Računalna forenzika za internet

Uzelac, Andrej

Sveučilište u Rijeci
Fakultet informatike
i digitalnih tehnologija

Sveučilišni prijediplomski studij Informatika

Andrej Uzelac

Računalna forenzika za internet

Završni rad

Mentor: Prof.dr.sc. Božidar Kovačić

Rijeka, rujan 2024.

Sadržaj

1. Sažetak, ključne riječi

Računalna forenzika, kao disciplina koja se bavi prikupljanjem, analizom i očuvanjem digitalnih dokaza, igra ključnu ulogu u borbi protiv cyber terorizma – specifičnog oblika terorizma u kojemu se računalni sustavi koriste za napade na kritičnu infrastrukturu, financijske institucije i državne sustave. Cyber terorizam obuhvaća uporabu tehnologije u svrhu zastrašivanja, izazivanja straha, financijskih gubitaka ili uništavanja. Povijesni razvoj cyber terorizma započinje s rastom interneta i digitalnih tehnologija krajem 20. stoljeća, dok su se sofisticirani napadi pojavili u posljednja dva desetljeća, kako su hakeri i teroristička organizacije prepoznale slabosti u globalnim mrežama.

Motivacija napada uključuje političke, religijske, financijske ili ideološke ciljeve. Glavne mete cyber terorista su kritična infrastruktura, kao što su energetski sustavi, transportne mreže i financijske institucije. Slabosti uključuju nedostatke u kibernetičkoj sigurnosti, neadekvatnu zaštitu sustava i ljudske pogreške. Posljedice napada mogu biti katastrofalne, uključujući financijske gubitke, prekid rada vitalnih usluga i širenje panike.

U obrani protiv cyber terorizma ključne su mjere poput unapređenja kibernetičke sigurnosti, međunarodne suradnje i implementacije tehnoloških rješenja kao što su napredni sustavi detekcije prijetnji. Etika i pravni aspekti cyber terorizma predstavljaju izazov, s obzirom na problematičnu primjenu zakona i ljudskih prava u digitalnom prostoru. Budućnost cyber terorizma ukazuje na rastuću sofisticiranost napada i potrebu za globalnim protumjerama.

Ključne riječi: **cyber terorizam; malware; DDoS; ransomware; phising; mete i slabosti; obrana; etika; pravo, kritična infrastruktura**

2. Uvod

Živimo u digitalnom dobu koje nam putem Interneta nudi mnoge prednosti u našem dnevnom životu i olakšava svakodnevne situacije. Poput svega tako i Internet ima svoje mane, probleme i opasnosti poput širenja lažnih informacija, ovisnosti o socijalnim mrežama, cyber bullying, gubitak privatnosti, krađa identiteta itd.

Ovaj rad se bavi još jednom osim prijašnje navedenih, a to je cyber terorizam. Cyber terorizam se pojavio kao velika opasnost u digitalnom dobu i predstavlja nove izazove i opasnosti sigurnosti pojedinaca, tvrtki (velikih ili malih), organizacija nacionalnoj sigurnosti te gospodarstvu i ekonomiji zemalja diljem svijeta. Kako napreduje tehnologija iz dana u dan, godine u godinu, tako napreduje i sofisticiranost cyber terorizma čime je jako bitno da vlade svih zemalja, razne organizacije i kompanije pa tako i „obični“ građani razumiju koliku opasnost i rizike predstavlja cyber terorizam kako bi se mogli obraniti od istoga. Ovaj rad će se baviti konceptima i vrstama cyber terorizma, načinima korištenja i mjerama obrane od njega.

Cyber terorizam se oslanja na korištenje Interneta i alata kako bi izvršio napad na pojedinu osobu, organizaciju, a sve češće i cijelu Vladu neke države. Koristi slabosti računalnih sustava i računalnih mreža kako bi uzurpirao korištenje usluga i/ili komprimirao osjetljive informacije o pojedincima ili organizacijama. Samim time uvodi strah i kaos u živote onih koji koriste iste te usluge koje su napadnute. Cyber teroristi najčešće napadaju sektore poput financija, zdravstva i transporta kako bi širili paniku ili nekome ekonomski naštetili. Sve to rade najčešće sa motivacijama poput financijske dobiti ili širenja vlastitih ideologija tako što kradu podatke ili šalju viruse tražeći nešto zauzvrat. Najveći izazov borbe protiv cyber terorizma je što se događa putem Interneta gdje je lako zadržati anonimnost i zagubiti trag napadača. Neki od načina obrane kojima se svi moraju posvetiti i shvatiti ih ozbiljno su kreiranje sigurnih mreža, redovito ažuriranje softvera koje koriste sa najnovijim sigurnosnim zakrpama te korištenje i poštivanje savjeta enkripcijskih alata.[38][40]

3. Povijest

3.1. Definicija cyber terorizma

Pojam cyber terora je prvi spomenuo i objašnjavao Barry C. Collin 1980-ih. Collin je tada bio viši istraživač na Institutu Sigurnosti i Obavještajnog rada u Americi. Opisao je cyber teror kao spoj cybernetike (Interneta i informacija) i terorizma sa ciljem izazivanja straha i panike. Tada je to još bio samo koncept, ali ubrzo je zaživio i u stvarnom svijetu te u zadnjih par desetljeća jako brzo evoluirao. Kako se Internet od svojih početaka 1983. godine (ARPANET) brzo razvijao kroz godine, njegovu evoluciju je pratio i cyber terorizam kakvog danas poznajemo. U početcima su se njime služili hakeri pod pojmom haktivisti. Koristili su svoje znanje i razumijevanje računalnih mreža i softvera u računalima kako bi širili svoje političke i ideološke ideje. Razumjeti povijest cyber terorizma je bitna kako bi lakše razumjeli i shvatili ozbiljnost koju predstavlja današnjem modernom društvu.[1][3]

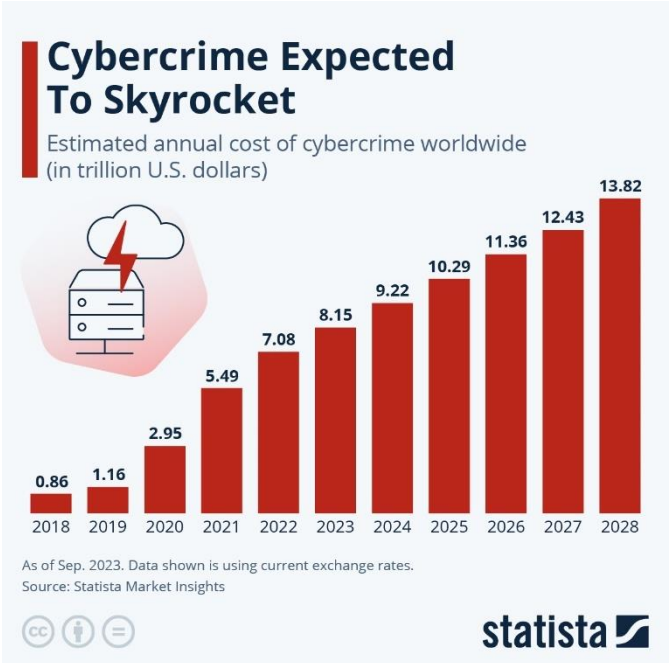
3.2. Početci

Prvi zabilježeni incident je Morris Worm. 1988. godine. Internet je zarazio zlonamjeran program pušten sa jednog od računala MIT-a (Massachusetts Institute of Technology). 6000 od tadašnjih 60 000 računala spojenih na Internet je bilo pod napadom. Nastradala je većina korisnika tek formiranog World Wide Weba među kojima su većinom bili fakulteti raznih američkih sveučilišta poput Berkleya, Harvarda, Princetona, Stanforda. Nastradala je i NASA te Nacionalna knjižnica Lawrence Livemore. Program je napadao računala koja su imala operacijski sustav zasnivan na Unixu. Identificirao je korisnike mreže i dizajniran je da bude sakriven. Iako nije oštetio niti brisao datoteke zaraženih računala, osnovne funkcije vojske i raznih sveučilišta su bile znatno usporene. E-mailovi su kasnili danima, komunikacija između korisnika je pala. Svi korisnici WWW-a su vijećali i istraživali kako se obraniti od programa. Pokušali su shvatiti kako on funkcionira i kako ga ukloniti. Neke od prije spomenutih institucija su u potpunosti brisale svoje sustave i gradili ih ispočetka dok su drugi od spojili svoja računala sa mreže na nekoliko tjedana. Teško je bilo procijeniti štetu ali same organizacije procjenjuju izazvanu štetu u minimumu od 100,000$, a cifra je rasla i do 1,000,000$ (današnjih 283,558$ do 2,835,585$). Tražio se i krivac za širenje takvog programa i nije se znalo je li za isto kriva osoba ili greška u jednom od računala. Ubrzo su se javila dva studenta koja su rekla da poznaju autora programa i da je on poput njih također student i njihov prijatelj. Jedan od studenata je na mrežu poslao kraću ispriku anonimnog programera koji je autor programa zajedno sa uputama kako otkloniti program, dok je drugi student koji je prijatelj autoru uputio anoniman poziv američkoj novinskoj agenciji *The New York Times* i objasnio kako je program trebao biti bezazlen eksperiment koji je postao zlonamjeran program zbog greške u programskom kodu. Reporterima su drugog prijatelja autora naveli da nenamjerno da inicijale autora i uspjelo im je, RTM. Ubrzo se saznalo da je program naziva Morris Worm kreirao Robert Tappan Worm, student Sveučilišta Cornell u Ithaci, saveznoj državi New York. Ubrzo je pokrenut istraga sa strane FBI-a i došli su do

zaključka kako je Robert Worm uistinu autor programa, ali ga nije napravio iz zle namjere već iz interesa kako bi vidio je li moguće napraviti program koji bi se sporo i u tajnosti širio Internetom. Kako bi sakrio svoj identitet, hakirao je računalo MIT-a sa svog terminala Sveučilišta u Cornellu. Unatoč tome što Worm nije imao loših namjera sa širenjem svog programa, i dalje po Zakonu o Računalnim Prevarama bio kriv te mu je izrečena kazna 400 sati rada za opće dobro. Iz tog incidenta je i dobiven naziv za prvi računalni virus svoje vrste odnosno zlonamjerni program – crv (eng. worm). Cijeli događaj je javno popraćen i javnost je mogla iz prve ruke vidjeti koliko su računala i računalne mreže napredovale, ali koliko su osjetljiva. Epilog događaja sa širenjem Morris Worm-a je da Ministarstvo obrane Sjedinjenih Američkih Država osnovalo tim koji je bavio i istraživao sigurnost računala i računalnih sustava te je započelo kreiranje softvera koji bi im pomogli u tome, dok je sa druge strane incidenta Morris Worm inspirirao novu generaciju hakera koji do današnjeg dana zlonamjerno napadaju računala i njihove korisnike. [1][3][6][9]

3.3. Cyber terorizam u 21. stoljeću

U svibnju 2007. je zabilježen prvi veći napad u novom stoljeću. Vladine službe, dio infrastrukture i privatne kompanije u Estoniji su tada bile tjednima pod napadima. DDoS (eng. distributed denial-of-service) napadi su doveli najveće estonske banke do zatvaranja i do nekoliko dana što je uključivalo i nemogućnost korištenja njihovih usluga. DDoS je zatrpao estonske web stranice sa masivnim zahtjevima za podacima i nakrcavanjem servera. Cjelokupni incident je doveo banke do štete vrijednosti milijun dolara, drugih većih šteta nije bilo. Ovaj napad na Estoniju poslužio je kao upozorenje da cyber terorizam postaje ozbiljna prijetnja u 21. stoljeću, što je prikazano u bilijunima dolara u grafu na Slici 1.[2][1]



Slika 1: "Cybercrime Expected to Skyrocket“. Izvor [43]

4. Vrste cyber terorizma

Cyber terorizam obuhvaća različite vrste napada koji koriste digitalne tehnologije za nanošenje štete ili izazivanje straha. Ove vrste napada često imaju različite ciljeve, metode i mete, a neki od najpoznatijih uključuju sljedeće:

4.2. Napadi distribucijom zlonamjernih programa (malware)

Malware je zajednički naziv za sve vrste zlonamjernog softvera koji se koristi za krađu podataka, ometanje rada računalnih sustava ili preuzimanje kontrole nad uređajima. Ova vrsta cyber terorizma može uključivati viruse, trojance, spyware, ad-ware, i druge oblike softvera koji se neovlašteno infiltriraju u sustave.[4]

Jedan od najpoznatijih primjera zlonamjernog softvera koji se koristio za terorizam je NotPetya napad iz 2017. godine, koji je prvenstveno ciljao Ukrajinu, ali se proširio i globalno. Ovaj ransomware je paralizirao tvrtke diljem svijeta, uključujući velike europske korporacije kao što su Maersk, prouzrokujući štetu u stotinama milijuna dolara. Cilj ovog napada bio je destabilizacija ukrajinske infrastrukture, ali je njegov efekt se raširio i van Ukrajine zbog brzog širenja putem zaraženih mreža.[29]

4.3. Distribuirani napadi uskraćivanja usluge (DDoS)

DDoS napadi spadaju među najčešće vrste cyber napada koji se koriste u cyber terorizmu. Ovi napadi funkcioniraju tako da napadači koriste mrežu zaraženih računala kako bi preplavili servere ili mreže žrtve s ogromnim brojem zahtjeva. Posljedica ovakvih napada je preopterećenje infrastrukture, što dovodi do usporavanja ili potpunog gašenja usluga.[4]

Jedan od poznatijih primjera DDoS napada je već spomenuti iz Estonije koji se dogodio 2007. godine, kada su državne institucije i privatne tvrtke bile pogođene valom napada koji su paralizirali internet usluge u zemlji nekoliko tjedana i označili prekretnicu u shvaćanju ozbiljnosti cyber napada na državnoj razini.

Hrvatski akademski i istraživački mrežni centar (CARNet) bio je meta velikog DDoS napada 2020. godine, što je dovelo do ozbiljnih problema s pristupom internetu za školske ustanove i druge korisnike ove mreže. Ovaj napad imao je ozbiljne posljedice jer je usred pandemije COVID-19 onemogućio učenicima i nastavnicima pristup online nastavi.[20]

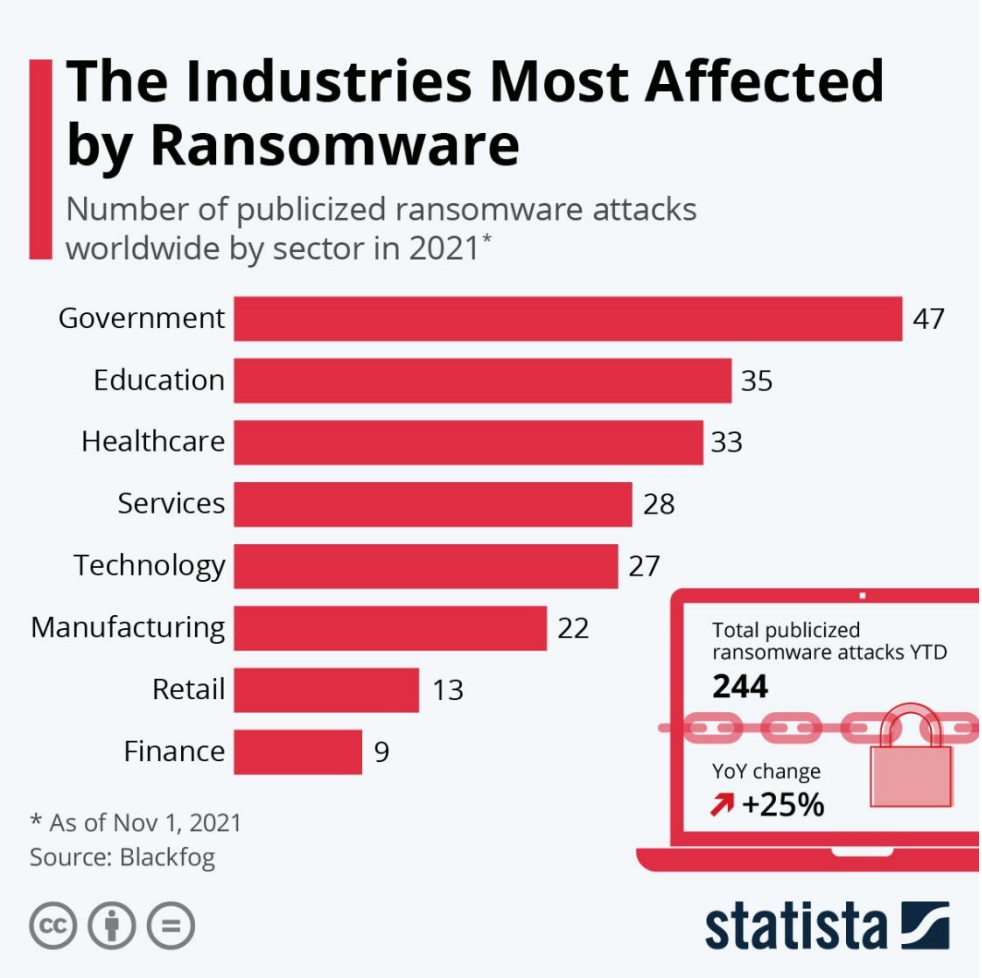
4.4. Ransomware

Ransomware je vrsta malwarea koja zaključava podatke na računalima, zahtijevajući otkupninu za njihovo vraćanje. Ova vrsta cyber napada postaje sve češća u kontekstu cyber terorizma jer omogućuje teroristima financiranje njihovih aktivnosti kroz otkupnine. Ransomware napadi postali su dominantna prijetnja u svijetu cyber terorizma. U ovim napadima, napadači koriste zlonamjerni softver kako bi zaključali ili šifrirali podatke žrtve nakon čega traže otkupninu za povrat pristupa tim podacima. Ovaj oblik napada često cilja

bolnice, vlade, obrazovne institucije i privatne tvrtke što je prikazano u istraživanju Statiste na Slici 2.[1][4]

Primjer jednog od najvećih ransomware napada bio je napad WannaCry 2017. godine, koji je zahvatio više od 150 zemalja. Ovaj napad paralizirao je brojne bolnice u Velikoj Britaniji, uzrokujući kašnjenja u liječenju pacijenata, dok su tisuće organizacija širom svijeta bile pogođene. U Hrvatskoj su također zabilježeni ransomware napadi, uključujući napade na sustave KBC-a Zagreb, koji su ugrozili ključne zdravstvene informacije i operativne sustave bolnica.[1]

Colonial Pipeline u SAD-u bio je žrtva masovnog ransomware napada, što je rezultiralo prekidom opskrbe gorivom na istočnoj obali SAD-a. Ovaj napad je izazvao veliku zabrinutost u svijetu jer je pokazao kako ransomware može poremetiti ključne infrastrukturne sektore[1]



Slika 2: "The Industries Most Affected by Ransomware". Izvor:[44]

4.5. Phishing

Phishing napadi uključuju slanje lažnih e-mailova ili poruka u pokušaju da se prevare žrtve kako bi otkrile svoje osjetljive podatke, poput lozinki ili brojeva kreditnih kartica. Ovi napadi često izgledaju kao legitimne komunikacije s poznatim institucijama, čime žrtve lako mogu biti prevarene. [4]

U Europi, phishing napadi su postali česta prijetnja, posebno u financijskom sektoru. 2021. godine, Europska centralna banka izvijestila je o povećanju phishing napada koji su ciljali na financijske institucije i njihove klijente. Ovi napadi često imaju ozbiljne posljedice, jer dovode do krađe financijskih sredstava i povjerljivih informacija.[5]

Hrvatska je također bila žrtva zlonamjernih programa proširenih e-mailom, a posljednji napad dogodio se 2024. godine, kada je zabilježen veliki broj napada na zdravstvene institucije HZZO-a spoofingom.[25]

4.6. Napadi na kritičnu infrastrukturu

Kritična infrastruktura odnosi se na sustave od nacionalne važnosti, kao što su energetski, vodovodni, zdravstveni i telekomunikacijski sustavi. Cyber teroristi često ciljaju ove sustave kako bi izazvali kaos i ugrozili živote građana. Jedan od najopasnijih oblika cyber terorizma su napadi na kritičnu infrastrukturu poput elektroenergetskih mreža, vodovodnih sustava, zračnih luka ili zdravstvenih sustava. Ovi napadi mogu uzrokovati ne samo financijsku štetu, već i ugroziti živote građana, što ih čini vrlo opasnima.[2][1][31]

Jedan značajan primjer napada na kritičnu infrastrukturu dogodio se u Ukrajini 2015. godine, kada je napad na elektroenergetsku mrežu ostavio više od 230.000 ljudi bez struje. Ovaj napad pripisan je hakerskoj skupini koja je povezana s ruskom državom. Takvi napadi pokazuju koliko cyber terorizam može imati razorne posljedice na nacionalnoj razini, pogotovo kada cilja ključne resurse.[5]

Hrvatska također nije bila izuzeta od ovakvih prijetnji. Jedan od većih slučajeva uključuje pokušaje napada na HEP (Hrvatska elektroprivreda), no uspješna suradnja s međunarodnim agencijama spriječila je ozbiljne posljedice. Ovi napadi pokazuju koliko je važno unaprijediti obrambene strategije i stalno ažurirati sigurnosne protokole.[21][22]

4.7. Botnet mreže

Botnet napadi uključuju stvaranje mreže zaraženih uređaja koje cyber teroristi kontroliraju daljinski, često bez znanja vlasnika uređaja. Ove mreže mogu biti korištene za različite vrste napada, uključujući DDoS napade, širenje zlonamjernog softvera ili krađu podataka. Botneti su postali jedan od glavnih alata u arsenalu cyber kriminalaca zbog svoje sposobnosti da kontroliraju ogroman broj uređaja istovremeno.[4]

Na globalnoj razini, poznati botnet napad uključuje mrežu Mirai, koja je 2016. godine srušila nekoliko velikih web stranica, uključujući Twitter, Netflix i GitHub. Mirai botnet koristio je zaražene IoT uređaje poput pametnih kamera i rutera kako bi izveo masivne DDoS napade.[21]

4.8. Napadi na zdravstveni sektor

Zdravstveni sektor postao je sve češća meta cyber terorizma zbog osjetljivih podataka koje bolnice i zdravstvene ustanove posjeduju. Napadi na ovaj sektor mogu uzrokovati kašnjenja u liječenju, gubitak medicinskih podataka ili potpunu paralizu operacija bolnica.

Napadi na zdravstvene ustanove često se motiviraju financijskim ciljevima, gdje napadači zahtijevaju otkupninu u zamjenu za vraćanje pristupa ključnim podacima.

4.9. Manipulacija informacijama i cyber propaganda

Cyber propaganda uključuje korištenje lažnih informacija i manipulaciju društvenim mrežama s ciljem širenja dezinformacija i izazivanja straha. Cyber teroristi često koriste ovu taktiku kako bi stvorili paniku, polarizirali društvo ili utjecali na političke odluke.[42]

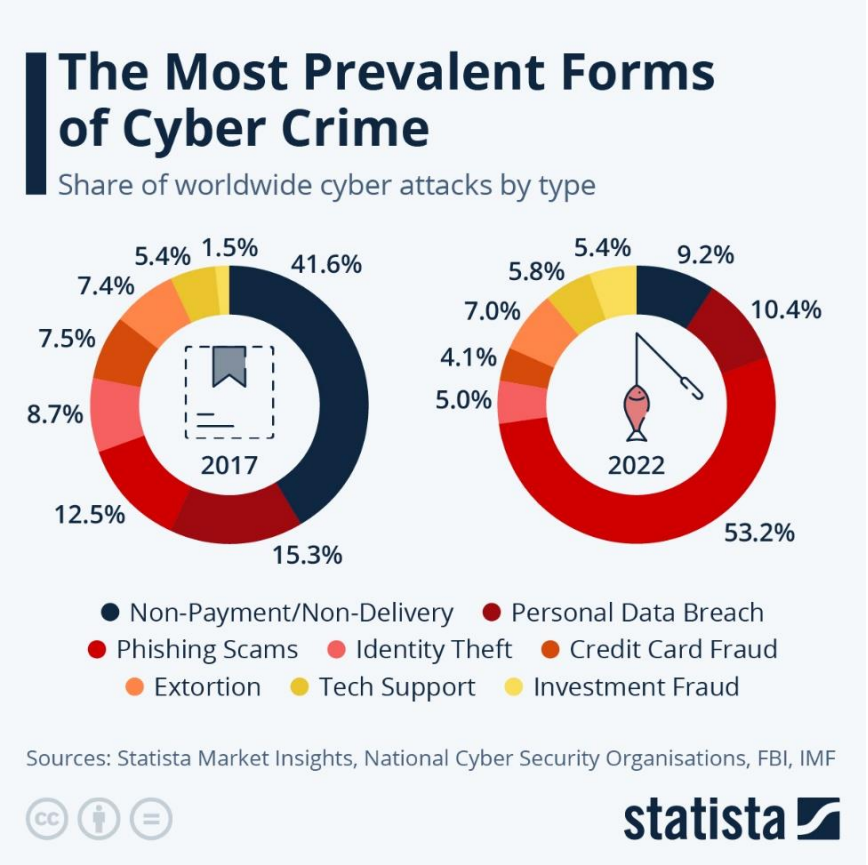
Jedan od najpoznatijih primjera cyber propagande dogodio se tijekom predsjedničkih izbora u SAD-u 2016. godine. Istraživanja su pokazala da su strane sile koristile lažne vijesti i manipulirale društvenim mrežama kako bi utjecale na javno mnijenje i destabilizirale politički proces. Iako nije riječ o klasičnom cyber napadu, ovaj slučaj pokazuje koliko su moderni mediji ranjivi na manipulaciju.[1]

U Hrvatskoj su također zabilježeni slučajevi širenja lažnih vijesti i manipulacija tijekom parlamentarnih izbora i referenduma. Lažne informacije često se šire putem društvenih mreža, s ciljem polarizacije građana i destabilizacije političkog okruženja.[26]

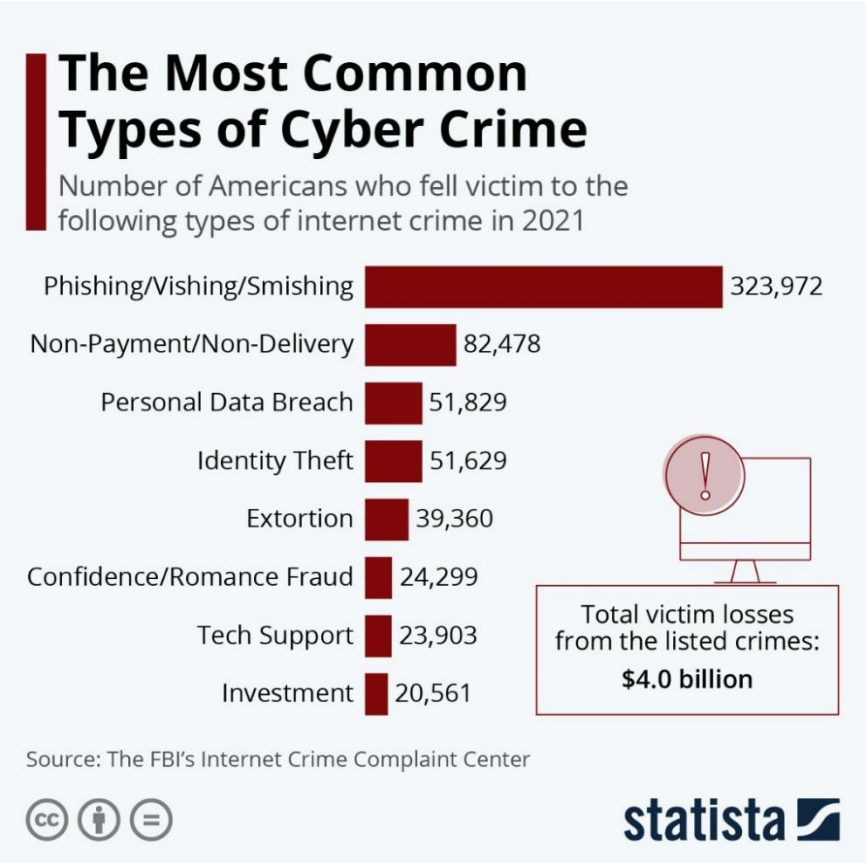
4.10. Napadi na financijske sustave

Financijski sektor jedan je od najranjivijih na cyber napade, a cyber teroristi često ciljaju banke i financijske institucije s ciljem krađe novca ili destabilizacije ekonomija što je uočljivo i na grafovima na Slici 3 i Slici 4.[45][46]

Hrvatska narodna banka (HNB) unatrag nekoliko godina zabilježila je nekoliko pokušaja napada na svoje sustave, iako nisu svi bili uspješni. Ovi napadi naglašavaju potrebu za jačanjem sigurnosti u financijskom sektoru, osobito zbog sve veće digitalizacije bankarskih usluga.[28][30]



Slika 3: "The Most Prevalent Forms of Cyber Crime". Izvor[45].



Slika 4: "The Most Common Types of Cyber Crime". Izvor [46].

5. Motivacija

Cyber teroristi imaju različite motive za provođenje svojih napada, a ti motivi mogu biti financijski, politički, ideološki ili čak psihološki. Svaki motiv donosi različite strategije i ciljeve, ali svi dijele zajednički cilj – destabilizacija ciljne infrast rukture ili izazivanje straha i kaosa.

5.2. Politička motivacija

Jedna od najčešćih motivacija cyber terorista je politička. Terorističke grupe često koriste cyber napade kako bi destabilizirale vlade, ometale političke procese ili širile svoju ideologiju. Ovi napadi mogu uključivati ometanje izbornih sustava, napade na vladine institucije ili širenje dezinformacija s ciljem polarizacije društva.[41]

Jedan od najpoznatijih primjera politički motiviranog cyber napada bio je već spomenuti napad na američke predsjedničke izbore 2016. godine. Cyber operativci, navodno povezani s ruskom vladom, koristili su taktike poput hakiranja računalnih sustava, manipulacije podacima i širenja lažnih vijesti kako bi utjecali na ishod izbora.

Sličan primjer možemo pronaći i u Europi, gdje su u Njemačkoj zabilježeni pokušaji hakiranja tijekom parlamentarnih izbora 2021. godine. Cyber teroristi, najvjerojatnije povezani s vanjskim akterima, pokušali su kompromitirati sustave i širiti lažne informacije s ciljem destabilizacije političkog sustava.[23]

5.3. Ideološka motivacija

Cyber terorizam često je motiviran ideološkim ciljevima, uključujući vjerske, socijalne ili ekološke agende. Terorističke grupe koriste cyber prostor kako bi promovirale svoje ideje, regrutirale članove i izvršavale napade na svoje ideološke protivnike.[41]

Jedan od primjera ideološki motiviranog cyber terorizma je napad ISIS-a na nekoliko zapadnih država. ISIS je koristio društvene mreže i dark web za regrutiranje novih članova, širenje svoje propagande i organiziranje terorističkih napada. Cyber napadi povezani s ISIS-om nisu uvijek uključivali tehnički sofisticirane metode, ali su pokazali kako digitalni prostor može biti alat za ideološku radikalizaciju i terorističke aktivnosti.[33]

Također, anarhističke i ekološke grupe često koriste cyber napade kao dio svojih protesta. Na primjer, tijekom prosvjeda protiv klimatskih promjena, nekoliko aktivističkih skupina u Europi pokrenulo je DDoS napade na energetske kompanije i vlade koje smatraju odgovornima za klimatsku krizu. U Hrvatskoj su zabilježeni slučajevi cyber napada od strane ideološki motiviranih grupa, posebno u kontekstu socijalnih i ekoloških pitanja.

5.4. Financijski motivi

Mnoge cyber terorističke grupe nisu motivirane samo političkim ili ideološkim ciljevima, već i financijskom dobiti. Ransomware napadi, krađa podataka i online prijevare postali su glavni izvori financiranja za terorističke organizacije. Financijski motivi su među

najčešćima u svijetu cyber terorizma. Ovi napadi ciljaju na krađu podataka, poput podataka o kreditnim karticama, osobnim informacijama ili čak na iznudu novca od žrtava putem ransomwarea. Financijski motivirani napadi često ciljaju velike korporacije ili državne institucije, jer one imaju kapacitet platiti visoke otkupnine ili podmiriti financijske gubitke.[40][41]

Primjer takvih napada su ransomware napadi koji uključuju šifriranje podataka i traženje otkupnine za vraćanje pristupa tim podacima. WannaCry, je bio jedan od najpoznatijih financijski motiviranih napada koji je zahvatio tisuće organizacija širom svijeta. Ovaj napad pokazao je koliko brzo i učinkovito cyber teroristi mogu izazvati globalni kaos, motivirani isključivo financijskom dobiti.

5.5. Politički motivi

Nacionalna sigurnost i geopolitika često su ključni motivi za državne sponzorisane cyber napade. Države koriste cyber prostor kao sredstvo za špijunažu, sabotiranje infrastrukture drugih zemalja ili čak kao oblik indirektnog ratovanja. Politički motivirani cyber napadi često su vođeni ciljem sabotiranja državnih institucija, manipuliranja javnim mnijenjem ili širenja političkih ideologija. Ovi napadi su često usmjereni na vlade, državne agencije, ili infrastrukture koje su ključne za funkcioniranje zemlje.[42]

Primjer ovako motiviranog napada možemo pronaći u napadu na iranski nuklearni program 2010. godine, poznat kao Stuxnet.[28] Ovaj napad, za koji se vjeruje da su ga pokrenuli izraelski i američki operativci, koristio je zlonamjerni softver kako bi sabotirao iranske nuklearne centrifuge. Ovaj napad pokazao je kako cyber oružja mogu biti korištena kao dio šireg geopolitičkog sukoba.

Mete cyber terorističkih napada variraju ovisno o motivima napadača, ali generalno uključuju sektore kritične infrastrukture, financijske institucije, zdravstvene ustanove, obrazovne institucije i privatne tvrtke. Svaka od ovih meta ima specifične slabosti koje cyber teroristi iskorištavaju kako bi proveli svoje napade.

5.6. Osobna i psihološka motivacija

Osim političkih, ideoloških, financijskih i nacionalnih motiva, neki cyber teroristi djeluju zbog osobnih razloga. Ovi napadi često imaju psihološku pozadinu, a motivi mogu uključivati osjećaj moći, osvete ili čak jednostavno zadovoljstvo u nanošenju štete.

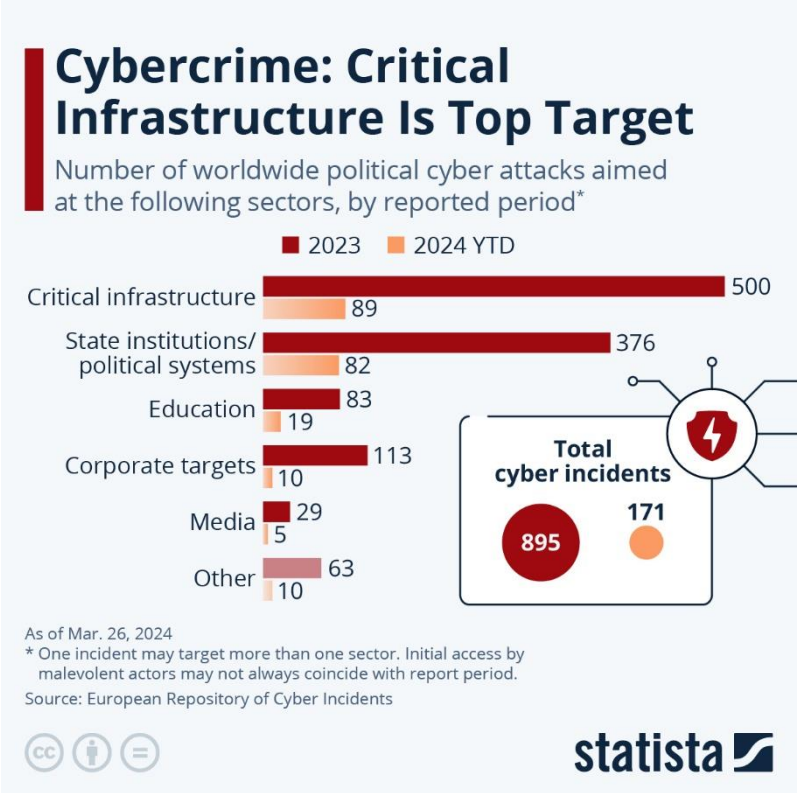
Primjer osobno motiviranog cyber napada dogodio se 2013. godine, kada je bivši zaposlenik američke obavještajne agencije Edward Snowden otkrio ogromnu količinu povjerljivih podataka javnosti. Iako Snowdenov napad nije bio klasičan teroristički napad, njegova motivacija bila je duboko osobna – osjećao je da mora razotkriti zlouporabe vlasti. Ovaj incident pokazuje kako osobni motivi mogu potaknuti ljude da poduzmu radikalne korake u cyber prostoru.[32]

5.7. Mete i slabosti

Cyber terorizam kao oblik modernog terorizma fokusira se na digitalni svijet, koristeći tehnologiju za napad na različite mete. Kako bi razumjeli kako cyber teroristi biraju svoje ciljeve i koje slabosti iskorištavaju, važno je analizirati vrste meta koje su podložne ovim napadima, kao i specifične slabosti tih sustava. U svijetu gdje su gotovo svi sektori ovisni o tehnologiji, meta cyber terorista mogu biti različiti sustavi poput kritične infrastrukture, financijskih institucija, obrazovnih sustava, te privatnih i javnih organizacija. Svaka od tih meta ima specifične slabosti koje napadači pokušavaju iskoristiti.[42]

5.8. Kritična infrastruktura

Kritična infrastruktura obuhvaća sektore koji su ključni za normalno funkcioniranje društva, poput energetike, vodoopskrbe, telekomunikacija i transporta. Cyber napadi na ove sektore mogu imati katastrofalne posljedice, ugrožavajući živote i uzrokujući štetu na nacionalnoj razini. Razlozi zašto su ove mete tako privlačne cyber teroristima leže u njihovoj složenosti i ovisnosti o zastarjelim tehnologijama koje su često podložne napadima. A često su motivirani iz političkih razloga što je prikazano na Slici 5.



Slika 5: "Cybercrime: Critical Infrastructure is Top Target“. Izvor[47].

5.8.1. Slabosti

Kritična infrastruktura često koristi zastarjele sustave koji nisu prilagođeni modernim sigurnosnim standardima. Softverske ranjivosti, nedovoljna segmentacija mreže, te nedostatak redovitih ažuriranja sigurnosnih protokola čine ove sustave podložnima napadima. Usto, fizička izolacija određenih komponenti ovih sustava može stvoriti lažan osjećaj sigurnosti, jer se mnogi pretpostavljaju da izolacija znači sigurnost, dok su mnogi sustavi međusobno povezani na neočekivane načine.

5.9. Financijske institucije

Financijske institucije, poput banaka i burzi, često su mete cyber napada zbog mogućnosti brzog pristupa novčanim sredstvima. Cyber teroristi koriste sofisticirane metode poput ransomwarea, phishing napada i krađe identiteta kako bi kompromitirali financijske sustave. Iako se financijski sektor u pravilu smatra jednim od najsigurnijih kada je riječ o kibernetičkoj sigurnosti, on također ima specifične slabosti koje su teroristi u stanju iskoristiti.

5.9.1. Slabosti

Glavne slabosti financijskih sustava uključuju složenost mreža, koje mogu biti međusobno povezane preko starih protokola koji nisu u skladu s modernim sigurnosnim standardima. Dodatna slabost je ljudski faktor – zaposlenici su često meta phishing napada, gdje ih napadači varaju kako bi otkrili svoje vjerodajnice ili preuzeli zlonamjerni softver. Nadalje, mnoge financijske institucije i dalje se oslanjaju na zastarjele sigurnosne mehanizme, poput slabo zaštićenih sustava za internetsko bankarstvo. Na globalnoj razini, jedan od najvećih napada na financijski sektor dogodio se 2016. godine, kada su napadači upali u sustav SWIFT – međunarodnu mrežu za financijske transakcije. Koristeći ranjivosti u mreži SWIFT, napadači su uspjeli prebaciti gotovo 101 milijun dolara s računa Bangladeške centralne banke. Ovaj napad pokazao je kako ranjivosti u financijskim sustavima mogu biti iskorištene za krađu velikih svota novca. [34]

5.9.2. Primjer

U Hrvatskoj su zabilježeni brojni pokušaji napada na financijske institucije, uključujući pokušaje krađe podataka o korisnicima iz nekoliko velikih banaka. Ovi napadi naglašavaju važnost jačanja sigurnosnih mjera u financijskom sektoru kako bi se spriječile buduće prijetnje.

5.10. Zdravstvene ustanove

Zdravstveni sektor također je popularna meta cyber terorista, uglavnom zbog osjetljivih podataka koje zdravstvene institucije posjeduju. Ovi podaci uključuju medicinsku povijest pacijenata, osobne informacije i financijske podatke, što ih čini vrijednom metom. Napadi na zdravstvene ustanove mogu imati ozbiljne posljedice, uključujući ugrožavanje života pacijenata.

5.10.1. Slabosti

Zdravstvene ustanove su posebna meta cyber terorista zbog osjetljivosti podataka o pacijentima i važnosti funkcioniranja bolničkih sustava. Napadi na zdravstvene ustanove mogu izazvati kašnjenja u liječenju, ugroziti privatnost pacijenata ili paralizirati cijele bolnice.

5.10.2. Primjer

U 2024. godini, napad na KBC Zagreb pokazao je koliko su bolnički sustavi ranjivi. Ovaj ransomware napad usporio je bolničke informacijske sustave na trenutak i otežao pristup medicinskim podacima, što je moglo imati ozbiljne posljedice po zdravlje pacijenata. Takvi napadi često koriste slabosti u IT sustavima koji nisu adekvatno zaštićeni.

5.10.3. Obrazovne ustanove

Obrazovne institucije, uključujući škole i sveučilišta, često su meta cyber napada zbog velikog broja korisnika i količine osjetljivih podataka koje posjeduju. Ovi sustavi često nemaju adekvatnu zaštitu, što ih čini ranjivima na različite vrste napada, uključujući ransomware, phishing, i DDoS napade. Sveučilišta su česće mete napada zbog svojih istraživačkih podataka, povjerljivih informacija o studentima i financijskim sredstvima. Ove institucije često posjeduju snažnu IT infrastrukturu, ali ne uvijek najjače sigurnosne mjere, što ih čini ranjivim na napade.

5.10.4. Slabosti

Glavne slabosti obrazovnih institucija su nedovoljna ulaganja u sigurnosne protokole i svijest o kibernetičkoj sigurnosti. Mnoge škole i sveučilišta koriste starije sustave za upravljanje podacima o učenicima i zaposlenicima, a ti sustavi često nisu dovoljno osigurani. Također, korisnici unutar tih sustava, poput studenata i nastavnog osoblja, nisu dovoljno educirani o sigurnosnim rizicima, što ih čini lakom metom za phishing napade.

5.10.5. Primjer

Tijekom pandemije COVID-19, obrazovne institucije diljem svijeta, uključujući i one u Hrvatskoj, bile su podložne cyber napadima. Zabilježeni su brojni ransomware napadi na online platforme za učenje, poput Zoom-a i Google Classrooma, kao i DDoS napadi koji su privremeno onemogućili pristup predavanjima i ispitima.[35]

5.11. Državne institucije

Državne institucije predstavljaju ključnu metu za cyber teroriste jer one igraju središnju ulogu u funkcioniranju države. Napadi na državne institucije često imaju za cilj destabilizirati vladu, ukrasti povjerljive informacije ili uzrokovati poremećaje u pružanju javnih usluga. Ovi napadi mogu dovesti do ozbiljnih političkih i društvenih posljedica.[18]

5.12. Privatne tvrtke

Privatne tvrtke, posebno one koje se bave tehnologijom, financijama ili komunikacijama, često su meta cyber terorista. Ove tvrtke posjeduju dragocjene informacije, uključujući podatke o klijentima, financijske izvještaje i poslovne tajne, što ih čini atraktivnim metama za napade.

Napad na Sony Pictures 2014. godine, koji je rezultirao curenjem povjerljivih podataka i internih komunikacija, pokazao je koliko su privatne tvrtke ranjive. Ovaj napad imao je ozbiljne posljedice, uključujući štetu za ugled tvrtke i financijske gubitke. U Hrvatskoj, mnoge privatne tvrtke suočile su se s ransomware napadima i napadima na njihove IT infrastrukture. Ovi napadi često uzrokuju prekid rada i gubitak povjerenja klijenata, a mnoge tvrtke odlučuju platiti otkupninu kako bi brzo obnovile svoje sustave.[5][1]

6. Posljedice

Posljedice cyber terorizma mogu biti raznolike i ovisiti o prirodi i opsegu napada. Ove posljedice nisu samo tehničke ili financijske, već mogu imati duboke društvene, političke i psihološke učinke. Razumijevanje posljedica cyber terorizma ključno je za razvijanje učinkovitih strategija obrane.

6.2. Financijski gubici

Financijski gubici su jedna od najočitijih posljedica cyber terorizma. Napadi poput ransomware napada često zahtijevaju velike otkupnine kako bi se povratili podaci ili ponovno uspostavio pristup IT sustavima. U nekim slučajevima, organizacije su prisiljene privremeno zaustaviti poslovanje, što uzrokuje dodatne gubitke. Koliki ti gubitci mogu biti pokazuje i graf na Slici 6 i Slici 7.

Na globalnoj razini, WannaCry napad prouzročio je milijarde dolara gubitaka za tvrtke širom svijeta. Osim direktnih financijskih gubitaka, napad je imao i neizravne posljedice u obliku izgubljenog vremena, poremećaja u radu i troškova obnove sigurnosnih sustava. Ransomware napad na KBC Zagreb doveo je do privremenog zatvaranja dijelova IT sustava bolnice, što je uzrokovalo kašnjenja u pružanju medicinskih usluga i povećanje operativnih troškova.

6.3. Gubitak povjerenja

Jedna od dugoročnih posljedica cyber napada je gubitak povjerenja među građanima i korisnicima. Kada dođe do napada na državne institucije, banke ili zdravstvene ustanove, povjerenje javnosti u sigurnost tih institucija može biti ozbiljno narušeno. Gubitak povjerenja može imati dalekosežne posljedice na funkcioniranje društva, ekonomiju i političku stabilnost.

Napadi poput onih u Estoniji 2007. godine uzrokovali su privremeni pad povjerenja u vladine sustave, a mnogi građani osjećali su se nesigurno u korištenju digitalnih usluga nakon napada. Slično, napadi na banke mogu dovesti do povlačenja sredstava ili opreza pri korištenju online bankovnih usluga.

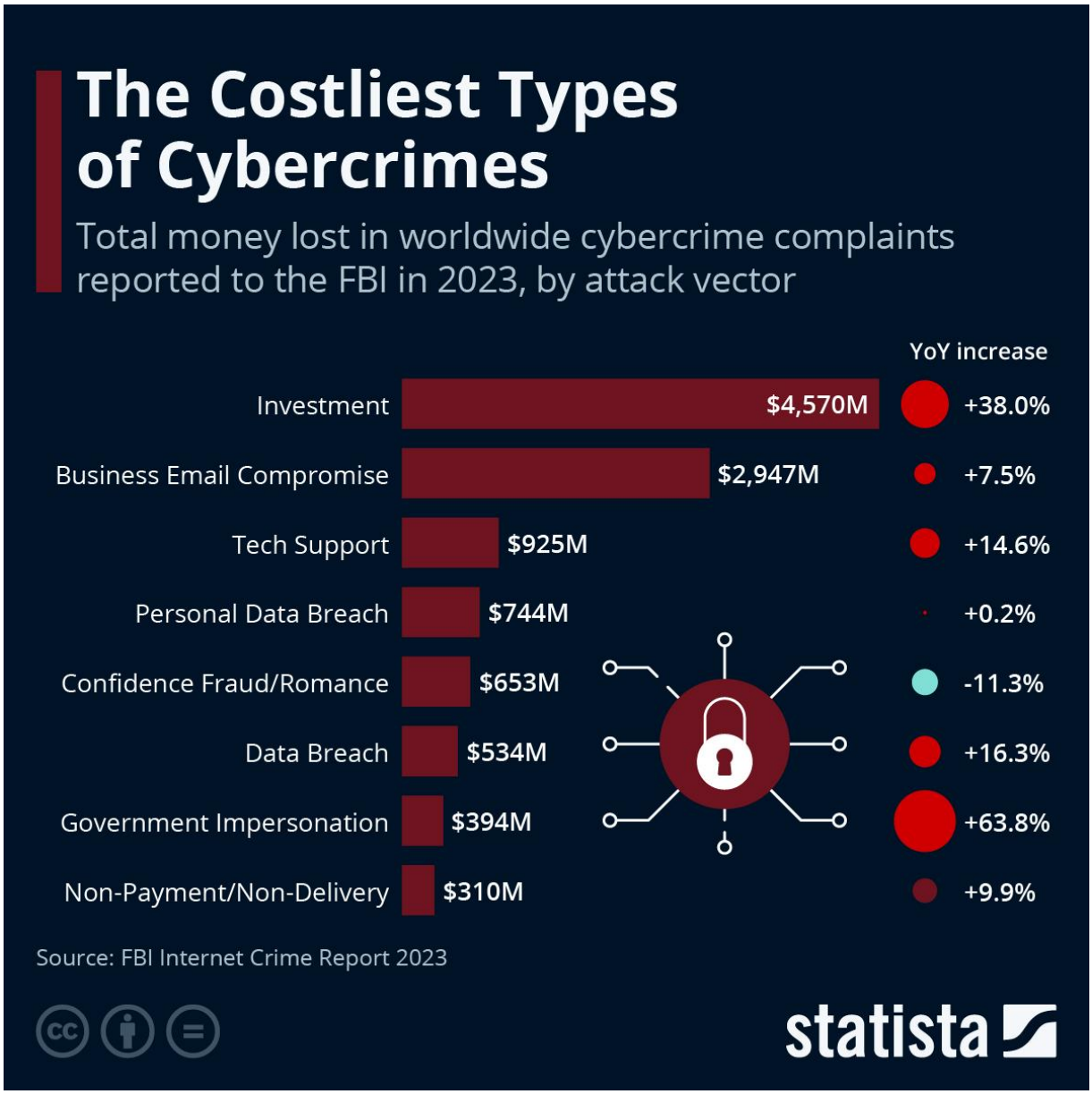
6.4. Paraliza ključnih usluga

Napadi na kritičnu infrastrukturu ili javne službe mogu uzrokovati potpunu paralizu ključnih usluga poput opskrbe strujom, vodom, zdravstvenih usluga ili komunikacija. Kada cyber napad pogodi ključne sektore, cijele zajednice mogu ostati bez osnovnih usluga, što može izazvati paniku i kaos.

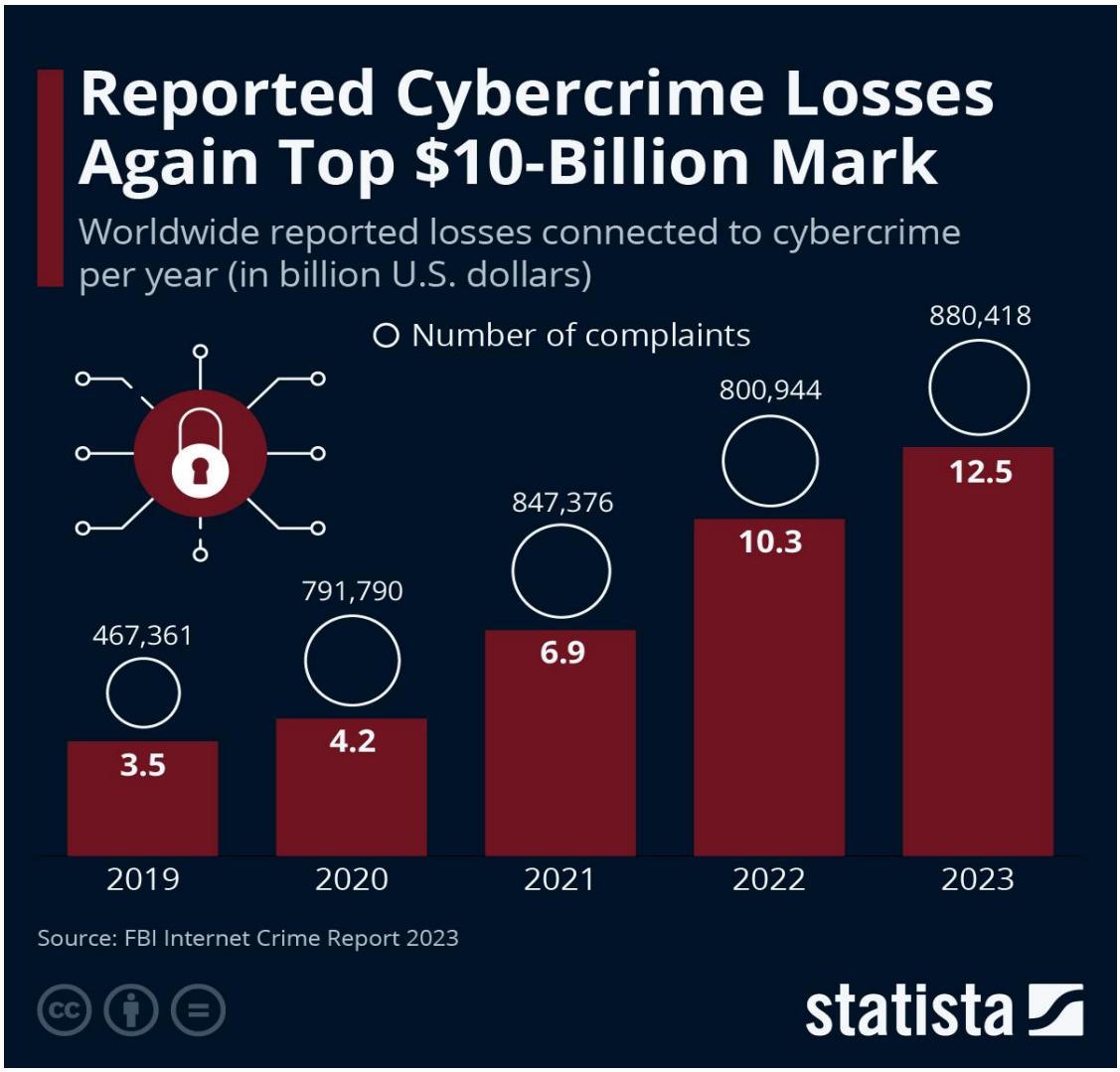
Primjer napada na ukrajinsku elektroenergetsku mrežu 2015. godine doveo je do višednevnog nestanka struje za stotine tisuća ljudi, što je imalo ozbiljne posljedice po svakodnevni život i sigurnost.

6.5. Psihološke posljedice

Cyber terorizam može imati ozbiljne psihološke posljedice za žrtve, posebno ako su napadi usmjereni na pojedince ili ako uzrokuju širenje straha i nesigurnosti u zajednici. Kada su pogođeni osobni podaci ili sustavi koji pružaju osnovne usluge, žrtve se mogu osjećati bespomoćno i traumatizirano. U mnogim slučajevima, žrtve ransomware napada, na primjer, osjećaju veliki pritisak zbog prijetnji gubitkom podataka ili objavljivanjem privatnih informacija. Ove prijetnje često uzrokuju emocionalni stres i strah, što dodatno pogoršava učinke napada.



Slika 6: "The Costliest Types of Cybercrimes". Izvor[48].



Slika 7: "Reported Cybercrime Losses Again Top $10-Billion Mark". Izvor[49]

7. Obrana i protumjere

Cyberterorizam je prijetnja koja je postala sve veća u posljednjih nekoliko desetljeća, jer su kritični sustavi širom svijeta digitalizirani i ovisni o računalnim mrežama. Različiti oblici cyber napada mogu imati ozbiljne posljedice za društvo, ekonomiju i pojedince, čime se otvara prostor za potrebu za učinkovitom obranom i protumjerama. Kako bismo se uspješno obranili od cyber terorizma, nužno je razumjeti kako napadači djeluju, koje alate koriste te kako se možemo koristiti naprednim softverima i tehnikama za zaštitu. Kako cyber napadi postaju sve sofisticiraniji, obrana od cyber terorizma postaje ključni prioritet za vlade, privatne tvrtke i organizacije širom svijeta. Postoje različite metode obrane i protumjere koje se mogu koristiti kako bi se smanjila prijetnja cyber terorizma i zaštitila kritična infrastruktura.

7.2. Edukacija i svijest

Jedna od najučinkovitijih obrambenih mjera je edukacija zaposlenika i šira svijest o prijetnjama koje predstavljaju cyber napadi. Često su zaposlenici prva linija obrane protiv phishing napada i drugih oblika socijalnog inženjeringa. Redoviti treninzi i obuka pomažu u smanjenju rizika od neovlaštenog pristupa sustavima. Primjer dobre prakse dolazi iz Estonije, gdje je nakon velikih napada 2007. godine, vlada pokrenula nacionalne programe edukacije i obuke za sve državne službenike i privatni sektor, s ciljem podizanja svijesti o cyber prijetnjama.

7.3. Vatrozidi (Firewall) kao osnovna linija obrane

Vatrozid je jedan od najosnovnijih, ali i najvažnijih elemenata zaštite mreže. Vatrozidi funkcioniraju kao barijere između interne mreže i vanjskog svijeta (interneta), filtrirajući sav ulazni i izlazni promet na temelju definiranih sigurnosnih pravila. Cilj vatrozida je blokirati potencijalno opasan promet i omogućiti samo pouzdane komunikacije. Vatrozidi analiziraju dolazne i odlazne pakete podataka i odlučuju hoće li ih proslijediti ili blokirati. To čine na temelju pravila definiranih od strane administratora. Ova pravila mogu biti postavljena na različitim razinama, uključujući IP adrese, portove, protokole i druge mrežne karakteristike.[6][10][11]

7.3.1. Vrste vatrozida

- **Packet-filtering firewall**: Ova vrsta vatrozida pregledava pojedinačne pakete podataka i odlučuje treba li ih propustiti ili blokirati. Glavna prednost ovog pristupa je brzina, ali nedostatak je nedostatna analiza sadržaja paketa.
- **Stateful inspection firewall**: Ovi vatrozidi prate stanje aktivnih konekcija i analiziraju pakete u kontekstu tih konekcija, što omogućuje veću sigurnost.
- **Next-Generation Firewall (NGFW)**: Ovi moderni vatrozidi kombiniraju tradicionalne funkcije s dodatnim značajkama poput integracije s IDS/IPS sustavima (Intrusion Detection/Prevention Systems), inspekcijom SSL/TLS prometa i otkrivanjem aplikacija.

7.3.2. Primjer softvera

- **pfSense** je popularni open-source vatrozid i rješenje za mrežnu sigurnost koje nudi širok spektar funkcionalnosti, uključujući filtriranje paketa, VPN podršku i IDS/IPS integraciju. pfSense omogućuje lako postavljanje i administraciju pravila za mrežnu sigurnost, čineći ga pogodnim za male i srednje tvrtke.[7]

7.4. IDS/IPS sustavi (Intrusion Detection/Prevention Systems)

IDS (Intrusion Detection System) i IPS (Intrusion Prevention System) su sustavi koji aktivno nadgledaju mrežni promet i otkrivaju potencijalno zlonamjerne aktivnosti. IDS sustavi identificiraju sumnjivi promet, dok IPS sustavi, osim detekcije, poduzimaju akcije kako bi spriječili napade, poput blokiranja sumnjivih IP adresa. IDS/IPS sustavi rade na temelju unaprijed definiranih pravila i uzoraka poznatih napada (signature-based detection) ili analizom nepravilnosti u mrežnom prometu (anomaly-based detection). Ako sustav detektira odstupanje od uobičajenih obrazaca ili prepoznaje poznatu prijetnju, može poslati upozorenje administratoru (IDS) ili odmah blokirati sumnjivi promet (IPS). Signature-based metoda ovisi o bazi poznatih prijetnji, što znači da su takvi sustavi ranjivi na napade koji koriste nove ili nepoznate metode. Anomaly-based metoda prepoznaje odstupanja od normalnog ponašanja mreže, ali može generirati više lažnih pozitivnih rezultata.[12][10]

7.4.1. Primjer softvera

- **Snort** je jedan od najpopularnijih open-source IDS/IPS alata. Snort koristi signature-based i anomaly-based metode za otkrivanje prijetnji. Njegova popularnost leži u fleksibilnosti i velikom broju dostupnih pravila za detekciju napada.[8]

7.5. Rješenja za enkripciju

Enkripcija je ključna tehnika za zaštitu podataka u digitalnom svijetu. Enkripcija osigurava da su podaci nečitljivi za neovlaštene korisnike, čak i ako su presretnuti. Postoje dvije glavne vrste enkripcije: simetrična i asimetrična.[13][14]

7.5.1. Simetrična enkripcija

Simetrična enkripcija koristi jedan ključ za enkripciju i dekripciju podataka. Ova metoda je vrlo brza, ali zahtijeva siguran kanal za razmjenu ključa.

7.5.2. Asimetrična enkripcija

Asimetrična enkripcija koristi dva različita ključa - javni i privatni. Javni ključ koristi se za enkripciju, dok se privatni ključ koristi za dekripciju. Ova metoda je sporija, ali omogućuje sigurnu razmjenu ključeva preko nesigurnih kanala.

7.6. Antivirusni softver

Antivirusni i antimalware softveri specijalizirani su za otkrivanje, blokiranje i uklanjanje zlonamjernog softvera s računalnih sustava. Antivirusni softveri rade na temelju prepoznavanja uzoraka poznatog zlonamjernog koda, dok moderniji alati koriste heuristiku i

ponašajnu analizu kako bi otkrili nove prijetnje. Antivirusni softver redovito skenira sistemske datoteke, memoriju i dolazni mrežni promet u potrazi za zlonamjernim kodom. Korištenjem baze podataka o poznatim virusima (virus signature database), antivirusni softver uspoređuje datoteke sa uzorcima kako bi otkrio prisutnost malwarea. Softver također koristi heuristiku za otkrivanje sumnjivog ponašanja koje nije nužno već klasificirano kao zlonamjerno.

7.6.1. Primjer softvera

- **Bitdefender** je jedan od vodećih komercijalnih antivirusnih rješenja, poznat po svojoj visokoj stopi detekcije i naprednim alatima za uklanjanje zlonamjernog softvera. Bitdefender koristi kombinaciju tradicionalnog signature-based skeniranja i napredne heurističke analize.[42]
- **Malwarebytes** je specijalizirani alat za detekciju i uklanjanje malwarea, koji se često koristi kao dodatak antivirusnim sustavima za uklanjanje zlonamjernog softvera koji je prošao kroz druge zaštitne mehanizme.[15]

7.6.2. Alati za analizu ranjivosti

Analiza ranjivosti je proces otkrivanja sigurnosnih rupa u sustavima i aplikacijama koje bi mogle biti iskorištene od strane napadača. Postoje brojni alati koji pomažu administratorima u otkrivanju i uklanjanju ovih ranjivosti prije nego što postanu ciljevi cyber napada. Alati za analizu ranjivosti skeniraju sustave i aplikacije, provjeravajući ih protiv baze podataka poznatih sigurnosnih rupa. Oni također testiraju sigurnosne postavke, konfiguracije i traže potencijalne slabosti koje mogu biti iskorištene.

8. Etika i pravo

Jedan od najzanimljivijih i najizazovnijih aspekata cyber sigurnosti je razumijevanje kako tehnološke inovacije i napadi na mreže utječu na etičke i pravne norme u društvu. Tema etike i prava u kontekstu cyber terorizma odnosi se na granicu između zakonitog i nezakonitog ponašanja u digitalnom prostoru, te kako zakoni prate, ali i često zaostaju za tehnološkim napretkom.

8.2. Etika u cyber prostoru

Cyber terorizam stavlja etičke dileme u prvi plan jer se napadi ne događaju samo u virtualnom svijetu, već mogu imati stvarne fizičke posljedice, poput prekida opskrbe energijom, kompromitiranja zdravstvenih podataka ili ugrožavanja nacionalne sigurnosti. Etika u informatici postavlja pitanja o odgovornosti stručnjaka i korisnika tehnologija. Je li etički opravdano hakirati sustave kao odgovor na prijetnju? Gdje se povlači linija između zaštite i napada?

U jednom dijelu, etika u cyber prostoru temelji se na osnovnim moralnim načelima, poput toga da ne smijemo činiti štetu drugima. U informatičkom svijetu, to bi značilo ne iskorištavati ranjivosti sustava za osobnu korist, bez obzira na potencijalne financijske ili društvene dobitke. Međutim, realnost je složenija. Stručnjaci za sigurnost često koriste tehnike slične onima koje koriste napadači kako bi identificirali slabosti sustava – tzv. etičko hakiranje. Etika hakiranja temelji se na ideji da je prihvatljivo koristiti određene metode za proboj u sustave, ali jedino u svrhu njihovog poboljšanja i zaštite od budućih napada. Postoji izrazita razlika između "bijelih šešira" (white hat) i "crnih šešira" (black hat) hakera, gdje prvi djeluju u interesu zaštite i poboljšanja sustava, a drugi isključivo iz vlastitih, često zlonamjernih interesa. Jedan od ključnih izazova u etičkom razmatranju cyber sigurnosti je i privatnost podataka. Ovdje se postavlja pitanje u kojoj mjeri vlade i organizacije smiju prikupljati podatke o pojedincima kako bi osigurale nacionalnu sigurnost. Primjer za ovo može se naći u programima masovnog nadzora poput PRISM-a koji je otkriven 2013. godine, kada je Edward Snowden upozorio na to koliko su daleko vlade spremne ići u nadzoru digitalnih komunikacija. Iako je cilj bio zaštita od terorističkih napada, etički upitno pitanje bilo je: Je li opravdano žrtvovati privatnost građana za sigurnost?[16][17]

8.3. Pravne norme i regulative

Pravni sustav još uvijek pokušava sustići brzinu tehnološkog razvoja. Cyber zakonodavstvo na globalnoj razini nije usklađeno, što otežava procesuiranje cyber kriminalaca, osobito kada se napadi odvijaju preko državnih granica. U mnogim slučajevima, napadi koji se klasificiraju kao cyber terorizam dolaze iz stranih zemalja, što stvara dodatne pravne složenosti. Kibernetički zločini često uključuju više jurisdikcija, a trenutni pravni sustavi nisu uvijek opremljeni za učinkovito surađivanje između država. U Europi, jedan od ključnih dokumenata koji uređuje pitanja cyber kriminala je Budimpeštanska konvencija o cyber kriminalu (Council of Europe Convention on Cybercrime).[36] Ovaj dokument postavlja osnovne okvire za kazneno pravo u vezi s ilegalnim pristupom sustavima,

oštećenjem podataka, prijevarama putem interneta i širenjem zlonamjernog softvera. Hrvatska je potpisnica ove konvencije i time preuzela obvezu uskladiti svoje zakone s ovim međunarodnim standardima. Unatoč zakonodavnim okvirima, cyber kriminalci često iskorištavaju pravne rupe i nepostojanje međunarodnih dogovora. To uključuje društveno hakiranje (social engineering), gdje pojedinci koriste lažne identitete i manipulaciju kako bi pristupili osjetljivim podacima, čime zaobilaze tehničke mjere zaštite koje možda nisu obuhvaćene zakonom.

Nadalje, pravni sustavi diljem svijeta suočeni su s izazovom kako definirati cyber terorizam. U mnogim slučajevima, napadači nisu službeno povezani s terorističkim organizacijama, što otežava njihovo procesuiranje pod zakonima protiv terorizma. Zakon o kibernetičkoj sigurnosti mora se kontinuirano ažurirati kako bi odražavao nove oblike prijetnji.

8.3.1. Primjeri iz prakse

U Hrvatskoj, pravni okvir za borbu protiv cyber terorizma i kriminala uređen je *Zakonom o kibernetičkoj sigurnosti* i drugim relevantnim zakonima. Hrvatska je, kao članica Europske unije, obvezna provoditi direktive i zakone koje donosi EU, kao što je Direktiva NIS (Direktiva o sigurnosti mrežnih i informacijskih sustava). Ova direktiva propisuje minimalne zahtjeve za cyber sigurnost u državnim institucijama i velikim poduzećima te potiče suradnju između država članica u borbi protiv cyber prijetnji.[37]

General Data Protection Regulation (GDPR) također je ključan zakon (nusprozivod Budimpeštanske konvencije) koji utječe na sigurnost podataka u Hrvatskoj i cijeloj Europskoj uniji. GDPR regulira način na koji se podaci prikupljaju, pohranjuju i koriste te postavlja stroge kazne za kompanije koje ne uspiju adekvatno zaštititi osobne podatke građana.

9. Budućnost cyber terorizma i izazovi

Tehnologija napreduje nevjerojatnom brzinom, a s njom se razvijaju i napredniji oblici napada. Budućnost cyber terorizma vjerojatno će biti obilježena povećanom složenošću napada, većom ulogom umjetne inteligencije (AI), ali i snažnijim protumjerama od strane sigurnosnih stručnjaka.

9.2. Povećanje korištenja AI i automatizacije

Jedna od najznačajnijih promjena koja će oblikovati budućnost cyber napada je automatizacija napada putem umjetne inteligencije. AI omogućuje napadačima da automatiziraju procese istraživanja sustava, otkrivanja slabosti i pokretanja napada bez potrebe za ljudskom intervencijom. To znači da će napadi biti brži i učinkovitiji, a sustavi će biti pod stalnim pritiskom od sofisticiranih prijetnji. Napadači mogu koristiti strojno učenje za stvaranje naprednijih malwarea koji mogu zaobići tradicionalne obrambene sustave.

Primjer za to je DeepLocker, zlonamjerni softver s ugrađenom AI tehnologijom. Ovaj malware koristi umjetnu inteligenciju kako bi prepoznao specifične mete i aktivirao se tek kada prepozna odgovarajuće okruženje, čime se izbjegava detekcija do trenutka kada je napad već neizbježan.[38]

9.3. IoT uređaji kao nova meta

Internet of Things (IoT) uređaji postaju sve više integrirani u naš svakodnevni život, ali i postaju nova meta za napade. IoT uređaji, poput pametnih kućnih aparata, kamera za nadzor i medicinskih uređaja, često nisu dovoljno sigurni. Jedna od najvećih prijetnji u budućnosti dolazi iz činjenice da mnogi od ovih uređaja koriste zastarjelu tehnologiju i imaju vrlo slabe sigurnosne mjere. U tom kontekstu, Mirai botnet napad 2016. godine može se smatrati pretečom budućih napada na IoT mreže. Ovaj napad koristio je tisuće zaraženih IoT uređaja za pokretanje DDoS napada koji su onesposobili mnoge važne web usluge.

U budućnosti možemo očekivati porast ovakvih napada jer broj povezanih uređaja eksponencijalno raste. Ovdje je ključno pitanje kako ćemo integrirati bolju sigurnost u te uređaje. Proizvođači moraju preuzeti odgovornost i razvijati uređaje s ugrađenim sigurnosnim mehanizmima.

10. Zaključak

Porast cyber prijetnji posljedica je sve veće globalne povezanosti, brze tehnološke evolucije i nedovoljno sigurnih sustava, osobito u sektorima poput energetike, zdravstva i financija.

Cyber teroristi sve češće koriste sofisticirane metode napada, uključujući ransomware, phishing i napade na lanac opskrbe, kako bi nanijeli što veću štetu ili ostvarili političke i financijske ciljeve. Prema prikazanim podacima, cyber zločini će u budućnosti postati sve češći i destruktivniji, s naglaskom na napade koji mogu destabilizirati čitave zemlje, kao što je bio slučaj s Estonijom. Očekuje se da će ove prijetnje postati još složenije, s naglaskom na umjetnu inteligenciju i Internet stvari (IoT), što će otvoriti nova vrata za cyber teroriste da napadaju osjetljive sustave.

Kako bi se odgovorilo na ove prijetnje, nužno je ulagati u napredne kibernetičke obrambene sustave, međunarodnu suradnju i pravnu regulativu koja će omogućiti bržu reakciju na sveprisutne prijetnje. Povećanje cyber zločina jasno upozorava na hitnost stvaranja učinkovitih protumjera koje će osigurati stabilnost i sigurnost u digitalnom dobu.

Literatura

[1] Maryville University „Cyber Terorism: What it is and How It's Evolved“ online.maryville.edu
https://online.maryville.edu/blog/cyber-terrorism/
(pristupljeno 28.5.2023.)

[2] Cyber Law Toolkit „Cyber attacks against Estonia (2007)“ cyberlaw.ccdcoe.org
https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)
(pristupljeno 29.5.2023.)

[3] Wikipedia „Cyberterrorism“ wikipeida.org
https://en.wikipedia.org/wiki/Cyberterrorism
(pristupljeno 28.5.2023.)

[4] Fortinet „Types of Cyber Attacks“ fortinet.com
https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks
(pristupljeno 10.7.2023.)

[5] SoftwareLab.org, Tibor Moes, softwarelab.org
Phishing Examples (2024): The 11 Worst Attacks of All Time (softwarelab.org)

[6] Saman Iftikhar „Cyberterrorism as a global threat: a review on repercussions and countermeasures“ National Library of Medicine ncbi.nlm.nih.gov
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10803091/
(pristupljeno 25.6.2024.)

[7] pfSense pf Sense Overview „Take A Tour of pfSense“ pfsense.org
https://www.pfsense.org/about-pfsense/
(pristupljeno 2.7.2024.)

[8] Snort snort.org
https://www.snort.org/
(pristupljeno 2.7.2024.)

[9] IBM „What is a cyberattack?“ ibm.com
https://www.ibm.com/topics/cyber-attack
(pristupljeno 2.9.2024.)

[10] Paloalto „Types of Firewalls Defined and Explained“ paloaltonetworks.com
https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls
(pristupljeno 8.6.2024.)

[11] NordLayer „Understanding the different types of firewalls“ nordlayer.com
https://nordlayer.com/learn/firewall/types-of-firewalls/
(pristupljeno 8.6.2024.)

[12] Wikipedia „Proactive cyber defence“ wikipedia.org
https://en.wikipedia.org/wiki/Proactive_cyber_defence
(pristupljeno) 8.6.2024.

[13] Kaspersky „What is Data Encryption?“ kaspersky.com
https://www.kaspersky.com/resource-center/definitions/encryption
(pristupljeno 10.6.2024)

[14] Simplilearn „What is Data Encryption; Types, Alghorithms, Techniques and Methods“ simlilearn.com

https://www.simplilearn.com/data-encryption-methods-article
(pristupljeno 10.6.2024.)
[15] Malwarebytes malwarebytes.com
https://www.malwarebytes.com/company
(pristupljeno 11.6.2024.)
[16] Our Lady Of The Lake University „Cybersecurity Ethics: Everything You Need To Know“ ollusa.edu
https://www.ollusa.edu/blog/cybersecurity-ethics.html
(pristupljeno 18.7.2024)
[17] Augusta University „Cybersecurity Ehics: What Cyber Professionals Need to Know“ augusta.edu
https://www.augusta.edu/online/blog/cybersecurity-ethics
(pristupljeno 18.7.2024.)
[18] Nacional „Zastrašujuća statistika: Tijekom 2020, godine hakerski napadi najčešći u vladinom i bankarskom sektoru brojnih zemalja“ nacional.hr
https://www.nacional.hr/zastrasujuca-statistika-tijekom-2020-godine-hakerski-napadi-najcesci-u-vladinom-i-bankarskom-sektoru-brojnih-zemalja/
(pristupljeno 20.7.2024.)
[19] Lider, Jozo Knez „Lani čak 311 posto više plaćenih otkupnina hakerima nego 2019- Pogledajte tko je najviše platio“ libermedia.hr
https://lidermedia.hr/poslovna-scena/svijet/najvece-ransomware-isplate-svih-vremena-137184 (pristupljeno 20.07.2024.)
[20] ICT Buisness Dražen Tomić „CARNet pod DDoS napadom“ ictbuisness.info
https://www.ictbusiness.info/internet/carnet-pod-ddos-napadom
(pristupljeno 20.7.2024.)
[21] Nacional, Sandra Carić Herceg, „Nacional doznaje: HEP dežurnim ekipama poslao upozerenje o opasnosti od mogućeg hakerskog napada“ nacional.hr
https://www.nacional.hr/nacional-doznaje-hep-dezurnim-ekipama-poslao-upozorenje-o-opasnosti-od-moguceg-hakerskog-napada/
(pristupljeno 20.7.2024.)
[22] Poslovni dnevnik Darko Bičak „HEP stvara IT sigurnosnu službu“ poslovni.hr
https://www.poslovni.hr/sci-tech/hep-stvara-it-sigurnosnu-sluzbu-344868
(pristupljeno 20.7.2024.)
[23] DW, Ben Knight, „How safe is German elections“, dw.com
https://www.dw.com/en/germany-fights-cyberattacks-and-fraud-claims-to-ensure-fair-election/a-58267635
(pristupljeno 20.7.2024.)
[24] Wikipedia „Mirai(malware)“ wikipedia.org
https://en.wikipedia.org/wiki/Mirai_(malware)
(pristupljeno 4.8.2024.)
[25] Bug.hr Sandro Vrbanus „HZZO pod „spoofing“ napadom, hakeri lažiraju njihove e-mailove“ bug.hr
https://www.bug.hr/sigurnost/hzzo-pod-spoofing-napadom-hakeri-laziraju-njihove-e-mailove-42253

(pristupljeno 4.8.2024.)
[26] Lider „EU izbori: Hrvatski Faktograf provjeravat će fake news na Facebooku“ lidermedia.hr https://lidermedia.hr/aktualno/eu-izbori-hrvatski-faktograf-provjeravat-ce-fake-news-na-facebooku-36921 (pristupljeno 4.8.2024.)
[27] Nacional „IZBORI 2024 Prijete hakerski napadi, lažne vijesti. Dezinformacije i umjetna inteligencija“ nacional.hr https://www.nacional.hr/trolovi-fake-news-i-ui-uoci-izbora-kiberneticki-napadi-jedan-su-od-najvecih-izazova/ (pristupljeno 4.8.2024.)
[28] HNB (HRVATSKA NARODNA BANKA) „Hakerski napad na web stranicu nije ugrozio informacijski sustav HNB-a“ hnb.hr https://www.hnb.hr/-/hakerski-napad-na-web-stranicu-nije-ugrozio-informacijski-sustav-hnb-a (pristupljeno 4.8.2024.)
[29] Kaspersky „New Petya / NotPetya / ExPetr ransomware outbrake“ kasperksy.com https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/ (pristupljeno 19.8.2024.)
[30] Poslovni dnevnik/Hina „Hakeri napali internetske stranice hrvatskih institucija: Ministarstvo financija, Poreznu upravu, HNB…“ poslovni.hr https://www.poslovni.hr/sci-tech/hakeri-napali-internetske-stranice-hrvatskih-institucija-ministarstvo-financija-poreznu-upravu-hnb-4446872 (pristupljeno 19.8.2024.)
[31] Wikipedia „Stuxnet“ wikipedia.org https://en.wikipedia.org/wiki/Stuxnet (pristupljeno 19.8.2024)
[32] The Guardian „Edward Snowden: the whistleblower behind the NSA surveillance revelations“ theguardian.com https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (pristupljeno 19.8.2024.)
[33] New York University, Makenzi Taylor, „ISIS Recruitment of Youth via Social Media“, wp.nyu.edu https://wp.nyu.edu/schoolofprofessionalstudies-ga_review/isis-recruitment-of-youth-via-social-media/ (pristupljeno 19.8.2024.)
[34] Wikipedia, „2015-2016 SWIFT banking hack“, wikipedia.org https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack (pristupljeno 19.8.2024.)

[35] ISACA, James G. Koomson, „Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic“, isaca.org https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic (pristupljeno 25.8.2024.)

[36] Council of Europe, „The Convention on Cybercrime(Budapest Convention, ETS No.185) and its Protocols“, www.coe.int
https://www.coe.int/en/web/cybercrime/the-budapest-convention
(pristupljeno 25.8.2024.)

[37] Narodne Novine, „Zakon o kibernetičkoj sigurnosti“, Ustav Republike Hrvatske, narodne-novine.nn.hr
https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html
(pristupljeno 25.8.2024.)

[38] blackhat, Dhilung Kirat, Jiyong Jang and Marc Ph. Stoecklin, „DeepLocker – Concealing Targeted Attacks with AI Locksmithing“, i.blackhat.com
https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf
(pristupljeno 2.9.2024.)

[39] Jilly Slay and Jordan Plotnek, Cyber Terrorism: A Homogenized Taxonomy and Definitonm, 2020

[40] ArmisteadTEC LLC, NoJournal of Information Warfare(Vol8 No1), chapter „A High-level Conceptual Framework of Cyber-Terrorism“, 2009, pp. 43-55

[41] ArmisteadTEC LLC, NoJournal of Information Warfare (Vol16 No1) chapter „Understranding Cyber Terrorism from Motivational Perspectives“, 2017 pp. 1-13

[42] Ali Al Mazari, Ahmed H. Anjariny, Shakeel A. Habib and Emmanuel Nyakwende, Cyber Terrorism and Threats: Concepts, Methodolgies, Tools and Applications, 2018, pp. 173-180, pp. 608-621

[43] Statista, Anna Fleck, „Cybercrime Expected To Skyrocket in Coming Years“, statista.com
https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
(pristupljeno 3.9.2024.)

[44] Statista, Florian Zandt, „The Industries Most Affected by Ransomware“, statisa.com
https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/
(pristupljeno 3.9.2024.)

[45] Statista, Florian Zandt, „The Most Prevalent Forms of Cyber Crime“, statista.com
https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/
(pristupljeno 3.9.2024.)

[46] Statista, Felix Richter, „The Most Common Types of Cyber Crime“, statista.com
https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/
(pristupljeno 3.9.2024.)

[47] Statista, Florian Zandt, „Cybercrime: Critical Infrastructure is Top Target“, statista.com https://www.statista.com/chart/31985/number-of-cyber-attacks-recorded-per-sector/ (pristupljeno 3.9.2024.)
[48] Statista, Florian Zandt, „The Costliest Types of Cybercrime“, statista.com https://www.statista.com/chart/27097/most-expensive-types-of-cyber-crime-us/ (pristupljeno 3.9.2024.)
[49] Statista, Florian Zandt, „How Much Money Is Lost to Cybercrime“, statista.com https://www.statista.com/chart/32341/worldwide-reported-losses-connected-to-cybercrime/ (pristupljeno 3.9.2024.)

Popis slika