугл не могу пронаћи такве странице. Приступ се врши често преко специјалних софтвера, на примјер Тор-браузер-пакета (Tor-Browser-Paketa). Овдје не постоји централни сервер коме приступају сви корисници, умјесто тога управља се страницама појединих рачунара.

Такви тамни паралелни универзуми могу да служе за планирање и извршавање радњи које спадају у сајбер криминал. Примјер за то је, прије свега, размјена и дистрибуција садржаја са дјечјом порнографијом, као и продаја и куповина оружја или дрога.

Али и поред оваквих мрежа, сајбер криминалци своје опаке радње врше нпр. путем „Phishing“ мејлова, који служе за добијање осјетљивих личних података. Посебно је уобичајена пракса инфицирање и манипулација компјутерских система путем вируса штетних софтвера.

Хаковање профила на друштвеним мрежама је један облик сајбер криминала. Помоћу тројанаца, познатих и под називом Малвер (Malware),

или других програма, долази се до личних података и лозинки. Тако се може украсти нечији идентитет, што сада починиоцима омогућава, на примјер, хаковање банковних рачуна или приступ друштвеним мрежама као што су нпр. фејсбук или твитер.

Исто тако, за финансијско богаћење користе се крипто-тројанци (Cryptotrojaner, Ransomware). Уз помоћ ових тројанаца, заражени апарати се блокирају. Они ће се деблокирати тек када се уплати тражени износ новца као откупнина. Овдје, на примјер, може да постоји елемент кривичног дјела уцјене.

Исто тако, постоје и такозване бот мреже (bot networks), дакле неколико заражених рачунара, које нападачи могу контролисати из даљине.

Шта каже статистика

Шта се субјективно доживљава као велика опасност може се потврдити погледом на бројчану статистику сајбер криминала. Према статистици је од 2013. до 2015. године, додуше, био смањен број регистрованих кривичних дјела интернетског криминалитета. Међутим, број од округло 70.000 случајева према полицијској статистици на нивоу 2015. године и даље је висок.

У погледу статистике, криминалитет на интернету у сјенку ставља, на примјер, кривична дјела крађе (око 45.000) и кривична дјела против Закона о оружју (око 30.000).

У току 2015. године највише је било компјутерских превара (око 24.000). Са знатно мањим бројем случајева слиједи праћење и крађа података (око 10.000) а на трећем мјесту се налази кривотворење доказних података (округло 7.000).

Зато није чудо што се 2014. године више од једне трећине њемачког становништва плашило да постану жртва крађе идентитета.

Ова оправдана забринутост се може умањити сталним дјеловањем полиције и Савезне управе криминалистичке полиције (Bundeskriminalamt, скр. BKA). Претпоставка за то је опсежно познавање профила починилаца.

Само на тај начин полиција може што прије ступити у борбу против дјела сајбер криминала, како би посљедице биле што мање. Треба имати у виду да појединачни хакерски напади неријетко могу бити и дио великог плана сајбер тероризма.

Какви људи се, дакле, крију иза таквих напада?

Типологија починилаца компјутерског криминалитета

Починиоци сајбер криминалитета су често обични неупадљиви ђаци или студенти. Полицијске истраге неријетко отежава то што су такозвани хакери непримјетни и немају дугачке кривичне досијее. У правилу се ради о ђацима и студентима, никако, дакле, о ИТ експертима. Они живе повучено и остварују контакте прије свега на информативној основи, умјесто да успостављају пријатељске везе. Ужитак, забава и знатижеља повезани са голицањем нерава често воде до тога да се хаковањем почну вршити противзаконита дјела. Осјећај моћи, контроле и освета могу исто тако бити мотив, као и финансијски аспекти или политички ставови.

Један аспект који доприноси криминализацији одређених особа су мали захтјеви властитих знања из информационих технологија. На интернету се све чешће налазе сумњиве понуде које и лаицима омогућују да манипулишу страним мрежама. Као и мотиви, мете напада сајбер криминалитета су различите. Зависно од интереса, велика предузећа у привредној бранши, веб-странице иза којих стоји држава, порно оператори или сајтови банака, исто тако су угрожени као и приватна лица.

Мјере државе и приватне технике самозаштите

У принципу, имамо два поља реакције, уколико дође до кривичних дјела сајбер криминала. Као прво, нападнута лица би требало да провјере властиту безбједност података, како би на тај начин и превентивно била заштићена од починилаца. Као друго, полиција би, по сазнању о интернет криминалу, требало да буде први контакт за жртву. Полиција располаже експертским групама или стручним центрима који се баве управо проблематиком сајбер криминалитета. Кривично гоњење од стране полиције и Савезне управе криминалистичке полиције у Њемачкој је задатак полиције у првом реду да истражује случајеве сајбер криминала и да починиоце који иза њих стоје приведе суду. Посебно је то дужност Покрајинских управа криминалистичке полиције (Landeskriminalamt скр. LKA). На нивоу државе, за сајбер криминал надлежна је Савезна управа криминалистичке полиције (БКА). Савезна управа криминалистичке полиције располаже специјалним јединицама које су најбоље оспособљене за разне облике сајбер криминала.

За спровођење истражних поступака, координацију националних и интернационалних активности за расвјетљавање сајбер криминала, у Савезној управи криминалистичке полиције формирана је једна група са ознаком „SO 4“.

Ова јединица припада Одјељењу за тешки и организовани криминал и она је специјална служба за контакте и истраге сајбер криминала.

Обрада сајбер криминала у стручном центру

Због све већег броја кривичних дјела која долазе са интернета, неке савезне земље су увеле такозване стручне центре, који се активирају увијек кад жртве пријаве случајеве сајбер криминалитета. Такве јединице постоје између осталих у Сјеверној Рајни-Вестфалији, Баден Виртмбергу и Баварској.

Стручни центар у Сјеверној Рајни-Вестфалији је основан 2011. године при Покрајинској управи криминалистичке полиције и у свако доба дана на располагање ставља стручњаке који примају упите и од државних органа и институција, као и из области науке, образовања и привреде. Ова јединица, осим тога, доприноси јачању свијести о опасностима и за поучавање о превентивним стратегијама.

Понуде Савезне управе за безбједност и информационе технологије (BSI)

Примарну државну службу за питања у вези са сајбер криминалом и безбједности на интернету представља Савезна управа за безбједност и информационе технологије.

Она помаже држави у вршењу свакодневних оперативних послова, сарађује са предузећим из привреде и грађанима служи као извор информација.

При Савезној управи за безбједност и информационе технологије 2006. године основан је пројекат CERT (Computer Emergency Response Team). Као прво, он пружа помоћ савезним органима код безбједносно релевантних опасности и случајева у компјутерским системима, а као друго, служи као платформа за информације и упозорења за грађане и мала предузећа. Редовно се врши анализа и процјена опасности на интернету, тако да се у конкретним ризицима корисницима шаљу упозорења.

Самозаштита је важна мјера за спречавање сајбер криминала као недозвољеног приступа трећих лица. Не само као нападнути или жртва, већ и за превентивну одбрану од опасности, корисници интернета могу на страницама BSI и CERT пронаћи важне савјете и препоруке како поступати у случају сајбер криминала. Посебно је важно да се осигурају лични подаци и да се са интернетом поступа опрезно.

Ево како се можете конзеквентно одбранити од појединих напада.

Сигурносне стратегије за одбрану од сајбер криминала

Ако подузмете извјесне мјере безбједности, можете драстично смањити шансу да постанете жртва сајбер криминала. Да бисте се заштитили од недозвољеног приступа других лица, можете сами урадити сљедеће:

– Редовна инсталација сигурносних надограњи (апдејта) оперативног система и инсталираних програма
– Актуализација кориштеног анти-вирус програма
– Постављање заштитног зида (Firewall)
– Ограничавање права корисничких налога (user account)
– Опрезно поступање са личним подацима
– Коришћење сигурних прегледача (Browser)
– Коришћење сигурних лозинки (password) и редовно обнављање
– Пренос података искључиво преко шифрованих веза (препознатљиви као „HTTPS“)
– Деинсталација софтвера који се не користе
– Прављење резервних копија, тзв. бекапа (Backup)
– Коришћење WLAN преко шифрованог стандарда WPA2
– Провјера сигурносног статуса компјутера.

Уколико би и поред свега тога постали жртва сајбер криминала, одмах се обратите полицији или чак потражите адвоката, прије свега за кривично право.

Мали глосар сајбер криминала

CERT: Computer Emergency Response Team; надлежан за превентивне и реактивне мјере заштите рачунарских система

Darknet (тамна мрежа): анонимне везе за које није омогућен јавни приступ

Malware: Општи појам за разне облике штетних програма (вируса)

→ Adware: не прави директну штету, увезује се у прегледач као алатка (toolbar) или Add-on и покушава убацити рекламу

→ Botnet (бот мрежа): низ заражених компјутера којима се управља са неког рачунара

→ Ransomware: Блокада система која се отклања само уз плаћање откупнине

→Spyware: Програм за похрањивање осјетљивих личних података корисника

→ Trojaner: бескористан програм који корисници преузму несвјесно и који онда оштећује компјутер

→ Virus: Датотека са штетним кодом који програме чини неупотребљивим и који се шири по цијелом рачунару

Превео и прилагодио:
Миленко Мршић, Управа за полицијску обуку, mrsicm@yahoo.com

Напомена преводиоца текста:

Овај текст је преузет са сајта www.anwalt.org. Аутор текста је група аутора удружења истакнутих правних експерата Савезне Републике Њемачке који на овом сајту редовно објављују радове на теме из разних области. То су углавном актуелне теме и теме које су од највећег значаја за грађане, које својим грађанима пружају корисне информације и упутства за поступање, прије свега с циљем очувања личне безбједности и остваривања личних и других права.