Vrste kibernetičkih napada na poduzeća i njihove mjere obrane

Ljuban, Rahela

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
SMJER Informatika (istraživački)
Ak. god. 2019./ 2020.

Rahela Ljuban

Vrste kibernetičkih napada na poduzeća i njihove mjere obrane

Diplomski rad

Mentor: dr. sc. Vedran Juričić, doc.

Zagreb, prosinac, 2020.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod

Kibernetički napad, ovisno o svom cilju i ozbiljnosti može oštetiti ili čak uništiti tvrtku. Čak 60% malih poduzeća koja su bila podvrgnuta kibernetičkim napadima prestane poslovati unutar narednih šest mjeseci od napada. Osim financijske štete, tvrtke trpe i oštećenu reputaciju te počinju gubiti svoje korisnike. Kako bi se tvrtka zaštitila od potencijalnih napada potrebno je razviti sigurnosne mjere koje se poduzimaju za sprječavanje napada, kao i mjere za uklanjanje i ublažavanje nastale štete u slučaju da se dogodi uspješan napad. Prema tome, računalna sigurnost danas predstavlja jedan od najvažnijih elemenata u korištenju računala i računalnih sustava. Kako bi se razvila efikasna zaštita protiv napada, sigurnosni tim tvrtke mora znati koji su potencijalni ciljevi napadača kao i mete njihova napada. Pokušavaju li hakeri doći do osjetljivih informacija koje bi mogle prouzročiti ozbiljne štete tvrtki i njezinom tržištu? Informacije o razvoju proizvoda, listama dobavljača, podaci o potrošačima, financijski zapisi o prihodima, dobicima i porezima te velik broj ostalih informacija mogu biti štetne za tvrtku ako dođu u krive ruke. Ponekad je cilj napada enkriptirati važne podatke sve dok tvrtka ne plati određenu svotu novca. Bilo koja vrsta napada može imati ozbiljne posljedice koje uključuju i pad vrijednosti dionica na tržištu pa čak i tužbe od strane nezadovoljnih ili zabrinutih potrošača ili poslovnih partnera. Kako bi se tvrtka zaštitila od svih navedenih (i nenavedenih) rizika, bitno je ih je predvidjeti i razumjeti, kao i poznavati tehnologije korištene za napade i obranu od istih.

2. Definicije računalne sigurnosti i kibernetičkog kriminala

Zbog rasta broja i vrsti kibernetičkih prijetnji i napada, kibernetička odnosno računalna sigurnost postala je vrlo bitno pitanje u poslovanju poduzeća. Najnoviji trendovi i statistike kibernetičkih napada prikazuju velik porast napadnutih računalnih sustava i podatkovnih proboja putem uređaja koji su sve češći na radnim mjestima, poput mobilnih uređaja i interneta stvari (engl. *Internet of Things* - IOT). Uz to, nedavna sigurnosna istraživanja sugeriraju i da većina poduzeća ima nezaštićene podatke te čak i lošu praksu računalne sigurnosti, što ih čini ranjivima na potencijalne napade koji bi mogli rezultirati gubitkom podataka (Identity Theft Resource Center, 2019). Kako bi se poduzeća uspješno borila protiv zlonamjernih kibernetičkih napada ili još bolje spriječila ih, nužno je imati svijest o računalnoj sigurnosti, prevenciji potencijalnih napada i najbitnije od svega, poznavati što točno podrazumijevaju pojmovi računalna sigurnost i kibernetički kriminal.

2.1. Definicija računalne sigurnosti

Kada se govori o računalnoj sigurnosti, pod nju se najčešće podrazumijeva zaštita računalnih sustava, podataka i informacija od štete, krađe, neovlaštene uporabe ili pristupa istima te remećenje ili pogrešno usmjeravanje usluga koje pružaju (Encyclopedia Britannica). Računalna sigurnost uključuje kontrolu fizičkog pristupa računalnom sklopovlju (engl. hardware), kao i zaštitu od štete koja može nastati mrežnim pristupom podacima i ubrizgavanjem koda te zbog zlouporabe od strane operatora, bilo namjerno, slučajno ili zato što ih je netko prevario kako bi ih naveo da odstupe od svojih sigurnih postupaka (Zlatanov, 2015).

Radi toga što današnje društvo uvelike ovisi o tehnologiji i oslanja se na računala i računalne sustave, potreba za zaštitom hardvera, softvera te informacija i usluga koje se nalaze na njima u stalnom je porastu i sve više se prepoznaje važnost računalne sigurnosti; posebice ako se u obzir uzme činjenica da bez nekih od usluga koje današnje tehnologije pružaju veliki dio društva uopće ne bi mogao funkcionirati, a baš se takvi sustavi nalaze pod najvećim rizikom od napada. Primjerice, financijski računalni sustavi poput bankomata, POS terminala (engl. *Point Of Sale* - hrv. prodajno mjesto) za plaćanje u trgovinama, mrežnih stranica koje pohranjuju i koriste bankovne račune i kartice (uključujući internetske trgovine) te velike korporacije vrlo su česta meta napadača koji na razne ilegalne načine žele ostvariti financijsku

dobit. Također, potrošački uređaji poput osobnih računala, mobitela, pametnih satova, tableta i slično, se napadaju u svrhu izopačenog ostvarivanja financijske dobiti, krađe osobnih podataka ili pak za stvaranje botneta kojim se zatim napada neka druga meta, najčešće u obliku DDoS napada (engl. *distributed denial of service*).

2.2. Definicija računalnog kriminala

Gore navedeni primjeri su najčešće mete računalnog, odnosno kibernetičkog kriminala. Računalni kriminal se definira kao upotreba računala kao instrumenta u nezakonite svrhe, kao što su počinjenje prijevare, trgovina dječjom pornografijom i intelektualnim vlasništvom, krađa identiteta ili kršenje privatnosti (Encyclopedia Britannica). Cilj računalnog kriminala nisu samo financijski podaci, već i podaci općenito. Broj i učestalost podatkovnih proboja (engl. *data breach*) i krađe podataka raste, a to zauzvrat dovodi i do sve više slučajeva prijevare i iznude (Interpol).

Interpol u svojoj definiciji kibernetičkog kriminala dodaje da je sam niz mogućnosti koje su računalni kriminalci pokušali iskoristiti čak i impresivan te navodi primjere poput korištenja *botneta* kao mreže uređaja zaraženih zlonamjernim računalnim programima bez znanja njihovih korisnika u svrhu prijenosa virusa koji stječu neovlašteno daljinsko upravljanje uređajima, krađu lozinki i onemogućavanje antivirusne zaštite, stvaranje "*backdoor*" pristupa na ugroženim uređajima kako bi se omogućila prilika za krađu novca i podataka ili daljinski pristup uređajima za stvaranje *botneta*, pranje klasičnih i virtualnih valuta, vršenje prijevara putem lažnih i varljivih mrežnih stranica ili putem internetskih i kartičnih sustava plaćanja, razni oblici seksualnog iskorištavanja djece na mreži, uključujući distribuciju sadržaja o seksualnom zlostavljanju djece i videoprijenos seksualnog zlostavljanja djece uživo, pružanje usluga ilegalnih operacija koje uključuju prodaju oružja, lažnih putovnica, krivotvorenih ili kloniranih kreditnih kartica i droga te usluge hakiranja (Interpol).

Postoje tri glavne kategorije u koje spada računalni kriminal te se vrste korištenih metoda i razine težine razlikuju ovisno o kategoriji, a te kategorije su "Vlasništvo", "Pojedinac" i "Vlada" (Panda Security).

Kategorija "Vlasništvo", slično stvarnom slučaju kriminalca koji nezakonito posjeduje pojedinosti o bankovnim podacima ili kreditnoj kartici, opisuje hakiranje u svrhu krađe bankovnih podataka neke osobe ili tvrtke kako bi se dobio pristup novčanim sredstvima te osobe ili tvrtke, za kupovinu putem interneta ili pokretanje prijevara za krađu identiteta,

odnosno phishing, kako bi ljudi hakerima slučajno dali svoje osjetljive podatke. Također postoji i mogućnost korištenja zlonamjernog softvera za dobivanje pristupa mrežnim stranicama s povjerljivim informacijama.

Kategorija "Pojedinac" računalnog kriminala opisuje jednog pojedinca koji distribuira zlonamjerne ili ilegalne informacije putem mreže. To može uključivati *cyberstalking*, distribuciju pornografije i trgovinu ljudima.

Kategorija "Vlada" je najrjeđa kategorija računalnog kriminala, ali ujedno i najteži prekršaj, počinjenje zločina protiv vlade također je poznat i kao kibernetički terorizam. Ova kategorija uključuje hakiranje vladinih mrežnih stranica, vojnih mrežnih stranica ili distribuciju propagande. Ovi su kriminalci često ili teroristi, ili pripadnici odnosno predstavnici neprijateljskih vlada drugih država.

2.3. Motivacije kibernetičkih kriminalaca

U najširem smislu, kibernetički kriminal u osnovi je iskorištavanje informacijskih sustava i tehnologija za počinjenje krađe, iznude, krađe identiteta, prijevare, a u nekim slučajevima i korporativne špijunaže. Tko su kibernetički zločinci koji počinjavaju te zločine i koji su njihovi motivi? Svaki kriminalac, bez obzira radi li se o tradicionalnom obliku kriminalca (koji primjerice krade robu iz dućana ili čak pljačka banku) ili kibernetičkom kriminalcu (koji svoje spletke izvodi putem računala), za počinjenje kaznenog djela uvijek ima svoj osobni (ili dijeljeni, ako se radi o kriminalnoj organizaciji) motiv.

Iako, moglo bi se reći da kibernetički kriminal zahtjeva manje resursa i planiranja (Cyber Attacks). Razlog za tu tvrdnju je očit, primjerice kako bi se (fizički, u stvarnom svijetu) opljačkala banka, kriminalci moraju temeljito sastaviti plan akcije, odnosno isplanirati datum i vrijeme, odrediti tko će im sve biti suučesnik, isplanirati način rutu bijega, nabaviti krinke i oružja, te nakon svega toga na isti način isplanirati popratni plan u slučaju da prvotni plan pođe po krivom, kako bi osigurali uspješno izvršavanje svog zločina (i usput riskirati šansu da će ih svejedno netko prepoznati ili uhvatiti u bijegu) (Cyber Attacks). U usporedbi s time, kibernetički kriminalac samo treba osmisliti svoj zlonamjerni program (ili na određenim stranicama za distribuciju zlonamjernih programa samo preuzeti program koji želi iskoristiti), smisliti način distribucije i širenja svog zlonamjernog programa, osigurati da se njegov identitet neće moći pratiti, i u najčešćim slučajevima nije potrebno više planiranja od toga. Uz to, računalni kriminalci najčešće napade izvršavaju na daljinu, često čak i iz većih daljina koristeći

računalne mreže, napadajući računala i mrežne stranice diljem svijeta (Csonka, 2006). Ako se ovaj napad uspije izvesti bez većih problema, kibernetički kriminalac će prikupiti osjetljive informacije od svojih meta napada i potencijalno će ih moći iskoristiti za kupovinu preko interneta ili druge transakcije (Cyber Attacks). U navedenim primjerima, može se sa sigurnošću primijetiti da je u pitanju motiv financijske dobiti. Ali, nije to jedini motiv koji kibernetički kriminalci mogu imati prilikom planiranja i izvršavanja kibernetičkih napada. Kibernetski kriminal je apsolutno sveprisutan, ne diskriminirajući između svojih meta i evidentno je da se dramatično brzo širi svijetom. Shinder (2010) i Khanse (2017) u svojim člancima o motivima kibernetičkih kriminalaca navode da su najčešći motivi kibernetičkih napada financijska dobit, politička odnosno vjerska uvjerenja, osveta te samodokazivanje ili zabava.

Financijska dobit je prvi motiv za počinjenje kibernetičkih zločina koji ljudima pada na pamet, a i s pravom: neki od najvećih kibernetičkih napada u posljednjih nekoliko godina bili su financijski orijentirani s ciljem iznude novčanih sredstava od svojih meta (poput temeljnih korisnika, poduzeća i organizacija) (Shinder, 2010). Za te napade koristilo se nekoliko različitih varijanti zlonamjernih ucjenjivačkih programa (engl. *ransomware*), s pretpostavljenom financijskom štetom 2019. godine od čak 11,5 milijardi američkih dolara (u taj iznos su osim troškova za otkupninu uključeni i troškovi oporavka napadnutih poduzeća od napada), a pretpostavlja se da će globalni troškovi oporavka od napada ucjenjivačkim programima 2021. godine doseći čak i do 20 milijardi američkih dolara (Cybercrime Magazine). Dapače, čak 41% kibernetičkih napada spada pod napade ucjenjivačkim programima koji su nanijeli štetu globalnoj ekonomiji u iznosu od 450 milijardi američkih dolara u 2016. godini, a taj broj raste kako se sve veći broj uređaja povezuje na internet i međusobno (Desjardins, 2018). Khanse (2017) navodi da kibernetički kriminalci često provode kibernetičke napade u svrhu financijske dobiti, a čine to ili pojedinačno ili u organiziranim zločinačkim grupama. Pri tome dodaje da kako bi uspjeli u svojim namjerama, najčešće koriste nekoliko različitih metoda, poput osmišljavanja lažne mrežne trgovine s ciljem prikupljanja osjetljivih podataka poput broja kreditnih kartica korisnika. Nerijetko pokušajima izravnih napada na poslužitelje poduzeća, organizacija i banaka pokušavaju također pokušavaju doći do takvih osjetljivih podataka njihovih korisnika. Uz pomoć tih dobivenih informacija, kibernetički kriminalci imaju mogućnost počiniti razne vrste prijevara uz pomoć tih kreditnih kartica (Khanse, 2017). Shinder (2010) navodi da kibernetički kriminalci također mogu pokušati upasti u bazu podataka nekog poduzeća kako bi ukrao zapise o identitetima korisnika koje potom može prodati drugim kibernetičkim kriminalcima. Dodaje da su mogući i slučajevi gdje neko

poduzeće potajice "unajmljuje" hakera koji će za njega ukrasti poslovne tajne drugih poduzeća. Naravno, kibernetički kriminalci ne moraju samo funkcionirati "izvana", oni mogu biti i zaposlenici samih poduzeća i organizacija. Primjerice, neki zaposlenik banke može koristiti svoj pristup računalima u banci kako bi pokušao prebaciti novčana sredstva s tuđeg računa na svoj (Shinder, 2010).

Drugi mogući motiv su politička ili vjerska uvjerenja; neki kibernetički kriminalci snažno podržavaju određene političke stavove ili vjerske pokrete te stoga planiraju i provode kibernetičke napade kako bi obznanili svoja politička ili vjerska stajališta (Cyber Attacks). Ovdje se često spominje pojam haktivizma (engl. *hacktivism*, od engl. *hack* - hrv. hakirati, i engl. *activism* - hrv. aktivizam) koji označava najčešće nenasilne internetske kampanje u svrhu postizanja nekog političkog, društvenog ili vjerskog cilja, koristeći se različitim sredstvima kao što su DDoS napadi, objavljivanje osobnih informacija i slično (Panda security). Sljedovno, mrežne stranice brojnih poduzeća, organizacija i vlada znaju trpiti haktivističke napade vandalizmom s ciljem slanja političkih ili vjerskih poruka (Oikarinen, 2019). Haktivisti se obično udružuju u skupine ljudi koji dolaze iz različitih krajeva svijeta, a ujedinjeni su zajedničkim, često kratkoročnim, ciljevima koje nazivaju Operacijama. U svojim ranim godinama je haktivizam bio prilično učinkovit, ali kako su sigurnosne mjere poboljšale učinkovitost obrane protiv ovih napada, broj Operacija se smanjio te su haktivisti počeli češće ciljati lakše mete na koje mogu lakše utjecati svojim napadima (Comtact). Kibernetički kriminalci koji sudjeluju u politički motiviranim napadima mogu biti i pripadnici ekstremističkih organizacija koji koriste internet za širenje propagande, napade na mrežne stranice i računalne mreže svojih politički neprijatelja, ili pak krađu novca u svrhu financiranja svojih budućih aktivnosti (Gandhi, Sharma, Mahoney, Sousan, Zhu, & Laplante, 2011). Gandhi et al. (2011) nadalje navode da se politički motivirani napadi mogu tako razlikovati kao prosvjedi protiv nekih političkih događaja, prosvjedi protiv određenih zakona ili javnih dokumenata te ogorčenost radi nekih specifičnih događaja.

Treći mogući motiv za kibernetičke napade je osveta. Povrijeđene emocije poput ljutnje ili ljubomore ponekad navode ljude da odluče nekome nešto učiniti nažao, tako i kibernetički kriminalci mogu djelovati iz bijesa i osvete i planirati napade kako bi se s nekim "izjednačili". Kibernetički kriminalci često planiraju kibernetičke napade radi svojih povrijeđenih osjećaja, iz bijesa, osvete, "ljubavi" ili neke vrste očaja (Shinder, 2010). Shinder (2010) također navodi da u ovu kategoriju spadaju i kibernetički napadi poput uhođenja osoba putem interneta (engl. *cyberstalking*) ili napastovanje porukama, ali i (osobne ili čak terorističke) prijetnje,

organizirani napadi distribuiranim uskraćivanjem usluge, krađa ili uništavanje podataka koji pripadaju nekom poduzeću, i slični napadi. To može uključivati bijesne zaposlenike koji su nezadovoljni odlukom poduzeća za kojeg rade ili čak kupce nezadovoljne promjenama u proizvodima, uslugama ili izvršnim odlukama poduzeća (Shinder, 2010).

Samodokazivanje ili zabava također predstavljaju motiv napada. Neki kibernetički kriminalci provode kibernetičke napade samo zato što mogu (Shinder, 2010). Drugim riječima, svjesni su da imaju sva potrebna znanja i mogućnosti da osmisle i izvrše kibernetički napad i baš zbog toga se odlučuju na provođenje nekog računalnog napada. Po njihovoj percepciji, uspješno izvršavanje kibernetičkog napada će ih učiniti poznatim i poštovanim članom među zajednicama kibernetičkih kriminalaca na internetu (Cyber Attacks). Nekada će htjeti upasti u neki računalni sustav samo da bi sami sebi postavili neki teži izazov i time dokazali svoje sposobnosti, ali najčešće ne iz želje da stvarno učine nešto zlonamjerno kad napokon uspostave kontrolu nad računalnim sustavom (iako ponekad znaju slučajno načiniti popratnu štetu na računalnom sustavu i time financijsku štetu radi potrebe popravka računalnog sustava nakon napada) (Khanse, 2017). Dapače, jedan dio organiziranog kibernetičkog kriminalnog djelovanja na internetu potaknut je prvenstveno nemonetarnim motivima, sa svrhom intelektualnog izazova, rasta individualne ili grupne slave, ideologije ili znatiželje.

Poznati su i primjeri slučajeva gdje su kibernetički napadi počinjeni iz želje za intelektualnim izazovom. Primjerice, slučaj Edwarda Pearsona koji je između siječnja 2010. i kolovoza 2011. godine ukrao 8 milijuna identiteta, 200,000 informacija o PayPal računima i 2,700 brojeva bankovnih kartica, koristeći zlonamjerne programe ZeuS i SpyEye koje je izmijenio prema svojim potrebama te je uspio ne samo upasti na mrežne stranice PayPal, već i u mreže AOL (engl. *America OnLine*) i Nokia, koje su kao posljedica napada bile srušene čak dva tjedna (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014). Pearson je uhićen nakon što je njegova djevojka pokušala krivotvorenim kreditnim karticama platiti hotelske račune. Pearsona su opisali kao nadarenog i pametnog računalnog programera te je nekoliko godina bio aktivan član raznih foruma za kibernetički kriminal. Njegov je odvjetnik prilikom suđenja tvrdio da Pearsona nisu zanimali financijski dobitci kada je osmišljao napad, već je sam sebi želio zadati intelektualni izazov provedbom ovog napada. Štoviše, jedan od tužilaca je utvrdio da je Pearson imao mogućnost potencijalno ukrasti čak 12 milijuna američkih dolara svojim napadom, ali je zapravo ukrao "samo" 3,700 američkih dolara koje je potrošio na naručivanje hrane i plaćanje telefonskih računa. Pearson je u travnju 2012. osuđen na 26 mjeseci zatvora (Broadhurst et al., 2014).

Za potrebe organiziranja napada većeg obujma, razlog za napad na računalne sustave može biti i uključivanje računala u DDoS napad (engl. *distributed denial of service - DDoS*) (Khanse, 2020). Kibernetički kriminalci ponekad provode pomno isplanirane napade kako bi na velik broj računalnih sustava uspjeli podmetnuti zlonamjeran program koji će to računalo dodati u mrežu daljinski kontroliranih uređaja (engl. *botnet*), u svrhu pokretanja kasnijih distribuiranih napada uskraćivanjem usluge (Cloudflare). Primjerice, jedan veći distribuirani napad uskraćivanjem usluge usmjeren je na tvrtku Dyn, jednog od većih pružatelja DNS usluga (engl. *domain name system* - hrv. domenski sustav imena), tijekom listopada 2016. godine koji je kao posljedicu je stvorio smetnje na mnogim većim mrežnim stranicama, uključujući Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit i GitHub (Cloudflare). To je učinjeno pomoću zlonamjernog programa zvanog Mirai, koji služi za stvaranje mreža daljinski kontroliranih uređaja (engl. *botnet*) koristeći internet stvari (engl. *Internet of Things - IOT*), uređajima kao što su kamere, pametni televizori, radio, pisači, pa čak i monitori za bebe. Dyn je uspio sanirati napad u roku od jednog dana, ali motiv napada nikada nije otkriven (Cloudflare).

3. Vrste kibernetičkih napada

Postoji velik broj vrsta kibernetičkih napada. To su primjerice zločini koji uključuju temeljna kršenja osobne ili korporativne privatnosti, kao što su napadi na integritet podataka koji se čuvaju u digitalnim repozitorijima i uporaba ilegalno dobivenih digitalnih podataka za ucjenu tvrtke ili pojedinca te zločin krađe identiteta koja je također rastući problem, zločini zasnovani na novčanim transakcijama poput prijevare, trgovine dječjom pornografijom, digitalnog piratstva, pranja novca i krivotvorenja (Encyclopedia Britannica). Osim zločina na individualnoj razini, računalni kriminal uključuje i pojedince u korporacijama ili vladinim birokracijama koji namjerno mijenjaju podatke ili informacije bilo zbog osobne dobiti ili dobiti stranke te zbog svojih ili tuđih političkih ciljeva (Encyclopedia Britannica). Druge vrste napada se provode s ciljem remećenja ispravnog rada usluga na internetu ili sprječavanje većeg broja korisnika da koriste neku internetsku uslugu. Tu spada neželjena pošta (engl. *spam*), hakiranje, distribuirani napadi u svrhu uskraćivanja neke usluge (engl. *distributed denial of service - DDoS*), ili činovi kibernetičkog terorizma odnosno korištenje interneta u svrhu remećenja javnog reda i mira ili čak smrti pojedinca (Encyclopedia Britannica).

3.1. Napadi zlonamjernim programima

Zlonamjerni program (engl. *malware*, koji je skraćenica izraza engl. *malicious software*) opširni je pojam koji opisuje bilo koji zlonamjerni program ili kôd koji je štetan za računalne sustave, namjerno dizajniran kao nametljiv i neprijateljski nastrojen program kojem je cilj napasti, oštetiti ili onemogućiti normalan rad računala, računalnih sustava, računalnih mreža, tableta i mobilnih uređaja, primjerice preuzimanjem djelomične kontrole nad radom uređaja (Malwarebytes). Nadalje, postoje brojne različite kategorije zlonamjernih programa, uključujući crve, trojanske programe, špijunski softver i hvatače unosa podataka, a sve veći broj vrsta zlonamjernih programa može koristiti kombinaciju različitih tehnika zaraze i napada. Iako zlonamjerni programi najčešće ne mogu oštetiti fizičko sklopovlje sustava ili mrežne opreme, oni mogu krasti, šifrirati ili izbrisati podatke, izmijeniti ili otimati osnovne funkcije računala i špijunirati aktivnost računala bez korisnikovog znanja ili dopuštenja (Akamai).

Nadalje, velika prijetnja za sve korisnike je hvatanje unosa podataka. Hvatači unosa podataka (engl. *keylogger*) su vrsta zlonamjernih programa koji su dizajnirani kako bi pratili pritiske tipki koje je korisnik napravio na svojoj tipkovnici te zatim te praćene pritiske

zapisivali u posebnu skrivenu datoteku iz koje kriminalci potom mogu iščitati osjetljive informacije poput elektroničkih adresa, lozinki, brojeva kreditnih i debitnih kartica i ostalih podataka koje bi napadači mogli smatrati korisnima za svoje loše namjere (Kaspersky). Drugim riječima, kriminalci koriste hvatače unosa podataka za krađu osobnih ili financijskih podataka poput bankovnih podataka, koje potom mogu prodati ili koristiti za svoj osobni profit (Malwarebytes). Međutim, hvatači unosa podataka također imaju i legitimnu upotrebu, primjerice u tvrtkama u svrhu rješavanja problema koji mogu nastati na računalima koje koriste zaposlenici, zatim u svrhu poboljšanja korisničkog iskustva ili nadgledanje zaposlenika i njihovog provođenja vremena tijekom rada, organi za provođenje zakona i obavještajne službe također koriste evidenciju unosa podataka u svrhu nadzora (Swinhoe, 2018). Količina podataka koje hvatači unosa podataka mogu prikupljati može se razlikovati ovisno o kvaliteti njegovog dizajna. Najosnovnije vrste mogu prikupljati samo podatke upisane na jednom mrežnom mjestu ili u određenoj aplikaciji, a napredniji oblici mogu snimiti sve što korisnik upiše bez obzira na korištenu aplikaciju, uključujući i podatke koje korisnik kopira i zalijepi (Swinhoe, 2018). Neke inačice hvatača unosa podataka, a posebno one koje ciljaju na mobilne uređaje, bilježe i informacije poput telefonskih poziva (uključujući povijest poziva i zvučne zapise), informacije iz korisnikovih aplikacija za razmjenu poruka, GPS lokaciju, snimaju korisnički zaslon, pa čak i ulaz podataka kroz mikrofon i kameru (Swinhoe, 2018). Hvatači unosa podataka mogu biti programskog oblika (engl. *software-based*) ili sklopovskog oblika (engl. *hardware-based*) (Rouse, 2020). Sklopovski oblici hvatača unosa podataka se mogu jednostavno podmetnuti postavljanjem između priključka tipkovnice i njezinog priključka na računalu te tako bilježi sav unos podataka putem tipkovnice. Programski hvatači unosa podataka mogu biti cjelovite aplikacije ili alati koje korisnici svjesno koriste ili preuzimaju, ili pak zlonamjerni program koji zarazi računalo bez korisnikovog znanja. Podaci koje hvatači unosa podataka tako uspiju snimiti mogu se zatim poslati napadačima putem elektroničke pošte ili učitavanjem zapisničke datoteke (engl. *log file*) na unaprijed definirane mrežne stranice, baze podataka ili FTP poslužitelje. U nekim slučajevima, napadač se može i sam daljinski prijaviti na napadnuto računalo i sam preuzeti datoteke sa zapisima o tipkovničkim unosima.

Još jedna moguća prijetnja za računalne sustave je *rootkit*. *Rootkit* se definira kao zbirka računalnog softvera, tipično zlonamjernog, dizajnirana da omogući pristup računalu ili dijelu njegovog softvera kojem pristup inače nije dopušten i često prikriva njegovo postojanje ili postojanje drugih programa (Rouse, 2018). Pojam *rootkit* spoj je riječi engl. *root* što je naziv za pristup računalu s najvišim privilegijama i riječi engl. *kit* koja se odnosi na skup programskih

alata, a naziv *rootkit* se najčešće povezuje s zlonamjernim programima iako su prvotno *rootkiti* služili kao zbirka alata koji su omogućavali pristup računalu ili računalnoj mreži na administratorskoj razini (Veracode). Drugim riječima, *rootkit* je skup programa ili kôda koji omogućuje neotkrivenu prisutnost na računalu. Greg Hoglund i James Butler (2006) u svojoj knjizi navode da je većina tehnologija i trikova kojima se koristi *rootkit* dizajnirano za skrivanje kôda i podataka u sustavu, primjerice skrivanje datoteka i direktorija. Ostale značajke *rootkita* obično služe za udaljeni pristup i prisluškivanje, primjerice, za analiziranje (engl. *sniffing*) paketa s računalne mreže. Napominju da se *rootkiti* ne koriste uvijek u kriminalne svrhe. Organi za provođenje zakona često znaju upotrijebiti izraz *rootkit* pritom odnoseći se na njihov sankcionirani program za stvaranje stražnjeg ulaza u računalnom sustavu (engl. *backdoor*), primjerice instaliranog na nečije ciljano računalo (npr. osobno računalo neke sumnjive osobe) uz zakonsko dopuštenje države, često i putem sudskog naloga. Velike tvrtke pak često koriste *rootkitove* za nadzor i provođenje svojih regulacija oko korištenja poslovnih računala (Hoglund & Butler, 2006).

Rootkit omogućuje nekome da zauzme kontrolu nad računalom, a da korisnik odnosno vlasnik računala to ne primijeti, a jednom kada je *rootkit* instaliran na korisnikovo računalo, upravitelj *rootkita* ima mogućnost daljinskog izvršavanja naredbi i promjene konfiguracija sustava na računalu, može pristupiti zapisničkim datotekama (engl. *log file*) i pratiti upotrebu pravog vlasnika računala (Veracode). Dvije glavne vrste *rootkita* su *rootkit* na korisničkoj razini (engl. *user-mode*) i rootkit na razini jezgre sustava (engl. *kernel-mode*) (Kaspersky). *Rootkit* na korisničkoj razini je ona češća vrsta *rootkita* i dizajniran je tako da se pokreće u istom dijelu operacijskog sustava računala kao i normalne, sigurne korisničke aplikacije i programi. Svoje zlonamjerno ponašanje izvršavaju otmicanjem (engl. *hijacking*) aplikacijskih procesa koji se izvode na računalnom sustavu ili prepisivanjem memorije koju aplikacija ili program koristi. *Rootkit* na razini jezgre sustava pokreće se na najnižoj razini operacijskog sustava računala i napadaču daje najviši skup privilegija na računalu. Nakon instalacije *rootkita* na razini jezgre sustava napadač ima potpunu kontrolu kompromitiranog odnosno zaraženog računala i ima mogućnost vršiti bilo kakvu radnju na njemu. *Rootkit* na razini jezgre sustava su složeniji od *rootkita* na korisničkoj razini te su zato i rjeđi. Ovu vrstu *rootkita* je također i teže detektirati i ukloniti.

Rootkitove je često teško otkriti, a najčešće se zaraze *rootkitom* rješavaju programskim alatima za njihovo uklanjanje ili pak potpunom reinstalacijom računalnog sustava (McAfee). Ne postoje lako dostupni komercijalni proizvodi koji imaju mogućnost pronaći i ukloniti sve

poznate i nepoznate *rootkite*. Postoje različiti načini pretraživanja zaraženog računala u potrazi za *rootkitovima* (Petters, 2020). Metode otkrivanja *rootkita* uključuju metode detekcije temeljene na ponašanju, odnosno proučavanje odvija li se neko neobično ponašanje na računalnom sustavu, skeniranje digitalnih potpisa (engl. *signature scanning*) i analizu memorijskih ispisa (engl. *memory dump*). Često je jedina opcija za uklanjanje *rootkita* u potpunosti obnoviti odnosno reinstalirati ugroženi računalni sustav (Petters, 2020).

Računalni crv (engl. *computer worm*) je zlonamjeran program koji se reproducira širenjem na što veći broj računala putem računalnih mreža bez potrebe za ljudskom interakcijom, usporavajući mrežu i preopterećujući mrežne poslužitelje, što ga čini posebno opasnim za tvrtke i organizacije (Norton). Računalni crvi spadaju u najčešće vrste zlonamjernog softvera. Računalni crvi mogu sadržavati i dodatni sadržaj (engl. *payload*) koji oštećuje zaražena računala (Veracode). Ti dodatni sadržaji, odnosno *payloadi* su dijelovi kôda napisani za izvođenje dodatnih radnji na zaraženim računalima, osim širenja računalnih crva. Obično su dizajnirani za usputnu krađu podataka ili brisanje datoteka tijekom širenja zaraze računalnim crvom, neki čak stvaraju i stražnje ulaze (engl. *backdoor*) na napadnutim računalima koji omogućuju da ih daljinski kontroliraju druga računala, primjerice računalo napadača koji je stvorio računalnog crva. Tako kontrolirana računala se potom mogu koristiti u svrhu stvaranja mreže daljinski kontroliranih uređaja (engl. *botnet*) u razne zlonamjerne svrhe, poput širenja neželjene elektroničke pošte ili izvršavanje distribuiranog napada uskraćivanja usluge (engl. *Distributed Denial of Service - DDoS*) (Veracode). Najveći broj računalnih crva dizajniran je tako da znaju iskorištavati poznate sigurnosne propuste u računalnim programima i računalnim sustavima, iako se neki uspijevaju širiti i putem uspješno izvedenih prijevara lakovjernih korisnika na internetu, primjerice uz pomoć elektroničke pošte i usluga za izravno slanje poruka (engl. *Instant Messaging - IM*) moguće je izvršavati masovno slanje računalnih crva tako što se stavljaju u privitak tih elektroničkih poruka koje korisnici mogu preuzeti te tako uspješno počinju sa zarazom računalnog sustava korisnika. Još jedan popularan način širenja računalnih crva je putem mreža ravnopravnih korisnika (engl. *peer-to-peer - P2P*) tako što napadači na mrežu postavljaju datoteke s primamljujućim imenima kako bi naveli korisnike da ih preuzmu na svoja računala (Belcic, 2020). Nakon što tako uspješno zarazi računalni sustav, računalni crv može koruptirati datoteke, krasti osjetljive informacije, instalirati skriveni stražnji pristup računalu ili mijenjati postavke na računalnom sustavu kako bi ono bilo još ranjivije. Također, postojanje računalnog crva na računalnom sustavu može znatno usporiti performanse tog sustava pa čak i zagušiti i usporiti internetsku vezu (McAfee).

Trojan, odnosno Trojanski konj (engl. *Trojan horse*), je zlonamjerni program koji se pretvara da je bezopasan (poput nekog korisnog ili zabavnog sadržaja) kako bi prevario korisnika da ga preuzme na svoje računalo, dok zapravo korisnikovom računalu nanosi štetu, krade njegove podatke, remeti stabilnost sustava ili općenito nanosi neku drugu štetnu radnju nad korisnikovim podatcima ili računalnom mrežom (Norton). Trojani su svestrani i vrlo popularni među kibernetičkim kriminalcima, pa je teško navesti i savršeno okarakterizirati svaku vrstu. Usprkos tome, većina trojanskih programa dizajnirana je da preuzme kontrolu nad korisnikovim računalom, krade podatke, špijunira korisnike ili naknadno ubacuje više novih zlonamjernih programa na žrtvino računalo (Kaspersky Lab).

Prema tome, klasificirani su prema vrsti štete ili specifičnih radnji koje mogu izvoditi na zaraženom računalu (Kaspersky Lab, Norton): *Backdoor, Exploit, Rootkit, Trojan-Banker, Trojan-DDoS, Trojan-Downloader, Trojan-Dropper, Trojan-FakeAV, Trojan-GameThief, Trojan-Ransom, Trojan-SMS, Trojan-Spy, Trojan-Mailfinder, Trojan-IM*. *Backdoor* stvara stražnji ulaz (engl. *backdoor*) na zaraženom računalu te omogućuje zlonamjernim korisnicima daljinsku kontrolu nad računalom. *Exploit* su programi koji sadrže podatke ili kôd koji iskorištavaju ranjivost unutar aplikacija i programa koji se izvode na zaraženom računalu. *Rootkiti* su često dizajnirani da sakriju određene predmete ili aktivnosti u zaraženom sustavu kako bi se produljilo vrijeme djelovanja zloćudnih programa. *Trojan-Banker* su dizajnirani za krađu podataka sa žrtvinih računa za internetsko bankarstvo, sustave plaćanja preko interneta i kreditne ili debitne kartice. *Trojan-DDoS* provode DoS (engl. *Denial of Service*) napade na određenu mrežnu adresu tako što sa mreže zaraženih računala šalje velik broj zahtjeva na mrežni poslužitelj s ciljem zagušenja računalne mreže. *Trojan-Downloader* služe za preuzimanje i instalaciju novih inačica zlonamjernih programa na zaraženo računalo. *Trojan-Dropper* koriste se za instalaciju dodatnih trojana i/ili virusa na računala ili za sprječavanje otkrivanja zlonamjernih programa. *Trojan-FakeAV* simulira ponašanje antivirusnih programa u svrhu zavaravanja korisnika tako što će ga uvjeriti da na računalu ima velik broj zaraženih datoteka koje se jedino mogu ukloniti ako korisnik plati punu verziju (lažnog) antivirusnog programa. *Trojan-GameThief* služi za krađu podataka o korisničkim profilima u online igrama. *Trojan-Ransom* šifrira podatke na zaraženom računalu s ciljem da zatim korisniku brani pristup svojim vlastitim podatcima sve dok napadačima ne plati određenu svotu novca kao otkupninu. *Trojan-SMS* novčano oštećuje korisnika slanjem SMS poruka s njegovog uređaja prema skupim, često inozemnim brojevima. *Trojan-Spy* špijunira i prati korisnika tako što prati njegovu aktivnost na računalu, uključujući njegovo pisanje odnosno unos podataka putem

tipkovnice, popis pokrenutih i korištenih aplikacija te izradu snimki zaslona zaraženog računala. *Trojan-Mailfinder* traži pohranjene adrese elektroničke pošte na zaraženom računalu. *Trojan-IM* dizajniran je za krađu informacija o korisničkim računima i lozinkama za prijavu na programe za slanje izravnih poruka (engl. *instant messaging - IM*) kao što su WhatsApp, Viber, Telegram, Discord, ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype i mnogi drugi.

Trojanski programi nisu problem samo za prijenosna računala i stolna računala, već sve češće napadaju i mobilne uređaje, vrebajući korisnike na neslužbenim i piratskim tržištima aplikacija, mameći korisnike da ih preuzmu tako što se na tim mrežnim stranicama predstavljaju kao pravi odnosno legitimni programi (Malwarebytes). Često se korisnika dodatno pokušava navesti na preuzimanje aplikacije ili mobilne igre tako što mu se obećaje da je inačica programa koju ondje može preuzeti bolja od stvarne legitimne verzije te aplikacije nudeći mu primjerice neograničene resurse u mobilnoj igri koju korisnik želi preuzeti. Kada korisnik preuzme trojanski program pod krinkom mobilne igre ili aplikacije, često nije svjestan da je time zarazio svoj mobilni telefon zlonamjernim programom koji će ga potom ometati skočnim oglasima tijekom rada te u čestim slučajevima pratiti njegove radnje prilikom korištenja mobilnog uređaja uz pomoć skrivenog hvatača unosa podataka (engl. *keylogger*) kojem je cilj ukrasti korisnikove osjetljive informacije u razne zlonamjerne svrhe, a nerijetko ti trojanski programi potajice i terete mobilni račun korisnika slanjem SMS poruka skupim inozemnim brojevima te tako generiraju prihod za autora tog trojanskog programa, drugim riječima napadača odnosno kibernetičkog kriminalca (Malwarebytes).

Trojanski program za daljinski pristup (engl. *Remote Access Trojan - RAT*) zlonamjerni je program koji na zaraženom računalom stvara stražnji ulaz u računalni sustav s dodijeljenom administrativnom kontrolom nad njime (Rouse, 2019). Trojanski programi za daljinski pristup se obično slučajno preuzimaju uz neki korisnički program, poput video igre ili korisničke aplikacije, a ponekad se šalju u privitcima elektroničkih poruka. Jednom kada je računalni sustav na kojega se trojanski program za daljinski pristup preuzeo kompromitiran, napadač odnosno autor tog trojanskog programa ga može koristiti za distribuciju više trojanskih programa u svrhu stvaranja više daljinskih pristupa na drugim ranjivim računalima i tako uspostaviti odnosno stvoriti svoju mrežu daljinski kontroliranih uređaja (engl. *botnet*) (Rouse, 2019). Teško se otkrivaju jer se obično ne pojavljuju na popisima pokrenutih i pozadinskih programa i zadataka u upravitelju zadataka (engl. *task manager*). Radnje koje ovi trojanski programi izvode mogu biti slične običnim i sigurnim korisničkim programima. Osim toga, ovi

trojanski programi često kontroliraju svoju vlastitu razinu korištenja raspoloživih računalnih resursa kako se na računalnom sustavu ne bi dogodio pad radnih performansi računala i time upozorio korisnik da nešto nije u redu sa njegovim računalom, što bi ga potaklo na traženje i čišćenje zaraze na njegovom računalnom sustavu (DNSstuff). Trojanski program za udaljeni pristup ponekad zna biti kombiniran s hvatačem unosa podataka (engl. *keylogger*) i tako ima priliku prikupiti osjetljive korisničke podatke kao što su primjerice adresa elektroničke pošte, lozinke, podatci za elektroničku prijavu na račune banaka kojih je napadnuti korisnik klijent te informacije o njegovim kreditnim karticama (DNSstuff). Osim ovih podataka, trojanski programi za udaljeni pristup nekad imaju mogućnost i diskretno uključiti korisnikovu mrežnu kameru (engl. *webcam*) ili mikrofon, ili čak i pristupiti korisnikovim osjetljivim fotografijama, videozapisima i ostalim dokumentima. Trojanski programi za daljinski pristup mogu se koristiti i za specifično zlonamjerne ciljeve poput brisanja sadržaja tvrdih diskova (formatiranja diska), preuzimanja ilegalnih sadržaja ili se čak lažno predstavljati identitetom žrtve na internetu (Interpol).

Nadalje, virus infektor datoteka (engl. *file infector virus*) određena je vrsta virusa koja se obično veže za izvršni kôd programa, poput računalnih igara ili programa za obradu teksta, a nakon što zarazi datoteku, ima mogućnost proširiti se i na druge programe, pa ponekad čak i na druge računalne mreže koje koriste te zaražene datoteke i programe, ponekad i praveći usputnu štetu (Temporary Error). Neki infektori datoteka sadržavaju i dodatne namjere i mogućnosti (engl. *payload*) koji mogu biti vrlo destruktivni, poput formatiranja tvrdog diska ili brisanja datoteka, ili manje destruktivnih poput običnog prikazivanja poruka u skočnim prozorima (engl. *pop-up windows*) (Trend Micro). Znači, uloga infektora datoteka je zaraziti datoteke i programe na korisnikovom računalu, pri čemu usputno može nanositi i značajnu štetu. Nakon pokretanja programa koji je oštećen infektorom datoteka, virus duplicira zlonamjerni kôd i primjenjuje ga na druge izvršne programe na računalu (Trend Micro). Često se spremaju u radnu memoriju računala, što znači da nakon pokretanja i izvršavanja svog kôda ostaju aktivni u radnoj memoriji računala i tako imaju priliku i mogućnost zaraziti još više drugih programa i datoteka. Najčešće datoteke koje su najosjetljivije i najpodložnije na ovu vrstu zaraze su izvršne datoteke s datotečnim nastavkom (engl. *file extension*) .exe (kratica za engl. *executable* - hrv. izvršne datoteke) i s datotečnim nastavkom .com (kratica za engl. *command* - hrv. naredba), iako i druge izvršne datoteke drugih datotečnih nastavaka također mogu biti podložne zarazi ovim virusom (Spamlaws).

Ucjenjivački zlonamjerni programi (engl. *ransomware*) su zlonamjerni programi koji korisnicima priječe pristup njihovom vlastitom računalnom sustavu ili osobnim datotekama ili programima te zauzvrat zahtijevaju plaćanje otkupnine u zamjenu za vraćanje pristupa zaključanim datotekama ili računalnom sustavu (Kaspersky). Prvi oblici ucjenjivačkih zlonamjernih programa stvoreni su kasnih 1980-ih godina, kada je radi tehnoloških ograničenosti bilo potrebno plaćanje otkupnine vršiti običnom poštom (engl. *snail mail*) (Chesti, Humayun, Sama, & Jhanjhi, 2020). Danas ucjenjivački zlonamjerni programi napadnutim korisnicima naređuju da plaćanje vrše putem određenih kriptovaluta (engl. *cryptocurrency*) ili svoje kreditne kartice (Malwarebytes). Kibernetičkim kriminalcima je u interesu svojim ucjenjivačkim zlonamjernim programima zaraziti što više računalnih sustava na što široj geografskoj lokaciji, a to postižu koristeći se više različitih metoda širenja zaraze. Primjerice, jedan od najčešćih metoda širenja ucjenjivačkih zlonamjernih programa je putem neželjene elektroničke pošte (engl. *spam*) čiji sadržaj krije razne pokušaje *phishinga* kako bi se primatelj elektroničke poruke prevario i uvjerio da slučajno preuzme zlonamjeran program, a kada se ta preuzeta varljiva datoteka zatim pokrene na računalu, započinje izvršavanje zlonamjernog kôda programa kojem je daljnja namjera potpuno preuzeti kontrolu nad korisnikovim računalnim sustavom tako što će enkriptirati odnosno zaključati pristup njegovim podatcima (Fruhlinger, 2020). Nakon što se ta enkripcija podataka na korisnikovom računalu izvrši, ujedno se i sprječava njegov normalan rad, tako što pri ovom koraku ucjenjivački program korisniku prikazuje poruku koja ga obavještava da su njegove datoteke odnosno njegov računalni sustav enkriptirani i zahtijeva plaćanje određene novčane naknade, drugim riječima otkupnine u zamjenu za ključ za dešifriranje koji će osloboditi korisnikovo računalo i njegove podatke te mu dozvoliti da nastavi s normalnim korištenjem svog računala. Ta se poruka u najviše slučajeva prikazuje pri prvom sljedećem pokretanju računalnog operacijskog sustava nakon što se ono zarazi ucjenjivačkim programom (Kaspersky).

Tijekom posljednjih nekoliko godina zabilježen je značajan porast broja uspješnih napada ucjenjivačkim zlonamjernim programima na organizacije. Morgan (2016) je za Cybercrime Magazine predviđao da će šteta prouzrokovana ucjenjivačkim programima prouzročiti globalnu štetu od 5 milijardi američkih dolara u 2017. godini, u usporedbi sa globalnom štetom od 325 milijuna američkih dolara u 2015. godini, što pokazuje zabrinjavajuće povećanje broja napada od čak 15 puta u samo dvije godine. Također se predviđalo da će globalna šteta za 2018. dosegnuti 8 milijardi američkih dolara, a za 2019. ta brojka iznosi 11,5 milijardi američkih dolara. Najnovije predviđanje je da će globalni troškovi

štete od napada ucjenjivačkim programima doseći 20 milijardi američkih dolara do 2021. godine, što je čak vrtoglavih 57 puta više nego što je bilo 2015. godine (Morgan, 2020). Posljedice napada ucjenjivačkim programima na poduzeća i organizacije imaju daleko širi utjecaj od samih troškova za plaćanje otkupnine u zamjenu za otključavanje računalnog sustava ili njegovih datoteka. U njihovim slučajevima, tvrtke trpe troškove povezane s gubitkom podataka, smanjenom produktivnošću, forenzičkim istragama, obnavljanjem podataka i računalnog sustava, izgubljenim prihodom i oštećenom reputacijom (Morgan, 2020).

Primjerice, Palmer (2017) za ZDNet izvještava o napadu na Reckitt Benckiser, vodeću svjetsku tvrtku za zdravstvenu i potrošačku robu, koja je obavijestila javnost da će zabilježiti smanjenje prihoda od 2% u drugom tromjesečju te godine zbog utjecaja nedavnog napada ucjenjivačkog programa Petya na tvrtkinu sposobnost fakturiranja i isporuke proizvoda svojim kupcima. Još jedan relativno nedavni poznati širokodosežni napad ucjenjivačkim programima bio je napad programom WannaCry koji je dostigao svoju "slavu" u svibnju 2017. godine kada je prijavljeno čak 400,000 njime zahvaćenih računala širom svijeta (Goode, 2017). Značajno su pogođene i javne i privatne organizacije, uključujući i britansku Nacionalnu zdravstvenu službu (engl. *National Health Service - NHS*), španjolsku telekomunikacijsku tvrtku Telefónica te nekoliko ruskih banaka (Goode, 2017). Srećom, stručnjaci za sigurnost uspjeli su zaustaviti rapidno širenje zaraze tako što su otkrili zaustavni prekidač (engl. *killswitch*) u tom ucjenjivačkom programu te je napad zaustavljen u roku od nekoliko dana. WannaCry se širio i bio uspješan u svoj napadu radi poznate sigurnosne ranjivosti u sustavu Windows (Checkpoint).

Nadalje, napad programom NotPetya, koji je drugačija inačica Petya ucjenjivačkog programa, brzo je uslijedio nakon napada WannaCry programom u lipnju 2017. te se prvi put se pojavio u Ukrajini (Brandom, 2017). Bio je distribuiran kao PDF datoteka u privitku elektroničke poruke, a za svoje širenje koristio je istu ranjivost operacijskog sustava koju je koristio WannaCry, pritom znatno utječući na rad javnih i privatnih organizacija diljem svijeta. Nagađalo se da je razlog ovog napada više bio kako bi uzrokovao poremećaje u Ukrajini nego radi financijske dobiti (Brandom, 2017).

Zastrašivajući program (engl. *scareware*) je vrsta zlonamjernog programa koji je dizajniran kako bi manipulirao korisnike i uvjerio ih da trebaju preuzeti ili kupiti zlonamjerni, ponekad beskorisni program kako bi se riješio neki lažni problem na njihovom računalu (Forcepoint). Za te svrhe često se koristi skočnim reklamama čiji sadržaj tvrdi da korisnikov računalni sustav treba hitno skenirati i popraviti ili očistiti od virusa, a najčešće koristi apsurdno

visoke brojke kako bi dodatno uplašio korisnika da je situacija na njegovom računalu stvarno toliko loša (Kaspersky). Ciljevi zastrašivajućih programa variraju od prodaje beskorisnih, lažnih antivirusnih alata do instalacije štetnih zlonamjernog programa sa svrhom krađe osjetljivih podataka, ili pak financijske dobiti jer se korisnika navodi da kupi program (Rafter, 2020). Postoje primjeri situacija u kojima zastrašivajući programi navode korisnika da slučajno instalira ucjenjivačke programe (engl. *ransomware*) koji na računalnom sustavu potom čine dodatnu štetu zaključavanjem pristupa korisničkim datotekama sve dok korisnik za njih ne plati otkupninu (Forcepoint). Najlakši načini za prepoznavanje zastrašivajućih programa je obraćanje pažnje na izgled tih reklama, primjerice je li sadržaj reklame namjerno napisan da zvuči zastrašujuće, upozorava li reklama na brzo djelovanje, je li reklame teško zatvoriti, zvuči li naziv poduzeća koje prodaje taj program poznato ili je potpuno nepoznata organizacija, također ako program glumi da skenira sustav i velikom brzinom navodi velik broj grešaka ili prijetnji, velike su šanse da je u pitanju zastrašivajući program (Rafter, 2020). Razlog zašto su ovi pokazivači toliko pouzdani za prepoznavanje zastrašivajućih programa je zato što stvarni proizvođači antivirusnih programa ne koriste takve taktike kako bi privukli korisnike, ali razlog zašto su zastrašivajući programi toliko uspješni je zato što su kibernetički kriminalci svjesni da to mnogi temeljni korisnici to ne znaju.

Špijunski program (engl. *spyware*) je zlonamjeran program koji se instalira na računalo, a zatim krade osjetljive podatke o korištenju računala, aplikacija i interneta te ostale informacije koje napadač smatra korisnima za svoje namjere (The Economic Times). Špijunski programi se smatraju vrstom zlonamjernih programa jer prate korisnikovo računalo, često bez njegovog znanja, prikupljajući korisnikove osobne podatke i slanjem istih oglašivačima, tvrtkama ili vanjskim korisnicima (Norton). Osim navedenog, koristi se i u druge svrhe, poput prodaje podataka o žrtvinim korisničkim navikama na internetu, krađe podataka o korisnikovoj kreditnoj kartici ili bankovnom računu te čak i krađe njegovog osobnog identiteta, praćenja podataka za prijavu na različite usluge i lozinki, i ostale osjetljive podatke (Norton). Špijunske programe često može biti teško otkriti, ali u najviše slučajeva prva naznaka koju korisnik ima da je računalni uređaj zaražen špijunskim programom je primjetno smanjenje brzine rada računalnog sustava ili računalne mreže (The Economic Times), a u slučaju mobilnih uređaja vidljiva je povećana potrošnja internetskog prometa i primjetno skraćeno trajanje baterije mobilnog telefona (TechSafety). Špijunski programi uglavnom se klasificiraju u reklamne programe (engl. *adware*), kolačiće za praćenje (engl. *tracking cookies*), pratitelje sustava (engl. *system monitoring*) i trojanske programe (Norton). Najčešća metoda instalacije špijunskih

programa na korisnikovo računalo je putem besplatnih programa u obliku neke skrivene komponente. Jedna od najopasnijih dodanih funkcija špijunskih programa su hvatači unosa podataka (engl. *keylogger*), kojeg špijunski program koristi za snimanje svih korisnikovih unosa preko tipkovnice, što može biti vrlo štetno ako korisnik negdje upiše svoju lozinku, podatke o kreditnoj kartici ili ostale osjetljive informacije (The Economic Times). Korisnik može slučajno dobiti špijunski program neopreznim ponašanjem, posebice ako zbog neredovitog ažuriranja operacijskog sustava na računalu nastanu sigurnosne ranjivosti, također ako radi manjka edukacije o sigurnom ponašanju na internetu korisnik povjeruje zavaravajućem marketingu koji bi ga mogao navesti na posjećivanje zlonamjernih stranica čiji je cilj instalacija zlonamjernih programa, uključujući špijunskih programa, na njegovo računalo, zatim lakovjernost u sadržaj elektroničkih poruka s nepoznatih adresa koje su najvjerojatnije pokušaj *phishinga*, te na kraju instalacija manje poznatih ili lažnih programa na svoje računalo koji bi u stvarnosti mogli zapravo biti trojanski programi koji mogu naknadno preuzeti špijunski program na korisnikovo računalo (Malwarebytes).

Reklamni programi (engl. *adware*) su programi koji služe za prikazivanje neželjenih oglasa na korisnikovom računalu, a obično će prikazivati korisniku skočne oglase (engl. *pop-up advertisements*), mijenjati početnu stranicu internetskog preglednika, potajice instalirati špijunske programe na računalo ili jednostavno zagušivati računalo oglasima te time remetiti normalan rad na računalu (Kaspersky Labs). Iako se reklamni programi sami po sebi ne klasificiraju pod viruse jer u nekim slučajevima nisu jednako zlonamjerni kao drugi primjeri zlonamjernih programa, činjenica je da ne samo da postojanje reklamnog programa na uređaju može biti naporno za korisnika prilikom svakog korištenja računala, već može uzrokovati i dugoročne probleme na pogođenom uređaju. Osim toga, razina zlonamjernosti reklamnog programa ovisi o njegovom tvorcu i njegovim namjerama (Gorrie, 2020). Kako bi se izbjegle zaraze reklamnim programima, korisnici bi trebali biti oprezni prilikom preuzimanja programa i aplikacija putem interneta, zatim bi trebali pročitati ugovor s krajnjim korisnikom (engl. *end-user license agreement*) prije preuzimanja i instalacije besplatnih programa kako bi saznali hoće li se u zamjenu za besplatno korištenje tog programa na računalu prikupljati korisnikove informacije, nadalje potrebno je koristiti zaštitu za blokiranje skočnih prozora i skočnih reklama (engl. *pop-up ad blocker*) kako bi se unaprijed spriječilo otvaranje neočekivanih i neželjenih prozora i reklama te je naravno poželjno izbjegavati klikanje na oglase koji se ne prikazuju na pouzdanom mrežnom mjestu (Rouse, 2017).

3.2. Ostale vrste napada

Phishing je zločin zavaravanja ljudi kako bi ih se prijevarom uvjerilo u dijeljenje osjetljivih podataka poput lozinki, računa za elektroničku poštu, brojeva kreditnih kartica, brojeve telefona, broj socijalnog osiguranja (engl. *Social Security Number - SSN*), kućnu adresu, žrtvino ime i prezime i druge osobne podatke (Porter, 2020). Naziv phishing potječe od engleskog prijevoda riječi "pecanje" (engl. *fishing*, a slovo f zamijenjeno je sa ph kao odavanje počasti prijašnjoj metodi hakiranja javnih telefona za besplatne pozive zvano *phreaking*), aludirajući na metodu pripreme i postavljanja zamke, odnosno "mamca" te se napadač oslanja na vjerojatnost da će bar jedna žrtva "zagristi" i povjerovati lažnoj poruci i tako nesvjesno odati svoje osjetljive podatke napadačima (Kay, 2004). Žrtve najčešće primaju zlonamjernu elektroničku poštu (također zvanu engl. *malspam*, od riječi engl. *malicious* - hrv. zlonamjerno i engl. *spam* - neželjena poruka; engl. *malspam* - hrv. zlonamjerna neželjena poruka) ili tekstualnu poruku (SMS) koja oponaša neku osobu, organizaciju ili tvrtku kojoj žrtva vjeruje, poput suradnika, banke ili vladinog ureda s ciljem prijevare korisnika ili širenja zlonamjernih programa (Malwarebytes). Porter (2020) za Norton navodi primjer *phishinga* slanjem elektroničkih poruka u kojem se napadač predstavlja kao korisnikova banka. Kada žrtva otvori tu elektroničku poštu ili tekst, pronalaze poruku napisanu s namjerom da čitatelja zastraši, primjerice tvrdeći da će bankovni račun korisnika biti ugašen radi neaktivnosti osim ako ne unesu svoje podatke na mrežnoj stranici kojoj mogu pristupiti preko poveznice koja se nalazi u toj poruci. Korisnik će, u nedostatku bolje prosudbe, pratiti upute u dobivenoj poruci te kao rezultat nesvjesno unijeti svoje podatke na lažnu mrežnu stranicu koja je dizajnirana kako bi što uvjerljivije izgledala kao primjerice mrežna stranica korisnikove banke kako bi korisniku dala lažan osjećaj sigurnosti. Sadržaj zlonamjernih neželjenih poruka uvijek je osmišljen s namjerom zastrašivanja koje treba prevladati žrtvinu bolju prosudbu ispunjavajući je strahom (Malwarebytes). Postoji još jedna specifična metoda *phishinga*, zvana *spear phishing*, koja je sve češći oblik krađe osjetljivih podataka na način da se napadač koristi informacijama o određenoj meti napada, poput privatne ili javne osobe (primjerice direktora neke tvrtke, političara, i sličnih osoba), tvrtke ili organizacije te se u elektroničkoj poruci obraća toj određenoj osobi, kako bi svoj napad učinio specifičnim, čak i više "osobnim" (Sjouwerman, 2019).

Iduća vrsta prijetnje je obiranje podataka. Obiranje podataka (engl. *skimming*) je metoda koju kradljivci identiteta koriste kako bi uspjeli "dohvatiti" žrtvine novčane transakcije te tako doći do osobnih informacija žrtve uz pomoć informacija na njezinoj kreditnoj kartici

(Kagan, 2020). Kriminalci se koriste raznim pristupima kako bi uspjeli dobaviti podatke s kreditnih kartica, a najnapredniji pristup uključuje korištenje obirača podataka (engl. *skimmer*), malog uređaja koji čita podatke pohranjene u magnetskoj traci ili mikročipu kreditne kartice koji se može instalirati na samoposlužne benzinske pumpe, POS aparate ili bankomate te tako prikupljati podatke s kreditnih kartica prateći transakcije koje se tamo provode (Identity Theft Resource Center). Neki obirači podataka mogu sadržavati i osjetilnu plohu (engl. *touchpad*) koja lopovu omogućuje unos sigurnosnog koda. Obirači podataka instalirani na bankomatima ponekad mogu imati i kamere ili dodatne preklopne osjetilne plohe koji potom služe za snimanje osobnih identifikacijskih brojeva (engl. *Personal Identification number - PIN*) korisnika tih bankomata te zbog toga banke često korisnicima napominju da prekriju tipkovnicu kada u bankomat upisuju osobni identifikacijski broj (PIN) svoje kreditne kartice (Kagan, 2020).

Mreža daljinski kontroliranih uređaja (engl. *botnet*, od riječi engl. *robot* i engl. *network* - hrv. mreža) je skup uređaja povezanih s internetom, što može uključivati osobna računala, mrežne poslužitelje, mobilne uređaje i internet stvari (engl. *Internet of Things - IoT*) koji su zaraženi određenom vrstom zlonamjernog programa koji njima upravlja. To se obično događa putem preuzimanja podmetnutih zlonamjernih programa sa mrežnih stranica ili zavaravanja korisnika na instalaciju trojanskog konja na računalo (Kaspersky Lab). Nakon što se program preuzme, mreža daljinski kontroliranih uređaja će kontaktirati svoje glavno odnosno središnje računalo operacije i obavijestiti ga da je sve spremno za planirani rad. Korisnikovo osobno računalo, telefon ili tablet je tada u potpunosti pod nadzorom napadača koji je stvorio mrežu daljinski kontroliranih uređaja (Norton). Vlasnici *botneta* mogu istovremeno imati pristup nekoliko tisuća računala i mogu im zapovijedati da izvršavaju zlonamjerne aktivnosti dobivanjem pristupa tim uređajima korištenjem posebnih trojanskih virusa za napad na sigurnosne sustave računala, prije nego što implementiraju softver namijenjen za zapovijedanje i kontrolu kako bi omogućili daljnje zlonamjerno djelovanje (Kaspersky Lab). Ovi se koraci mogu automatizirati kako bi se potencijalno potaknulo što više istovremenih napada. Organizatori napada, najčešće kibernetički kriminalci, daljinski upravljaju zaraženim uređajima i koriste ih za određene radnje, pazeći pritom da zlonamjerne radnje ostaju skrivene za korisnika. Mreže daljinski kontroliranih uređaja se obično koriste za slanje neželjene elektroničke pošte, sudjelovanje u kampanjama klik prijevara (engl. *click fraud campaigns*) - vlasnicima mrežnih stranica koje objavljuju oglase plaća se novčani iznos koji se određuje prema tome koliko posjetitelja mrežnog mjesta klikne na oglase (tzv. plaćanje po kliku - engl.

pay-per-click, PPC) (Akamai). Prijevara nastaje kada osoba, automatizirana skripta ili računalni program oponaša legitimnog korisnika mrežnog preglednika klikom na takav oglas bez stvarnog zanimanja za sadržaj tog oglasa) i generiranje zlonamjernog prometa za distribuirane napade uskraćivanja usluge (engl. *Distributed Denial of Service, DDoS*). U drugim slučajevima, kibernetički kriminalci će prodati pristup svojoj mreži daljinski kontroliranih uređaja tako da drugi kibernetički kriminalci mogu koristiti tu mrežu za svoje vlastite zlonamjerne aktivnosti, poput pokretanja kampanje slanja neželjene elektroničke pošte (Cloudflare).

Distribuirani napad uskraćivanja usluge (engl. *Distributed Denial of Service, DDoS*) je zlonamjerni mrežni napad prilikom kojeg kibernetički kriminalci koriste velik broj uređaja povezanih s internetom kako bi slali mrežne zahtjeve nekom mrežnom poslužitelju koji pruža mrežne usluge ili mrežne aplikacije koje kibernetički kriminalci žele onesposobiti preplavljujući ga lažnih prometom ili zahtjevima (Hulme, 2020). DDoS napadi se mogu izvršavati iz osvete, u svrhu haktivizma, ili pak iz čiste zabave, a mogu rezultirati manjim smetnjama u radu mrežne usluge ali i nekim težim posljedicama koje bi poduzeće moglo dugoročno oštetiti (primjerice smanjeno povjerenje kupaca, narušena reputacija, pad vrijednosti dionica i slično). Primjer jednog od najvećih provedenih DDoS napada do sad je napad na mrežnu uslugu GitHub u veljači 2018. godine (Petters, 2020). Tijekom dvadesetak minuta trajanja napada GitHubovi mrežni poslužitelji bili su zagušeni istovremenim zahtjevima koji su dostigli čak 1.35 terabita po sekundi, kasnije je promet dosegao 400 gigabita po sekundi (Ranger, 2018). Ovaj napad bio je zabilježen kao najveći DDoS napad u povijesti sve dok NETSCOUT Arbor nije u ožujku 2018. godine, doslovno mjesec dana nakon prethodno postavljenog rekorda za volumen DDoS napada, potvrdio da je uspio ublažiti DDoS napad od čak 1.7 terabita po sekundi kojem je meta bio jedan od američkih davatelja usluga, kojeg NETSCOUT Arbor nije otkrio (Morales, 2018). Najnoviji pak DDoS napad izvršen je u veljači 2020. godine sa 2.3 terabita po sekundi. Meta DDoS napada bio je Amazon, čija je usluga AWS Shield uspjela ublažiti taj napad (Cimpanu, 2020). Postoji više vrsta DDoS napada, a oni su napad aplikacijskog sloja, protokolarni napad i volumetrijski napad (Petters, 2020). Cilj napada aplikacijskog sloja (engl. *Application Layer Attack*) je iscrpiti resurse napadnute mrežne stranice ili mrežne usluge slanjem kompleksnih zahtjeva na mrežni poslužitelj mete napada, koji se potom preoptereti pristižućim zahtjevima i uspori s radom ili čak potpuno sruši. Tijekom protokolarnog napada (engl. *Protocol Attack*) napada se mrežni sloj ciljanog sustava, s ciljem preopterećenja i onesposobljavanja osnovnih mrežnih usluga, vatrozida, ili uravnoteživača

opterećenja koji šalje zahtjeve poslužitelju. Volumetrijski napad (engl. *Volumetric Attack*) koristi mreže daljinski kontroliranih računala (engl. *botnet*) kako bi stvorio i slao velike količine prometa prema ciljanom mrežnom serveru te ga time usporio ili onesposobio.

SQL injekcija (engl. *SQL injection*) je napad kojim se umeće (odnosno "ubrizgava") SQL upit putem obrazaca za unos podataka (Rouse, 2019). Uspješno korištenje SQL injekcija napadaču može omogućiti čitanje osjetljivih informacija iz baze podataka, mijenjanje podataka baze podataka putem naredbi kao što su INSERT (hrv. umetanje), UPDATE (hrv. ažuriranje) ili DELETE (hrv. brisanje), izvršavanje administrativnih radnji nad bazom podataka poput isključivanja sustava za upravljanje bazom podataka (engl. *database management system* - DBMS), oporavljanje sadržaja neke datoteke prisutne u datoteci sustava za upravljanje bazom podataka (DBMS) te izdavanje naredbi operacijskom sustavu (OWASP). Pravilno izvršena SQL injekcija može omogućiti pregled i krađu intelektualnog vlasništva tvrtke ili organizacije, osobne podatke kupaca, administrativne vjerodajnice ili privatne detalje o poslovanju (Rouse, 2019). SQL injekcija obično se događa kada se od korisnika zatraži unos nekih podataka, poput korisničkog imena, a korisnik umjesto korisničkog imena upisuje SQL izraz koji će se pokrenuti u bazi podataka bez znanja vlasnika te baze podataka (PortSwigger). Primjerice, ako neka mrežna stranica ili aplikacija traži od korisnika da se u nju prijavi sa korisničkim imenom i lozinkom, neki zlonamjerni napadač bi mogao poželjeti doći do tablice s podacima o svim korisnicima ili svim njihovim lozinkama. Kako bi uspio u tom naumu, napadač će pokušati te podatke dobiti korištenjem SQL injekcije. Ako mrežna stranica odnosno aplikacija nema zaštitu protiv SQL injekcija, ona je pod velikim rizikom od krađe podataka (Veracode). Primjerice, baza podataka neke aplikacije korisničke prijave autentificira sljedećom SQL naredbom (w3schools):

```
SELECT * FROM users WHERE username='username_val' AND password='password_val';
```

gdje username_val i password_val označavaju korisničko ime i lozinku korisnika. Ako korisnik kao korisničko ime upiše "john" a kao lozinku "123", SQL naredba će izgledati ovako:

```
SELECT * FROM users WHERE username='john' AND password='123';
```

Ali ako napadač odluči na ovoj aplikaciji izvršiti SQL injekciju, umjesto normalnog korisničkog imena i lozinke mogao bi upisati unos kao što je:

```
' OR 'x'='x
```

u kojem slučaju SQL naredba će izgledati ovako:

```
SELECT * FROM users WHERE username='' OR 'x'='x' AND password=''
OR 'x'='x';
```

Ova naredba je prihvatljiv SQL izraz i pošto dio naredbe koji kaže WHERE 'x'='x' je uvijek istinit, naredba će napadaču vratiti sve redove iz tablice Users. Gledajući ovaj primjer, očito je da bi uz pomoć mnogih drugih naredbi napadači mogli doći do velikog broja osjetljivih podataka i iskoristiti ih u zlonamjerne svrhe (TutorialRepublic). Kako bi se poduzeća i organizacije zaštitili od napada SQL injekcijama, potrebno je redovito ažurirati svoje sustave za upravljanje bazama podataka (DBMS), provoditi načelo najmanjih privilegija (engl. *principle of least privilege, PoLP*) (odnosno, svaki korisnički račun ima samo dovoljno pristupa za obavljanje svog posla i ništa više od toga) te zapošljavati kompetentne i iskusne programere (Malwarebytes).

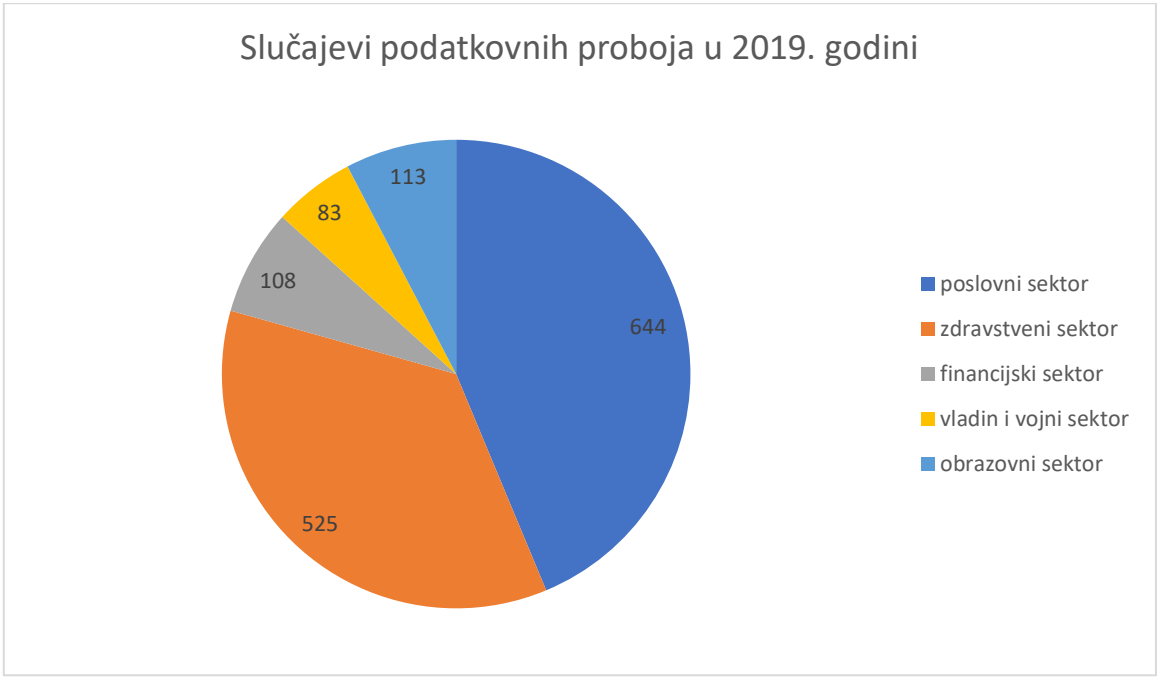
3.3. Statistike podatkovnih proboja u 2019. i prvoj polovici 2020. godine

Iako softver postupno postaje sve sigurniji i programeri osmišljaju nove pristupe računalnoj sigurnosti, napadači postaju sve spretniji i bolje opremljeni. A kako svijet sve više ovisi o digitalnim uslugama i pohrani te prema tome ima i rastuću potrebu za većom međusobnom povezanošću, nastaje sve više slabosti, rupa u sigurnosti i ostalih rizika koje napadači iskorištavaju kako bi dobili pristup najosjetljivijim informacijama. Primjerice, slučajevi podatkovnih proboja (engl. *data breach*) postali su učestali u Sjedinjenim Američkim Državama (Identity Theft Resource Center, 2019). Resursni centar za krađu identiteta (engl. *Identity Theft Resource Center*, ITRC) podatkovne proboje definira kao incident u kojem je nečije pojedinačno ime, broj socijalnog osiguranja (engl. *Social Security Number*, SSN), broj vozačke dozvole, zdravstveni karton odnosno povijest bolesti, financijski podaci (uključujući kreditne i debitne kartice) potencijalno izloženo riziku od krađe ili zloupotrebe tih podataka, bilo elektronički (digitalno, primjerice u web trgovinama) ili analogno (primjerice papirnatim putem poput fizičke pošte) (Identity Theft Resource Center, 2019). Općenito se ovi podatkovni proboji sastoje od otkrivanja korisničkih imena, e-adresa i lozinki, bez nužnog uključivanja osjetljivih osobnih podataka. Resursni centar za krađu identiteta objavljuje godišnja izvješća o dokumentiranim slučajevima podatkovnih proboja tijekom protekle godine te u tim izvješćima navodi broj kibernetičkih napada po sektoru i ukupno, broj kompromitiranih (primjerice neovlašteno pristupljenih, ukradenih, oštećenih ili obrisanih) podataka, popis poduzeća koja su

imala incident vezan za kibernetičke napade u protekloj godini te metode korištene prilikom tih kibernetičkih napada.

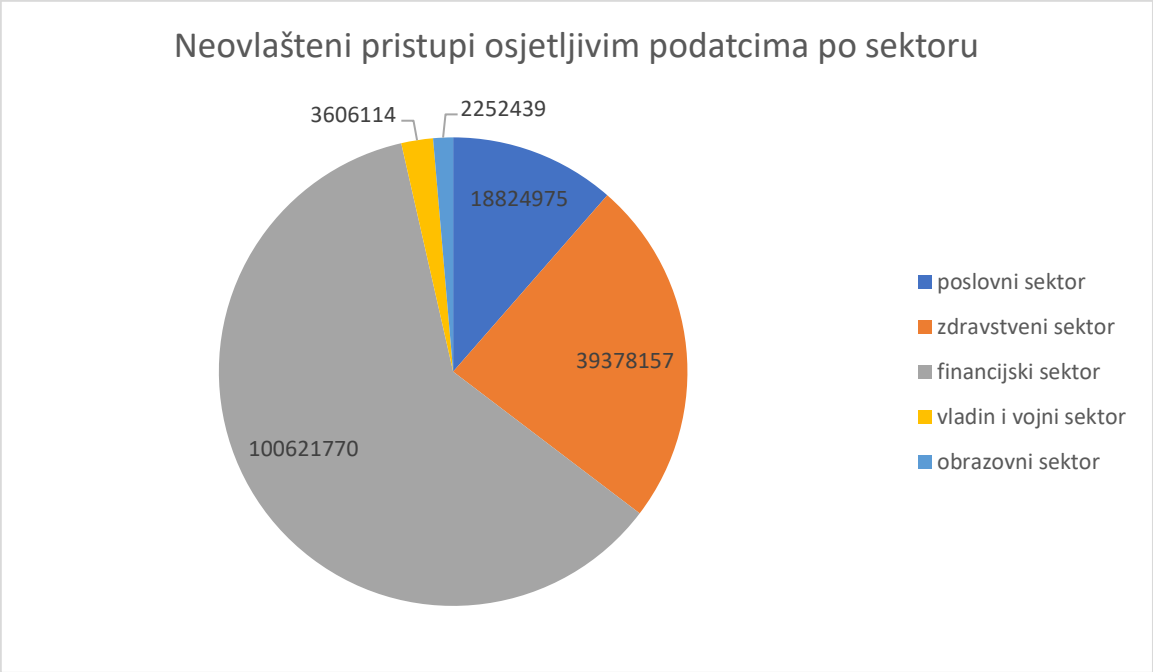
Prema istraživanju Resursnog centra za krađu identiteta (ITRC) o kibernetičkim napadima tijekom 2019. godine, te godine zabilježeno je 1,473 slučajeva podatkovnih proboja, što je rezultiralo neovlaštenim pristupom 164,683,455 osjetljivih podataka te 705,174,054 ostalih podataka, sveukupno kroz nekoliko različitih sektora. Detaljno o tome pišu u svom godišnjem izvještaju *End-of-Year Data Breach Report 2019* (Identity Theft Resource Center, 2019).

U istraživanju se zabilježilo 644 slučaja podatkovnih proboja u poslovnom sektoru, 525 slučajeva u zdravstvenom sektoru, 108 slučajeva u financijskom sektoru, 83 slučaja u vladinom i vojnom sektoru te 113 slučaja u obrazovnom sektoru.



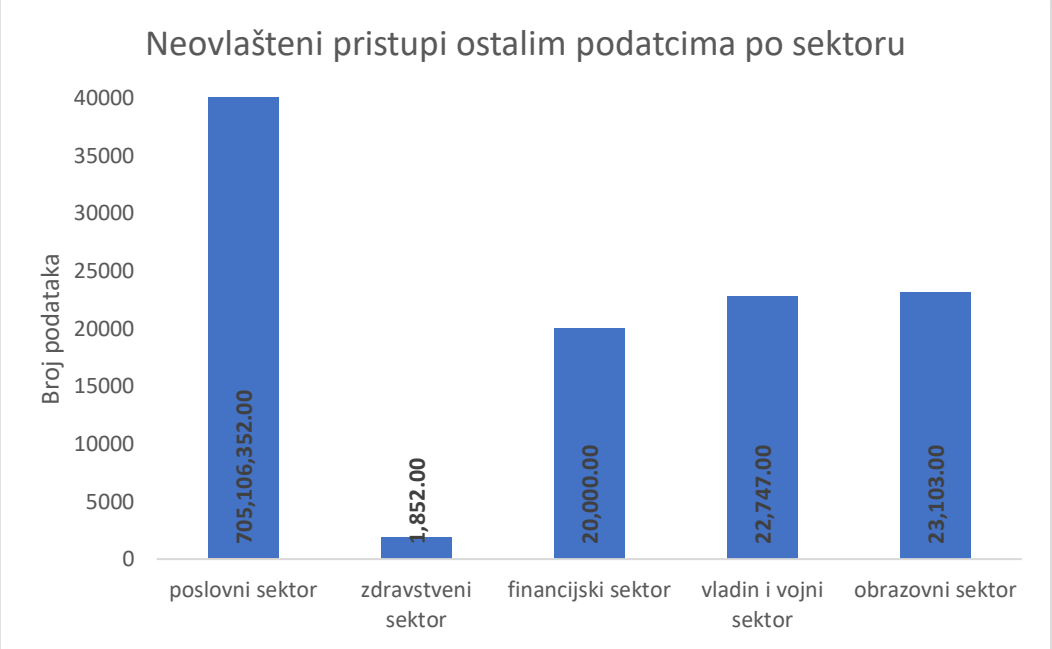
Grafikon 1: Slučajevi podatkovnih proboja u 2019. godini

Tijekom tih podatkovnih proboja, ostvaren je neovlašten pristup 18,824,975 osjetljivih podataka u poslovnom sektoru, 39,378,157 osjetljivih podataka u zdravstvenom sektoru, 100,621,770 osjetljivih podataka u financijskom sektoru, 3,606,114 osjetljivih podataka u vladinom i vojnom sektoru te 2,252,439 osjetljivih podataka u obrazovnom sektoru.



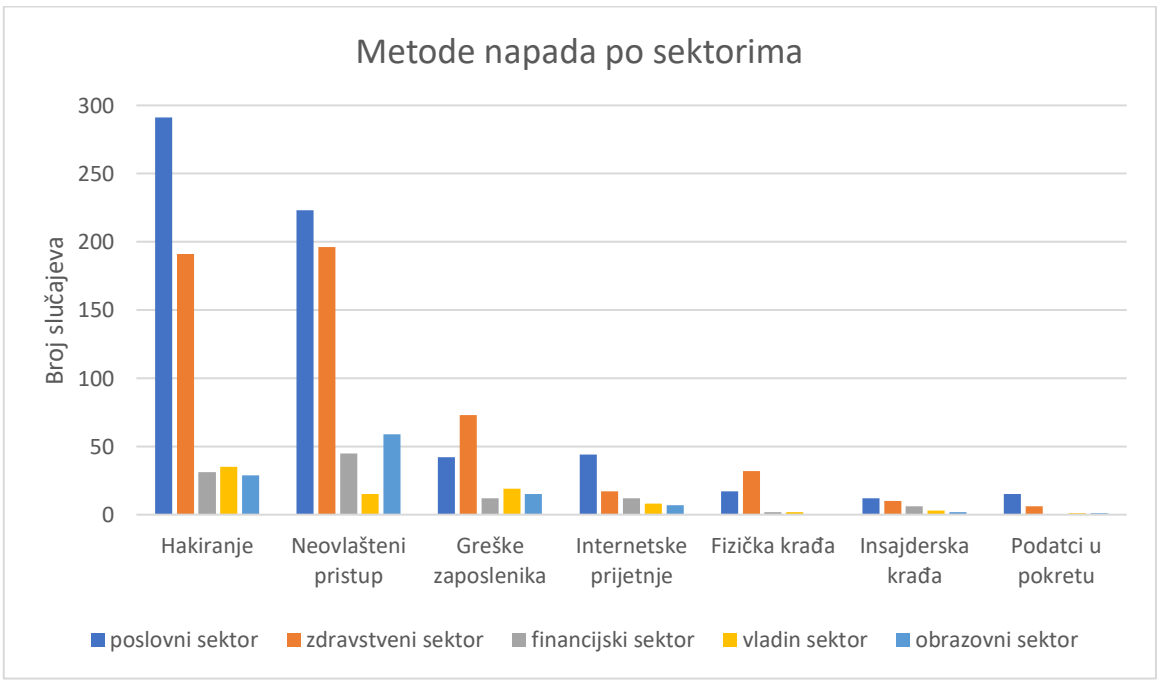
Grafikon 2: Neovlašteni pristupi osjetljivim podatcima po sektoru

Nadalje, u statistici se navode i neovlašteni pristupi ostalim podatcima, pa je tako zabilježen neovlašten pristup 705,106,352 podataka u poslovnom sektoru, 1,852 podataka u zdravstvenom sektoru, 20,000 podataka u financijskom sektoru, 22,747 u vladinom i vojnom sektoru te 23,103 u obrazovnom sektoru.



Grafikon 3: Neovlašteni pristupi ostalim podatcima po sektoru

Što se tiče metoda korištenih za izvršavanje ovih kibernetičkih napada 2019. godine, Resursni centar za krađu identiteta u svojoj statistici za metode kibernetičkih napada u 2019. godini navodi nekoliko različitih metoda kibernetičkih napada ili razloge za njihove uspješne provedbe te njihov zabilježeni broj slučajeva po navedenim sektorima (Identity Theft Resource Center, 2019):



Grafikon 4: Metode napada po sektorima

Hakiranje, uključujući *phishing*, *ransomware*, zloćudne programe i *skimming*, sa zabilježenih 291 slučajem u poslovnom sektoru, 191 slučajem u zdravstvenom sektoru, 31 slučajem u financijskom sektoru, 35 slučajeva u vladinom sektoru te 29 slučajeva u obrazovnom sektoru, što ukupno donosi brojku od 577 zabilježenih slučajeva kibernetičkih napada metodom hakiranja.

Neovlašteni pristup, sa zabilježenih 223 slučaja u poslovnom sektoru, 196 slučajeva u zdravstvenom sektoru, 45 slučajeva u financijskom sektoru, 15 slučajeva u vladinom sektoru te 59 slučajeva u obrazovnom sektoru, što ukupno donosi brojku od 538 zabilježenih slučajeva kibernetičkih napada koji su rezultirali omogućenim neovlaštenim pristupom osjetljivim i ostalim podacima.

Greške ili nemar od strane zaposlenika, nepravilno raspolaganje podacima ili njihovo nepravilno uklanjanje te gubitak podataka uzrokovano lošom politikom tvrtke ili greškom zaposlenika, sa zabilježenih 42 slučaja u poslovnom sektoru, 73 slučaja u zdravstvenom sektoru, 12 slučajeva u financijskom sektoru, 19 slučajeva u vladinom sektoru te 15 slučajeva u obrazovnom sektoru, što ukupno donosi brojku od 161 zabilježenih slučajeva kibernetičkih napada koji su bili uzrokovani nemarom ili greškama u poslovanju ili radu.

Slučajna izloženost prijetnjama putem interneta, sa zabilježenih 44 slučaja u poslovnom sektoru, 17 slučajeva u zdravstvenom sektoru, 12 slučajeva u financijskom sektoru, 8 slučajeva u vladinom sektoru te 7 slučajeva u obrazovnom sektoru, što ukupno donosi brojku od 88 zabilježenih slučajeva kibernetičkih napada koji su bili uzrokovani slučajnim stvaranjem ranjivosti neopreznim korištenjem interneta.

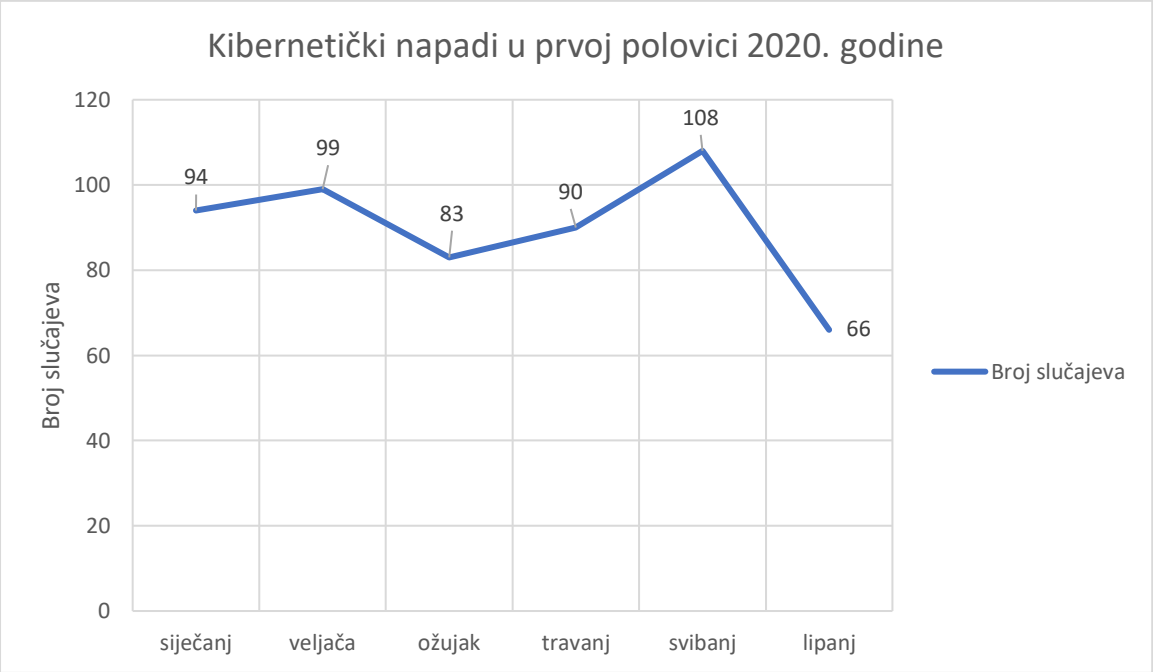
Fizička krađa podataka ili dokumenata, sa zabilježenih 17 slučajeva u poslovnom sektoru, 32 slučaja u zdravstvenom sektoru, 2 slučaja u financijskom sektoru, 2 slučaja u vladinom sektoru te nasreću niti jedan slučaj u obrazovnom sektoru, što ukupno donosi brojku od 53 zabilježena slučaja kibernetičkih napada koji su bili uzrokovani fizičkom krađom podataka ili dokumenata koji su omogućili kasnije napade ili sami po sebi bili dovoljno vrijedni podaci da naknadan napad nije bio potreban.

Insajderska krađa, odnosno krađa iznutra, sa zabilježenih 12 slučajeva u poslovnom sektoru, 10 slučajeva u zdravstvenom sektoru, 6 slučajeva u financijskom sektoru, 3 slučaja u vladinom sektoru te 2 slučaja u obrazovnom sektoru, što ukupno donosi brojku od 33 zabilježena slučaja kibernetičkih napada koji su bili uzrokovani krađom podataka ili dokumenata unutar same

tvrtke ili organizacije putem insajdera koji su time omogućili kasnije napade ili sami po sebi bili dovoljno vrijedni podaci da naknadan napad nije bio potreban.

Podaci u pokretu, sa zabilježenih 15 slučajeva u poslovnom sektoru, 6 slučajeva u zdravstvenom sektoru, niti jedan slučaj u financijskom sektoru, 1 slučajem u vladinom sektoru te 1 slučajem u obrazovnom sektoru, što ukupno donosi brojku od 23 zabilježena slučaja kibernetičkih napada koji su bili uzrokovani krađom podataka ili dokumenata iskorištavanjem ranjivosti mogućnosti pristupa i kretanja podataka neovisno o mjestu pristupa tim podacima (primjerice slanje važnih dokumenata putem elektroničke pošte, pohrana podataka na oblak sa lošim sustavom zaštite, i sl.).

Resursni centar za krađu identiteta je također objavio izvještaj o kibernetičkim napadima u prvoj polovici 2020. godine, u kojem navodi da se do 30. lipnja 2020., dogodilo 540 prijavljenih podatkovnih proboja, koji su utjecali na 163,551,023 individualna korisnika. Detaljno o tome pišu u svom godišnjem izvještaju *2020 First Half Report* (Identity Theft Resource Center, 2020).



Grafikon 5: Kibernetički napadi u prvoj polovici 2020. godine

Tijekom siječnja 2020., zabilježeno je 94 slučaja podatkovnih proboja koji su utjecali na 1,248,643 individualna korisnika.

Tijekom veljače 2020., zabilježeno je 99 slučaja podatkovnih proboja koji su utjecali na 122,717,723 individualna korisnika.

Tijekom ožujka 2020., zabilježeno je 83 slučaja podatkovnih proboja koji su utjecali na 7,249,555 individualnih korisnika.

Tijekom travnja 2020., zabilježeno je 90 slučaja podatkovnih proboja koji su utjecali na 24,956,140 individualnih korisnika.

Tijekom svibnja 2020., zabilježeno je 108 slučaja podatkovnih proboja koji su utjecali na 7,262,475 individualnih korisnika.

Tijekom lipnja 2020., zabilježeno je 66 slučaja podatkovnih proboja koji su utjecali na 163,551,023 individualna korisnika.

Ova analiza pokazuje pad broja podatkovnih proboja za 33 posto u odnosu na prvu polovicu 2019. godine (811), a broj oštećenih individualnih korisnika pao je za 66 posto u odnosu na isti vremenski period u 2019. godini (493,011,910). Predviđa se da će ukupan broj podatkovnih proboja u 2020. godini biti oko 1080, a da će ukupan broj oštećenih individualnih korisnika iznositi oko 327,102,046.

Resursni centar za krađu identiteta (ITRC) napominje da unatoč padajućem trendu koji je dobra vijest za potrošače i tvrtke, emocionalni i financijski utjecaj podatkovnih proboja i dalje ima veliki značaj jer potencijalno može potpuno promijeniti nečiji život, osobito tijekom trenutne pandemije virusa COVID-19, jer su kibernetički kriminalci prepoznali priliku i pojačali su pokušaje *phishing* prijevara i ostalih prijevara (Identity Theft Resource Center, 2020).

4. Obrana od kibernetičkih napada

Tvrtke raznih veličina još uvijek imaju uvjerenje da je samo dovoljno razviti strategiju za kibernetičku sigurnost i da je njezino postojanje te provođenje ispravnih poslovnih i sigurnosnih politika cjelovit odgovor na obranu i zaštitu od kibernetičkog kriminala (Grimes, 2017). Međutim, stvarnost je takva da je najčešće potrebno mnogo više za postizanje snažne zaštite protiv kibernetičkih napada u današnjem ranjivom digitalnom okruženju. Dapače, prema nedavnom istraživanju vlade Ujedinjenog Kraljevstva o probojima u kibernetičke sigurnosne sustave 2020., gotovo polovica britanskih poduzeća (46%) prijavila je podatkovni proboj ili druge napade u posljednjih 12 mjeseci (Johns, 2020). Neki se podatkovni proboji lako mogu izbjeći, ali se oni često uspješno infiltriraju u računalne sustave i mreže zbog nedostatka znanja o računalnoj sigurnosti unutar poduzeća. Da bi postigle optimalnu razinu kibernetičke sigurnosti, tvrtke moraju osigurati ispravnu poslovnu politiku o primjeni sigurnosnih postupaka prilikom rada s računalnim i mrežnim sustavima te obrade podataka (Johns, 2020). Unatoč tome što se u obranu računalnih sustava poduzeća od napada ulaže mnogo resursa velik broj poduzeća i organizacija ipak ne provodi adekvatnu procjenu rizika od kibernetičkih napada ili pak nepravilno usklađuje mjere obrane s obzirom na prijetnje koje bi potencijalno mogle predstavljati najveći rizik za računalne sustave i mreže tog poduzeća ili organizacije (Grimes, 2017).

Rastući i konstantno mijenjajući broj sigurnosnih prijetnji na internetu dodatno otežava pravilno suočavanje s rizikom i prepoznavanje razine prijetnje koju one predstavljaju te to može dovesti do loših ili samo djelomičnih odnosno neučinkovitih primjena sigurnosnih pravila tijekom rada na računalnim sustavima i mrežama u tom poduzeću ili organizaciji (Grimes, 2017). Bitno je biti svjestan činjenice da je računalne sustave danas lako napasti ako oni na sebi imaju neredovito ažurirane programe. Iako se najprije ovdje govorilo o neažuriranim operacijskim sustavima, u novije vrijeme kibernetički kriminalci pronalaze načine za iskorištavanje sigurnosnih propusta i u ostalim programima i aplikacijama koje se mogu instalirati na računalo ili neki uređaj, primjerice internetski preglednici (Grimes, 2017). Messier (2019) napominje da "sama tehnologija ne može pružiti zaštitu, već je važno i mjesto na kojem se nalazi te odluke koje se temelje na idejama o obrani sustava u dubinu i širinu" (Messier, 2019, str 50). Drugim riječima, nije dovoljno samo isplanirati i implementirati plan za zaštitu računalnih sustava i mreža, potrebno je i osmisliti adekvatna sigurnosna pravila i poslovne politike poduzeća koja se neće samo odnositi na same računalne sustave i programske

pakete za zaštitu od zlonamjernih programa i kibernetičkih napada, već je potrebno i provesti adekvatnu edukaciju zaposlenika poduzeća i korisnika njihovih usluga.

4.1. Penetracijsko testiranje

Penetracijski test (engl. *penetration test* ili *pen test*) je vrsta etičkog hakiranja, odnosno autoriziranog kibernetičkog napada na neki računalni sustav s ciljem procjene sigurnosti tog računalnog sustava (Rouse, 2018). Pomaže u pronalaženju i prepoznavanju sigurnosnih propusta aplikacija, programa, računalne mreže i operativnog sustava. Ako penetracijski test uspije pronaći slabosti računalnog sustava prije nego što to uspiju kibernetički kriminalci, poduzeće ili organizacija koja je platila provođenje penetracijskog testa moći će isplanirati i učinkovito provesti obrambene strategije kako bi zaštitilo svoje najvažnije računalne sustave i podatke (Rouse, 2018). Penetracijski test je metoda kojom se prepoznaju sve slabosti i propuste koji bi mogli ugroziti sigurnost računalnog sustava, primjerice neotkrivene ili nezakrpljene ranjivosti u operacijskim sustavima, aplikacijama i ugrađenih programa (engl. *firmware*), loše konfigurirani poslužitelji, mreže, aplikacije, ugrađeni programi i operativni sustavi, logički manjci mrežnih aplikacija, primjerice konfiguracija cijena i upravljanja korisnicima (PGI). Penetracijska testiranja provode sigurnosni stručnjaci, bilo na daljinu ili na licu mjesta. Kada se napokon utvrde slabosti i nedostaci računalnih sustava i računalnih mreža poduzeća ili organizacije, preporuča se konzultacija sa savjetnicima za sigurnost kako bi se pravilno pojačale mjere obrane od kibernetičkih napada (PGI).

Postoji više vrsta penetracijskih testova (Cloudflare): penetracijsko testiranje principom "otvorene kutije", penetracijsko testiranje principom "zatvorene kutije", prikriveno penetracijsko testiranje, vanjsko penetracijsko testiranje i unutarnje penetracijsko testiranje. Penetracijsko testiranje principom "otvorene kutije" (engl. *Open-box pen test*) podrazumijeva davanje nekoliko informacija o računalnoj sigurnosti poduzeća unajmljenom etičkom hakeru prije početka samog testiranja. Penetracijsko testiranje principom "zatvorene kutije" (engl. *Closed-box pen test*), također je poznato kao jednostruko slijepo testiranje, zato što u ovoj varijanti penetracijsko testiranja etičkom hakeru poduzeće ne šalje unaprijed nikakve informacije o računalnoj sigurnosti poduzeća. Prikriveno penetracijsko testiranje (engl. *Covert pen test*), također je poznato kao dvostruko slijepo testiranje, jer u ovoj vrsti penetracijskog testiranja o provedbi testiranja se ne obavještava niti jedan djelatnik poduzeća koje unajmljuje penetracijsko testiranje, čak se ne obavještavaju ni informatički i sigurnosni stručnjaci

poduzeća čiji je posao reagirati na kibernetičke napade uključujući napad uzrokovan ovim testiranjem. Što se tiče ovog načina penetracijskog testiranja i činjenice da ga nije svjestan niti jedan djelatnik poduzeća, od unajmljenog etičkog hakera zahtijeva se napismeno iznesen potpuni plan i opseg napada odnosno penetracijsko testiranja, kako bi se izbjegle moguće komplikacije ili problemi sa zakonom. Vanjsko penetracijsko testiranje (engl. *External pen test*) podrazumijeva napad u kojem unajmljeni etički haker targetira "vanjski" dio poslovanja poduzeća, poput mrežnih stranica ili vanjskih mrežnih poslužitelja. Kod nekih dogovora za ovu vrstu testiranja, unajmljenom etičkom hakeru se ne dozvoljava ulaz u zgradu poduzeća, već se od njega očekuje da kibernetički napad odnosno testiranje slabosti i nedostataka računalnih sustava i računalnih mreža poduzeća provede s neke udaljene lokacije ili iz vozila parkiranog u blizini zgrade poduzeća. Unutarnje penetracijsko testiranje (engl. *Internal pen test*) je vrsta penetracijskog testiranja koju unajmljeni etički haker izvršava unutar računalne mreže tvrtke. Razlog za provođenje ove vrste testiranja je određivanje količine potencijalne štete koju bi mogao počiniti neki ljutiti zaposlenik koji bi se možda odlučio na kibernetički napad na poduzeće iz želje za osvetom. Prilikom unutarnjih penetracijskih testiranja, provode se provjere sigurnosti i pouzdanosti specifičnih sustava, pravila i tehnologija koje poduzeće ili organizacija koristi u svom poslovanju te ta provjera sadržava i nekoliko metoda testiranja. Testiranje se provodi putem privatne lokalne mreže unutar poduzeća, što znači da se prilikom ovog testiranja provjeravaju mrežne aplikacije i usluge na intranetu poduzeća. Ovo testiranje također podrazumijeva da unajmljeni etički haker ne zna pristupne informacije potrebne za spajanje na lokalnu mrežu poduzeća.

Unutarnje penetracijsko testiranje tako provjerava sigurnosti više mrežnih aplikacija (Funk, 2019): testiranje *proxy* poslužitelja, testiranje filtera za neželjenu poštu, testiranje vatrozida, testiranje sigurnosnih slabosti, testiranje enkripcije certifikata, testiranje internetskih kolačića, testiranje obrazaca za kontakt poduzeća, testiranje otvorenih portova, testiranje stranice za prijavu u mrežnu aplikaciju, testiranje poruka o greškama, testiranje HTTP metoda, testiranje korisničkih imena i lozinki, skeniranje podataka, testiranje SQL injekcija, XSS testiranje, testiranje dopuštenja pristupa, testiranje korisničkih sesija, testiranje napada na silu, testiranje protiv napada uskraćivanjem usluge, te testiranje pristupa datotečnim direktorijima.

Proxy poslužitelji igraju bitnu ulogu u kontroli priljeva korisnika koji koriste mrežne aplikacije poduzeća te također služe za prepoznavanje mogućih zlonamjernih aktivnosti (Funk, 2019). Znači, poželjno je da se poduzeće pobrine da su njihovi *proxy* poslužitelji kvalitetni i učinkoviti u svom radu, a u te svrhe sigurnosni stručnjaci poduzeća mogu koristiti različite

alate kao što su Burp Proxy, TemperIE, WebscarabTemper Data ili OWSAP ZAP (Balaji, 2020). Nadalje, testiranje filtera za neželjenu poštu, koji skreće pozornost na važnost pravilnog rada filtera za neželjenu poštu (Funk, 2019). Provjerava se filtrira li se pravilno pristigla i izlazna elektronička pošta te jesu li ti filtri pravilno implementirani (BreachLock). Pravilan rad filtera za elektroničku poštu važniji je nego na prvi pogled jer je neželjena pošta jedna od najpopularnijih metoda pokušaja brojnih vrsta kibernetičkih napada (BizTech). Testira se i vatrozid mreže, jer korištenje vatrozida i njegova pravilna konfiguracija neizostavan je dio računalne i mrežne sigurnosti općenito, a time pogotovo u poduzećima koja su česta meta pokušaja kibernetičkih napada (Funk, 2019). Pravilno konfigurirani vatrozid i njegove sigurnosne postavke će uspješno obraniti računalne sustave poduzeća od nadolazećih pokušaja prodiranja u sustav (Funk, 2019). Prilikom testiranja sigurnosnih slabosti provjeravaju se različiti aspekti mrežnih aplikacija poduzeća kao što su primjerice mrežni poslužitelji i mrežni uređaji, te se stvara popis sigurnosnih propusta i slabosti te rizika koji oni predstavljaju (Funk, 2019). Sigurnosni propusti mogu se nalaziti u poslužiteljima, bazama podataka, mrežnim aplikacijama i slično (BreachLock). Testiranjem enkripcije certifikata provjerava se jesu li sva pohranjena korisnička imena i lozinke enkriptirani i šalju li se putem sigurnih "HTTPS" protokola u svrhu sprječavanja incidenata u kojima bi hakeri mogli doći do ovih informacija putem kibernetičkih napada (Funk, 2019). Potrebno je testirati i internetske kolačiće. Internetski kolačići služe za spremanje informacija o korisničkim sesijama na mrežnim aplikacijama, pa je očito da su oni prilično osjetljivi podatci koji bi mogli ugroziti sigurnost korisnika mrežnih aplikacija poduzeća dospiju li te informacije u ruke kibernetičkih kriminalaca (Funk, 2019). Radi toga je poželjno da se poduzeće pobrine da internetske kolačiće sprema na sigurno mjesto i da su oni enkriptirani jer ne bi bilo poželjno da se ovakve informacije otkriju nekim kibernetičkim kriminalcima (BreachLock). Bitno je testirati i obrasce za kontakt poduzeća, pošto postojanje obrazaca koje korisnici mogu ispuniti kako bi kontaktirali poduzeće predstavlja prilično visok rizik da bi neki korisnici mogli kroz njega slati neželjenu poštu, bitno je da poduzeće osigura pravilno programiranje tih obrazaca kako bi oni mogli pravilno razlikovati pokušaje slanja neželjene pošte i legitimne upite korisnika (Funk, 2019). Jedan od najjednostavnijih načina za provedbu ove sigurnosne mjere je implementacija CAPTCHA testova (BreachLock). Također se provodi i testiranje otvorenih portova. Postojanje otvorenih portova na mrežnom poslužitelju koji pruža usluge mrežnih aplikacija poduzeća također predstavljaju visok rizik od izloženosti kibernetičkim napadima (Funk, 2019). Zbog toga je od iznimne važnosti osigurati nepostojanje otvorenih portova na mrežnom poslužitelju poduzeća, odnosno koristiti samo portove nužne za mrežnu aplikaciju poduzeća ili

bi u protivnom bili izloženi riziku od napada (BreachLock). Zatim, testiranje stranice za prijavu u mrežnu aplikaciju jedna je od korisnih metoda osiguranja protiv neovlaštene provale u mrežnu aplikaciju je zaključavanje pristupa nakon nekoliko neuspješnih pokušaja autentifikacije korisnika te se poduzeća potiču da implementiraju bar ovaj jednostavni oblik zaštite svoje mrežne aplikacije (Funk, 2019). Nadalje, testiraju se i poruke o greškama. Cilj ovog testiranja je osiguravanje da greške koje mrežna aplikacija prikazuje ne odaje problem korisnicima u previše detalja (Funk, 2019): primjerice, dovoljno je reći "neuspjela autentifikacija" umjesto "krivo korisničko ime" ili "netočna lozinka", jer bi netko sa zlonamjernim planovima mogao iskoristiti ovaj propust kako bi uspio provaliti u mrežnu aplikaciju ili sustav. Prilikom testiranja HTTP metoda bitno je provjeriti kojim HTTP metodama mrežna aplikacija poduzeća komunicira s korisnicima, primjerice sigurnosni stručnjaci poduzeća trebali bi se pobrinuti da metode poput PUT i DELETE nisu omogućene jer bi ih u protivnom napadači mogli iskoristiti u zle namjere (Funk, 2019). Potrebno je i testiranje korisničkih imena i lozinki. Mrežne aplikacije poduzeća trebale bi se automatski pobrinuti za to da korisnici imaju korisnička imena koja se ne mogu lako pogoditi i da koriste sigurne i kompleksne lozinke, a u protivnom bi aplikacija trebala upozoriti korisnika da prejednostavnim lozinkama stavlja u rizik osjetljive informacije sa svog korisničkog profila (Funk, 2019). Zatim se provodi skeniranje podataka. Svi podatci i datoteke moraju biti skenirani prije učitavanja istih na mrežni poslužitelj ili aplikaciju (BreachLock). U protivnom se javlja rizik od nastanka zaraze zlonamjernim programima koji bi mogli oštetiti poslovanje poduzeća i smanjiti povjerenje korisnika. Važno je i testiranje SQL injekcija. SQL injekcije su popularna metoda prodiranja u mrežne aplikacije te bi iz tog razloga poduzeće trebalo osigurati visok stupanj sigurnosti svoje baze podataka kako ona ne bi bila ranjiva na pokušaje napada SQL injekcijama (Funk, 2019). Provodi se i XSS testiranje jer mrežna aplikacija poduzeća također mora biti otporna na skriptiranje i XSS napade (Funk, 2019). Zatim se testira dopuštenje pristupa. Poduzeće bi se trebalo pobrinuti da korisnici imaju pristupe samo onim dijelovima mrežne aplikacije kojima bi trebali imati pristup, i ničemu više (Funk, 2019). Ako korisnici imaju pristup svim datotekama na poslužitelju, napadači bi imali jednostavan pristup osjetljivim informacijama poduzeća (BreachLock). Iduće testiranje je testiranje korisničkih sesija. Važno je pobrinuti se da korisnička sesija stvarno završi onog trenutka kada se korisnik odjavi iz mrežne aplikacije (Funk, 2019). U suprotnom, napadači bi mogli iskoristiti sesije koje su još u trajanju kako bi postigli razne zlonamjerne radnje, poput pregledavanja datoteka kojima taj korisnik ima dozvoljen pristup (BreachLock). Testiranje napada na silu pomaže spriječiti napade na silu (engl. *brute force attack*), koji su napadi u kojima napadač pokušava

unijeti velik broj lozinki ili korisničkih imena s nadom da će eventualno uspjeti upasti u mrežnu aplikaciju ili sustav (Funk, 2019). Poduzeća su dužna osigurati se protiv ovih pokušaja provale tako što će testirati pokušaje upada na silu i zatim isplanirati obranu u slučaju da neki napadač stvarno pokuša provaliti u mrežnu aplikaciju ili sustav na ovaj način. Prilično važno je i testiranje protiv napada uskraćivanjem usluge. Napadi uskraćivanjem usluge (engl. *Denial of Service - DoS*) opterećuju mrežni poslužitelj slanjem većeg broja zahtjeva nego što on može podnijeti što rezultira rušenjem sustava mrežnog poslužitelja (BizTech). Korištenjem pravilnih alata za testiranje poduzeća se mogu osigurati da njihova mrežna aplikacija ili poslužitelj ostanu sigurni u slučaju napada uskraćivanjem usluge (Balaji, 2019). Testiranje pristupa datotečnim direktorijima provjerava da korisnici nemaju pristup datotečnim direktorijima na mrežnom poslužitelju jer bi u protivnom napadači mogli doći do osjetljivih ili povjerljivih podataka na njemu (Funk, 2019).

Nakon što završi penetracijske testove, unajmljeni etički haker se konzultira s sigurnosnim stručnjacima poduzeća i govori im koje je sve sigurnosne propuste uspio pronaći. Te se informacije potom mogu koristiti za provedbu sigurnosnih nadogradnji kako bi se uklonile sve ranjivosti otkrivene tijekom penetracijskih testova (Cloudflare).

4.2. Korištenje sigurnosnih tehnologija

Poduzeće koje je svjesno svih rizika kojima bi moglo biti podložno tijekom mrežnog poslovanja mora se pobrinuti da isplanira sigurnosne standarde i educira svoje zaposlenike o sigurnosnim postupcima i općenito sigurnom ponašanju prilikom korištenja mrežnih servisa i interneta (Honigman, 2015). Važnost toga posebice je velika za poduzeća koja osim svojih poslovnih podataka na svojim mrežnim poslužiteljima pohranjuju i osjetljive podatke svojih korisnika jer bi u slučaju kibernetičkog napada mnogobrojne privatne informacije mogle biti ukradene i iskorištene u zlonamjerne svrhe. Ali bez obzira na tu činjenicu poduzeća različitih veličina, a pogotovo mala poduzeća, česta su meta kibernetičkih napada radi loše implementiranih ili čak nepostojećih sigurnosnih politika za obranu od kibernetičkih napada (Honigman, 2015).

Kako bi se zaštitila od kibernetičkih napada različitih vrsta, poduzeća bi morala osigurati bar neke navedene osnovne mjere sigurnosti u svojem poslovanju (Popat, 2018). Popat (2018) navodi da je jedan od najosnovnijih načina zaštite osjetljivih poslovnih podataka provedba zaštite računalne opreme i računalnih sustava u poduzeću implementacijom

kompleksnih lozinki koje će znati samo korisnici tog računala ili profila, a sve djelatnike poduzeća ili korisnike usluga savjetovati da radije upamte lozinku umjesto da je zapisuju na papir ili tekstualne datoteke na koje bi bilo tko mogao naići. Osim toga, zaposlenici bi trebali proći osnovnu edukaciju o sigurnom korištenju interneta i opasnostima koje potencijalno predstavljaju neželjene elektroničke pošte, kako bi se spriječio bilo koji budući pokušaj *phishinga* na kojeg bi zaposlenici mogli nasjesti. Također, instalacija programa za geolokacijski pronalazak izgubljenog uređaja korisna je za pronalazak uređaja, računala, laptopa ili mobitela u slučaju fizičke krađe. Nadalje, enkripcija važnih i osjetljivih podataka, uključujući i podatke korisnika mrežnih usluga poduzeća, može osigurati da ti podaci ne budu ugroženi čak i ako dođe do kibernetičkog napada na mrežne sustave ili usluge poduzeća. Stvaranje sigurnosnih kopija koje će se pohranjivati na drugim lokacijama pak može uvelike pomoći poduzeću u slučaju kibernetičkih napada koji su rezultirali gubitkom podataka ili u slučaju napada ucjenjivačkim programima (engl. *ransomware*), kako bi poduzeće uvijek bilo korak ispred kibernetičkih kriminalaca. Sljedovno, poduzeća bi trebala za svaki slučaj osigurati podatke tako da se u slučaju proboja podataka financijska šteta može bar do neke mjere ublažiti (Popat, 2018).

Djelatnici poduzeća ipak su samo ljudi, i kao takvi podložni su ljudskim greškama koje bi mogle dovesti poduzeće u rizik od kibernetičkih napada. Rješenje za ovaj problem nije otpuštanje djelatnika sa slabijim poznavanjem računalne sigurnosti, već edukacija djelatnika o sigurnom korištenju interneta i njegovih usluga. Enkripcija elektroničkih poruka i ostalih komunikacija stvara dodatni sloj zaštite za kojeg bi kibernetički kriminalci trebali zaobilaziti tijekom napada i trošiti više resursa prilikom pokušaja probijanja te zaštite (Honigman, 2015). Što se tiče elektroničkih poruka koje pristižu od izvora izvan poduzeća, djelatnici moraju znati prepoznati sumnjive poruke koje predstavljaju mogući pokušaj *phishinga*. Prepoznavanje nekih očitih pokazatelja da se radi o varljivoj poruci, poput sumnjivih ili nepoznatih adresa elektroničke pošte, priloženih dokumenata koje primatelj nije tražio ni od koga, velikog broja gramatičkih grešaka u tijelu poruke koji mogu indicirati na pokušaj prevare (prevaranti često nisu ni materinji govornici jezika u kojemu je poruka pa koriste internetske prevoditelje kako bi mogli slati poruke u više različitih zemalja svijeta), a u slučaju da djelatnik i preuzme priloženu datoteku ili klikne na sumnjivi link, bitno je da računalo ima adekvatnu antivirusnu zaštitu, vatrozid i redovito ažurirani operacijski sustav kako bi se smanji rizik od zaraze, odnosno uopće zaustavio pokušaj pokretanja zlonamjernog programa na računalu (Honigman, 2015).

5. Zaključak

Računalna sigurnost podrazumijeva zaštitu računalnih sustava, podataka pohranjenih na njima te osjetljivih informacija od oštećenja, krađe i neovlaštenog pristupa prouzrokovanih kibernetičkim napadima. Kibernetički napadi podrazumijevaju korištenje računala i mrežnih uređaja u protuzakonite svrhe poput krađe podataka probijanjem u računalne sustave, krađe identiteta, prevare korisnika na internetu putem phishing spletki, organiziranja masovnih DDoS napada, i slično. Pošto poduzeća i organizacije, kao i društvo općenito, uvelike ovise o modernim tehnologijama i internetu za potrebe svog poslovanja, potrebno je unaprijed isplanirati zaštitu računalnih sustava i mreža poduzeća kako bi se smanjio rizik od gubitka ili kompromitiranja osjetljivih poslovnih ili korisničkih informacija. Računalni sustavi i mrežne usluge poduzeća i organizacija nalaze se pod najvećim rizikom od kibernetičkih napada, a napadaju se zbog financijske dobiti, krađe osobnih podataka ili stvaranja mreža daljinski kontroliranih uređaja (engl. *botnet*) u svrhu napadanja neke druge mete u obliku DDoS napada. Resursni centar za krađu identiteta (ITRC) godišnje objavljuje rezultate statističkih analiza broja prijavljenih slučajeva podatkovnih proboja. Njihova statistika za 2019. godinu pokazala je da se tijekom te godine dogodilo čak 1,473 prijavljenih slučajeva podatkovnih proboja u poslovnom, financijskom zdravstvenom, vladinom i obrazovnom sektoru. Tijekom prve polovice 2020. godine prijavljeno je 540 slučajeva podatkovnih proboja, a do kraja 2020. godine se predviđa oko 1080 mogućih slučajeva podatkovnih proboja. Osim podatkovnih proboja, velik sigurnosni rizik poduzeću predstavljaju i mnogobrojni oblici zlonamjernih programa, poput špijunskih programa, trojanskih programa, ucjenjivačkih programa, računalnih crva, *rootkita* i infektora datoteka te ostalih oblika kibernetičkih napada poput DDoS napada, SQL injekcija, obiranja podataka i prisilno regrutiranje računala i uređaja u mrežu daljinski kontroliranih uređaja u svrhu izvršavanja DDoS napada na neko određeno poduzeće, organizaciju ili individualnog korisnika, koje može biti motivirano osvetom, novcem, politikom ili pak samo željom za dokazivanje svojih sposobnosti. Radi toga je bitno uložiti dovoljno vremena i resursa kako bi se poduzeća i organizacije adekvatno zaštitili od kibernetičkih napada implementacijom sigurnosnih politika, redovitim provjerama sigurnosti računalnih i mrežnih sustava penetracijskim testovima i pravilnom edukacijom djelatnika.

6. Literatura

1. Akamai. (n.d.). *What is a botnet attack?* Preuzeto 3. rujna 2020, s https://www.akamai.com/us/en/resources/what-is-a-botnet.jsp
2. Akamai. (n.d.). *What Is Malware?* Preuzeto 8. rujna 2020, s https://www.akamai.com/us/en/resources/what-is-malware.jsp
3. Balaji. N. (2019.). *Web Application Penetration Testing Checklist – A Detailed Cheat Sheet*. Preuzeto 10. listopada 2020, s https://gbhackers.com/web-application-penetration-testing-checklist-a-detailed-cheat-sheet/
4. Belcic, I. (2020). *What is a computer worm?* Preuzeto 25. rujna 2020, s https://www.avast.com/c-computer-worm
5. Bishop, M. (2003). What is computer security? *IEEE Security & Privacy*, 1 (1), 67-69. Preuzeto 3. rujna 2020, s http://nob.cs.ucdavis.edu/bishop/papers/2003-spcolv1n1/whatis.pdf
6. BizTech. (2019.). *Checklist: what's looked at in a web application penetration test?* Preuzeto 10. listopada 2020, s https://biztech.com.au/resources/checklist-whats-looked-at-in-a-web-application-penetration-test/
7. Brandom, R. (2017). *The Petya ransomware is starting to look like a cyberattack in disguise.* Preuzeto 19. rujna 2020, s https://www.theverge.com/2017/6/28/15888632/petya-goldeneye-ransomware-cyberattack-ukraine-russia
8. BreachLock. (2019.). *Web Application Penetration Testing Checklist*. Preuzeto 10. listopada 2020, s https://www.breachlock.com/web-application-penetration-testing-checklist/
9. Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology January-June 2014*, Volume 8 (1), 1-20., Preuzeto 20. rujna 2020, s https://ssrn.com/abstract=2461983

10. CheckPoint. (n.d.). *WannaCry Ransomware Attack*. Preuzeto 19. rujna 2020, s https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/wannacry-ransomware/

11. CheckPoint. (n.d.). *What is Hacktivism?* Preuzeto 1. listopada 2020, s https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/

12. Chesti, I. A.; Humayun, M.; Sama, N. U.; Jhanjhi, N. Z. Evolution, Mitigation, and Prevention of Ransomware. *2020 2nd International Conference on Computer and Information Sciences (ICCIS).* Preuzeto 18. prosinca 2020, s https://ieeexplore.ieee.org/document/9257708/authors#authors

13. Cimpanu, C. (2020). *AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever*. Preuzeto 10. listopada 2020, s https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

14. Cisco. (n.d.). *What Are the Most Common Cyber Attacks?* Preuzeto 1. listopada 2020, s https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks

15. Cloudflare (n.d.). *Famous DDoS attacks: The largest DDoS attacks of all time.* Preuzeto 1. listopada 2020, s https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

16. Cloudflare. (n.d.). *What Is Click Fraud?: How Click Bots Work.* Preuzeto 20. kolovoza 2020, s https://www.cloudflare.com/learning/bots/what-is-click-fraud

17. Cloudflare. (n.d.). *What Is Penetration Testing? What Is Pen Testing?* Preuzeto 10. listopada 2020, shttps://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

18. Comtact. (2019). *Infographic: The life cycle of a penetration test.* Preuzeto 2. listopada 2020, s https://www.comtact.co.uk/blog/infographic-the-life-cycle-of-a-penetration-test/

19. Comtact. (2019). *The 8 most common types of cyber attacks explained.* Preuzeto 1. listopada 2020, s https://www.comtact.co.uk/blog/common-types-of-cyber-attacks-explained/

20. Csonka, P. (2006.) . The council of europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit pénal*, 77, 473-501. Preuzeto 18.

prosinca 2020, s https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm

21. Cyber Attacks. (n.d.). *Criminal Motives.* Preuzeto 1. listopada 2020, s https://siwm-cyberattack.weebly.com/criminal-motives.html#

22. Desjardins, J. (2018). *Why Hackers Hack: Motives Behind Cyberattacks.* Preuzeto 1. listopada 2020, s https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/

23. DNSstuff. (2020). *Top 6 Common Types of Cyberattacks in 2020.* Preuzeto 1. listopada 2020, s https://www.dnsstuff.com/common-types-of-cyber-attacks

24. DNSstuff. (2020). *What Is RAT? Best Remote Access Trojan Detect Tools*. Preuzeto 27. rujna 2020, s https://www.dnsstuff.com/remote-access-trojan-rat

25. Encyclopedia Britannica. (2016). *Types of Cybercrime.* Preuzeto 7. rujna 2020, s https://www.britannica.com/topic/cybercrime#ref235699

26. Encyclopedia Britannica. (2019). *Computer Security*. Preuzeto 3. rujna 2020, s https://www.britannica.com/technology/computer-security

27. Encyclopedia Britannica.(2016). *Cybercrime*. Preuzeto 7. rujna 2020, s https://www.britannica.com/topic/cybercrime

28. Engle, B. (2019). *10 ways to protect your business from cyber-attacks.* Preuzeto 9. listopada 2020, s https://www.ifsecglobal.com/cyber-security/10-ways-to-protect-your-business-from-cyber-attacks/

29. Europol. (2019). *Cybercrime*. Preuzeto 7. rujna 2020, s https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

30. Europol. (n.d.). *How to protect yourself against Remote Access Trojans and other malware.* Preuzeto 27. rujna 2020, s https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/how-to-protect-yourself-against-remote-access-trojans-and-other-malware

31. Forbes. (2019). *How Can Companies And Individuals Protect Themselves From Cyber-Crime?* Preuzeto 5. listopada 2020, s https://www.forbes.com/sites/quora/2019/05/15/how-can-companies-and-individuals-protect-themselves-from-cyber-crime/#1a1faeba6479

32. Forcepoint. (n.d.). *What is Scareware? Scareware Defined, Explained, and Explored.* Preuzeto 19. rujna 2020, s https://www.forcepoint.com/cyber-edu/scareware

33. Fruhlinger, J. (2020). *Ransomware explained: How it works and how to remove it.* Preuzeto 27. rujna 2020, s https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

34. Funk, M. (2019). *Web Application Penetration Testing Checklist (* New* Updated 2019).* Preuzeto 10. listopada 2020, s https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/

35. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., & Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *Technology and Society Magazine, IEEE.* 30. 28 - 38. https://www.researchgate.net/publication/224223630_Dimensions_of_Cyber-Attacks_Cultural_Social_Economic_and_Political

36. Goode, B. (2017). *Combating cybercrime.* Preuzeto 19. rujna 2020, s https://cib.db.com/insights-and-initiatives/flow/combatting_cybercrime.htm

37. Gorrie, M. (2020). *What Is Adware?* Preuzeto 19. rujna 2020, s https://us.norton.com/internetsecurity-emerging-threats-what-is-grayware-adware-and-madware.html

38. Grimes, R, Aa. (2017). *Fixing the #1 Problem in Computer Security: A Data-Driven Defense.* Preuzeto 3. listopada 2020, s https://gallery.technet.microsoft.com/Fixing-the-1-Problem-in-2e58ac4a/view/Discussions#content

39. Hoglund, G. & Butler, J. (2005). Rootkits: Subverting the Windows Kernel. *Hoboken, NJ: Addison-Wesley Professional.* https://books.google.hr/books?id=fDxg1W3eT2gC&printsec=frontcover&hl=hr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

40. Honigman, B. (2015). *4 Ways Your Small Business Can Better Prevent Cyber Crime.* Preuzeto 10. listopada 2020, s https://www.entrepreneur.com/article/245102

41. Hulme, G. V. (2020). *DDoS explained: How distributed denial of service attacks are evolving.* Preuzeto 10. listopada 2020, s https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html

42. Identity Theft Resource Center. (2019). *End-of-Year Data Breach Report 2019.* Preuzeto 20. kolovoza 2020, s https://notified.idtheftcenter.org/s/resource

43. Identity Theft Resource Center. (2019). *E-Skimming is a New Cybercrime That is Just in Time for the Holidays.* Preuzeto 6. rujna 2020, s https://www.idtheftcenter.org/e-skimming-is-a-new-cybercrime-that-is-just-in-time-for-the-holidays/

44. Identity Theft Resource Center. (2020). *2020 First Half Report.* Preuzeto 5. listopada 2020, s https://notified.idtheftcenter.org/s/resource

45. Interpol. (2017). *Cybercrime*. Preuzeto 7. rujna 2020, s https://www.interpol.int/en/Crimes/Cybercrime

46. Ismail, N. (2017). *'46%' of British businesses experienced cyber attack – 'vendors' to blame.* Preuzeto 2. listopada 2020, s https://www.information-age.com/46-british-businesses-experienced-cyber-attack-breach-123465807/

47. Johns, E. (2020). Cyber Security Breaches Survey 2020. *London: Department for Digital, Culture, Media & Sport.* Preuzeto 1. kolovoza 2020, s https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

48. Kagan. J. (2020). *What is Skimming?* Preuzeto 6. rujna 2020, s https://www.investopedia.com/terms/s/skimming.asp

49. Kaspersky. (n.d.). *What is a Trojan Virus? - Definition.* Preuzeto 25. rujna 2020, s https://usa.kaspersky.com/resource-center/threats/trojans

50. Kaspersky. (n.d.). *What is Adware: What You Should Know and How to Protect Yourself.* Preuzeto 19. rujna 2020, s https://usa.kaspersky.com/resource-center/threats/adware

51. Kaspersky. (n.d.). *What is Keystroke Logging and Keyloggers?* Preuzeto 25. rujna 2020, s https://www.kaspersky.com/resource-center/definitions/keylogger

52. Kaspersky. (n.d.). *What is Scareware?* Preuzeto 19. rujna 2020, s https://www.kaspersky.com/resource-center/definitions/scareware

53. Kay, R. (2004). *Sidebar: The Origins of Phishing.* Preuzeto 8. rujna 2020, s https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html

54. Khanse, A. (2017). *Why would someone want to hack my computer?* Preuzeto 1. listopada 2020, s https://www.thewindowsclub.com/why-someone-want-hack-computer

55. Malenkovich, S. (2013). *What is a rootkit and how to remove it.* Preuzeto 27. rujna 2020, s https://www.kaspersky.com/blog/rootkit/1508/

56. Malwarebyte. (n.d.). *Malspam*. Preuzeto 18. prosinca 2020, s https://blog.malwarebytes.com/glossary/malspam/

57. Malwarebytes. (n.d). *Cybersecurity basics & protection*. Preuzeto 1. listopada 2020, s https://www.malwarebytes.com/cybersecurity/

58. Malwarebytes. (n.d.). *Keyloggers - What is a Keystroke Logger?* Preuzeto 25. rujna 2020, s https://www.malwarebytes.com/keylogger/

59. Malwarebytes. (n.d.). *Malware*. Preuzeto 19. rujna 2020, s https://www.malwarebytes.com/malware/

60. Malwarebytes. (n.d.). *Ransomware*. Preuzeto 27. rujna 2020, s https://www.malwarebytes.com/ransomware/

61. Malwarebytes. (n.d.). *Spyware*. Preuzeto 19. rujna 2020, s https://www.malwarebytes.com/spyware/

62. Malwarebytes. (n.d.). *SQL Injection*. Preuzeto 11. rujna 2020, s https://www.malwarebytes.com/sql-injection/

63. Malwarebytes. (n.d.). *What is phishing?* Preuzeto 25. rujna 2020, s https://www.malwarebytes.com/phishing/

64. McAfee. (2014). *What is a Computer Worm?* Preuzeto 27. rujna 2020, s https://www.mcafee.com/blogs/consumer/what-is-worm

65. Messier, R. (2019). *CEHTM v10 : Certified Ethical Hacker Study Guide.* Indianapolis : John Wiley & Sons, Inc.

66. Morales, C. (2018). *NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us.* Preuzeto 10. listopada 2020, s https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

67. Morgan, S. (2019). *Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021.* Preuzeto 19. rujna 2020, s https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

68. Norton. (2019). *What is a botnet?* Preuzeto 3. rujna 2020, s https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

69. Norton. (2019.). *What is spyware? And how to remove it.* Preuzeto 19. rujna 2020, s https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

70. Norton. (n.d.). *What is a computer worm, and how does it work?* Preuzeto 8. rujna 2020, s https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

71. Norton. (n.d.). *What is a Trojan? Is it a virus or is it malware?* Preuzeto 25. rujna 2020, s https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

72. Oikarinen, A. (2019). *Cyber attack motives, part 1: Why hackers hack? Who are they?* Preuzeto 1. listopada 2020, s https://www.nixu.com/blog/cyber-attack-motives-part-1-why-hackers-hack-who-are-they

73. OWASP. (n.d.). *SQL Injection.* Preuzeto 11. rujna 2020, s https://owasp.org/www-community/attacks/SQL_Injection

74. Palmer, D. (2017). *Petya ransomware: Companies count the cost of massive cyber attack.* Preuzeto 19. rujna 2020, s https://www.zdnet.com/article/petya-ransomware-companies-count-the-cost-of-massive-cyber-attack/

75. Panda Security. (2018). *Types of Cybercrime.* Preuzeto 7. rujna 2020, s https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

76. Panda Security. (2020). *What is Hacktivism? Campaigns That Shaped the Movement*. Preuzeto 18. prosinca, s https://www.pandasecurity.com/en/mediacenter/technology/what-is-hacktivism/

77. Petters, J. (2020). *What is a Rootkit? How Can You Detect it?* Preuzeto 25. rujna 2020, s https://www.varonis.com/blog/rootkit/

78. PGI. (n.d.). *Penetration testing.* Preuzeto 10. listopada 2020, shttps://www.pgitl.com/cyber-security-services/penetration-testing/

79. Popat, A. (2018). *Five Ways To Protect Your Company Against Cyber Attacks.* Preuzeto 10. listopada 2020, s https://www.entrepreneur.com/article/316886

80. Porter, K. (2020). *What is phishing? How to recognize and avoid phishing scams*. Preuzeto 1. listopada 2020, s https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html

81. Portswigger. (n.d.). *SQL injection.* Preuzeto 11. rujna 2020, s https://portswigger.net/web-security/sql-injection

82. Protecting against File Infectors. (n.d.). *Protecting against File Infectors.* Preuzeto 27. rujna 2020, s https://www.spamlaws.com/file-infectors.html

83. Raam, M. (2019). *Web Application Penetration Testing Checklist (* New* Updated 2019).* Preuzeto 2. listopada 2020, s https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/

84. Rafter, D. (2020). *What is scareware? And how to spot online scareware scams.* Preuzeto 19. rujna 2020, s https://us.norton.com/internetsecurity-online-scams-how-to-spot-online-scareware-scams.html

85. Ranger, S. (2018). *GitHub hit with the largest DDoS attack ever seen.* Preuzeto 10. listopada 2020, s https://www.zdnet.com/article/github-was-hit-with-the-largest-ddos-attack-ever-seen/

86. *Rootkits, Part 1 of 3: The Growing Threat.* (2006). Santa Clara, CA: McAfee. Preuzeto 3. rujna 2020, s https://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf

87. Rouse, M. (2009). *RAT (remote access Trojan).* Preuzeto 27. rujna 2020, s https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

88. Rouse, M. (2017). *Adware*. Preuzeto 19. rujna 2020, s https://searchsecurity.techtarget.com/definition/adware

89. Rouse, M. (2018). *What is pen test (penetration testing)?* Preuzeto 9. listopada 2020, s https://searchsecurity.techtarget.com/definition/penetration-testing

90. Rouse, M. (2019). *SQL Injection.* Preuzeto 19. rujna 2020, s https://searchsoftwarequality.techtarget.com/definition/SQL-injection

91. Rouse, M. (2019). *What is a Botnet and How Does it Work?* Preuzeto 3. rujna 2020, s https://searchsecurity.techtarget.com/definition/botnet

92. Rouse, M. (2020.). *Keylogger (keystroke logger or system monitor).* Preuzeto 25. rujna 2020, s https://searchsecurity.techtarget.com/definition/keylogger

93. Shinder, D. (2010). *Profiling and categorizing cybercriminals.* Preuzeto 1. listopada 2020, s https://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/

94. Sjouwerman, S. (2019). *91% of cyberattacks begin with spear phishing email.* Preuzeto 19. rujna 2020, s https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email

95. Swinhoe, D. (2018.). *What is a keylogger? How attackers can monitor everything you type.* Preuzeto 25. rujna 2020, s https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html

96. Switchfast. (n.d.). *Why Small Businesses Can't Afford to Ignore Basic IT Security Steps.* Preuzeto 9. listopada 2020, s https://www.switchfast.com/guide/protect-your-business-from-cyber-criminals

97. TechSafety. (2017.). *Is there spyware on my phone?* Preuzeto 18. prosinca 2020, s https://techsafety.org.au/blog/2017/08/18/is-there-spyware-on-my-phone/

98. Temporary Error. (2020.). *File Infector Virus A Parasite Virus Overwriting The Files.* Preuzeto 27. rujna 2020, s https://temporaryerror.com/file-infector-virus/

99. The Economic Times. (n.d.). *Definition of 'Spyware'.* Preuzeto 19. rujna 2020, s https://economictimes.indiatimes.com/definition/Spyware

100. TrendMicro. (n.d.). *File Infecting Viruses.* Preuzeto 27. rujna 2020, s https://www.trendmicro.com/vinfo/us/security/definition/file-infecting-viruses

101. TutorialRepublic. (n.d.). *SQL Injection.* Preuzeto 1. listopada 2020, s https://www.tutorialrepublic.com/sql-tutorial/sql-injection.php

102. Veracode. (n.d.). *SQL Injection: Vulnerabilities & How To Prevent SQL Injection Attacks.* Preuzeto 11. rujna 2020, s https://www.veracode.com/security/sql-injection

103. Veracode. (n.d.). *What is a computer worm?* Preuzeto 8. rujna 2020, s https://www.veracode.com/security/computer-worm

104. w3schools. (n.d.). *SQL Injection.* Preuzeto 11. rujna 2020, s https://www.w3schools.com/sql/sql_injection.asp

105. Zlatanov, N. (2015). *Computer Security and Mobile Security Challenges.* U Tech Security Conference. San Francisco, CA. Preuzeto 3. rujna 2020, s https://www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges

Vrste kibernetičkih napada na poduzeća i njihove mjere obrane

Sažetak

Kibernetički napad, ovisno o svom cilju i ozbiljnosti može oštetiti ili čak uništiti tvrtku. Šteta nastala prilikom ovih napada je najčešće financijska, ali također tvrtka trpi i oštećenu reputaciju i smanjeno povjerenje korisnika. Kako bi se izbjegla bilo kakva šteta prouzrokovana kibernetičkim napadima, potrebno je poznavati kakve vrste prijetnji postoje. Osim različitih vrsta zlonamjernih programa (engl. *malware*) poput računalnih crva (engl. *computer worm*), trojanaca, špijunskih programa (engl. *spyware*), ucjenjivačkih programa (engl. *ransomware*) i ostalih štetnih programa, postoje i organizirani napadi poput distribuiranog napada uskraćivanja usluge (DDOS) na poslužitelje poduzeća koji mogu onemogućiti pružanje usluge njihovim korisnicima ili kupcima. Osim poznavanja vrsta prijetnji, bitno je predvidjeti i motivacije potencijalnih napadača. Osim financijskih razloga, postoji li mogućnost da poduzeće bude napadnuto iz želje za osvetom ili iz nezadovoljstva poslovanjem tvrtke (tzv. haktivizam, engl. *hacktivism*), ili jednostavno iz zabave ili dokazivanja svojih mogućnosti? Sigurnosni tim poduzeća će zato provesti niz testova za utvrđivanje slabosti sigurnosnih sustava računalnih i mrežnih sustava poduzeća i po otkrivanju slabosti poduzeti mjere za otklanjanje tih slabosti i unaprjeđivanje cjelokupne računalne sigurnosti poduzeća. Te mjere podrazumijevaju instalaciju različitih sigurnosnih programskih paketa, ali i edukaciju zaposlenika kako ne bi postojao rizik od ljudskog nemara; poznavanje rizika i načina za prepoznavanje istih je prvi korak u sprječavanju potencijalnih kibernetičkih napada na poduzeće.

Ključne riječi: kibernetički napad, računalna sigurnost, sigurnosne prijetnje, poduzeća, zaštita od napada

Types of cyberattacks on enterprises and their countermeasures

Summary

Cyberattacks, depending on their goals and severity can damage or even ruin an enterprise. The damage resulting from these attacks in most cases are financial, but the enterprise also suffers a damage to its reputation and a loss of consumer trust. In order to avoid any damage caused by a cyberattack, it's necessary to know what kinds of threats exist. Aside from many different types of malware, such as computer worm, trojan horse, spyware, ransomware and others, there are types of organized cyberattacks, like distributed denial of service attacks (DDOS) on the enterprises' servers which can disable the provision of services to their users or customers. Along with knowing the types of threats, it's important to foresee the motivations of potential attackers. Beside financial motivations, there is a possibility that the enterprise might be attacked out of revenge or because of dissatisfaction with the enterprise's business practices (also known as hacktivism), or simply for fun or out of a wish to prove one's skills. The enterprise's security team will therefore carry out a number of tests to determine vulnerabilities of the computer and network systems' security systems, and after finding any vulnerabilities, take necessary measures to mend and remove those vulnerabilities and thus improving the overall cybersecurity of the enterprise. Those measures imply installation of security software packages, but also education of employees in order to eliminate the risk of human error; knowing the risks and means of recognizing one is the first step in avoiding potential cyberattacks on an enterprise.

Key words: cyberattacks, computer security, security threats, enterprise, protection against attacks