Ugroze u kibernetičkom prostoru

Šabić, Mirko

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University Department for Forensic Sciences / Sveučilište u Splitu, Sveučilišni odjel za forenzične znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:227:881314

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

UGROZE U KIBERNETIČKOM PROSTORU

MIRKO ŠABIĆ

Split, rujan 2023.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA FORENZIČNE ZNANOSTI

ISTRAŽIVANJE MJESTA DOGAĐAJA

DIPLOMSKI RAD

UGROZE U KIBERNETIČKOM PROSTORU

MENTOR: izv. prof. dr. sc. TONI PERKOVIĆ

MIRKO ŠABIĆ

0018121888

Split, rujan 2023.

Rad je izrađen na Sveučilišnom odjelu za forenzične znanosti u Splitu,

pod nadzorom mentora Izv. prof. dr. sc. Toni Perković

u vremenskom razdoblju od 15.06.2023.g. do 08.09.2023.g.

Datum predaje diplomskog rada: 14. rujan 2023.g.

Datum prihvaćanja rada: 15. rujan 2023.g.

Datum usmenog polaganja: 21. rujan 2023.g.

Povjerenstvo: 1. prof. dr.sc Josip Kasum

2. doc. dr. sc Nina Mišić Radanović

3. izv. prof. dr. sc Toni Perković

SADRŽAJ

1. UVOD

Zahvaljujući ogromnom razvoju na području informacijskih tehnologija, danas nema ozbiljnijeg poslovnog subjekta na tržištu a da se njima u svom radu ne koristi. Bilo da se radi o sustavima sigurnosti država, gospodarskim subjektima, nekim automatiziranim procesima u industriji ili o svakodnevnom korištenju bankarskih sustava za transakcije koje koristi većina građana u razvijenim zemljama – svim tim sustavima je zajedničko korištenje računalne mreže.

Prema izvještaju pod nazivom Digital 2023 Global digital Overview (January 2023), koje je izradio u suradnji sa partnerima i objavio DataReportal od početka 2023. u svijetu više od 5,16 milijardi ljudi koristi Internet, a društvene mreže preko 4,76 milijardi. Gotovo 64,4 posto svjetske populacije koristi mrežu, a polovica svjetskog stanovništva koristi društvene mreže. Globalno, preko 5,44 milijardi ljudi koristi mobilni telefon. Prosječni korisnik interneta dnevno na mreži provede šest sati i 37 minute. Internet vezu ne koristi ukupno 2,85 milijarde ljudi. Prema izvješću, u svijetu 92,3 posto korisnika se povezuje sa Internetom putem mobilnih uređaja. Mobilne aplikacije se koriste u svim aspektima života (komuniciranje, plaćanje računa i sl.) i koriste se u 10 od provedenih 11 minuta uz mobilne uređaje. Korisnici pametnih telefona su preuzeli više od 200 milijardi mobilnih aplikacija i na njih potrošili 120 milijardi dolara.[1]

Razvojem IT sustava, paralelno su se razvijali i razni nezakoniti načini utjecaja na te sustave, kako bi izvršitelji tih napada time zadovoljili neku od svojih potreba. Računalni sustavi uvijek mogu sadržavati neku programersku pogrešku koju napadači nastoje pronaći i putem nje se okoristiti. Takvi neovlašteni upadi redovito izazivaju štete u pogledu sigurnosti i povjerljivosti samih sustava, no ukoliko je cilj napadača krađa osjetljivih ili tajnih podataka, odnosno krađa financijskih sredstava i sl. štete mogu biti golemih razmjera. Mete takvih napada mogu biti svi. Nekada će napadač tražiti „samo“ nezgodne i kompromitirajuće fotografije nekog korisnika, kako bi ga kasnije mogao ucjenjivati, a drugi put će biti meta njegov tekući račun otvoren u banci. Državne institucije i tijela su naročito poželjni trofeji. Ponekad će te institucije biti meta čisto radi oglasa počinitelja ili neozbiljne šale nedovoljno zrelih osoba, ali

[1] Datareportal, https://datareportal.com/reports/digital-2023-global-overview-report, pristup 11.8.2023.

najčešće će se raditi o ciljanim i dobro promišljenim napadima koji imaju uz kriminalnu i neku drugu svrhu ili kombinaciju više njih, poput gospodarske, političke, financijske i sl.

Šteta je uvijek prisutna, počevši sa osjećajem srama radi ostavljenog lošeg dojma u sigurnost sustava ili kompetentnost osoba. Iz razloga sramote postoji i velika mogućnost ne prijavljivanja djela nadležnim tijelima, pa se sve svede na eventualnu unutarnju istragu unutar nekog subjekta, a isto tako ukoliko se radi o ukradenim kompromitirajućim materijalima, vjerojatnost da će se oštećeni igdje oglasiti o neovlaštenom proboju je mala. Naravno postoje podaci i vode se evidencije o prijavljenim napadima, ali iz gore navedenih razloga, u pogledu broja prijavljenih napada sigurno postoji velika tamna brojka onih koji nisu prijavljeni. Države kroz pozitivni zakonodavni sustav nastoje maksimalno regulirati područja zaštite podataka i informacijske sigurnosti, mnogi subjekti ulažu ogromna sredstva u opremu, softver i IT stručnjake. Za područja sigurnosti i zaštite IT sustava održavaju se razne edukacije i doškolovanja kako IT stručnjaka, tako i onih koji se tim sustavima koriste u svom redovnom radu. Iako se sustavi redovito ažuriraju, provjeravaju i osuvremenjuju novom i sofisticiranijom opremom, mnogi subjekti nastoje dosegnuti samo najveću moguću razinu sigurnosti. Naravno, razina sigurnosti svakog sustava ovisi o velikom broju čimbenika i uvijek treba imati u vidu činjenicu da mnogi sigurnosni stručnjaci vjeruju da ne postoji 100 % siguran sustav. Svi podaci neovisno o mjestu njihova nastanka ili pohrane, a koji mogu pružiti informacije potrebne za izvršavanje prodora, odnosno neovlaštenog ulaska u neki IT sustav predstavljaju podatke koji se moraju štititi od nepozvanih osoba i kao takvi moraju odolijevati od bilo kakvih pokušaja njihova otkrivanja, mijenjanja, uništavanja ili protuzakonitog iskorištavanja. Prijetnje informacijskoj sigurnosti uključuju neovlašteno presretanje podataka, neovlašteno mijenjanje podataka, otkrivanje informacija neovlaštenim osobama i uništavanje hardvera, softvera i/ili sigurnosno zaštićenih informacija kako bi se zaštitila njihova povjerljivost, integritet i dostupnost.[2]

Rad će se fokusirati na analizu različitih oblika cyber prijetnji, uključujući malware, phishing, ransomware, DDoS i drugo. Student će također pružiti pregled različitih metoda zaštite, poput vatrozida, antivirusnog softvera, šifriranja podataka i praksa sigurnosne kulture. Posebna pažnja će biti posvećena izazovima koje sa sobom donosi brzi razvoj tehnologije i sve prisutnije digitalno društvo. Istražit će se utjecaj kibernetičke sigurnost na promjenu

[2] Workman, M. Gaining access with social engineering: An empirical study of the threat, Information Systems Security, Vol. 16, 2007, str. 317.

tehnoloških trendova te mogućim strategijama za upravljanje ovim rizicima u budućnosti. Rad će biti temeljen na kombinaciji teorijskih i praktičnih istraživanja, koristeći studije slučaja kako bi ilustrirao specifične primjere cyber napada.

1.1. Cilj rada

Glavna svrha ovog diplomskog rada je istražiti raznolike aspekte kibernetičkih prijetnji i opasnosti, istovremeno pružajući sveobuhvatne smjernice za zaštitu od istih. Pružit će se pregled raznih strategija zaštite od kibernetičkih prijetnji, fokusirajući se na izazove koji proizlaze iz rapidnog napretka tehnologije i sveprisutnosti digitalnog društva.

U okviru ovog istraživanja, analizirat će se različiti scenariji kibernetičkog kriminala, uključujući zlonamjerni softver, prevaru putem elektronske pošte, ucjenjivačke napade (ransomware), napade preopterećenja usluga (DDoS) i mnoge druge vrste napada. Poseban fokus bit će stavljen na DDoS napade i njihove potencijalne posljedice, uz detaljnu analizu phishing napada i preporuke za efikasnu zaštitu od njih.

Glavni cilj ovog rada je osigurati dragocjene smjernice o zaštiti od kibernetičkih prijetnji, kroz analizu najnovijih incidenata i njihovih potencijalnih posljedica. Kroz čitanje ovog rada, čitaoci će steći znanje o prepoznavanju kibernetičkih prijetnji i adekvatnim mjerama zaštite. Na kraju, krajnji cilj ovog rada je podići svijest o kibernetičkim prijetnjama i pružiti korisne informacije o njihovoj prevenciji i zaštiti.

1.2. Definiranje kibernetičkog prostora

Kibernetički prostor, novi peti prostor ratovanja nakon kopna, mora, zraka i svemira, obuhvaća sve računalne mreže na svijetu i sve što one povezuju i kontroliraju putem kabela, optičkih vlakana ili bežično. To nije samo internet - otvorena mreža. Iz bilo koje mreže na internetu, trebalo bi moći komunicirati s bilo kojim računalom spojenim na bilo koju od internetskih mreža. Dakle, kibernetički prostor uključuje internet uz mnoge druge mreže računala, uključujući one koje se teoretski ne bi smjele moći pristupiti s interneta. Neki od tih privatnih mreža izgledaju baš kao internet, ali su, barem teoretski, odvojeni. Drugi dijelovi kibernetičkog prostora su transakcijske mreže koje rade stvari poput slanja podataka o

novčanim tokovima, burzovnim transakcijama i kreditnim karticama. Osim toga, postoje mreže koje su nadzorno upravljački sustavi i sustavi prikupljanja podataka (engl. Supervisory Control and Data Acquisition-SCADA) koji samo omogućuju strojevima da komuniciraju s drugim strojevima: kontrolne ploče koje razgovaraju s pumpama, dizalima, generatorima itd.

Dakle, kibernetički prostor se sastoji od ogromnog broja računala, poslužitelja, usmjerivača, preklopnika, optičkih kabela i bežičnih komunikacija, koje omogućuju kritičnoj infrastrukturi da funkcionira. Postoje brojne definicije kibernetičkog prostora. Prema jednoj takvoj definiciji, "kibernetički prostor nije fizičko mjesto - on izmiče mjerenju u bilo kojoj fizičkoj dimenziji ili vremensko-prostornom kontinuumu. To je kratki naziv koji se odnosi na okruženje stvoreno sastankom suradničkih mreža računala, IT sustava i telekomunikacijskih infrastruktura, uobičajeno poznatih kao World Wide Web."[3]

Prema Kramer, Starr i Wentz (2009) "kibernetički prostor je operativna domena čiji su jedinstveni i različiti karakter oblikovani uporabom elektronike i elektromagnetskog spektra za stvaranje, pohranu, izmjenu, razmjenu i iskorištavanje informacija putem međusobno povezanih informacijsko-komunikacijskih tehnologija i njihovih pridruženih infrastruktura".[4] Ove umrežene i međusobno povezane informacijske sustave istodobno nalazimo u fizičkom i virtualnom prostoru, unutar i izvan zemljopisnih granica.
Njihovi korisnici sežu od država i njihovih organizacijskih elemenata i zajednica sve do pojedinaca i amorfnih transnacionalnih skupina koje možda ne iskazuju odanost tradicionalnim organizacijama ili nacionalnim subjektima. Oslanjaju se na tri različita, ali međusobno povezana učinka triju dimenzija: fizičke, informacijske i kognitivne. Zajedno čine globalno informacijsko okruženje kako je navedeno u doktrini informacijskih operacija: fizičke platforme, sustavi i infrastrukture koje osiguravaju globalnu povezanost za međusobno povezivanje informacijskih sustava, mreža i ljudskih korisnika; goleme količine informacijskog sadržaja koji se može digitalno i elektronički slati bilo kamo, bilo kada, gotovo bilo kome; i ljudska spoznaja koja proizlazi iz znatno povećanog pristupa sadržaju, što može imati dramatičan utjecaj na ljudsko ponašanje i donošenje odluka.[5]

[3] Wingfield, T.C. *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., 2000, str. 17.
[4] Kramer, F.D., Starr, S. & Wentz, L.K. *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books, 2009.
[5] Kramer, F.D., Starr, S. & Wentz, L.K. *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books, 2009.

Ratovanje 21. stoljeća koje uključuje protivnike koji posjeduju suvremene tehnologije, nije moguće bez pristupa kibernetičkom prostoru. Uporaba elektroničkih tehnologija za stvaranje i „ulazak“ u kibernetički prostor te korištenje energije i svojstava elektromagnetskog spektra, kibernetički prostor izdvajaju od drugih područja te ga čine jedinstvenim.

1.3. Kibernetički kriminal

Razvoj tehnologije sve više usmjerava društvo prema virtualnom svijetu. Digitalne tehnologije omogućuju stvaranje i širenje digitalnih sadržaja. Zbog toga informacijski sustavi sve više koriste ovu tehnologiju za međusobnu komunikaciju. Iako funkcionalnija, ona je podložnija napadima zbog veće umreženosti. Struktura interneta, iako je nastala s dobrim namjerama, olakšava štetne aktivnosti koje mogu biti vrlo učinkovite. Ključan čimbenik je sveprisutnost interneta u životu ljudi. S rastom broja korisnika i uređaja, rastu i prijetnje te učestalost napada.

Prema Marinkoviću (2008) „povećanjem broja napada, proporcionalno se povećavaju i nastale štete kao posljedice tih napada, te je jasno zašto je sve veći naglasak stavljen na sigurnost informacijskih sustava, kao i na implementiranje raznih strategija zaštite.“[6]

Kriminalne aktivnosti poput krađa, prijevara i sabotaža sve više se odvijaju putem računala i interneta. Zloupotreba tehnologije u svrhu nezakonitih radnji postaje sve učestalija. Neovlašteni pristup osjetljivim podacima, krađa identiteta i financijskih sredstava te narušavanje sigurnosti sustava predstavljaju prijetnju. Oduvijek postoji bojazan od kompromitiranja povjerljivih informacija od nacionalnog značaja.

U današnje vrijeme, uz pristup zaštićenim podacima, prijeti i preuzimanje kontrole nad računalnim sustavima i programima. Borba protiv kibernetičkog kriminala zahtijeva stalnu budnost i unapređivanje mjera zaštite. „Nakon probijanja sigurnosnih postavki na jednom računalu unutar mreže, jednostavno se može infiltrirati na ostale sustave unutar te mreže. Uporabom komercijalnih ali i besplatnih programskih alata kao što su mrežna njuškala (engl. network sniffers) te TCP/IP analizatori mrežnog prometa (i jedni i drugi su naširoko dostupni

[6] Marinković, M. Maliciozan kod, Beograd, 2008.

i besplatni - freeware), omogućuje se neovlaštenim stranama prikupljanje vitalnih informacija sustava kao što su korisnička imena te njihove pristupne šifre, ulazni i izlazni mrežni promet iz sustava, te specifični podaci vezani za operacijski sustav.“[7] Nakon neovlaštenog pristupa sustavu, najveća šteta može nastati preuzimanjem kontrole nad čitavom mrežom, kao što je globalna informacijska infrastruktura. „Tako se može kontrolirati kritična infrastruktura, kao što su naftovodi, plinovodi, električna mreža, nuklearne centrale, telekomunikacijske i telefonske mreže, sustavi transakcija i financija te radio i TV signali.“[8]

Različiti akteri poput vlada, vojnih organizacija, terorističkih skupina i pojedinaca vode borbe u digitalnom prostoru odnosno cyber ratovanja. Prema Janczewski (2007) „kibernetičko ili cyber ratovanje (eng. Cyberwarfare) označava uporabu računala, interneta i drugih sredstava države ili nacije za provođenje napada na neprijateljske informacijske sustave s ciljem nanošenja štete ili blokade informacijsko-komunikacijske tehnologije.“[9] Dakle, cyber ratovanje se odvija korištenjem informacijsko-komunikacijskih tehnologija, ali može imati stvarne posljedice.

1.4. Pojavni oblici kibernetičkog ratovanja

Kibernetički rat ili rat u kibernetičkom prostoru može poprimiti različite oblike, ali uvijek uključuje zloupotrebu informacijsko-komunikacijskih tehnologija. Oblici kibernetičkog ratovanja ovise o korištenim metodama napada poput hakiranja, zaraze zlonamjernim programima, botnetova, trojanskih konja i slično.

1.4.1. Zlonamjerni programi - malware

„Organizacija NIST (engl. National Institute of Standards & Technology), utvrdila je definiciju malicioznog koda: Pojam malware se odnosi na program koji je, tajno ubačen u sustav sa namjerom kompromitiranja povjerljivosti, integriteta ili dostupnosti žrtvinih podataka, aplikacija ili operacijskog sustava, ili na neki drugi način pokušava ometati žrtvu.“[10] Zlonamjerni programi karakterizira to što se izvode neovlašteno i bez znanja

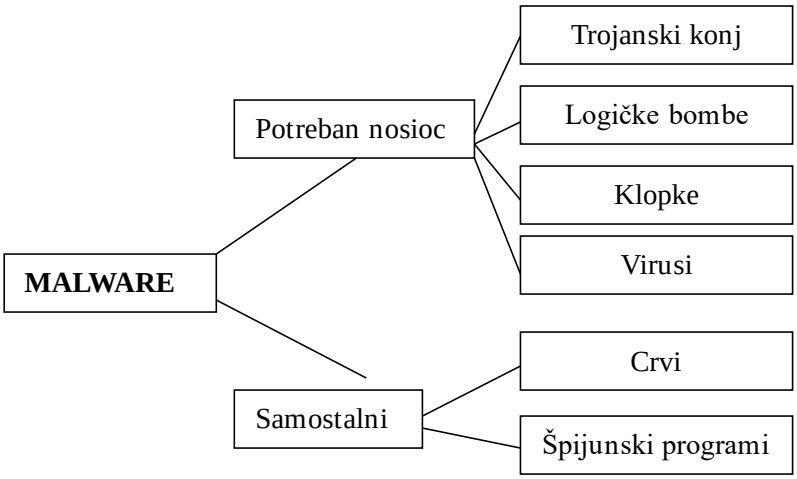
[7] Hrvatski vojnik, http://www.hrvatski-vojnik.hr/hrvatski-vojnik/2802010/it_sec.asp, pristup 11.8.2023.
[8] http://www.hrvatski-vojnik.hr/hrvatski-vojnik/2802010/it_sec.asp
[9] Janczewski, C. Cyberwarfare and CyberTerorism, Information Science Reference, USA, 2007.
[10] Cert, http://www.cert.hr, pristup 11.8.2023.

korisnika te uzrokuju štetne posljedice. Neki od najčešćih oblika su računalni virusi, crvi, logičke bombe i špijunski programi. Zajedničko im je nezakonito i skriveno djelovanje koje može ugroziti rad računala i povjerljivost podataka.

Zlonamjerne programe se može kategorizirati prema načinu širenja i učincima na:

- zlonamjerne infektivne programe - virusi, crvi
- zlonamjerne rograme za prikriveni pristup - trojanski konji, backdoori, rootkitovi
- zlonamjerne programe za financijsku dobit - špijunski programi, advertovi, keyloggeri, botnetovi

Neprekidni rast zlonamjernih programa povezan je s širenjem upotrebe računala i tehnološkim napretkom. Krajem 20. stoljeća bilo je nekoliko tisuća vrsta virusa, početkom 21. stoljeća na desetke tisuća vrsta, a samo desetljeće kasnije čak u milijunskim razmjerima.



Slika 1. Prikaz podjele zloćudnih programa

Postoji više vrsta zlonamjernih programa. Osnovna podjela je na samostalne i one koji ovise o nekom "programu domaćinu" da bi funkcionirali. Prema Budić, Špoljarić i Kramar (2011) „neovisni zlonamjerni kodovi mogu se izvršavati samostalno bez potrebe za domaćinskim programom. Pokreću se zajedno s operacijskim sustavom, poput računalnih crva. Zlonamjerni kodovi koji ovise o domaćinskom programu ne mogu funkcionirati bez njega. Ugrađuju se u domaćinski program i mijenjaju njegovo ponašanje na štetu korisnika. Za razliku od neovisnih kodova, ovisni kodovi trebaju domaćinski program kao nositelja da bi se mogli izvršiti i ostvariti svoje štetno djelovanje.. U ovu vrstu pripadaju virusi, trojanci i slično."

Virus je dio računalnog koda koji se implementira na program ili datoteku tako da slobodno putuje preko host programa ili datoteke od računala do računala i prenosi zarazu. Virusi mogu oštetiti software, hardware i datoteke. Prema Budić, Špoljarić i Kramar (2011) " da bi se virusi mogli širiti i replicirati, moraju imati određene sposobnosti i dopuštenja poput mogućnosti izvršavanja vlastitog koda i zapisivanja u memoriju. Bez tih funkcionalnosti virusi ne bi mogli inficirati programe ili datoteke niti se prenositi s jednog računala na drugo. Stoga je ključno da virusi dobiju izvršna dopuštenja kako bi ostvarili svoje štetno djelovanje."[11]

Virusi se ugrađuju u izvršni kod drugih programa kako bi dobili potrebna dopuštenja. Kada korisnik pokrene zaraženi program, pokreće se i virus, uz funkcije originalnog programa. Virusi se dijele na rezidentne i nerezidentne ovisno o načinu na koji lociraju domaćinski program. Rezidentni virusi se instaliraju u memoriju računala i aktivni su dok je računalo uključeno. Nerezidentni virusi inficiraju datoteke na disku te se aktiviraju prilikom pokretanja tih datoteka. Oba tipa ovise o domaćinskom programu da bi se mogli replicirati i širiti.

Nerezidentni virusi traže domaćine koje mogu inficirati, inficiraju ih i na kraju predaju kontrolu host programu kojeg su zarazili. Rezidentni virusi ne traže host program nego se oni odmah učitaju u memoriju i predaju kontrolu host programu. Takvi virusi ostaju aktivni u potrazi za sljedećim domaćinom. Virusi mogu inficirati razne vrste host programa. Neke od glavnih izvršnih datoteka su binarne izvršne datoteke (kao što su .com datoteke ili .exe datoteke ili slične datoteke na ostalim operacijskim sustavima).

Prema Budić, Špoljarić i Kramar (2011) "postoji nekoliko vrsta računalnih virusa:

- Polimorfni virusi - prilikom repliciranja stvaraju funkcionalne kopije koje se razlikuju na razini bitova, čineći ih težim za detekciju.
- Boot sector virusi - zaraze master boot record ili boot sektor diska, premještajući originalni kod i zamjenjujući ga svojim.
- Makro virusi - niz naredbi u aplikacijama poput Worda koje izgledaju legitimno ali uzrokuju štetu. Čine 2/3 virusa.

[11] Budić, S., Špoljarić, I. & Kramar, M. Maliciozni kod: analiza modernih malicioznih kodova. http://maliciozni-kod-analiza-modernih- malicioznih- kodova. googlecode.com/files /Tema_06_ MALICIOZNI%20KOD_ANALIZA%20MODERNIH %20MALICIOZNIH%20KODOVA.pdf, pristup 11.8.2023.

- E-mail virusi - šire se e-mail prilozima, tipično preko Word makroa.
- Stealth virusi - skrivaju promjene koje naprave na datotekama ili boot sektoru dok su aktivni.“

Različiti tipovi virusa koriste specifične tehnike i slabosti sustava kako bi se replicirali i širili.

Trojanski konj je vrsta zlonamjernog programa koji svoje pravo djelovanje prikriva izgledom korisne ili zabavne aplikacije. Korisnik ga pokreće misleći da radi nešto korisno, a zapravo omogućuje napadaču pristup sustavu i podacima. Za razliku od virusa, trojanski konj se ne replicira već korisnik mora sam pokrenuti zaraženu aplikaciju. Nakon pokretanja može imati različite štetne učinke - od usporavanja rada do krađe osjetljivih podataka kao što su lozinke ili bankovni podaci.
Često se širi preko komunikacijskih programa kao privici koji izgledaju bezazleno. Otvara sigurnosne rupe koje omogućuju napadaču pristup i preuzimanje kontrole nad zaraženim računalom. Zbog prikrivenog djelovanja korisnici često nisu ni svjesni da su zaraženi trojancem. Postoji nekoliko vrsta trojanskih konja:

- Dropper - služi za instaliranje pravih virusa na zaraženo računalo.
- Backdoor - omogućuje udaljeni pristup i kontrolu nad zaraženim računalom, iskorištavajući sigurnosne propuste.
- Downloader - preuzima zlonamjerne datoteke s interneta i pokreće ih na zaraženom računalu.
- Banking trojanci - kradu bankovne podatke i lozinke.
- Ransomware - šifriraju podatke na računalu i traže otkupninu.
- Spyware - prikupljaju osobne i povjerljive podatke.

Različiti trojanci imaju specifične funkcije, ali zajednički otvaraju sistem za zloupotrebu i krađu podataka.

Računalni crvi su vrsta zlonamjernog programa koja se, za razliku od virusa, širi sama bez interakcije korisnika. Koriste ranjivosti sustava za širenje od računala do računala putem mreže.
Njihova opasnost je u mogućnosti samorepliciranja, tako da s jednog zaraženog računala mogu poslati na tisuće svojih kopija i time usporiti mrežu i sustav. Crv pronalazi kontakte na

zaraženom računalu i šalje se e-mailom dalje do sljedećeg računala, replicirajući se eksponencijalnom brzinom. Osim toga, crvi otvaraju sigurnosne rupe koje omogućuju udaljenu kontrolu zaraženog računala. Njihovo brzo širenje i destructive potencijal čine ih izrazito opasnim oblikom zlonamjernog koda.

Prema Zetter (2012) "vrste računalnih crva:[12] [13]

- Crv - može oštetiti podatke i komprimirati sigurnost računala
- Mailer i mass mailer - sami se šalju elektroničkom poštom
- Miješane prijetnje - kombiniraju karakteristike virusa, crva i trojanskih konja s propustima softvera za svoje pokretanje, prijenos i širenje napada.

Crvi i virusi su kreirani za prijenos payloada na računalo. Payload je kreiran za provođenje specifičnih funkcija kao što su brisanje ili promjena podataka, instaliranje softvera na računalo i kreiranje stražnjih vrata koja napadač može kasnije upotrijebiti da bi dobio neovlašten pristup računalu. Internet crvi i virusi stvaraju probleme inficiranim računalima, ali crvi mogu napraviti veću štetu zbog mrežnog prometa koji generiraju prilikom širenja Internetom.

„Rootkitovi su vrsta zlonamjernog softvera čija je svrha preuzimanje kontrole nad operacijskim sustavom na prikriven način.“[14] Oni mijenjaju sistemske datoteke i procese bez dopuštenja korisnika kako bi ostali nevidljivi. Rootkit je skup alata za prikrivanje prisutnosti i aktivnosti na sustavu. Nakon instalacije, rootkit koristi funkcije operacijskog sustava da sakrije sebe i druge zlonamjerne programe. Time omogućuje neovlaštenim osobama preuzimanje kontrole nad sustavom. Rootkitovi su vrlo opasni jer napadaču omogućuju potpunu kontrolu nad sustavom bez znanja korisnika.

Prema Budić, Špoljarić i Kramar (2011) "rootkitovi su se originalno pojavili na Unix sustavima kao skup alata za dobivanje i zadržavanje administratorskog pristupa.“ Na Windows sustavima, naziv rootkit se koristi za alate koji skrivaju procese i programe od korisnika. Nakon instalacije, Windows rootkit koristi funkcije operacijskog sustava da sakrije

[12] Zetter, K. Mahdi, the Messiah, Found Infecting Systems in Iran, Israel. http://www.wired.com/threatlevel/2012/07/mahdi/, pristup 11.8.2023.
[13] Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers. http://www.wired.com/threatlevel/2012/05/flame/, pristup 11.8.2023.
[14] Mačković, D. Rootkit. Rootkit. http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm, pristup 11.8.2023.

sebe i druge zlonamjerne programe od detekcije. Dakle, iako su se prvo pojavili na Unixu, danas se rootkitovi najčešće povezuju s alatima za prikrivanje zlonamjernih aktivnosti na Windows operacijskim sustavima. Koriste ugrađene funkcije Windows OS-a kako bi prikrili svoje prisustvo. Rootkit cilja firmware uređaja kao što su mrežne kartice, hard disk ili sam BIOS, hypervisor, kernel, ali najčešće napada korisničke aplikacije i korisniče račune. Rootkitovi često sadrže i backdoor, odnosno ulaz u sustav neovlaštenim osobama bez znanja korisnika. Autori virusa sve češće koriste rootkitove kako bi sakrili svoje programe od korisnika i antivirusnih programa. Danas na internetu postoji mnoštvo rootkit-ova i zato nas ne čudi njihova velika upotreba.

Backdoor je vrsta zlonamjernog programa koji omogućava udaljeni pristup i kontrolu nad računalom bez znanja korisnika. Za razliku od legitimnih alata za udaljeni pristup, backdoor se instalira i koristi skriveno.
Iskorištava sigurnosne propuste sustava kako bi zaobišao uobičajene provjere i kontrole. Djeluje kao skriveni ulaz koji napadaču dopušta nesmetan pristup sustavu i podacima. Može dati kontrolu nad aplikacijama, datotekama i dozvolama. Backdoor se često koristi u kombinaciji s drugim vrstama zlonamjernog softvera kao inicijalni način za dobivanje pristupa sustavu koji se onda dalje zloupotrebljava. Zbog skrivenog i potencijalno pogubnog djelovanja, smatra se iznimno opasnim oblikom zlonamjernog programa.

Spyware je vrsta zlonamjernog softvera koji se tajno instalira na računalo žrtve i prikuplja osjetljive informacije koje šalje tvorcima spywarea. Za razliku od virusa i crva, spyware se ne mora sam širiti već se često instalira prikriveno uz neki drugi program. Najčešće prikuplja povjerljive podatke poput korisničkih imena, lozinki, brojeva kreditnih kartica, kontakata iz e-maila i slično. Iako ponekad i drugi oblici zlonamjernog softvera prikupljaju takve podatke, spyware je specijaliziran upravo za krađu informacija. Ne replicira se kao virusi i crvi. Prvi put se spominje 1995., a tijekom 2000-ih postaje raširena prijetnja zbog masovne instalacije putem drugih programa. Krađa osjetljivih podataka glavna je svrha i opasnost spywarea.

- Postoji više vrsta spywarea:
- Adware - prikuplja informacije o korisniku i bombardira ga ciljanim oglasima.
- Keylogger - bilježi sve pritisnute tipke i šalje tvorcima. Izrazito opasan.
- Browser hijacker - preusmjerava browser na zlonamjerne stranice, umeće oglase.

- Komercijalni spyware - legalan oblik koji prati aktivnosti uz pristanak korisnika.
- Dialer - mijenja postavke modema da bi ostvario skupe pozive i nanio financijsku štetu.
- Tracking cookie - prati aktivnosti preglednika i korisničke navike.
- Spyware za udaljeno promatranje - omogućuje nadzor zaslona i aktivnosti.
- Različiti oblici imaju specifične metode krađe podataka i zloupotrebe sustava u svrhu financijske dobiti ili kompromitiranja privatnosti.

Spyware koristi razne metode kako bi se instalirao i aktivirao u računalu korisnika. Određen varijante spywarea se instaliraju uz određeni legitimni softver, a najčešće u obliku dodatne alatne trake koja se prikazuje u web pregledniku (toolbar). Druge varijante spywarea kombiniraju načine pristupa trojanaca, pa se predstavljaju da su neki drugi (obično popularni) softver, te ih tako korisnik percipira kao korisne i instalira.
Jedan od najčešćih problema koje iskorištava spyware su rupe (bugovi i exploiti) u web preglednicima. Primjerice, starije verzije Internet Explorera imale su problema s ActiveX komponentama te se spyware Internet Exploreru često prikazivao kao sasvim legitiman softver. Korisnik je najčešće instalirao sve što mu je bilo ponuđeno od strane Internet Explorera, smatrajući to autoriziranim i sigurnim, budući da mu je sam preglednik to ponudio. U novijim inačicama ovog preglednika greške ovakvog tipa su ispravljene te je i sam preglednik dosta sigurniji. Spyware je postao jedan od najopasnijih oblika malicioznog softvera koji je posebno orijentiran na korisnike operacijskog sustava Windows. Internet Explorer je vrlo integriran u operacijski sustav Windows, pa je time i instalirani spyware u većoj mogućnosti prikupiti podatke o korisniku i njegovom radu na računalu.

Botnet je mreža zaraženih računala pod kontrolom napadača, tzv. zombi računala ili botova. Stvara se instaliranjem zlonamjernog softvera poput crva na velik broj računala, koja onda mogu biti kontrolirana i iskorištena za razne aktivnosti. Botnetom upravlja napadač putem naredbi koje šalje botovima. Koristi se za slanje spam poruka, distribuciju zlonamjernog sadržaja, DDoS napade i druge zlonamjerne aktivnosti. Cilj je financijska dobit ili povećanje reputacije napadača, ovisno o veličini botneta. Računala postaju dio botneta bez znanja vlasnika. Zato je važna zaštita od zaraze zlonamjernim programima koji pretvaraju računala u botove pod tuđom kontrolom. Botnet je mreža zaraženih računala koja se mogu iskoristiti u razne svrhe, legalne i ilegalne. Najčešće se koristi za distribuirane napade uskraćivanja usluge

(DDoS), slanje spam poruka i širenje zlonamjernog sadržaja. Računala postaju dio botneta jer nisu adekvatno zaštićena - nemaju antivirus ili vatrozid ili su loše konfigurirana. Napadači koriste ranjivosti da instaliraju zlonamjerni softver poput trojanca, koji ostaje neaktivan dok ga napadač ne aktivira jednostavnom IRC naredbom. Iako se botnetovi uglavnom povezuju s kriminalnim aktivnostima, u distribuiranom računalstvu se koriste i botnetovi legalnih, dobronamjernih čvorova. No najčešće pod botnetom podrazumijevamo mrežu zaraženih računala pod externalnom kontrolom.

1.4.2. DDoS napadi

Distributed Denial of Service (DDoS) napad je vrsta napada usmjerena na onemogućavanje normalnog funkcioniranja nekog sustava ili usluge. Cilj je uskratiti legitimnim korisnicima pristup određenoj mrežnoj usluzi poput web stranice.
DDoS se provodi slanjem velike količine mrežnog prometa s mnogo izvora prema meti napada, što dovodi do preopterećenja i nemogućnosti sustava da odgovori na legitimne zahtjeve. Napadači često koriste botnetove zaraženih računala za provođenje DDoS napada. Ova vrsta napada predstavlja ozbiljnu prijetnju dostupnosti mrežnih resursa i usluga. Cilj je onemogućiti normalan rad sustava bombardiranjem lažnim prometom s Distributed (distribuiranih) izvora.

Definicija prema Stein (2003) kaže da je DDoS ustvari "napad koji koristi više računala za pokretanje koordiniranog DoS napada protiv jednog ili više ciljeva.“[15] „Koristeći klijent/poslužitelj arhitekturu, napadač je u mogućnosti razmnožiti učinkovitost DoS napada iskorištavanjem resursa računala suučesnika u napadu, koristeći ih kao platformu napada. Obično je DDoS master instaliran na jednom računalu i upravlja većim brojem agenata, bilo gdje na internetu. Agenti koje se broje u stotinama ili tisućama, kada dobiju naredbu pokreću napad." „Temeljne su tri kategorije DDoS napada prema Arbor1, N.D.: napadi na propusnost, napadi bazirani na protokolu i napadi aplikacijskog sloja.“[16]

DDoS napad funkcionira tako da veliki broj napadača šalje ogromne količine lažnog mrežnog prometa prema meti napada koristeći krivotvorene IP adrese. To uzrokuje preopterećenje

[15] Stein, L. (2003). The World Wide Web Security FAQ. http://www.w3.org/Security/Faq/wwwsf6.html#DOS-Q2 pristup 11.8.2023.
[16] Arbor1 (n.d.). About DDoS Attacks. ARBOR. http://www.arbornetworks.com/attack-ddos pristup 11.8.2023.

sustava i onemogućuje pružanje usluge legitimnim korisnicima. Mrežni resurs ili usluga postaje nedostupna ili jako usporena zbog prezasićenosti lažnim zahtjevima. To posebno pogađa usluge koje zahtijevaju nisku latenciju i visoku propusnost poput video streamingea ili bankarstva. Broj napadača u DDoS napadu može biti i nekoliko stotina ili tisuća kako bi se generirao dovoljan promet za obaranje sustava. Cilj je onemogućiti normalan rad servisa bombardiranjem s distribuiranih lokacija. Glavni problem kod DDoS napada je veliki broj distribuiranih izvora napada koji otežava obranu. Napadači su često dio botneta, mreže zaraženih računala, i nisu svjesni da sudjeluju u napadu. Zbog velikog broja lažnih izvora prometa s raznih lokacija, nije moguće jednostavno blokirati određene IP adrese, za razliku od standardnog DoS napada. Distribuirana priroda otežava detekciju i zaustavljanje napada. Botnetovi pružaju kriminalskim skupinama ogroman broj računala za pokretanje masovnih DDoS napada i prikrivanje stvarnih izvora. Zato je ovaj oblik napada teže kontrolirati i nanosi veću štetu nego DoS iz manjeg broja izvora.

Napad uskraćivanjem usluge (DoS) predstavlja prijetnju stabilnosti mreže. Uspješno blokiranje dolaznog prometa sa određene adrese je izazov. Međutim, postoje načini da se rizik umanji. Vatrozidi i pravila usmjeravanja mogu pomoći. Također, pružatelji internet usluga imaju alate za detekciju neuobičajenih aktivnosti. Ključno pitanje kod distribuiranog DoS napada je razlikovanje legitimnih i zlonamjernih zahtjeva. Potrebno je pronaći rješenja za prepoznavanje lažnih identiteta i zaštitu resursa mreže. Suradnja između davatelja usluga i korisnika je neophodna za uspješnu obranu od ove prijetnje.

Motivi napada prema Zeltser (2011) „mogu biti različiti: iznuda putem prijetnje napadom, internet sukobi različitih skupina (na primjer u industriji video igara), anti-konkurencija (plaćanje napada sa ciljem rušenja ugleda konkurenciji), kazna za određene nepoželjne radnje određene osobe ili tvrtke, iskazivanje ljutnje i kritike (na primjer prema određenim medijskim portalima), dokazivanje moći ili pak čista dosada bez ikakvog razloga. Internet je dostupan velikom broju ljudi i teško je kontrolirati postupak svakog od njih, a pogotovo kada je riječ o skupinama napadača kao što je ovdje slučaj.[17]

Zbog svoje distribuirane prirode, DDoS napadi predstavljaju ozbiljnu prijetnju dostupnosti mrežnih resursa. Njihova rasprostranjenost i potencijalna šteta čine ih jednim od najvećih izazova cyber sigurnosti. Postoje brojni načini obrane koji se razlikuju po učinkovitosti.

[17] Zeltser, L. (2011). 8 Reasons for Denial-of-Service (DoS) Attacks. http://blog.zeltser.com/post/10775687288/reasons-for-denial-of-service-attacks pristup 11.8.2023.

Moderne strategije obično kombiniraju softverska i hardverska rješenja. Neke uobičajene točke obrane su kod pružatelja usluga, vatrozidi, usmjerivači i sustavi za detekciju upada. Optimalna obrana često uključuje višeslojni pristup implementiran na nekoliko mrežnih čvorova. Ključno je razviti sveobuhvatan i prilagodljiv sustav zaštite koji može prepoznati i ublažiti DDoS prijetnje u realnom vremenu. Suradnja i dijeljenje informacija između dionika je također važna komponenta uspješne obrane.

1.4.3. Phishing napadi

Termin "phishing" potječe od spoja engleskih riječi "password" (lozinka) i "fishing" (pecanje).
Ova riječ opisuje vrstu prijevare putem interneta u kojoj napadač pokušava prikupiti osjetljive podatke korisnika kao što su lozinke ili brojevi bankovnih računa. Phishing se često provodi putem lažnih e-mail poruka ili internetskih stranica koje nalikuju legitimnim stranicama. Cilj je zavarati korisnika da otkrije svoje privatne podatke, slično kao što ribolovac "peca" svoj plijen. Kombinacija riječi "lozinka" i "pecanje" slikovito opisuje suštinu ove prijetnje cyber sigurnosti.

Kibernetički kriminalci koriste phishing kako bi prevarili korisnike da otkriju povjerljive podatke. Šalju zavaravajuće poruke putem instant messaginga, e-pošte ili SMS-a koje sadrže linkove na lažne web stranice pod njihovom kontrolom. Na tim stranicama žrtve upisuju osjetljive informacije kao što su lozinke ili brojevi bankovnih računa. Phishing je kombinacija socijalnog inženjeringa i tehnologije. Cilj je prikupljanje podataka za pristup resursima žrtve. Najčešći oblik phishinga usmjeren je na krađu bankovnih podataka za financijsku dobit ili pranje novca. Korisnici trebaju biti oprezni pri otvaranju sumnjivih poruka i linkova te provjeriti autentičnost web stranica prije upisivanja osobnih podataka. Budnost i edukacija ključni su u obrani od ove rastuće cyber prijetnje.

U sofisticiranim phishing napadima, kibernetički kriminalci preusmjeravaju financijska sredstva između računa pod njihovom kontrolom kako bi prikrili tok novca od jedne strane do druge. Iako se sredstva ne kradu direktno, ovi transferi služe za pranje novca ili financiranje kriminalnih i terorističkih aktivnosti. Zbog toga phishing predstavlja prijetnju ne samo potencijalnim žrtvama i financijskim institucijama, već cijelom društvu. Napredne phishing

tehnike zahtijevaju koordinirane napore na nacionalnoj i međunarodnoj razini kako bi se otkrili i zaustavili tokovi sumnjivih transakcija. Borba protiv phishinga je odgovornost svih - pojedinaca, tvrtki i vlada - kako bi zaštitili financijski sustav i nacionalnu sigurnost od zloupotrebe u kriminalne svrhe.

Iako većina phishing napada još uvijek nije pretjerano sofisticirana, vidljiv je trend njihovog postajanja sve naprednijima, kako tehnološki tako i u manipulativnom smislu. Rastuća učestalost phishinga prisiljava organizacije na poduzimanje mjera zaštite i razvoj protumjera. Bez jasnog rješenja, borba protiv phishinga se nastavlja kao igra mačke i miša u kojoj obje strane pokušavaju predvidjeti sljedeći potez.
Današnje phishing poruke elektroničke pošte obično oponašaju legitimne poruke financijskih institucija i sadrže linkove na lažne web stranice koje izgledaju identično originalu. Na tim stranicama korisnici upisuju svoje podatke za prijavu koji se onda prosljeđuju kiberkriminalcima. Korisnici moraju biti oprezni i provjeravati autentičnost poruka i web stranica kako bi izbjegli krađu osjetljivih informacija putem phishinga.

Jedan od učinkovitijih pristupa u borbi protiv phishinga je pravovremeno otkrivanje napada. Čim se uoči phishing stranica ili poruka, organizacija čiji identitet se zloupotrebljava treba odmah djelovati i zatražiti uklanjanje lažne stranice. Pružatelji usluga na čijim se poslužiteljima nalazi phishing sadržaj (često i sami žrtve) tada mogu brzo reagirati. Mogućnosti detekcije se poboljšavaju zahvaljujući honeypot zamkama, kolaborativnom dijeljenju informacija i poticanju korisnika da prijave sumnjive poruke. Ključno je osigurati brzu razmjenu podataka između svih dionika kako bi se phishing sadržaji uklonili prije nego uzrokuju štetu. „Dok za računalnog kriminalca postoji mala šansa da bude uhvaćen prilikom detekcije njegovog napada, gašenjem baze prikupljenih lozinki, zaustavlja se njegovo daljnje prikupljanje te time ograničava razinu uspjeha njegovih napada. Zaustavljanje napada potiče računalne kriminalce da primjenjuju agresivnije napade.“[18]

„Phishing napadi su klasificirani u raznolike kategorije na temelju načina krađe podataka, mnoga ih istraživanja zovu različitim imenima poput varljivih, malver baziranih, ubacivanje sadržaja phishing napadima i drugo.“[19] Jedno od ključnih sredstava u jačanju obrane od phishinga je edukacija korisnika. Poseban naglasak je na podizanju svijesti i informiranju

[18] Jakobsson, M. & Young, A. Distributed Phishing Attacks, 2005.
[19] Suryavanshi, N. A Review of Various Techniques for Detection and Prevention for Phishing Attack, 2013.

korisnika i studenata o ispravnom postupanju kako bi se izbjeglo nasedanje na phishing trikove. Edukacijski programi bi trebali objasniti kako prepoznati sumnjive poruke i web stranice te ih ne otvarati. Korisnici bi također trebali naučiti provjeravati autentičnost prije dijeljenja osjetljivih podataka. Kontinuirana edukacija svih dobnih skupina je ključna za stvaranje "imuniteta" na phishing napade. Informirani korisnici su najbolja obrana.

„Evo jednog prijedloga za preoblikovanje navedenih savjeta: [20]

- Nikada ne otkrivati osjetljive podatke poput lozinki ili brojeva kartica u porukama elektroničke pošte ili drugim online komunikacijama.
- Budite oprezni pri otvaranju linkova i privitaka u porukama od nepoznatih pošiljatelja. Provjerite jesu li linkovi legitimni prije klikanja.
- Uvijek provjerite autentičnost web stranice prije unosa osjetljivih podataka. Pazite da je veza sigurna i šifrirana.
- Redovito pratite stanje i aktivnosti na svojim računima kako biste pravovremeno uočili svaku sumnjivu transakciju.
- Održavajte računalo i mobilne uređaje ažuriranim te koristite antivirus i firewall za dodatnu zaštitu.
- Budite oprezni i kritički razmislite prije dijeljenja osjetljivih podataka online.“

Iako se čini da su ovi savjeti jednostavni za slijediti, očito je da dosadašnji napori u edukaciji nisu bili dovoljno uspješni u pružanju zaštite od phishing napada. Primjećeni su određeni nedostaci tradicionalnih edukacijskih metoda koje koriste simulirane napade i naknadno ciljano obučavanje onih koji su podložni phishingu. Problem može biti što ako se korisnici obrazuju da traže određene znakove legitimnosti, oni mogu lakše nasjesti na phishing poruke koje imitiraju te indikatore. Potreban je sveobuhvatan i višeslojan pristup edukaciji o phishingu i cyber sigurnosti općenito. Osim tehničkog znanja, korisnici moraju razviti kritičko razmišljanje i sposobnost prepoznavanja znakova upozorenja. Kontinuirana izobrazba i podsjećanje su ključni. Simulacije napada također mogu biti korisne ako su dobro osmišljene i praćene detaljnim povratnim informacijama. Najvažnije je razviti "cyber higijenu" i budnost kod svih korisnika.

[20] Nohlberg, M. Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks 2008.

Postoje indicije da bolje razumijevanje funkcioniranja internet protokola može pomoći korisnicima u pružanju otpora phishing napadima. Osim edukacije, postoje i tehnički pristupi zaštiti od phishinga. Najpoznatiji su anti-phishing programi koji upozoravaju korisnike na potencijalno štetne sadržaje. Neki moderni internet preglednici već imaju ugrađene alate za detekciju phishinga.
Na organizacijskoj i sistemskoj razini postoje brojne strateške mjere koje mogu ojačati obranu, poput uvođenja enkripcije, digitalnog potpisivanja poruka, snažne autentifikacije i sustava za nadzor. Stručnjaci za sigurnost svakodnevno otkrivaju na tisuće pokušaja napada. Stoga je zaštita kritične infrastrukture prioritet nacionalne sigurnosti, jer napadi na vitalne sustave mogu imati katastrofalne posljedice. Kontinuirano unaprjeđenje tehničkih mjera i obrazovanje korisnika ključni su u obrani od ove rastuće cyber prijetnje.

1.4.4. Infrastrukture informatičkog ratovanja

Napadi na internet infrastrukturu i umrežene sustave predstavljaju samo jednu vrstu sigurnosnih incidenata s kojima se suočava moderna informacijska tehnologija. Internet kao globalna komunikacijska platforma nosi sa sobom brojne prijetnje po sigurnost podataka i sustava. Osim direktnih napada na mrežnu infrastrukturu, postoje i drugi oblici zlonamjernih cyber aktivnosti poput phishinga, prijevara, krađe podataka i slično. Za učinkovitu obranu potreban je sveobuhvatan pristup koji uključuje tehničke mjere zaštite, edukaciju korisnika, pravni okvir i međunarodnu suradnju. Borba protiv cyber kriminala zahtijeva neprekidnu budnost i prilagodbu novim prijetnjama.

„Prema NIAC (engl. National Infrastructure Advisory Council) izvještaju iz 2004. godine, navedeni su i slijedeći tipovi incidenta koji uključuju, i to: pokušaj dobivanja pristupa, traženje ranjivosti, neautoriziran pristup, prisluškivanje prometa, DoS napadi, te postavljanje zlonamjernih programa.“[21]

Internetski napadi imaju nekoliko prednosti u odnosu na fizičke napade. Mogućnost udaljenog djelovanja omogućuje napadačima da prikriju svoj identitet, lokaciju i način proboja u sustav. Za razliku od fizičkih napada, kibernetički se mogu izvoditi iz bilo kojeg dijela svijeta, što

[21]Janczewski, C. Cyberwarfare and CyberTerorism, Information Science Reference, USA, 2007.

otežava njihovo sprečavanje i progon počinitelja. Zbog toga je zaštita kritične infrastrukture od internetskih prijetnji iznimno važna za nacionalnu sigurnost. Vitalni sustavi poput opskrbe energijom, transporta, komunikacija i financija izloženi su potencijalnim napadima koji mogu imati katastrofalne posljedice.

Posebnu opasnost predstavljaju terorističke aktivnosti usmjerene na ugrožavanje kritične infrastrukture. Kontinuirano unaprjeđenje mjera cyber sigurnosti i međunarodna suradnja ključni su za ublažavanje ovog rizika. Kako bi se spriječile potencijalno katastrofalne posljedice, države često ulažu u skupe, visokotehnološke sigurnosne sustave za bolje upravljanje kriznim situacijama. Kritična infrastruktura koja uključuje međusobno povezane sustave i resurse ključne za funkcioniranje društva, posebno je izložena terorističkim napadima, špijunaži i hakerskim upadima. Zbog velike važnosti, ove lokacije zahtijevaju zaštitu i od industrijskih nesreća i prirodnih katastrofa. Primjerice, oštećenje brane može prouzročiti prekide u opskrbi vodom, poplavama, nestancima struje i drugim teškim posljedicama. Stoga je osiguravanje otpornosti i kontinuiteta rada kritične , prioritet nacionalne sigurnosti. To iziskuje sveobuhvatan i višeslojan pristup, uključujući redundanciju, fizičku zaštitu, kibernetičku sigurnost, planove za hitne slučajeve i suradnju javnog i privatnog sektora.

Osim fizičkih prijetnji, kritična infrastruktura je izložena i sve češćim hakerskim napadima, posebice zbog rasta cloud computinga i umrežavanja. Stoga su podatkovni centri postali ključna točka za upravljanje rizicima. Američki Nacionalni institut za standarde i tehnologiju izdao je Okvir za cyber sigurnost koji sadrži smjernice za zaštitu kritične infrastrukture od kibernetičkih prijetnji. Ovaj dokument podržala je Bijela kuća kako bi pomogao organizacijama u prepoznavanju i prioritizaciji mjera za smanjenje rizika od napada. Jačanje cyber otpornosti kritičnih sustava zahtijeva višeslojan pristup, uključujući enkripciju podataka, kontrole pristupa, detekciju upada, treninge zaposlenika i redovito testiranje ranjivosti. Suradnja javnog i privatnog sektora ključna je za osiguravanje nesmetanog funkcioniranja vitalnih usluga. „Između ostalog, u tom priručniku se nalazi i opis preporuka za razne aktivnosti u svrhu kvalitetnijeg i boljeg upravljanja rizika od napada.“[22] Zaštita kritične infrastrukture zahtijeva dugoročna ulaganja u tehnološka rješenja. To često dovodi do mješavine novih i zastarjelih sustava koji se istodobno koriste. S obzirom na kompleksnost i

[22] Asadria. http://www.asadria.com/index.php/teme/izdvojeno/319-najvece-sigurnosne-prijetnje-za-kriticnu-infrastrukturu, pristup 11.8.2023.

broj objekata i instalacija, organizirano upravljanje elektroenergetskim mrežama predstavlja značajan izazov.

Kako bi se osigurao kontinuitet usluga i otpornost na prijetnje, potrebna je modernizacija i standardizacija opreme. Legacy sustavi zahtijevaju posebnu pažnju jer mogu biti osjetljivi na napade. Redundancija i diverzifikacija ključnih komponenti također povećava sigurnost. Jasno definirani protokoli reagiranja i oporavka od kriznih situacija su neophodni. Upravljanje sigurnošću kritične infrastrukture iziskuje strateški i cjelovit pristup na nacionalnoj razini.

Da bi se sustavima kritične infrastrukture na više lokacija moglo efikasno upravljati, ključno je integrirati i centralizirati operacije. Jača integracija omogućava centralizirani nadzor i upravljanje, što olakšava održavanje kontinuiteta usluga. Istovremeno, potrebno je pojačati oprez prema fizičkim i kibernetičkim prijetnjama. Centralizirane operacije dopuštaju bolju koordinaciju reagiranja na incidente i brži oporavak sustava. Potrebno je uspostaviti jasne protokole i lanac zapovijedanja. Redundancija i rezervni kapaciteti također povećavaju otpornost. Kontrole pristupa, enkripcija podataka i praćenje aktivnosti važni su za cyber sigurnost. Fizička zaštita objekata i osoblja ne smije se zanemariti. Integrirani pristup upravljanju na strateškoj razini ključan je za osiguravanje pouzdanosti i sigurnosti kritičnih sustava.

„Upravljanje rizicima za kritičnu infrastrukturu, predstavlja složen postupak za operatera infrastrukture, i to zbog složenog rasporeda različitih sistema, uređaja i postrojenja na širem području. Za ovakvu infrastrukturu naročito su pogodni višeslojni sustavi zaštite perimetra koji mogu ponuditi sveobuhvatnu zaštitu od različitih prijetnji, poput vandalizma, neovlaštenih upada, terorističkih napada i dr. Tako se predviđa se da će vrijednost globalnog tržišta senzora za elektronsku zaštitu perimetra i video nadzor u elektranama i rafinerijama zabilježiti golem rast, usprkos dubokoj ekonomskoj krizi. Ovakve tendencije nastaju zbog korištenja video nadzora na daljinu i umreženih senzora za potrebe daljinskog podešavanja i upravljanja uređajima.“[23] Nuklearna postrojenja zahtijevaju robustne višeslojne sustave zaštite perimetra. Arhitektonski dizajn takvih objekata obično uključuje zone senzora za detekciju, počevši od vanjskog pojasa. Kod osiguravanja perimetra važna je adekvatna integracija video

[23] Asadria. http://www.asadria.com/index.php/teme/izdvojeno/319-najvece-sigurnosne-prijetnje-za-kriticnu-infrastrukturu, pristup 11.8.2023.

nadzora i sustava za detekciju uljeza. Svaki neovlašteni ulazak treba automatski aktivirati alarm i poslati snimku kontrolnom centru, kako bi se spriječio fizički napad. Redundantni sustavi video nadzora s analitikom pokreta i termalnim kamerama pružaju robustnu perimetralnu zaštitu. Kontrolni centri moraju biti opremljeni naprednim softverom za koordinaciju reagiranja i brzu mobilizaciju interventnih snaga.

Prilazi, ograda i ostale fizičke barijere također su važne za odvraćanje i usporavanje uljeza. Sveobuhvatna strategija integrirane fizičke i tehničke zaštite ključna je za osjetljive lokacije. Osnovni cilj zaštite kritične infrastrukture je omogućiti osoblju brzo uočavanje prijetnji. Izuzetno je važno imati centralizirani sustav upravljanja za koordinirano reagiranje. Osim toga, sigurnosni sustavi poput video nadzora, kontrole pristupa i zaštite perimetra mogu se integrirati preko zajedničke platforme s IT sustavima, sustavima za detekciju dima i požara, protupožarnom zaštitom, komunikacijama i automatizacijom. Sigurnosno rješenje ne podrazumijeva samo povezivanje opreme, već i uspostavljanje protokola za brz i učinkovit odgovor na krizne situacije. Potrebno je definirati jasne procedure, lance komunikacije i odgovornosti. Redovito testiranje, obuka osoblja i simulacije incidentnih scenarija također su ključni. Cilj je postići koordiniranu reakciju različitih timova kako bi se ublažile posljedice i osigurao kontinuitet rada kritičnih sustava.

1.5. METODE OTKRIVANJA UPADA U SUSTAV

1.5.1. IDS (Intrusion Detection System)

„Sustav za otkrivanje uljeza je uređaj koji može biti softverski ili hardverski, otkriva napade na način da skuplja podatke o informacijskim sustavima i mreži, te na taj način analizira simptome sigurnosnih problema (incidenata).“[24] S obzirom da su upadi u kritičnu infrastrukturu iznimno opasni, IDS ima veliku ulogu u njihovom sprečavanju. IDS kontinuirano prikuplja i analizira podatke o događajima u mreži i sustavima kako bi identificirao zlonamjerne aktivnosti. Koriste se metode prepoznavanja poznatih obrazaca napada i detekcije anomalija. Mrežni promet, aktivnosti servera, integritet datoteka i slično se nadziru u potrazi za indikatorima upada. Učinkoviti IDS zahtijeva kombinaciju više tehnika, uključujući heuristiku, strojno učenje i crowdsourcing prijetnji. Rano otkrivanje i brzi

[24] Jaiganesh, Mangayarkarasi, Sumathi IJARCC - International Journal of Advanced Research in Computer and Communication Engineering

odgovor su ključni za ublažavanje štete od upada. Kontinuirano unaprjeđenje detekcijskih sposobnosti važno je za održavanje sigurnosti kritičnih sustava.

Detekcija zlouporabe otkriva upade uspoređivanjem aktivnosti s poznatim obrascima napada i potpisima. Detekcija anomalija pokušava identificirati zlonamjerne aktivnosti na osnovi odstupanja od uobičajenog ponašanja. Kod detekcije anomalija, IDS prikuplja podatke o uobičajenim operacijama sustava u određenom vremenskom razdoblju. Te se informacije onda koriste za prepoznavanje neuobičajenih promjena koje mogu ukazivati na zlonamjerne aktivnosti. Zbog oslanjanja na obrasce normalnog ponašanja, ova se tehnika još naziva i detekcija ponašanja. Ključno je ažurirati profile normalnih operacija kako bi se održala preciznost u identifikaciji anomalija koje ukazuju na mogući upad.

Prednost detekcije anomalija je mogućnost otkrivanja nepoznatih napada na temelju analize podataka, dok ponekad može propustiti prepoznati poznate napade. S druge strane, detekcija potpisa efikasno otkriva poznate obrasce, ali ne može identificirati nove prijetnje. Kombiniranjem ovih tehnika uz korištenje rudarenja podataka za izdvajanje uobičajenih aktivnosti, mogu se nadvladati njihovi nedostaci. Na taj način IDS može preciznije prepoznati stvarne napade. U osnovi, upadi se otkrivaju otkrivanjem sigurnosnih propusta u sustavu. IDS ima pasivan pristup - samo motri aktivnosti i alarmira o potencijalnim incidentima. No pravovremeno otkrivanje prijetnji ključno je za reagiranje i sprječavanje većih šteta. Kontinuirano poboljšanje sposobnosti detekcije, uz adekvatne procese reagiranja, pomaže održati visoku razinu sigurnosti kritičnih sustava.

1.5.2. Identifikacija i lokalizacija digitalnih adresa na Internetu

Iako je internet razvijen od strane američke agencije DARPA kroz ARPANET projekt, široku upotrebu doživio je tek sredinom 1990-ih. Danas je neizostavan dio modernog društva. No sve veća ovisnost o internetu donosi i probleme u vidu ranjivosti na cyber napade, kako digitalnih tako i fizičkih sustava povezanih na mrežu. Velik broj internet aplikacija oslanja se na IP (engl. Internet Protocol) i transportne protokole TCP i UDP. IP omogućuje isporuku paketa različitim rutama što ga čini otpornim na prekide u mreži, ali ne pruža sigurnost. TCP i UDP također nemaju ugrađene sigurnosne mehanizme. Zbog toga su potrebni dodatni protokoli i tehnologije za osiguravanje pouzdanosti i integriteta kritičnih podataka.

Kontinuirano unaprjeđenje arhitekture interneta ključno je za održavanje raspoloživosti i otpornosti na sve sofisticiranije cyber prijetnje. „IP paket se usmjerava između dva domaćina putem posredničkih routera, a svaki router donosi odluku gdje će usmjeriti paket.“[25] Digitalne adrese identificiraju korisnike, uređaje, usluge i resurse na internetu. Primjeri uključuju MAC adrese, IP adrese, AS brojeve, DNS domene, URL-ove i e-mail adrese. IANA (engl. Internet Assigned Numbers Authority) je krovna organizacija koja dodjeljuje i koordinira globalne IP adrese i AS (engl. Autonomous System) brojeve. Ove jedinstvene adrese omogućuju uspostavljanje komunikacije između različitih mreža i krajnjih točaka. Centralizirana administracija adresnog prostora je nužna za interoperabilnost interneta. IANA osigurava da se adrese dodjeljuju na strukturiran i hijerarhijski način kako bi se izbjegli sukobi i dupliciranje. To je ključno za pouzdano funkcioniranje globalne internet infrastrukture. Korisnik na Internetu spojen je sa različitim bazama podataka vezanim za njegovu registraciju, primjerice IP adresa je registrirana u IP WHOIS bazi, njegova domena je registrirana u DNS WHOIS bazi, ainformacije o njegovoj lokaciji na Internetu su pohranjene u tablicama prosljeđivanja (engl. routing tables).

Sve ove informacije mogu poslužiti kako bi dobili ostale informacije o samoj lokaciji i identifikaciji adresa korisnika na Internetu.“[26] Da bi se mogao pratiti trag na internetu, treba poznavati interakciju između različitih protokola, svaki protokol može imati svoj način adresiranja, pri čemu je potrebno otkriti najnižu razinu adrese, odnosno hardversku adresu na fizičkoj mreži kako bi povezali adresu sa korisnikom ili njegovom lokacijom.

1.6. Zaštita sigurnosti informacijskih sustava

Kada se govori o informacijskoj sigurnosti, važno je shvatiti da je to kontinuirani proces koji nikad nije dovršen. Apsolutna sigurnost ne postoji, a ljudski faktor igra veliku ulogu. Sigurnost ovisi o identificiranju i adresiranju ranjivosti, implementaciji tehničkih kontrola i stalnim poboljšanjima. Potrebno je razviti sveobuhvatan pristup upravljanja rizikom i razumjeti da je sigurnost dinamično područje koje zahtijeva stalnu evaluaciju i unaprjeđenje. Pogrešno je smatrati da postoji konačno rješenje.

[25] Janczewski, C. Cyberwarfare and CyberTerorism, 2008.
[26] Janczewski, C. Cyberwarfare and CyberTerorism, 2008.

Umjesto toga, organizacije moraju kontinuirano educirati zaposlenike, provoditi revizije, uvoditi nove tehnologije i procese te prilagođavati sigurnosne mjere novim prijetnjama. Budnost i proaktivnost svih dionika su ključni za održavanje primjerene razine sigurnosti informacijskih sustava.

„Sigurnost informacijskog sustava je niz mjera i postupaka koji se poduzimaju da bi se omogućila funkcionalnost informacijskog sustava i integritet sadržaja u svim uobičajenim oblicima njegovog djelovanja.“[27] Zadaća sigurnosnih sustava je osigurati pouzdan prijenos poruka između sudionika komunikacije bez izmjena ili gubitaka. Prilikom uspostave sigurnosti informacijskog sustava, važno je voditi računa da troškovi provedenih mjera ne budu veći od potencijalne štete uslijed kompromitiranja informacija. Sigurnosne kontrole treba pažljivo odabrati kako bi pružile optimalnu zaštitu uz prihvatljive troškove. Potrebno je procijeniti vrijednost informacijskih resursa i identificirati realne prijetnje. Mjere poput enkripcije, kontrole pristupa, praćenja aktivnosti i backupa treba implementirati ondje gdje donose najveću korist. Informacijska sigurnost zahtijeva pronalaženje ravnoteže između zaštite i praktičnosti. Kontrole ne smiju biti prekomjerne, međutim, ni nedovoljne. Kontinuirana procjena rizika i cost-benefit analiza pomažu optimalnom osiguranju sustava.

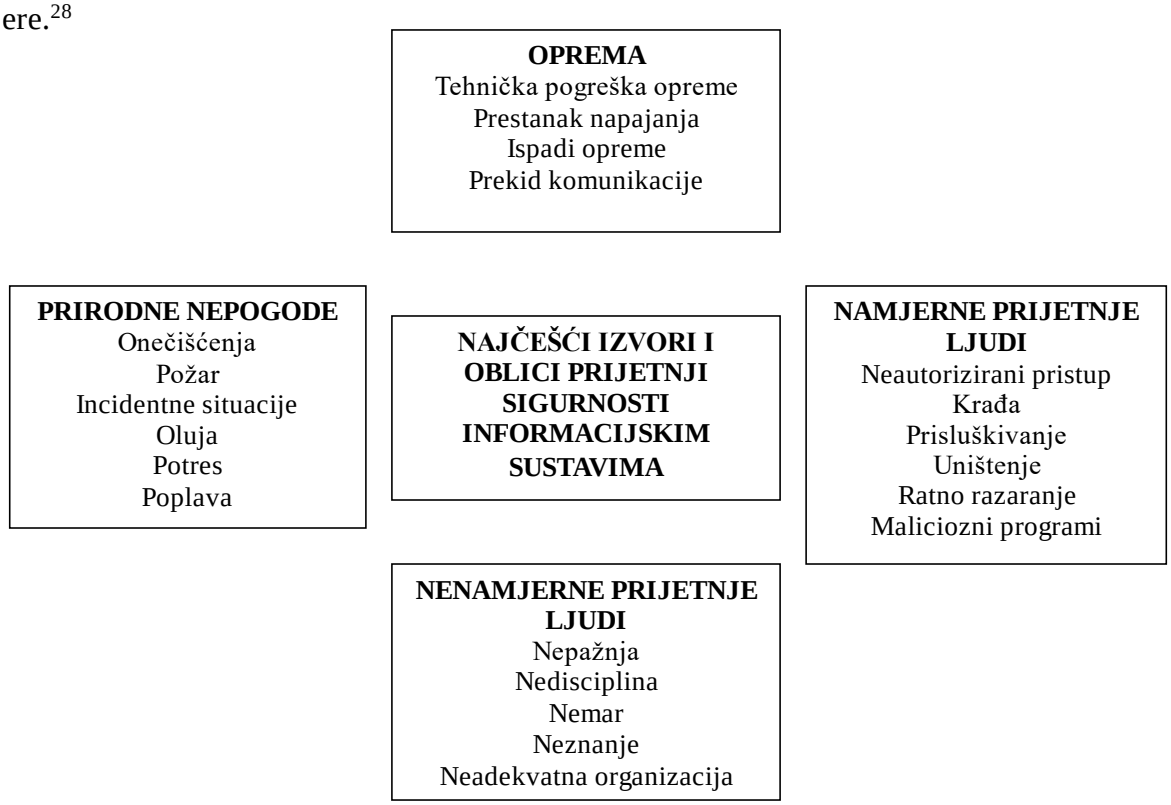
Da bi se odabrala odgovarajuća sigurnosna rješenja, potrebno je provesti dvije ključne procjene:

1. Procjena važnosti podataka - određuje se vrijednost i osjetljivost informacija na temelju zakonskih propisa i poslovnih zahtjeva.
2. Procjena prijetnji - identificiraju se potencijalni unutarnji i vanjski izvori prijetnji te njihovi mogući oblici, u skladu s procjenom važnosti podataka.

Ove analize daju okvir za odabir prikladnih tehničkih i organizacijskih mjera zaštite koje će osigurati povjerljivost, integritet i dostupnost informacija. Kontinuirano preispitivanje procjena omogućuje prilagodbu sigurnosnih kontrola promjenjivom okruženju prijetnji i poslovnih zahtjeva. Vjerojatnost prijetnje ovisi o zainteresiranosti drugih subjekata za pojedine sadržaje. S toga, kao što je vidljivo na slici 2, razlikuje se četiri izvora prijetnji informacijskom sadržaju, i to su: priroda, tehnička greška i čovjek s atribucijom namjernosti i nenamjernosti.

[27] Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.

Kao što se može pretpostaviti, na prirodu se ne može djelovati, ali se mogu izgraditi mjere prevencije ili smanjivanja rizika, pa tako razlikujemo organizacijske, građevinske i tehničke mjere.[28]



Slika 2. Izvori i oblici prijetnji sigurnosti

Tehničke pogreške su vrlo vjerojatne i predvidljive prijetnje čije se posljedice relativno lako mogu ublažiti. Mjere zaštite od tehničkih grešaka uglavnom su tehničke prirode, što olakšava upravljanje sigurnosnom razinom i funkcionalnosti informacijskog sustava. Ljudski faktor je ipak najčešći uzrok prijetnji informacijskoj sigurnosti, bilo namjernim ili nenamjernim radnjama. Pogreške ili zlonamjerne radnje ljudi teže je kontrolirati tehničkim mjerama. Zato su edukacija korisnika, jasne sigurnosne politike i motiviranje zaposlenika ključni za ublažavanje ljudskog faktora kao izvora prijetnji. Sveobuhvatan program informacijske sigurnosti mora uzeti u obzir i tehničke i ljudske aspekte kako bi sustav bio otporan na razne vrste prijetnji.

[28] Hutinski,Ž. Informatika za ekonomiste, FET, Pula, 2002.

„Kao jedna od najučinkovitijih mjera za obranu od ovog tipa prijetnji, svakako susocijalne i organizacijske mjere, odnosno ulaganje u radno zadovoljstvo zaposlenika i njihovu sigurnost, dok ostale nisu toliko učinkovite i zahtijevaju veća ulaganja ali i češće dovode do neuspjeha, ukoliko se prijetnja nalazi u samom sustavu.“[29] U praksi postoje brojni načini kojima se može ugroziti informacijska sigurnost. Tri glavna oblika prijetnji su: neovlašteno korištenje podataka, neidentificirana izmjena i uništenje informacija. Kontrola pristupa ili autorizacija je jedan od ključnih mehanizama obrane koji osigurava tajnost i sprječava zloupotrebu informacija. Autorizacijom se regulira koji korisnici mogu pristupiti kojim podacima i radnjama. Time se štite informacije od upada hakera i drugih neovlaštenih osoba. Ograničavanjem pristupa na najmanju potrebnu razinu, primjenom načela najmanjih privilegija, smanjuje se rizik od zlonamjernih radnji. Autorizacija je dio sveobuhvatnog pristupa zaštiti od uobičajenih prijetnji povjerljivosti, integritetu i dostupnosti informacija.

Postoji više modela kontrole pristupa koji na različite načine organiziraju korisnička ovlaštenja. Neki uobičajeni mehanizmi za poboljšanje sigurnosti su kriptografija, autentifikacija i autorizacija. Svrha kontrole pristupa je provođenje sigurnosnih politika kroz definiranje ovlasti pristupa. Ovlasti se određuju prema razini rizika, odnosno potrebi osiguranja:

- Povjerljivosti - pristup informacijama dopušten je samo autoriziranim korisnicima.
- Integriteta - samo ovlašteni korisnici mogu mijenjati informacije.
- Raspoloživosti - pristup informacijama omogućen je autoriziranim korisnicima kada je to potrebno.

Kontrolom pristupa upravlja se rizicima i štite povjerljivost, točnost i dostupnost informacija prema definiranim sigurnosnim politikama. Kontrola pristupa ima za cilj očuvati povjerljivost i integritet informacija. Postoje različiti modeli implementacije kontrole pristupa:

- Diskrecijski model (DAC) kontrolira pristup računalnim resursima kao što su datoteke i direktoriji.
- Mandatorni model (MAC) ograničava pristup resursima samo na subjekte s odgovarajućom dodijeljenom klasifikacijom. Kontrolu provodi operacijski sustav prema definiranim pravilima.

[29] Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.

- Model grupa i uloga dodjeljuje pristup na osnovi pripadnosti korisnika određenim grupama ili ulogama.

Bez obzira na model, kontrola pristupa uspoređuje operaciju koju korisnik pokušava izvršiti s unaprijed definiranom sigurnosnom politikom kako bi odobrila ili zabranila pristup.

Time se osigurava da samo ovlašteni korisnici mogu pristupiti osjetljivim informacijama. Ključna razlika između mandatornog i diskrecijskog modela je što se kod mandatornog sigurnosna politika provodi centralizirano. Treći model je model temeljen na ulogama (RBAC) koji ograničava pristup prema dodijeljenim ulogama korisnika. RBAC model nudi fleksibilniju alternativu mandatornom i diskrecijskom pristupu. Korisnici se svrstavaju u grupe s definiranim ulogama kojima su pridružena specifična ovlaštenja pristupa. RBAC omogućuje lakšu administraciju većeg broja korisnika i njihovih privilegija. Prednost RBAC modela je što može implementirati i mandatorna i diskrecijska ograničenja pristupa. Svakoj ulozi se dodjeljuju potrebne autorizacije, čime se osigurava da korisnici imaju pristup samo informacijama i resursima nužnim za obavljanje svojih zadataka. To pojednostavljuje upravljanje pristupom uz održavanje sigurnosti.

„Potrebno je naglasiti razliku između grupa i uloga, gdje grupu definira skup određenih pravila, a ulogu uređeni skup prava pristupa koja se mogu, u nekom vremenskom periodu upotrebe određenog resursa, vezati uz pravila.“ [30] Neovlašteno korištenje sadržaja najčešće se ostvaruje kroz špijunažu i krađu podataka. Ovo predstavlja prijetnju povjerljivosti informacija. Neidentificirana izmjena sadržaja može imati ozbiljne posljedice za poslovni sustav. Kompromitiranje integriteta podataka dovodi u pitanje njihovu točnost i pouzdanost. Obje vrste prijetnji zahtijevaju pažljivo osmišljene mjere zaštite. Povjerljivost se osigurava kontrolom pristupa i kriptiranjem osjetljivih podataka. Integritet se štiti autorizacijom izmjena, digitalnim potpisima, detekcijom upada i praćenjem aktivnosti. „Uništenje sadržaja je najagresivnija metoda, te se najlakšeotkriva i iz tog razloga se rijetko koristi.“[31] Informacijski sustav se sastoji od 6 osnovnih komponenti: hardware, software, lifeware, orgware, netware i dataware. Mjere zaštite se mogu primijeniti na svakoj od tih komponenti i dijele se u nekoliko kategorija:

[30] Cis, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-218.pdf, pristup 11.8.2023.

[31] Hutinski,Ž. Informatika za ekonomiste, FET, Pula, 2002.

- Zaštita sadržaja podataka - kriptiranje, anonimizacija, kontrola pristupa
- Zaštita nositelja podataka - enkripcija medija, kontrola fizičkog pristupa
- Programska zaštita i zaštita programa - autorizacija, autentifikacija, antivirus, IDS
- Fizičke i tehničke mjere - kontrola pristupa, video nadzor, UPS, zaštita od požara
- Organizacijske mjere - sigurnosne politike, procedure, obuka korisnika
- Pravne mjere - ugovori, regulacija privatnosti i zaštite podataka

Sveobuhvatna strategija uključuje kombinaciju različitih mjera na svim elementima sustava kako bi se osigurala povjerljivost, integritet i dostupnost informacija. S aspekta informacijske sigurnosti, podaci su jedini nenadoknadivi element sustava. Podaci predstavljaju apstraktne informacije koje opisuju stanje sustava u određenom trenutku. Da bi se mogli koristiti, podaci moraju biti pohranjeni na nekom fizičkom mediju. Budući da su jednom izgubljeni podaci nepovratni, oni su najkritičniji dio za zaštitu. Međutim, podatke ne možemo zaštititi odvojeno od nositelja na kojima su zapisani. Stoga je osiguravanje fizičkih nositelja poput diskova, traka ili čipova ključno za očuvanje samih podataka. Sveobuhvatna strategija uključuje mjere kao što su enkripcija, kontrola pristupa, geografski distribuirane pohrane i sigurnosne kopije kako bi se osigurala dostupnost i integritet kritičnih podataka. Zaštita nositelja i samih podataka mora biti višeslojna kako bi se informacije mogle pouzdano koristiti i čuvati.

1.6.1. Programske mjere zaštite

Neki uobičajeni oblici programske zaštite su:

- Zaštita na razini operacijskog sustava - kontrola pristupa, zakrpe, ograničenje privilegija.
- Zaštita aplikacija - autorizacija i autentifikacija korisnika, validacija ulaza.
- Sigurnosno kopiranje - periodičko arhiviranje i pohrana kopija podataka.
- Enkripcija podataka - šifriranje podataka u prijenosu i pohrani.
- Antivirusni alati - detekcija i uklanjanje zlonamjernog koda.
- Vatrozid - filtriranje mrežnog prometa prema definiranim pravilima.
- IDS/IPS - nadzor i detekcija upada u sustav i mrežu.

Sveobuhvatna zaštita zahtijeva kombinaciju više tehnika za osiguravanje povjerljivosti, integriteta i dostupnosti programske podrške i podataka. Višekorisnički operacijski sustavi

moraju odvojiti resurse i podatke svakog korisnika. To se postiže autentifikacijom korisničkih računa lozinkama. Računi se dijele na administratorske s više privilegija i obične s ograničenim ovlastima.
Nakon odobrenog pristupa, korisnik mora unijeti lozinku i za pokretanje pojedinih aplikacija. Time se dodatno ograničava pristup. Za zaštitu podataka koriste se metode redundantnih diskovnih polja RAID koja povećavaju dostupnost i integritet podataka. Druge mjere uključuju enkripciju pohrane i komunikacija, praćenje aktivnosti, ograničavanje privilegija i redovito sigurnosno kopiranje. Višeslojna autentifikacija i autorizacija na razini sustava, aplikacija i podataka ključne su za zaštitu višekorisničkih okruženja.

Osim RAID polja, neke druge uobičajene metode izrade sigurnosnih kopija i osiguravanja dostupnosti podataka su:

- Back-up serveri - namjenski poslužitelji za pohranu arhivskih kopija podataka
- NAS (Network Attached Storage) - mrežni diskovi za dijeljenje podataka i sigurnosno kopiranje
- Prijenosni mediji velikih kapaciteta - vanjski diskovi, trake, optički mediji za arhiviranje podataka
- Cloud backup - kopiranje podataka na udaljene cloud spremišta
- Replikacija - automatsko umnožavanje kopija podataka na više lokacija

Kombinacija više tehnika, zajedno s planovima oporavka od katastrofe, osigurava dostupnost missijskih kritičnih podataka u slučaju oštećenja ili gubitka originalnih kopija. Tri glavne metode izrade sigurnosnih kopija su:

- Potpuno kopiranje - kopiraju se svi podaci
- Inkrementalno - kopiraju se samo promjene u odnosu na zadnju kopiju
- Diferencijalno - kopiraju se datoteke promijenjene od potpune kopije

Kod distribuiranih sustava javlja se potreba za sigurnom razmjenom podataka na udaljenim lokacijama. Da bi se osigurala autentičnost i povjerljivost, koriste se kriptografski protokoli. Poruke se kodiraju algoritmom pri slanju, a primatelj dekodira i provjerava integritet. Time se sprječava neovlašteno korištenje ili izmjena sadržaja. Postoje razni standardi enkripcije poruka i podataka u prijenosu i mirovanju. Višeslojni pristup uključuje kriptiranje,

autentifikaciju korisnika, autorizaciju i druge mjere za osiguravanje informacija u prijenosu, pohrani i pristupu.

Tako su ranije bili poznati supstitucijski sustavi kojima se jedan slovni znak zamjenjivao s drugim ili grupom znakova, dok se danas preoblikuje poruka pomoću ključa. Istim ključem se obavlja idešifriranje poruke.

Točno, korištenje asimetrične kriptografije s javnim i privatnim ključem pruža veću sigurnost u zaštiti podataka. „Ovakvi sustavi zaštite su postali neophodni kod elektronskog trgovanja i poslovanja, gdje je izuzetno važno osigurati sadržaj od promjene ili zloporabe sadržaja.“[32] Mrežna komunikacija zahtijeva zaštitu od zlonamjernog koda kao što su virusi, crvi i trojanski konji. Koriste se preventivne i sanacijske mjere zaštite:

- Organizacijske - zabrana unosa medija, kontrola izvora programa
- Nadzorne - antivirusni programi, skeniranje, provjera integriteta datoteka
- Sanacijske - detekcija, izolacija zaraženih sustava, uklanjanje prijetnji
- Ažuriranje antivirusnih baza, zakrpe za OS i aplikacije
- Ograničavanje izvršavanja i instalacije programa, whitelisting
- Obrazovanje korisnika o prijetnjama i vektorima zaraze

Optimalna strategija kombinira tehničke alate, politike, svijest korisnika i brzi odgovor kako bi se minimizirao rizik od malicioznog koda u mrežnom okruženju.

„Za razliku od nadzornih, kod sanacijskih mjera, postupak koji se provodi prilikom zaraze, treba otkriti zarazu, izolirati i ograničiti ju, očistiti maliciozni kod i vratiti podatke, te na kraju ponovno instalirati programsku podršku.“[33]

U sustavima s mrežnom komunikacijom neizostavna je ugradnja vatrozida (engl. firewalla). Firewall filtrira dolazni i odlazni mrežni promet prema definiranim pravilima kako bi onemogućio pristup neovlaštenim korisnicima i zlonamjernom sadržaju. Firewall dopušta samo autoriziranu komunikaciju određenih aplikacija i protokola između unutarnje mreže i interneta. Provodi se kontrola i filtriranje dolaznog prometa te autorizacija svakog izlaznog zahtjeva. Time se ostvaruje segmentacija mreže i ograničava pristup samo nužnim servisima. Pravilno konfiguriran vatrozid u kombinaciji s ostalim mjerama poput autentifikacije

[32] Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.

[33] Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.

korisnika, antivirusne zaštite i ažuriranja softvera ključan je za osiguravanje perimetra mreže od vanjskih prijetnji. Potrebno ga je kontinuirano nadzirati i prilagođavati sigurnosnim zahtjevima.

„Dok poslužitelj provjerava ovlasti korisnika koji pokušava pristupiti lokalnoj mreži, kontrola ulaznog sadržaja se postiže na način da korisnik lokalne mreže u zaglavlju ugrađuje identifikacijske elemente koji se provjeravaju.“[34]

1.6.2. Cyber obrana

Kibernetički prostor i internet su pokretači društvenog razvoja i izvori moći u tehnološkoj eri. Međutim, ta ovisnost nosi i rizike kibernetičkih prijetnji. Stoga je nužno sustavno ulagati u jačanje kibernetičke sigurnosti, jer je to ključ napretka. Osnovna ranjivost proizlazi iz potrebe za prikupljanjem i razmjenom ogromnih količina podataka. To zahtijeva podizanje svijesti i zajedničke napore u suzbijanju prijetnji. Potrebna je međunarodna suradnja, koja je za sada nedovoljna. Uz pravnu regulativu, sve važnije postaju ljudski potencijali i vrhunska edukacija stručnjaka. Ulaganje u tehnološki razvoj i ljudske resurse imperativ je za suprotstavljanje rastućim izazovima kibernetičke sigurnosti. Obrana mora biti sveobuhvatna, proaktivna i kontinuirano unaprjeđivana. Naglasak treba biti na prevenciji, a ne samo reagiranju na incidente. Samo zajedničkim naporom svih dionika moguće je izgraditi otporan kibernetički prostor.

Zbog povećane prijetnje u posljednje vrijeme članice Europske unije u sklopu NATO programa sigurnosti razvijaju i posebnu strategiju zaštite informatičkog prostora zemalja članica. Tako je i Hrvatska u tom smislu prihvatila aktualne transformacijske ciljeve koji se odnose na „... razvoj sposobnosti štićenja informacijskih sustava i sposobnosti cyber-obrane informatičkog prostora. „Podrazumijeva se da kao zemlja saveznik i partner, sudjeluje u izgradnji i zaštiti vlastitih ali i savezničkih sposobnosti obrane informatičkog odnosno cyber-prostora, edukacija osoblja organiziranjem odnosno sudjelovanjem u seminarima dio su alata ostvarenja ciljeva razvoja cyber-sposobnosti“.[35] Informatički prostor omogućuje nove oblike špijunaže i sabotaže, kako u miru tako i u sukobima. Strateški podaci se mogu prikupljati

[34] Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.
[35] Hrvatski vojnik, broj 426, srpanj 2013.

cyber napadima, a kritična infrastruktura destabilizirati. Zbog tih prijetnji, NATO razvija nove koncepte djelovanja u kibernetičkom prostoru. To uključuje organizacijske promjene, doktrinarne inovacije i tehnološki razvoj.
Cilj je izgraditi sposobnosti za prevenciju, odvraćanje i reagiranje na širok spektar cyber prijetnji. To zahtijeva višenacionalnu suradnju i koordinaciju NATO saveznika. Ključno je razviti robustnu cyber obranu kritičnih sustava i mreža. Nove cyber sposobnosti integrirat će se s tradicionalnim domenskim operacijama. Cilj je osigurati informacijsku superiornost Saveza u suočavanju s novim izazovima sigurnosnog okruženja. Jedinstveni pristup obrani kibernetičkog i fizičkog prostora nužan je za učinkovito odvraćanje i reagiranje na prijetnje.

Takvim pristupom obuhvaćeno je više značajnih pitanja, kao što su „...definiranje kritične infrastrukture, primjena vojnih i civilnih resursa u upravljanju u krizama, upućivanja i prihvata forenzičara u istragama, izdavanja naredbi ili uvjeravanju davatelja internet usluga za blokadu prometa, aktivne obrane s ciljem narušavanja zapovjedno-upravljačke infrastrukture koja onemogućava napad i sl.“[36] U toj NATO strategiji, definiran je i pojam cyber-ratovanja „...u strogo vojnom kontekstu i sustavu glavni motivi napada podrazumijevaju pokušaj narušavanja operativnog ciklusa protoka informacija, promišljanja, donošenja odluka i zaključno operativnog tempa i snage djelovanja“.[37] Trenutno stanje kibernetičke sigurnosti u sustavu Ministarstva obrane RH nalazi se u fazi unapređenja i jačanja, s ciljem daljnjeg razvoja planova za ostvarivanje NATO standarda i uspostave vlastitog okvira za izgradnju obrambenih cyber kapaciteta.

2. STUDIJE SLUČAJA UGROZA U KIBERNETIČKOM PROSTORU U 20. i 21. STOLJEĆU

Dolaskom hakerske scene u Narodnoj Republici Kini, koja se pojavila kao odgovor na organizirani ustanak u Indoneziji u svibnju 1998., okupilo se oko 3000 hakera u grupu nazvanu Kineski hakerski centar za hitne sastanke. Ova grupa je zatim pokrenula napade na internetske stranice indonezijske vlade. „To je prvi zabilježeni masovniji oblik hakerskog okupljanja radi informatičkih napada.“[38] Nakon NATO bombardiranja kineskog

[36] Hrvatski vojnik, broj 426, srpanj 2013.
[37] Hrvatski vojnik, broj 426, srpanj 2013.
[38] Cyberwar – Kibernetičko ratovanje, Tokensb

veleposlanstva u Beogradu u svibnju 1999., u Kini je osnovana nova hakerska grupa pod nazivom Kineski crveni hakerski savez. Oni su zatim pokrenuli niz napada na stotine internetskih stranica vlade Sjedinjenih Američkih Država. „Nakon sudara kineskog borbenog zrakoplova s američkim vojnim zrakoplovom iznad Južnog kineskog mora 2001. godine, 80.000 hakera je pokrenulo obrambeni informatički rat, budući da je taj čin protumačen kao agresija SAD-a.“[39]

Godine 2008. došlo je do kibernetičkog rata između izraelskih i arapskih hakera u sklopu izraelsko-palestinskog sukoba. Širenje i rastuća opasnost ovakvih napada vidljivi su i u korištenju kibernetičkog prostora u rusko-čečenskom ratu od 1997. do 2001. godine. Ruska Savezna Sigurnosna Služba (FSB) onesposobila je dva ključna čečenska web sitea istovremeno s ruskim oružanim napadom na čečenske teroriste. Slično se dogodilo i u sukobu SSSR-a i Estonije, gdje su opsežni DDoS napadi onesposobili estonske vladine stranice i stranice kritične infrastrukture (parlament, ministarstva, komunikacije i sl.).

Prvi kibernetički napad u rusko-gruzijskom ratu 2008. godine pokrenut je istovremeno s kopnenom, pomorskom i zračnom invazijom, čime je započeo koordinirani kibernetički rat napadima na stranice gruzijske vlade i druge strateški važne stranice, uključujući one američkog i britanskog veleposlanstva. Slični oblici kibernetičkih napada zabilježeni su i u Iranu, Sjevernoj Koreji i drugdje. S obzirom na opseg i složenost napada te značajne posljedice, u praksi se ističe nekoliko značajnijih slučajeva ratova u kibernetičkom prostoru, koji uglavnom ukazuju na Kinu kao vodeću državu u kibernetičkoj špijunaži.

2.1. Moonlight Maze

Moonlight Maze je šifrirani naziv za vrlo ozbiljan sigurnosni incident koji stručnjaci za informacijsku sigurnost i obavještajne službe smatraju jednim od najdugotrajnijih APT (naprednih kontinuiranih prijetnji) napada u novijoj povijesti. Dogodio se 1999. godine i zabilježen je kao prvi kibernetički napad u nizu protiv računalnih sustava SAD-a. Prvi puta uočen je u ožujku 1998. kada su primijećene neuobičajene aktivnosti u zatvorenim mrežama. Metom napada bila je kritična infrastruktura kao što su Pentagon, NASA, Ministarstvo energetike, laboratoriji za naoružanje i sveučilišta širom SAD-a. Cilj je bio krađa povjerljivih

[39] Kibernetičko ratovanje, Tokensb

podataka o informacijskim sustavima i pohranjenim informacijama. „Taj napad je trajao dvije godine, pri čemu su napadači pregledavali tisuće dokumenata, uključujući planove vojnih instalacija, razmještanja vojnih trupa i planove vojne opreme.“[40] Prema američkoj saveznoj istražnoj agenciji FBI, upute za ovaj napad su došle iz Kine, budući da je bio iznimno dobro strukturiran, isplaniran i proveden s visokom razinom stručnosti. „Kao rezultat istraživanja ovog napada, Pentagon je dodijelio značajna sredstva za novu kriptografsku opremu, i za nadograđivanje IDS (engl. Intrusion Detection System) sustava i Firewalla.“[41]

Činjenica da mrežni promet prije napada nije sustavno nadziran, omogućila je izvršenje ovog kibernetičkog napada. Osim toga, ovaj napad je ukazao na ranjivost informacijskih sustava i mreža SAD-a, budući da oni imaju nezamjenjivu ulogu u kritičnoj infrastrukturi. „Napadači su primijenili isti način izvršenja, pri čemu je napadač pronašao sve adrese mreže, potom skenirao sustav radi traženja ranjivosti, identificirao ih, iskoristio ih, te instalirao Backdoor program koji je omogućavao višestruku neprimijećeni neprimjetno upad u sustav, oštećujući datoteke, skupljajući i uništavajući podatke.“[42] Postoji sumnja da su hakeri ukrali veliku količinu podataka, uključujući tajne mornaričke šifre i informacije o navođenim projektilima.

2.2. Titan Rain

Titan Rain je šifrirani naziv koji je američka vlada dala seriji koordiniranih kibernetičkih napada na informacijske sustave SAD-a koji su se odvijali od 2003. godine.
Napadi označeni kao Titan Rain pripisani su Kini iako identitet napadača kao i precizni ciljevi napada ostaju nepoznati. Ovi napadi kategorizirani su kao APT (napredne kontinuirane prijetnje). Napadači su pristupili mnogim mrežama koristeći tehnike poput DDoS napada i raznih vrsta zlućudnog softvera.

Cilj je bio prikupljanje povjerljivih informacija o informacijskim sustavima SAD-a. Između ostalog, provalili su u računalne mreže tvrtki Lockheed Martin, Sandia National Laboratories, NASA-e i vojne pošte Redstone Arsenal. Od 2003. hakerska grupa provodi opsežne napade na vladine sustave SAD-a kako bi ukrala osjetljive podatke u sklopu masovne kibernetičke špijunaže. Infiltrirali su se skeniranjem mreža u potrazi za zaraženim računalima preko kojih

[40] Llongueras, A. Moonlight Maze: The beginning of a new era, 2011.
[41] Llongueras, A. Moonlight Maze: The beginning of a new era, 2011.
[42] Llongueras, A. Moonlight Maze: The beginning of a new era, 2011.

su neopaženo krali podatke. U samo jednoj noći istovremeno su napali više kritičnih infrastruktura u SAD-u, što govori o prirodi i cilju napada. Otkrivene su ranjivosti u vojnim obrambenim informacijskim sustavima, agencijama i zapovjedništvima. Treba naglasiti da su napadači uspješno prodrli u sustav i napustili ga bez ikakvih tragova, uspjevši postaviti backdoor unutar 30 minuta od početka napada.

„S obzirom na to, da ovakva akcija zahtijeva visoko sofisticiranu opremu i vještine, jasno upućuje na činjenicu da su ju mogle izvršiti samo strukture uz pomoć države.“[43] Unatoč tome što vojne mreže zbog sigurnosnih razloga nisu izravno spojene na internet, meta napada bile su mreže s neklasificiranim sustavima. Valja spomenuti da ti sustavi sadrže povjerljive informacije i osiguravaju logističku potporu vojsci. Neovisno o tome jesu li hakeri iz Titan Raina prikupljali industrijske podatke ili samo testirali sposobnost infiltriranja u vojne sustave (neprijatelja), vlada SAD-a ovu prijetnju shvaća iznimno ozbiljno. „Kao pouka, koja je proizašla iz ovih napada ukazuje koliko je izuzetno važno da informatičari komuniciraju sa samim vrhom menadžmenta u kritičnim infrastrukturnim institucijama.“[44]

2.3. Operacija Aurora

Početkom 2010. godine Google je obznanio da je bio meta hakerskih napada, poznatih javnosti pod nazivom Operacija Aurora.

Vjeruje se da su ti napadi izvedeni pod okriljem kineskih vlasti, s ciljem otkrivanja koji su kineski obavještajci u SAD-u pod nadzorom američkih službi. S druge strane, postoji sumnja da su Kinezi pokušali zavarati američke službe plasirajući im lažne informacije o obavještajcima. U sklopu Operacije Aurora Google nije bio jedina meta, već je utvrđeno da su istovremeno napadnuti i serveri Microsofta, pri čemu je glavni cilj bio prikupljanje informacija o nadzoru američkih obavještajnih agencija. „Osim toga, kineski hakeri su nadzirali kako je utvrđeno istodobno i više od 20 američkih kompanija u području obrane, tehnologije, zrakoplovstva, naftne industrije i sl.“[45] Zero-day ranjivost u Microsoft Internet Exploreru koja je korištena kao ulaz operacije Aurora za sve ove napade, otkrio je McAfee Labs. „Napad je pri tome iniciran navođenjem korisnika da posjete određenu inficiranu web

[43] Homelandsecuritynewswire, http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management, pristup 11.8.2023.
[44] Homelandsecuritynewswire, http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management, pristup 11.8.2023.
[45] Wired, http://www.wired.com/2010/03/source-code-hacks/, pristup 11.8.2023.

stranicu za koju se smatra da je sigurna, a koja im je ubacila zaraženi kod na računala i povezala ih sa centralnim serverom.“[46]

2.4. Stuxnet

Za razliku od većine računalnih virusa dizajniranih za napade na računalne sustave, Stuxnet crv je bio osmišljen kako bi inficirao industrijske sustave u Natanzu i još pet iranskih postrojenja koja se bave obogaćivanjem urana. „Njegova učinkovitost posebno je došla do izražaja u sabotiranju iranskog nuklearnog programa. Američka i izraelska obavještajna služba ovu operaciju su vodili pod nazivom Olimpijske igre.“[47] Industrijski sustavi kontrole se sastoje od programibilnih logičkih kontrolera (PLC), što su u osnovi mini računala koja se mogu programirati iz sustava Windows. Programeri koriste softver za pisanje koda koji kontrolira automatizaciju industrijskih procesa, a zatim postavljaju svoj kod na PLC, gdje se Stuxnet skriva. Stuxnet se sastoji od 3 elementa: crva koji izvršava zlonamjerni program, povezanih datoteka koje automatski šire kopije crva i rootkit komponente koja skriva sve zlonamjerne datoteke i procese, onemogućavajući detekciju Stuxneta. Vjeruje se da su vrlo opasni računalni crv Stuxnet zajednički razvili Sjedinjene Američke Države i Izrael kako bi napali iransko nuklearno postrojenje u Natanzu. Stuxnet se prvotno širio neselektivno, ali sadržavao je visoko specijalizirani korisni teret usmjeren tako da napada samo SCADA sustave.

Glavni problem bio je kako instalirati zlonamjerni program u iransko nuklearno postrojenje koje je iz sigurnosnih razloga bilo isključeno s interneta. Premda način prodiranja zlonamjernog programa Stuxnet u postrojenje Natanz nije u potpunosti razjašnjen, pretpostavlja se da je infekciju u sustav unio neki nepažljivi djelatnik ili tajni agent putem USB memorijskog uređaja. Jednom kad se proširio, štetni kôd se rasprostirao mrežom tragajući za Siemensovim Step 7 aplikacijama na računalima koja upravljaju programibilnim logičkim kontrolerom, kojeg je Stuxnet namjeravao srušiti budući da se taj softver koristio za prepravljanje PLC uređaja. Ukoliko nijedan od ta dva uvjeta nije bio zadovoljen, Stuxnet je postajao neaktivan na računalu. No ako su oba kriterija bila ispunjena, Stuxnet je preuzeo rootkit i inficirao PLC i Step 7 program, mijenjajući kôd i izdajući neočekivane zapovijedi PLC-u, dok je korisnicima vraćao povratnu informaciju da sustav potpuno funkcionira.

[46] Računalo.hr, http://www.racunalo.com/mcafee-i-operacija-aurora, pristup 11.8.2023.
[47] AV gurus, http://av-gurus.blogspot.com/2012/06/kako-je-sad-napravio-stuxnet-i-kako-je.html, pristup 11.8.2023.

Sredinom 2010. godine dogodio se propust zbog programske pogreške, jer je zlonamjerni softver vjerojatno slučajno "iscureo" iz iranskog nuklearnog postrojenja i proširio se internetom, čime je postao poznat javnosti. Otkriće tog tajnog kibernetičkog naoružanja zahtijevalo je stvaranje poboljšane inačice Stuxneta, koja je kasnije još jednom dorađivana. Računalni crv Stuxnet izazvao je pogubne posljedice na iranskom nuklearnom programu ubrzavajući rad centrifuga koje su se zbog toga zaustavljale, čime je iz pogona isključeno oko 1000 od 5000 naftnih centrifuga, zbog čega je iranski nuklearni program zaostao dvije godine. Time je Stuxnet postao prvo poznato oružje u kibernetičkom ratovanju, s ciljem uništenja ključne infrastrukture neke države. Kasnije se pojavio i virus Flame, za koji stručnjaci vjeruju da je također moćno oružje kibernetičkog špijuniranja, kao i prethodno otkriveni nasljednik Stuxneta - Duqu. Stalni razvoj kibernetičkog oružja ukazuje na nastavak utrke u naoružanju, ne samo konvencionalnog oružja nego i kibernetičkog oružja poznatog kao oružje 21. stoljeća kojim se ostvaruju isti ciljevi.

Stuxnet je iskoristio slabosti Windows operativnog sustava koje su bile nepoznate u trenutku napada. Na početku se širio preko zaraženih prijenosnih memorija poput USB stickova, a zatim je aktivirao dodatne sigurnosne propuste i tehnike poput peer-to-peer RPC (daljinski poziv procedure) kako bi prodro u i nadogradio preostala računala unutar izolirane mreže koja nije bila izravno spojena na internet.

„Broj ranjivosti nultog dana je neuobičajen, jer ih je iznimno malo i vrlo su vrijedni, te je teško za shvatiti zašto su na Stuxnetu, upotrijebljene čak 4 ranjivosti nultog dana.“[48] Stuxnet ima neuobičajenu prirodu i karakteristike za računalni virus. Znatno je veći od uobičajene veličine virusa i napisan je u više programskih jezika poput C i C++, što je rijetkost za zlonamjerne programe. Windows komponenta ovog crva omogućila je njegovo brzo i neselektivno širenje. Za razliku od tipičnih virusa, Stuxnet je bio izrazito složen i specijaliziran, što ukazuje na visoku razinu stručnosti i resursa uloženih u njegov razvoj. „U Stuxnetu, rootkit ima i dva moda, korisnički i jezgreni mod unutar Windowsa, te driveri uređaja imaju digitalni potpis sastavljen od privatnih ključeva, čiji su certifikati ukradeni od strane tvrtki Realtek i Jmicron.“[49]

[48] Symantec, http://www.symantec.com/connect/blogs/stuxnet-p2p-component, pristup 11.8.2023.
[49] AV gurus, http://av-gurus.blogspot.com/2012/06/kako-je-sad-napravio-stuxnet-i-kako-je.html, pristup 11.8.2023.

Prema provedenim istraživanjima, kada bi Stuxnet zarazio Windows sustav, inficirao bi projektne datoteke programa WinCC/PCS7 SCADA, odnosno Step7, te bi uništio ključnu komunikacijsku biblioteku naziva s7otbxdx. Na taj način presretao bi komunikaciju između WinCC aplikacije i ciljanih Siemens PLC uređaja. Dakle, nakon infiltriranja računala, Stuxnet bi preuzeo kontrolu nad datotekama potrebnim za rad industrijskih kontrolnih sustava i onesposobio vitalnu komunikacijsku komponentu, čime bi prekinuo vezu između nadzornog računala i industrijske opreme koju je trebao nadzirati i upravljati njome. „Na taj način, Stuxnet sam sebe može instalirati na PLC uređaje i ostati neotkriven, te kasnije zamaskira sam svoju prisutnost od WinCC ako kontrolni program nastoji pročitati inficirani blok memorije iz PLC sustava.“[50] Kao odgovor na Stuxnet, tvrtka Siemens je objavila alat za njegovo otkrivanje i uklanjanje. Uz to su preporučili korisnicima da kontaktiraju njihovu službu za korisnike i instaliraju nadogradnje koje je objavio Microsoft za zakrpanje sigurnosnih propusta koje je Stuxnet iskoristio. Siemens je brzo reagirao kako bi pomogao svojim klijentima da se zaštite i oporave od napada. Suradnjom s Microsoftom, osigurali su dostupnost zakrpa i alata potrebnih za uklanjanje zlonamjernog programa i saniranje štete koju je napravio.

3. IZVORI PODATAKA I METODE

U ovom diplomskom radu, korištene su razne metode i izvori podataka kako bi se istražilo različite oblike kibernetičkih prijetnji i opasnosti.
Korištena je raznovrsna literatura, uključujući knjige, članke i druge publikacije. Literatura je bila odabrana na temelju relevantnosti za temu istraživanja, a posebno pažnja je posvećena literaturi koja je objavljena u posljednjih nekoliko godina.

U fokusu su bile sljedeće metode istraživanja:

- Pregled literature: Pregledana je literatura drugih autora kako bi identificirali ključne teme i trendove u području kibernetičkih prijetnji.
- Analiza statističkih podataka: Analizirani su statistički podaci o kibernetičkim napadima kako bi se utvrdila prevalencija i posljedice tih napada.

[50] AV gurus, http://av-gurus.blogspot.com/2012/06/kako-je-sad-napravio-stuxnet-i-kako-je.html, pristup 11.8.2023.

- Sinteza primjera najnovijih kibernetičkih napada: Sintetizirani su primjeri najnovijih kibernetičkih napada kako bi se ilustriralo različite vrste prijetnji i njihovu evoluciju.

Na temelju analize dostupnih podataka i literature drugih autora, pružene su sljedeće preporuke za zaštitu od kibernetičkih prijetnji:

- Implementacija jakih sigurnosnih kontrola: Organizacije bi trebale implementirati jake sigurnosne kontrole kako bi zaštitile svoje sustave i podatke. To uključuje mjere kao što su snažne lozinke, ažurirana softverska rješenja i sigurni sustavi za pohranu podataka.
- Edukacija zaposlenika o kibernetičkoj sigurnosti: Zaposlenici bi trebali biti svjesni kibernetičkih prijetnji i kako se zaštititi od njih. Organizacije bi trebale pružiti edukaciju zaposlenicima o sigurnosnim praksama i kako prepoznati i prijaviti sumnjive aktivnosti.
- Planiranje odgovora na kibernetičke napade: Organizacije bi trebale imati plan kako odgovoriti na kibernetičke napade. To uključuje mjere kao što su postupci za brzo otkrivanje i rješavanje napada, kao i plan za komunikaciju s korisnicima i drugim zainteresiranim stranama.

4. REZULTATI I RASPRAVA

U ovom poglavlju predstavljeni su glavni rezultati istraživanja o kibernetičkim prijetnjama.
Rezultati istraživanja pokazuju da postoje mnoge različite vrste kibernetičkih prijetnji koje mogu uzrokovati značajnu štetu pojedincima, organizacijama i državama. Najčešće vrste kibernetičkih prijetnji uključuju zlonamjerni softver, prevarantske e-pošte, ucjenjivanje (ransomware) i preopterećenje usluga (DDoS).
Postoji nekoliko načina kako prepoznati i zaštititi se od kibernetičkih napada. Neki od najvažnijih savjeta uključuju:

- Biti oprezan s e-poštom i drugim porukama koje primate od nepoznatih pošiljatelja.
- Redovito ažurirati svoje računalstvo i softver.
- Koristiti snažne lozinke i ne koristiti ih za više računala ili usluga.
- Šifrirati svoje podatke, ako je to moguće.

Kibernetički kriminal i ratovanje su u stalnom razvoju. Neki od najnovijih trendova uključuju upotrebu umjetne inteligencije (AI) i strojnog učenja za razvoj novih vrsta zlonamjernog softvera i napada, upotrebu dronova za izvođenje kibernetičkih napada i zamjenu tradicionalnih napada novim metodama, kao što su napadi na kritičnu infrastrukturu.
Metode zaštite od kibernetičkih prijetnji također su u stalnom razvoju. Neke od najperspektivnijih metoda uključuju upotrebu oblačnih računalstva za decentralizaciju podataka i aplikacija, upotrebu blockchain tehnologije za osiguravanje integriteta podataka i upotrebu sigurnosnih rješenja zasnovanih na umjetnoj inteligenciji i strojnom učenju.
Kibernetičke prijetnje predstavljaju značajan rizik za pojedince, organizacije i države. U budućnosti se mogu očekivati nove i sofisticiranije prijetnje, što otežava njihovu zaštitu. Međutim, postoje razne metode koje se mogu koristiti za smanjenje rizika od kibernetičkih napada.

U budućnosti bi se mogle odraditi rasprave o sljedećim temama:

- Kako se prilagoditi novim trendovima u kibernetičkim prijetnjama?
- Kako osigurati da nove metode zaštite od kibernetičkih prijetnji budu učinkovite?
- Koja je uloga pojedinaca, organizacija i vlada u zaštiti od kibernetičkih prijetnji?
- Ove rasprave bi mogle pomoći u razvoju novih strategija za zaštitu od kibernetičkih prijetnji.

5. ZAKLJUČCI

U ovom radu analizirani su različiti oblici ugroza kibernetičkih prijetnji, kao što su malware, phishing, ransomware, DDoS i drugi. Uočeno je da napadači neprestano razvijaju nove i sofisticiranije metode napada kako bi iskoristili ranjivosti tehnoloških sustava. S druge strane, za učinkovitu obranu ključne su različite metode zaštite poput vatrozida, antivirusnog softvera, šifriranja podataka i implementacije sigurnosne kulture.

Brzi razvoj tehnologija i sve veća digitalizacija donose brojne pogodnosti, ali i otvaraju nove rizike po informacijsku sigurnost. Stoga je nužno kontinuirano unaprjeđivati i prilagođavati mjere zaštite u skladu s novim prijetnjama. Pitanja kibernetičke sigurnosti snažno utječu na tehnološke trendove, primjerice razvoj kriptografije, biometrijskih kontrola pristupa i blockchaina.

Za uspješno upravljanje rizicima u budućnosti, organizacije i vlade morat će ulagati u istraživanje i razvoj novih sigurnosnih tehnologija. Jednako važna je i primjena principa sigurnosne kulture među svim dionicima. Samo cjelovit i proaktivan pristup omogućit će izgradnju pouzdanog i otpornog kibernetičkog okruženja.

6. LITERATURA

1. Hutinski, Ž. Informatika za ekonomiste, FET, Pula, 2002.
2. Jaiganesh, Mangayarkarasi, Sumathi IJARCC - International Journal of Advanced Research in Computer and Communication Engineering
3. Jakobsson, M. & Young, A. Distributed Phishing Attacks, 2005.
4. Janczewski, C. Cyberwarfare and CyberTerorism, Information Science Reference, USA, 2007.
5. Kramer, F.D., Starr, S. & Wentz, L.K. *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books, 2009.
6. Llongueras, A. Moonlight Maze: The beginning of a new era, 2011.
7. Marinković, M. Maliciozan kod, Beograd, 2008.
8. Nohlberg, M. Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks 2008.
9. Suryavanshi, N. A Review of Various Techniques for Detection and Prevention for Phishing Attack, 2013.
10. Wingfield, T.C. *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., 2000, str. 17.
11. Workman, M. Gaining access with social engineering: An empirical study of the threat, Information Systems Security, Vol. 16, 2007, str. 315–331.

WEB IZVORI:

1. Arbor1 (n.d.). About DDoS Attacks. ARBOR. http://www.arbornetworks.com/attack-ddos pristup 11.8.2023.
2. Asadria. http://www.asadria.com/index.php/teme/izdvojeno/319-najvece-sigurnosne-prijetnje-za-kriticnu-infrastrukturu, pristup 11.8.2023.
3. AV gurus, http://av-gurus.blogspot.com/2012/06/kako-je-sad-napravio-stuxnet-i-kako-je.html, pristup 11.8.2023.
4. Budić, S., Špoljarić, I. & Kramar, M. Maliciozni kod: analiza modernih malicioznih kodova. http://maliciozni-kod-analiza-modernih- malicioznih- kodova. googlecode.com/files /Tema_06_ MALICIOZNI%20KOD_ANALIZA%20MODERNIH%20MALICIOZNIH%20KODOVA.pdf, pristup 11.8.2023.
5. Cert, http://www.cert.hr, pristup 11.8.2023.
6. Cis, http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-218.pdf, pristup 11.8.2023.
7. Datareportal, https://datareportal.com/reports/digital-2023-global-overview-report, pristup 11.8.2023.
8. Homelandsecuritynewswire, http://www.homelandsecuritynewswire.com/lesson-titan-rain-articulate-dangers-cyber-attack-upper-management, pristup 11.8.2023.
9. Hrvatski vojnik, http://www.hrvatski-vojnik.hr/hrvatski-vojnik/2802010/it_sec.asp, pristup 11.8.2023.
10. Mačković, D. Rootkit. Rootkit. http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm, pristup 11.8.2023.
11. Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. http://www.wired.com/threatlevel/2012/05/flame/, pristup 11.8.2023.
12. Računalo.hr, http://www.racunalo.com/mcafee-i-operacija-aurora, pristup 11.8.2023.
13. Stein, L. (2003). The World Wide Web Security FAQ. http://www.w3.org/Security/Faq/wwwsf6.html#DOS-Q2 pristup 11.8.2023.
14. Symantec, http://www.symantec.com/connect/blogs/stuxnet-p2p-component, pristup 11.8.2023.
15. Wired, http://www.wired.com/2010/03/source-code-hacks/, pristup 11.8.2023.

16. Zeltser, L. (2011). 8 Reasons for Denial-of-Service (DoS) Attacks. http://blog.zeltser.com/post/10775687288/reasons-for-denial-of-service-attacks pristup 11.8.2023.
17. Zetter, K. Mahdi, the Messiah, Found Infecting Systems in Iran, Israel. http://www.wired.com/threatlevel/2012/07/mahdi/, pristup 11.8.2023.

SAŽETAK

„Ugroze u kibernetičkom prostoru“ („Cyber threats“)

U digitalnom dobu sveprisutne tehnologije, kibernetičke prijetnje su sve raširenije i naprednije, stvarajući ozbiljan rizik za pojedince, organizacije i čak države. Ovaj rad temeljito analizira različite oblike kibernetičkih prijetnji, uključujući zlonamjerne softvere, prevare putem elektroničke pošte, ucjenjivačke napade (ransomware), preopterećenja usluga (DDoS) i brojne druge. Paralelno s razvojem ovih prijetnji, evoluiraju i metode zaštite. Rad istražuje važnost vatrozida, antivirusnih programa, šifriranja podataka te usvajanja sigurnosne svijesti kao ključnih zaštita. S brzim tehnološkim napretkom i sveprisutnom digitalizacijom društva, izazovi za očuvanje kibernetičke sigurnosti postaju sve kompleksniji. Posebno se analiziraju utjecaji tehnoloških trendova na kibernetičku sigurnost te strategije za upravljanje budućim rizicima. Kroz kombinaciju teorijskih spoznaja i praktičnih primjera, rad koristi stvarne slučajeve kibernetičkih napada kako bi ilustrirao konkretnu prirodu ovih prijetnji, pružajući čitatelju dublje razumijevanje ove iznimno važne teme.

Ključne riječi: ugroze, prostor, kibernetički

ABSTRACT

„Ugroze u kibernetičkom prostoru“ („Cyber threats“)

In the digital age of ubiquitous technologies, cyber threats are becoming increasingly widespread and sophisticated, posing a serious risk to individuals, organizations, and even nations. This paper thoroughly analyzes various forms of cyber threats, including malicious software, email scams, ransomware attacks, distributed denial-of-service (DDoS) attacks, and many others. Concurrently with the development of these threats, methods of protection are also evolving. The paper explores the importance of firewalls, antivirus programs, data encryption, and the adoption of security awareness as key safeguards. With rapid technological advancements and the pervasive digitization of society, challenges in preserving cyber security are becoming increasingly complex. The impacts of technological trends on cyber security are particularly analyzed, as well as strategies for managing future risks. By combining theoretical knowledge and practical examples, the paper utilizes real-life cases of cyber attacks to illustrate the concrete nature of these threats, providing the reader with a deeper understanding of this highly important topic.

Key words: threats, space, cyber

ŽIVOTOPIS

Osobni podaci:

Ime i prezime: Mirko Šabić

Datum rođenja: 03.12.1979

Mjesto rođenja: Split, Hrvatska

Adresa: Ulica don Ivana Vuletina, 21217 Kaštel Novi

Mobitel: +385911559105

E-mail: mirkosabic@gmail.com

Obrazovanje:

Osnovnu školu završio u Zmijavcima, upisao Opću gimnaziju u Imotskome koju je završio 1998.g.

Potom je 1999/2000 upisao kriminalistiku i stekao obrazovanje kriminalist sa 180 ECTS bodova.

Nakon toga upisao je četvrtu godinu na Pravnome fakultetu Upravni studij kojom prilikom je dobio naziv stručni specijalist javne uprave sa 240 ECTS bodova.

Radno iskustvo:

Od 2006-2007.g. radio kao zaštitar da bi se 3.12.2007.g. zaposlio kao policijski službenik u Ministarstvu unutarnjih poslova RH čiji je i danas zaposlenik:

U MUP-u RH bio je rapoređen na sljedećim radnim mjestima:

- 2007.-2012. – policijski službenik za maloljetničku delinkvenciju i obradu kriminaliteta

- 2012.-2015. – Pomoćnik načelnika za krim policiju u Policijskoj postaji Trogir

- 2015.-2018 – Policijski službenik za obradu kriminaliteta u Policijskoj postaji Trogir

2018.-2021 – Pomoćnik načelnika za krim policiju u Policijskoj postaji Kaštela

2021.-2023 – Policijski službenik za obradu organiziranog kriminaliteta u Službi organiziranog kriminaliteta Policijske uprave Splitsko – dalmatinske

2023. – Pomoćnik načelnika za krim policiju u Policijskoj postaji Kaštela

Za vrijeme službe i to 2012.g. završio specijalistički tečaj za kriminalističke službenike koji postupaju u predmetima kaznenih djela maloljetnika

Također 2020.g. položio ispit za zvanje Viši policijski inspektor

SVEUČILIŠTE U SPLITU

Sveučilišni odjel za forenzične znanosti

Izjava o akademskoj čestitosti

Ja, Mirko Šabić, izjavljujem da je moj diplomski rad pod naslovom „Ugroze u kibernetičkom prostoru“ rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Nijedan dio ovoga rada nije napisan na nedopušten način, odnosno nije prepisan bez citiranja i ne krši ičija autorska prava.

Izjavljujem da nijedan dio ovoga rada nije iskorišten u ijednom drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Split, 8.9.2023. godine

Potpis studenta: