Najpoznatiji hakerski napadi i online sigurnost

Široki, Katarina

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Diplomski sveučilišni studij

Katarina Široki

Najpoznatiji hakerski napadi i online sigurnost

The most famous hacker attacks and online security

Završni rad

Opatija, 2023.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Diplomski sveučilišni studij
Sigurnost informacijskih sustava

Najpoznatiji hakerski napadi i online sigurnost

The most famous hacker attacks and online security

Završni rad

Kolegij:	**Sigurnost informacijskih sustava**	Student:	**Katarna ŠIROKI**
Mentor:	Izv. prof. dr. sc. Ljubica PILEPIĆ STIFANICH	Matični broj:	25017/19

Opatija, srpanj 2023..

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Katarina Široki	**25017/19**
(ime i prezime studenta)	(matični broj studenta)

Najpoznatiji hakerski napadi i online sigurnost
(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor diplomskog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog diplomskog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, 20. Srpnja, 2023._____

K. Široki
Potpis studenta

Sažetak

Online okruženje postalo je svakodnevica ljudi u suvremenom svijetu. S pojavom interneta pojavile su se i brojne prijetnje u internetskom okruženju. Navedene prijetnje mogu ugroziti pojedince, poduzeća, institucije ili cijele nacije. Među ključne prijetnje uvrštavaju se hakerske prijetnje. Hakiranje je s razvojem interneta postalo sve više praksa, a s napretkom tehnologije ono je poprimilo sve veće razmjere. Riječ je o vrlo ozbiljnim prijetnjama koje mogu imati velike i dalekosežne posljedice. Kako bi se što bolje upravljalo ovim rizikom, treba implementirati sigurnosne sustave koji će smanjiti mogućnost djelovanja ovih prijetnji te treba implementirati preventivne mjere na tom području. Rad se bavi analizom ključnih prijetnji u online okruženju u kontekstu hakerskih napada, te sigurnosnim mehanizmima i metodama zaštite informacijskih sustava. Analizira se šteta i posljedice koje takva vrsta napada može ostaviti na pojedine osobe, te na poslovanje poduzeća.

Ključne riječi: hakerski napadi, internet, online sigurnost

Sadržaj

1. Uvod

1.1 Predmet, ciljevi i metode istaživanja

Razumijevanje sigurnosnih prijetnji u bilo kojem području je vrlo važno. U suvremenom svijetu, u kojem dominira Internet, ovo pitanje je još više dobilo na značaju. Iz navedenog razloga danas se znanstvena i stručna literatura kao i stručnjaci na području informacijske sigurnosti sve više usredotočuju na identificiranje ključnih prijetnji i napada te načina kako njima upravljati. Danas više nije rijetkost da razne kompanije izvještavaju o neovlaštenom pristupu bazi podataka korisnika.

Predmet istraživanja u ovom radu je identificiranje ključnih prijetnji u online okruženju u kontekstu hakerskih napada. Ovim radom promatrane su ključne prijetnje u online okruženju te identifikacija mogućih zaštitnih mjera

Iz predmeta i problema istaživanja mogu se postaviti sljedeći ciljevi istraživanja:

- Koje su to najčešće prijetnje koje se danas javljaju u suvremenom poslovanju?
- Na koje načine hakeri dokaze do podataka?
- Kako se zaštititi od napada?

Svrha rada je prikaz najčešćih hakerskih napada na informacijske sustave, te načini zaštite od istih.

Znanstvene metode koje su korištene u ovom radu su metode deskripcije, te metode analize. U ovom radu korištena je domaća i strana literatura, te su tako prikazani sekundarni podaci. Pri obradi teme su korišteni podaci sa službenih internet stranica koje su pomogle u pronalasku relevantnih informacija.

1.2 Struktura rada

Rad se sastoji od sedam međusobno povezanih cjelina. U prvom uvodnom dijelu rada objašnjen je predmet i problem istraživanja, identificirani su ciljevi istraživanja te prikazane znanstvene metode. Uvod završava prikazom strukture rada prema poglavljima.

Drugo poglavlje nosi naziv "Online sigurnost". U ovome dijelu rada iznosi se razrada terminologije vezane za sigurnost na intenetu, objašnjava se uloga i namjena web poslužitelja, te identificiraju problemi u online okruženju vezani za računalnu i informacijsku sigurnost.

Treće poglavlje pod nazivom "Napadi na web poslužitelje" objašnjava osnovne slobosti tj. ranjivosti sustava, istražuje osnovne vrste napada na mreži u okviru kibernetičkog prostora te donosi klasifikaciju kibernetičkih napada i kontrola upada.

"Hakiranje" je naziv četvrtog poglavlja u ovome radu. Poglavlje započinje definicijom samih aktera online kriminalnih djela te se navodi tipologija hakera i osnovni motivi koji stoje iza svih napada ovakve vrste.

U petom poglavlju ovoga rada pod nazivom "Najpoznatiji hakerski napadi" daje se pregled najpoznatijih hakerskih napada u svijetu koji su ostali trajno zabilježeni u povijesti kibernetičkog kriminala, kako zbog sofisticiranosti same izvedbe tako i zbog izrazito razornih šteta i ne malih posljedica mjerljivih u visokim novčanim izdatcima.

Šesto poglavlje ovoga rada iznosi niz sigurnosnih mjera i kontrolnih mehanizama koje se obično primjenjuju u kombinaciji kako bi se postigla viša razina kibernetičke sigurnosti a sigurnosni rizik sveo na najmanju moguću mjeru bilo da se radi o preventivnim, detektivnim ili reaktivnim mjerama kibernetičke sigurnosti.

Rad završava zaključkom u kojem se iznosi sinteza cjelokupnog rada i daju smjernice za očuvanje kibernetičke sigurnosti.

2. Online sigurnost

Pojavom sve većeg razvoja informatizacije u našem svakodnevnom životu povećava se ptreba za zaštitiom infomacijsko-komunikacijskih sustava koji se koriste. Zaštita sigurnosti računalnih sustava potrebna je unutar mnogih poduzeća, kao i kod zaštite podataka svake individualne osobe. „Internet je sastavni dio života suvremenog čovjeka, koji ga rabi s punom sviješću o njegovoj koristi, ali nerijetko s nedovoljno informacija o ugrozama koje izravno ili u paketu s njim ugrožavaju njegovu privatnost u užem, ali i sigurnost u širem smislu.“[1]

Sigurnost podataka označava sve procese zaštite koje individualne osobe i razna poduzeća primijenjuju kako bi zaštitili svoje osobne podatke dok se koriste internetom. Ovaj proces obuhvaća razne aspekte unutar kojih se mogu izbjeći razne prijevare i krađe podataka. Sa razvojem internetskih procesa u poslovanjima, sve je veća potreba za sprječavanjem internetskog zlostavljanja i zaštitu od zlonamjernih softvera i drugih internetskih prijetnji.

Sve veća potreba za zaštitom računalnih sustava javlja se osamdesetih godina prošlog stoljeća kada se i pojaljuje nova grana koja analizira i primjenjuje različite načine sigurnosti računalnih sustava. U to vrijeme pojavljuju se prvi virusi i programi koji štete sustavima. Počele su se pojavljivati i prve neželjene električne poruke. Otežavanje rada i strahom za sigurnost, razvija se svijet među korisnicima za potrebom online sigurnosti. Ciljevi ove grane su brojni. Sustavi se bave ispitivanjem sigurnosnih rizika u računarstvu, te proučavanjem raspoloživih zaštitnih mjera koje se mogu primjenjivati.

2.1 Uloga Web poslužitelja

Osnovna uloga interneta je dijeljenje informacija, a kako bi ti podaci bili dostupni i razumljivi krajnjim korisnicima, koriste se web serveri ili poslužitelji. U tom kontekstu, web server je kompjuterski program, no ovaj se pojam, također, često povezuje s kombinacijom hardware-a i

[1] Antoliš, K. (2010) Internetska forenzika i cyber terorizam. Policija i sigurnost, 19(1), str. 121.

software-a. Web server predstavlja skupinu programa/software-a koji korisnicima omogućava korištenje dokumenenata/informacijama te omogućava izmjenu ili dopunu. Nadalje, web server omogućuje vlasnicima/administratorima da dodaju, mijenjaju i/ili brišu dokumente.[2]

Uloga web poslužitelja je omogućiti korištenje podataka, usluga i određenih uređaja svim registriranim klijentima. Nadalje, uloga mu je zaštita sigurnosti ne nadzor nad radom svih klijenata.[3] Pojava web servera na internetu bitno je utjecala na[4]:

- Proizvođače baza podataka –dolazi do sve veće želje za micanjem monopol hostova na internetskim poslužiteljima. Postavljanje proizvoda na vlastite web servere. Tim se omogućuje direktan pristup proizvodima.
- Jednostavnost postavljanja informacija na web servere. Rezultat toga su brojni info izvori od pojedinaca do raznih poduzeća.
- Razvoj internetske mreže –omogućava širenje i pristup krajnjih korisnika. U poslovanju i privatnom životu povećava se broj računala u upotrebi.

Porast popularnosti web servera omogućava sve veči razvoj. Njihova praktičnost olakšava i ubrzava procese koji osiguravaju brzo širenje, a tome su pridonijele i nove tehnologije koje olakšavaju interakciju sa serverima. Web server omogućuje komunikaciju s web uslugama.

[2] Jovanović, N. (2003) Računarske mreže. Viša poslovna škola, https://www.researchgate.net/profile/Nenad-Jovanovic-4/publication/323538579_Racunarske_mreze/links/5a9ac56ca6fdcc3cbacb3d2a/Racunarske-mreze.pdf
[3] Telekomunikacija I računalne mreže, http://www.unizd.hr/portals/1/primjena_rac/brodostrojarstvo/predavanje_5.pdf
[4] Toth, T. (2000) Od hostova do web-servera: jesu li nam informacije dostupnije danas nego jučer? U: Upravljanje informacijama u gospodarstvu i znanosti : zbornik radova = Information management in industry and science : proceedings / [Konferencija] CROinfo 2000, Dubrovnik, 16.- 18. X. 2000. ; [organizatori = organizers Nacionalna i sveučilišna knjižnica, Zagreb [i] PLIVA] ISBN 953600089X / Stipanov, Josip - Zagreb : Nacionalna i sveučilišna knjižnica, str. 160, 163. 171.

2.2 Namjena Web poslužitelja

Namjera web poslužitelja je omogućavanje sigurne komunikacije i razmjene informacija na internetu. U tom kontekstu razvijene su brojne mogućnosti kojima se nastoji postići brza, sigurna i kvalitetna razmjena informacija i podataka.

REST (engl. *Representational State Transfer*) teorijski je model programske arhitekture za ostvarivanje raspodijeljenih sustava. Nastao iz WWW tehnologije na način da su uvedena određena ograničenja koja predstavljaju osnovu REST modela. Postavlja temelje načina na koji se podaci svjetske internetske mreže mogu koristiti. Namjera uvođenja ovih temelja je kreiranje jedinstvenog sustava. Budući da web servisi često implementiraju samo dio teorijskih načela REST modela, koristi se naziv RESful web servisi. Na taj se način ističe da se koriste neka REST načela, ali ne sva.[5]

U ključna načela REST modela ubrajaju se[6]:

- Osnovni element u REST modelu je sredstvo. Svako sredstvo ima svoj posebni identifikator URI (engl. *Uniform Resource Identifier*) On predstavlja jedinskrevu oznaku unutar globane mreže.
- Međusobno povezivanje sredstava – sredstva mogu imati vezu jedno s drugim, te ih je potrebno međusobno povezivati. Poradi navedenog, prilikom davanja odgovora na zahtjev za sredstvima često se daje skup dodatnih poveznica koje označavaju druga sredstva. To klijentu omogućava promjenu stanja sustava prateći poveznice koje je dobio u odgovoru.
- Uporaba standardnih metoda –istu skupinu metoda može korisiti svako sredstvo, a pomoću njih se može doći do željenih rezultata.
- Sredstva s višestrukim reprezentacijama – problem kod izrade web servisa je osiguravanje ispravnog prenošenja poslanih podataka na strani klijenta. Web servisi samo šalju informacije, a klijentska ih aplikacija prikazati. No, da bi se klijentu poslala

[5] CIS (2012) Ispitivanje sigunosti web servera, http://www.cis.hr/files/dokumenti/CIS-DOC-2012-02-040.pdf
[6] http://www.cis.hr/files/dokumenti/CIS-DOC-2012-02-040.pdf

ispravna poruka namjera svakog web servisa je podrška isporuke sredstava u željenom formatu.

- Komunikacija bez održavanja stanja – REST model predlaže da podatke o stanju servisa uvijek bude sadržana unutar samog sredstva koje se koristi. Stanje podrazumijeva bilo koje podatke koji utječu na rezultat odaziva web servisa, a koje su posljedica prethodnih interakcija s web servisom.

2.3 Problemi sigurnosti u online okruženju

„Zaštita privatnosti jedan je od ključnih problema upotrebe interneta. Naime, postojeće tehnologije omogućile su da se vrlo jednostavno i gotovo besplatno prikupljaju osobni podaci i nadziru online aktivnosti korisnika, što je plodno tlo za njihovu zloupotrebu. Zbog toga su korisnici interneta posebno zabrinuti za zaštitu privatnosti.“[7] Kada govorimo o sigurnosti i zaštiti informacijskih sustava i mreže, bitno je napomenuti kako danas ne postoji potpuna sigurnost od napada, te da svaka osoba u mogučnosti posati meta napada.

Danas je hakiranje velika prijetnja privatnosti. Uz hakiranje veliku prijetnju predstavlja i nezaštićeno preuzimanje, lokalne mreže te jedan od najčešćih virusa, trojanski konj. „Zaštita privatnosti i sigurnost podataka sve više dobivaju na važnosti u poslovanju. Istodobno se povećava zabrinutost potrošača zbog moguće zlouporabe njihovih osobnih podataka.“[8]

Svatko od nas dio je nekog informacijskog sustava. Ti sustavi nisu apsolutno pouzdani u smislu sigurnosti podataka pa tako mogu ugoziti našu privatnost i preuzeti naše privatne podatke. Jedna od mogućih mjera zašitie je izrada sigurnosnih kopija programa i podataka. Na taj način izražuje se istovjetna kopija pohranjena fizički na drugom mjestu od izvornika.

Kao drugi način zašite navodi se pojam vatrozida, koji služi kao zašita propuštanja podataka iz uređaja i mreže. On može ograničiti i podatke koji se iz računalne mreže šalju u

[7] Brautović, M. (2007) Zaštita privatnosti kod hrvatskih online medija. Medianali – znanstveni časopis za medije, novinarstvo, masovno komuniciranje, odnose s javnostima i kulturu društva, 1(1), str. 27.
[8] Sudar–Kulčar, M. (2006) Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni marketing. Politička misao, 2(4), str. 97.

okolinu. Služi za zaštitu jednog računala osiguravajući da na njega ne dođu neželjeni podaci. Osigurava sigurnost podataka, te smanjuje brigu krajnjih korisnika

Informacijski se sustavi sve više otvaraju prema okolini. Pravilno korištenje informacijskom sigurnošću je zadatak cjelokupnog poduzeća, odnosno korisnika unutar tvrtke. Upravljanje informacijskom sigurnošću je trajna djelatnost, a ne zadatak određenog trajanja.

Sigurnost na mreži pomaže u zaštiti svih osjetljivih podataka, kao što su financijski podaci i osobni podaci, od pada u pogrešne ruke. To smanjuje rizik od krađe identiteta, prijevare ili zlouporabe osobnih podataka. Budući da se unutar sustava poduzeća prikupljaju podaci vitalnog interesa za organizaciju, od velikog je interesa da ostanu tajni i zaštićeni

Kako bi se osigurala sigurnost podataka, potrebno je jasno definirati organizaciju i propisati pravila za sve koja mogu utjecati na sigurnost. Potrebno je odrediti tijela i osobe, kao i propisati njihova prava, obveze i sankcije za kršenje propisa,

One osobe koje dolaze u dodir s informacijskim sustavom mogu se podijeliti, primjerice, u dvije skupine. Prva od skupina su oni koji se mogu služiti informacijskim sustavom, mogu pregledavati, mijenjati i brisati podatke, no nisu odgovorni za instalaciju i održavanje sustava. Upravo za ove dvije funkcije zadužena je druga skupina. Na taj način pospješuje se sama sigurnost podataka.

Svaki sustav je potrebno naučiti da bi utvrdili ustrojstvo informacijskog sustava, programa i podataka, načina upotrebe i sl. Intenzivna primjena informacijskih susava u poslovanju donosi brojne prednosti, ali donosi i nove opasnosti s neželjenim posljedicama

Ključno je biti informiran o najnovijim prijetnjama, educirati se o najboljim primjerima iz prakse i njegovati odgovorno digitalno ponašanje kako biste se sigurno kretali internetskim svijetom.

3. Napadi na web poslužitelje

Kibernetički (cyber) napadi uvrštavaju se u širi kontekst od onoga što se tradicionalno naziva informacijskim operacijama. To je napad pokrenut s računala na web stranicu, računalni sustav ili pojedinačno računalo koji ugrožava povjerljivost, integritet ili dostupnost računala ili informacija pohranjenih na njemu. Cyber napadi imaju mnoge oblike.

Ciljevi kibernetičkih napada su[9]:

- Dobivanje ili pokušaj dobivanja neovlaštenog pristupa računalnom sustavu ili njegovim podacima.
- Neželjeni napadi prekidom ili uskraćivanjem usluge, uključujući rušenje cijelih web stranica.
- Instalacija virusa ili zlonamjernog softvera – odnosno zlonamjernog koda na računalni sustav.
- Neovlašteno korištenje računalnog sustava za obradu ili pohranu podataka.
- Promjene karakteristika hardvera, firmvera ili softvera računalnog sustava bez znanja, uputa ili pristanka vlasnika.
- Neodgovarajuće korištenje računalnih sustava od strane zaposlenika ili bivših zaposlenika.

3.1 Kibernetički napad i prijetnje kibernetičkog prostora

Ne postoji univerzalno prihvaćena definicija kibernetičkog napada. Međutim, u većini slučajeva kibernetički napad je namjeran ulazak u računalni sustav sa zlonamjernom namjerom. Riječ kibernetički napad obično opisuje politički motivirani napad, bilo od strane država ili nedržavnih aktera poput terorista. Kibernetički kriminal najčešće opisuje aktivnost u čisto kriminalne svrhe, iako se ova definicija mijenja kako kibernetički kriminal raste u sofisticiranosti i veličini.

[9] SBIT STTR, Introduction to cyberthearts, https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf

Kibernetički napadi često koriste informacijske i komunikacijske tehnologij(ICT) kako bi povećali uobičajene zločine, poput, krađe intelektualnog vlasništva, uznemiravanja i prijevare. Drugi oblici kriminala, poput, krađe identiteta, znatno su porasli u kibernetičkom prostoru.[10]

Stručnjaci iz pravnih i tehničkih područja dali su različite definicije kibernetičkog napada. Richard Clark[11] navodi da su kibernetički napadi radnje koje zemlje poduzimaju kako bi se infiltrirale u računala ili računalne mreže zemlje ili drugih zemalja s ciljem izazivanja štete ili poremećaja. U ovoj definiciji mogu se identificirati tri elementa: počinitelj napada, svrha i namjera napada. Osim toga, u smislu počinitelja napada općenito se spominju samo države, no ako je napad u kontekstu i geografskom području pod kontrolom i jurisdikcijom države (kibernetički prostor mreža pod kontrolom država) od strane pojedinaca i ako nevladine i privatne skupine djeluju protiv treće zemlje, to je izvan opsega navedene definicije.

Michael Hayden[12] kibernetički napad definira kao svaki namjerni pokušaj ometanja ili uništavanja računalnih mreža druge zemlje. Ova je definicija, također, vrlo općenita i ne određuje nikakvu razliku između kibernetičkog kriminala, kibernetičkog napada i kibernetičkog rata. Martin Libicki[13] kibernetičke napade definira kao digitalne napade na računalne sustave koji uzrokuju da se napadnuti računalni sustavi čine normalnima, ali zapravo proizvode i izdaju neistinite odgovore. Ovakav pristup definiranju kibernetičkih napada zapravo isključuje širok raspon potencijalnih prijetnji nacionalnoj sigurnosti zemlje čija je kibernetička infrastruktura bila meta, ali nije dosegla razinu i prag smislenih napada. Činjenica je da te prijetnje mogu oštetiti računalne sustave i mreže zemalja koje se kibernetički napadaju.

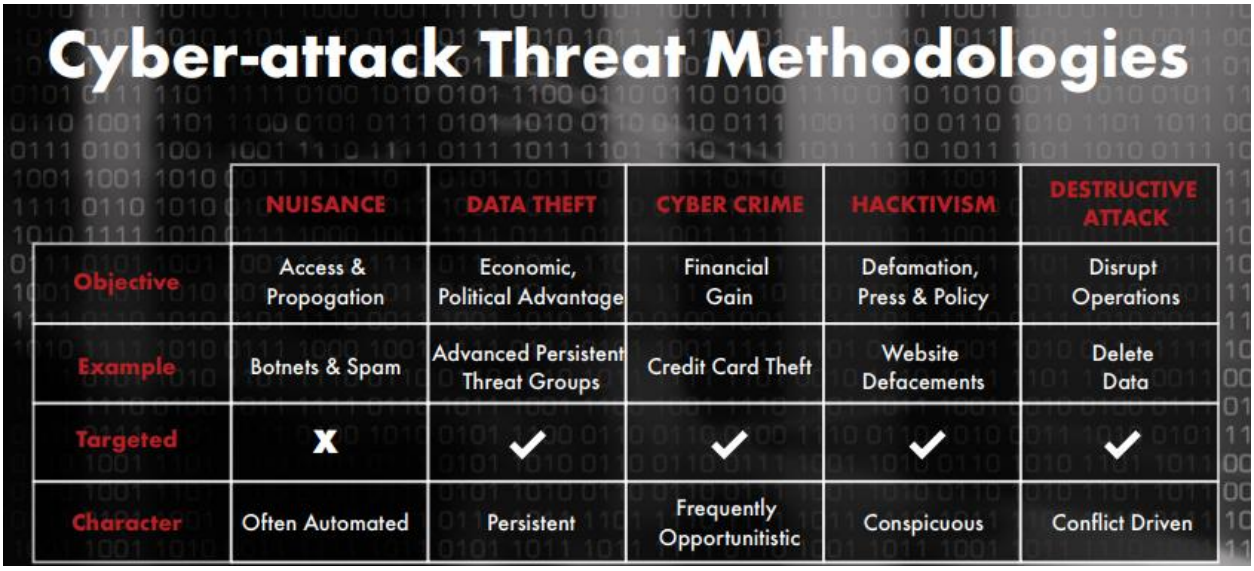
Stoga, kibernetički prostor sve više utječe na sigurnosne zadaće i funkcije svake zemlje. Zbog globalne proizvodnje softverskih i hardverskih proizvoda, nemoguće je dati jamstva u procesu lanca nabave proizvoda. Cyber prijetnje imaju vrlo širok raspon učinaka. Kao i mnogim

[10] Motsch W. i sur. (2020) Approach for dynamic price-based demand side management in cyber-physical production systems Procedia Manuf., 51, str. 1748-1754.
[11] Motsch W. i sur. (2020) Approach for dynamic price-based demand side management in cyber-physical production systems Procedia Manuf., 51, str. 1756-1758.
[12] Robinson M., Jones K., Janicke H. (2015) Cyber warfare: Issues and challenges Comput. Secur., 49, str. 70-94.
[13] Quigley K., Burns C., Stallard K. (2015) 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection Gov. Inf. Q., 32 (2), str. 108-117.

drugim područjima znanja, operacije unutar kibernetičkog prostora kontrolira relativno mali broj pojedinaca.

Promjene u području kibernetike događaju se brzo i temelje se na stalnom razvoju računalnih i komunikacijskih tehnologija. Cyber kohezija povećava ovo ubrzanje. Svaka promjena stvara novu eru ranjivosti i odgovora. Distribucija kibernetičke imovine široko je rasprostranjena u svim vrstama organizacija, od zatvorenih sustava i sustava pod kontrolom vlade do sustava u vlasništvu i pod upravljanjem privatnog sektora. Priroda kibernetičkog prostora je takva da trenutno ne postoji tehnička mogućnost dodjele aktivnosti pojedincima, grupama ili organizacijama, s visokim stupnjem povjerenja.[14]

Slika 1 prikazuje metodologiju kibernetičkog napada.



Slika 1. Metodologija kibernetičkog napada

Izvor: SBIT STTR, Introduction to cyberthearts, https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf

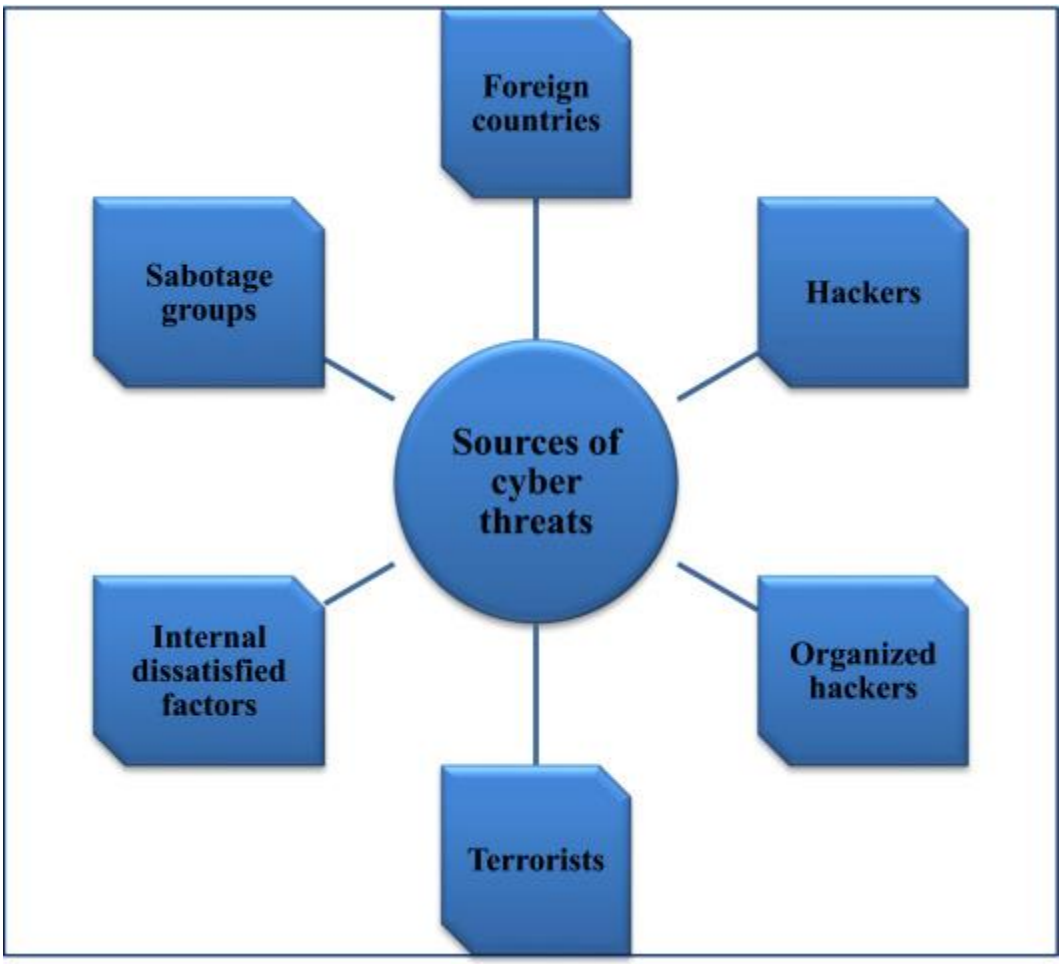
Osnovne prijetnje u kibernetičkom prostoru su: strane prijetnje, unutarnje prijetnje, prijetnje u opskrbnom lancu roba i usluga te prijetnje zbog nedovoljne operativne sposobnosti

[14] Zhao Z. i sur. (2021) Control-theory based security control of cyber–physical power system under multiple cyber attacks within unified model framework Cogn. Robot.

lokalnih snaga. Strane obavještajne službe koriste se cyber alatima za izvođenje nekih od svojih aktivnosti vezanih uz prikupljanje obavještajnih podataka i špijunaže. Diljem svijeta realizirani su brojni takvi slučajevi zlouporabe i uništavanja informacijskih infrastruktura zemalja, uključujući računalne sustave, internetske informacijske mreže te procesore i kontrolere ugrađene u vitalne industrije. Drugi izvor napada su skupine ljudi koje napadaju kibernetičke sustave kako bi zaradile novac. Osim toga, skupine (hakeri) ponekad ulaze u mrežu kako bi se izrazili. U trenutnoj situaciji moguće je infiltrirati se u mreže s minimalnim znanjem i vještinama, preuzimanjem potrebnih programa i protokola s interneta i njihovim korištenjem protiv drugih stranica. Skupne s političkim motivima napada napadaju popularne web stranice ili hostove e-pošte. Ove grupe obično nameću povećana opterećenja hostovima elektroničke pošte, a infiltracijom na web stranice objavljuju svoje političke poruke.[15]

S druge strane, interni nezadovoljni agenti koji djeluju unutar organizacije glavni su izvor kibernetičkog kriminala, a ti agenti ne moraju imati značajno znanje o kibernetičkim napadima jer uglavnom imaju neograničen pristup sustavu. Teroristi su još jedan izvor prijetnje koji nastoji uništiti, onesposobiti ili zlonamjerno iskoristiti vitalnu infrastrukturu kako bi ugrozili nacionalnu sigurnost, nanijeli velike gubitke, oslabili gospodarstvo zemlje i potkopali javni mentalitet i povjerenje.[16]

[15] Solomon R. (2017) Electronic protests: Hacktivism as a form of protest in Uganda Comput. Law Secur. Rev., 33 (5), str. 718-728.
[16] Isto.



Slika 2. Izvori cyber prijetnji

Izvor: Solomon R. (2017) Electronic protests: Hacktivism as a form of protest in Uganda Comput. Law Secur. Rev., 33 (5), str. 718-728.

3.2 Klasifikacija i kontroliranje napada

Preljev spremnika (engl. *buffer overflow*) predstavlja programsku smetnju koja zaustavlja rada programa. Naime, u određenome trenutku u polje određene duljine želi zapisati podatak koji je veći od veličine samoga polja. Dolazi do kopiranja memorijskih lokacija koje nisu namijenjene za pohranu podataka koji se zapisuju u polje u trenutku kada se nevedeno događa.[17]

[17] FER, Preljev spremnika, http://sigurnost.zemris.fer.hr/ns/malware/2007_klaric/buffer_overflow.html

U prekoračenja međuspremnika, kada se u međuspremnik unese više infomracija od mogućeh kapaciteta, višak informacija može prebrisati susjedne memorijske lokacije, kao što su drugi međuspremnici, kontrolni podaci ili čak izvršni kod programa. To može dovesti do raznih posljedica, uključujući padove, nenamjerno ponašanje i sigurnosne nestabilnosti.

Iskorištavanje ranjivosti prekoračenja međuspremnika može biti osobito opasno jer napadač može iskoristiti prebrisanu memoriju za izvršavanje proizvoljnog koda ili ubacivanje zlonamjernog sadržaja. Izradom posebno izrađenih ulaznih podataka, napadač može prebrisati povratnu adresu funkcije ili manipulirati kontrolnim tokom programa, potencijalno dovodeći do neovlaštenog pristupa, eskalacije privilegija ili daljinskog izvršavanja koda.

Ranjivosti prekoračenja međuspremnika često se pojavljuju u programskim jezicima koji ne pružaju ugrađene mehanizme za automatsko upravljanje memorijom. U tim jezicima programeri su odgovorni za upravljanje dodjelom memorije i osiguravanje da se granice međuspremnika ne krše ako bi ublažili ranjivosti prekoračenja međuspremnika, programeri bi trebali usvojiti sigurne prakse kodiranja, kao što je korištenje programskih jezika s ugrađenim mehanizmima za upravljanje memorijom.

Napad se izvodi na taj način da se sadržaj instrukcijskog registra prepiše zajedno sa adresom memorijske lokacije na koju je napadač već pohranio zlonamjeran program koji se dalje izvršava neprimjetno za korisnika.[18]

Slijedeći napad je napad uskraćivanja posluživanja. Naime napad uskraćivanja posluživanja (engl. *DoS – Denial of Service*) je takva vrsta napada na sustav u kojem svim korisnicima sustava uskrati uslugu. Primarni cilj napada je zatrpati metu bujicom nelegitimnih zahtjeva ili prekomjernim prometom, čineći je nesposobnom odgovoriti na legitimne zahtjeve korisnika. Tada računalni sustav nije u mogučnosti odgovoriti na sve zahtjeve koje šalju legitimni korisnici pa samim time i sustav postaje neupotrebljiv sa strane legitimnog korisnika. Preopterećenjem ovih resursa, napadač može uzrokovati usporavanje ciljnog sustava, prestanak reakcije ili potpuni pad. Ovi oblici napada mogu nanjeti ozbiljne štete kao što su ometanje mrežnih usluga, nanošenje financijskih gubitaka, narušavanje ugleda ili dovođenje do produženog prekida

[18] FER, Preljev spremnika, http://sigurnost.zemris.fer.hr/ns/malware/2007_klaric/buffer_overflow.html

rada. DoS napad također može biti korišten kao varka dok se provede neke druge zlonamjerne aktivnosti.

DoS napad se može provoditi na različite načine. Jedan od njih je i "smurf" napad koji iskorištava neispravno podešene računalne mreže. Napadači tada lažiraju IP adresu izvorišta paketa što odgovara meti napada. Sva računala dobiju pakete preko adrese za razašiljanje te meta napada postaje pretrpana. Također se može oslanjati na grešku u samoj funkciji za sastavljanje paketa u različitim operacijskim sustavima i to na način da se šalju paketi s prevelikim podatkovnim dijelom koji se preklapaju u fragmentima drugog paketa.[19]

Tu su i zlonamjerni programi kojima se vrše zlonamjerne aktivnosti kao što su povrede podataka ili pokušaji upada u mrežu. Najčešća podjela je sljedeća:

- Virusi
- Crvi
- Trojanci
- Adware
- Spyware.

Slika 3. Zlonamjerni programi

Izvor: Sigurnost na internetu, Što je malware?, http://web1.os-sradic-oprisavci.skole.hr/sigurni-na-internetu/internet/malware/sto-je-malware/

[19] Martins, A. (2023) Cyberattacks and Your Small Business: A Primer for Cybersecurity, https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

Računalni virusi obično se pričvršćuju na izvršne datoteke, kao što su programske datoteke ili dokumenti, i mogu se širiti različitim sredstvima, uključujući privitke e-pošte, zaražene prijenosne medije, zlonamjerna preuzimanja s interneta ili mrežne ranjivosti. Korisnici nisu ni svjesni da su izvršne datoteke na njihovu računalu uopće zaražene virusom.

Slijedeći tip zlonamjernih programa su crvi. Oni za razliku od virusa imaju mogućnost samostalnog širenja nakon što su pokrenuti od strane napadača. Za širenje najčešće koriste neispravljene greške u operacijskim sustavima ili drugim programima.[20]

Trojanski virus, koji se često naziva trojanski konj, vrsta je zlonamjernog softvera koji se maskira kao legitiman ili benigni softver. Slično mitskom trojanskom konju, trojanski virus korisniku se čini bezopasnim ili korisnim, ali nosi zlonamjernu namjeru. Trojanski virusi obično se distribuiraju prijevarnim metodama, kao što su privici e-pošte, preuzimanja softvera iz nepouzdanih izvora ili prerušeni u legitimne programe. Kada korisnik nesvjesno pokrene ili instalira trojanac, on izvodi zlonamjerne aktivnosti na zaraženom sustavu. Trojanci virus može ukrasti osjetljive informacije iz zaraženog sustava, podaci o kreditnoj kartici ili osobni dokumenti. Ove ukradene informacije često se šalju natrag na poslužitelj napadača za neovlaštenu upotrebu ili prodaju.

Adware podrazumijeva program koji se financira reklamama (advertising-supported program) a osnovna svrha je prikaz reklama. Kada se takav program instalira u računalo, kreće prikaz promotivnog materijala, kao što su pop-up reklame, oglasi na natpisima, linkovi u tekstu i sl. Adware se obično objavljuje za promoviranje srodnih stranica i generiranje zarade svojim developerima. No, kad se takav program doda pregledniku, taj software može također prikupljati osobne neidentificirajuće podatke o aktivnosti korisnika na internetu.

Spyware je vrsta zlonamjernog softvera koji se još naziva i "špijunski" program". Obično se instalira na računalo bez znanja krajnjeg korisnika. Upada u sustav, krade osjetljive informacije i podatke o korištenju interneta i prosljeđuje ih oglašivačima, tvrtkama za obradu podataka ili vanjskim korisnicima. Bilo koji softver može se klasificirati kao špijunski ako je preuzet bez autorizacije korisnika. Špijunski softver je kontroverzan jer, čak i kada je instaliran iz relativno bezazlenih razloga, može narušiti privatnost krajnjeg korisnika i postoji mogućnost zlouporabe.

[20] Difference between Virus, Worm and Trojan Horse, https://www.geeksforgeeks.org/difference-between-virus-worm-and-trojan-horse/

Špijunski softver jedna je od najčešćih prijetnji korisnicima interneta. Jednom instaliran, nadzire internetsku aktivnost, prati vjerodajnice za prijavu i špijunira osjetljive informacije. Primarni cilj špijunskog softvera obično je dobivanje brojeva kreditnih kartica, bankovnih podataka, lozinki i sl. No spyware se također može koristiti za praćenje lokacije osobe. Često ljubomorni supružnici, bivši partneri, pa čak i zabrinuti roditelji tajno instaliraju na mobitele, ova vrsta špijunskog softvera može pratiti fizičku lokaciju žrtve, presresti njihovu e-poštu i poruke, prisluškivati njihove telefonske pozive i snimati razgovore te pristupiti osobnim podacima , kao što su fotografije i videozapisi. Spyware može biti teško otkriti. Često je prva naznaka koju korisnik ima da je računalo zaraženo špijunskim softverom primjetno smanjenje brzine procesora ili mrežne veze i u slučaju mobilnih uređaja, potrošnja podataka i smanjenje trajanja baterije. Antispyware alati mogu se koristiti za sprječavanje ili uklanjanje špijunskog softvera. Oni mogu pružiti zaštitu u stvarnom vremenu skeniranjem mrežnih podataka i blokiranjem zlonamjernih podataka ili mogu izvršiti skeniranje za otkrivanje i uklanjanje špijunskog softvera koji je već u sustavu.[21]

Više o pojedinim pojedinim vrstama zlonamjernih programa pogledati u poglavlju 4. ovoga rada.

[21] Techtarget, https://www.techtarget.com/searchsecurity/definition/spyware

4. Hakiranje

Haker može biti bilo tko ako ima osnovno znanje, želju, motivaciju i (ponekad) nešto novca. Osim ovih karakteristika, uspješan haker mora imati i veliku dozu strpljenja i sposobnosti planiranja. Međutim, niti su svi hakeri isti niti svi hakeri imaju iste ciljeve.

4.1 Hakeri

Hakeri se obično kategoriziraju u tri glavne skupine:[22]

1. Black-hat hakeri
2. White-hat hakeri
3. Gray-hat hakeri.

Haker s crnim šeširom je osoba koja pokušava pronaći sigurnosne propuste računala i iskoristiti ih za osobnu financijsku korist ili druge zlonamjerne razloge. Black hat hakeri su hakeri koji provaljuju u računalne mreže sa zlom namjerom. Također, mogu objaviti zlonamjerni softver koji uništava datoteke, drži računala kao taoce ili krade lozinke, brojeve kreditnih kartica i druge osobne podatke.

Black hat hakeri često počinju kao početnici koristeći kupljene hakerske alate za iskorištavanje sigurnosnih propusta. Neke za hakiranje obučavaju šefovi željni brze zarade. Vodeći crni šeširi obično su vješti hakeri koji rade za sofisticirane kriminalne organizacije koje ponekad svojim radnicima pružaju alate za suradnju i klijentima nude ugovore o uslugama, baš kao i legitimne tvrtke. Black hat kompleti zlonamjernog softvera koji se prodaju na dark webu povremeno čak uključuju jamstvo i korisničku službu.

Hakiranje je postalo sastavni alat za prikupljanje obavještajnih podataka za vlade, ali je uobičajenije da crni hakeri rade sami ili s organizacijama organiziranog kriminala. Black hat hakiranje je globalni problem zbog čega ga je izuzetno teško zaustaviti. Izazovi za provedbu

[22] Iwugo, D. (2022) What are White Hat, Black Hat, and Red Hat Hackers? Different Types of Hacking Explained, https://www.freecodecamp.org/news/white-hat-black-hat-red-hat-hackers/

zakona su to što hakeri često ostavljaju malo dokaza, koriste se računalima žrtava koje ništa ne sumnjaju i prelaze više jurisdikcija. Iako vlasti ponekad uspiju zatvoriti hakersku stranicu u jednoj zemlji, ista se operacija može izvesti i drugdje, omogućujući grupi da nastavi.[23]

Haker s bijelim šeširom je stručnjak za računalnu sigurnost koji provaljuje u zaštićene sustave i mreže kako bi testirao i procijenio njihovu sigurnost. White-hat hakeri koriste svoje vještine za poboljšanje sigurnosti izlažući ih ranjivosti prije nego što ih zlonamjerni hakeri (poznati kao black hat hakeri) mogu otkriti i iskoristiti. Obavljaju zadatke kao što su[24]:

- Skeniranje mreža
- Konfiguriranje IDS-ova (sustava za otkrivanje upada)
- Etičko hakiranje računala kako bi se pronašle ranjivosti i prijavile ih kako bi se mogle riješiti
- Programiranje honeypots
- Praćenje mrežne aktivnosti za sumnjive aktivnosti.

Haker sa sivim šeširom je netko tko može prekršiti etičke standarde ili načela, ali bez zle namjere koja se pripisuje hakerima s crnim šeširom. Hakeri sa sivim šeširom često rade za opće dobro.[25]

Glavna razlika između bijelih, crnih i sivih hakera je motivacija ili namjera koju svaki tip hakera ima kada provali u računalne sustave. Bijeli hakeri istražuju slabosti kibernetičke sigurnosti kako bi pomogli organizacijama da razviju jaču sigurnost, hakeri crnog šešira motivirani su zlom namjerom, a sivi hakeri djeluju u području između - nisu zlonamjerni, ali nisu uvijek ni etični.[26]

[23] Kaspersky, Black hat, White hat, and Gray hat hackers – Definition and Explanation, https://www.kaspersky.com/resource-center/definitions/hacker-hat-types
[24] Iwugo, D. (2022) What are White Hat, Black Hat, and Red Hat Hackers? Different Types of Hacking Explained, https://www.freecodecamp.org/news/white-hat-black-hat-red-hat-hackers/
[25] Black Hat. Black Hat Hacker, http://www.blackhat.com
[26] Avast, Hacker Types: Black Hat, White Hat, and Gray Hat Hackers, https://www.avast.com/c-hacker-types

Slika 4. Razlike između pojedinih tipova hakera

Izvor: Avast, Hacker Types: Black Hat, White Hat, and Gray Hat Hackers, https://www.avast.com/c-hacker-types

Zanimljivo je da svi koriste iste alate i metode, a glavna razlika je u ciljevima i rezultatima. S druge strane, hakeri se mogu podijeliti u nekoliko skupina prema znanju i vještinama. Najvišu razinu čine hakeri koji točno znaju što rade, koji su vrlo dobro upoznati sa sustavom i sposobni su kreirati odgovarajući softver, uključujući viruse i druge zlonamjerne programe. Srednju razinu čine takozvani "tehničari" koji su u mogućnosti koristiti alate koji se mogu kupiti na tržištu softvera i hardvera. Treću, najnižu razinu hakera, čine takozvani "script kiddies". Skript kiddies je pogrdni izraz za nezrelog, ali često jednako opasnog iskorištavača sigurnosnih propusta na internetu. Oni iskorištavaju slabosti internetskih računala često nasumično i s malo pažnje ili možda čak i razumijevanja potencijalno štetnih posljedica.[27]

[27] ROUSE, M. Script Kiddy, http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy

4.2 Tipovi hakiranja

Hakiranje se može realizirati na različite načine, a neki od najčešće korištenih načina za realizaciju hakiranja su:

1. Trojanski programi koji dijele datoteke putem instant messengera.
2. Phishing
3. Lažne web stranice
4. Spoofing
5. Spyware
6. Elektroničke oglasne ploče
7. Informacijski brokeri
8. Internet javne evidencije
9. Trojanski konji
10. Wormhole Attack.

4.2.1 Trojanski program

Instant messenger omogućuje dijeljenje datoteka na računalu. Svi sadašnji popularni programi za razmjenu trenutnih poruka imaju mogućnosti dijeljenja datoteka ili omogućuju korisnicima korištenje navedene funkcije instaliranjem zakrpa ili dodataka. To je, također, velika prijetnja sadašnjoj informacijskoj sigurnosti. Ovaj komunikacijski softver, također, otežava postojećoj metodi za sprječavanje hakiranja da spriječi i kontrolira sigurnost informacija.

Hakeri koriste mogućnost trenutne komunikacije kako bi podmetnuli trojanski program u nesumnjivi program. Podmetnuti program je vrsta daljinski upravljanog alata za hakiranje koji se može prikriti i neovlašten je. Trojanski program se nesvjesno izvršava, kontrolirajući zaraženo računalo. Može čitati, brisati, premještati i izvršavati bilo koju datoteku na računalu. Prednosti

hakerske zamjene daljinski instaliranih backdoor trojanskih programa s instant messengerima za pristup datotekama su[28]:

- Kada je žrtva online, haker je o tome obaviješten. Tako haker može pratiti i pristupiti zaraženom računalu te neprestano krasti korisničke podatke.
- Haker ne mora otvoriti novi port za izvođenje prijenosa, već može obavljati svoje operacije preko već otvorenog porta za instant messenger. Ako i računalo koristi dinamičke IP adrese, njegovo zaslonsko ime se ne mijenja.

4.2.2 Otmica i lažno predstavljanje

Postoje različiti načini na koje haker može lažno predstavljati druge korisnike. Najčešće korištena metoda je prisluškivanje korisnika koji ništa ne sumnjaju kako bi se saznali korisnički računi, lozinke i druge informacije vezane uz korisnike. Krađa broja korisničkog računa i povezanih informacija vrlo je ozbiljan problem u bilo kojem internet messengeru. Na primjer, haker nakon što ukrade podatke o korisniku oponaša korisnika, korisnički kontakti ne znajući da je korisnički račun hakiran vjeruju da je osoba s kojom razgovaraju korisnik te ih se nagovara da izvrše određene programe ili otkriju povjerljive podatke. Dakle, krađa korisničkog identiteta ne ugrožava samo korisnika, već i okolne korisnike.

Zaštita od internetskih sigurnosnih problema trenutno je u fokusu istraživanja; jer bez dobre zaštite računalo može biti lako napadnuto, uzrokujući velike gubitke. Hakeri koji žele doći do korisničkih računa mogu to učiniti pomoću trojanca dizajniranih za krajnje lozinke. Ako klijent instant messengera pohranjuje svoju lozinku na svoje računalo, tada haker može poslati trojanski program korisniku koji ništa ne sumnja. Kada korisnik izvrši program, program će tražiti korisničku lozinku i poslati ga hakeru. Postoji nekoliko načina na koji trojanski program može poslati poruku natrag hakeru. Metode uključuju instant messenger, IRC, e-poštu itd. Najčešće

[28] Alassouli, H. M., Common Windows, Linux and Web Server Systems Hacking Techniques, https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Common_Windows,_Linux_and_Web_Server_Systems_Hacking_Techniques.pdf

korišteni instant messengeri su AIM, Yahoo! Messenger, ICQ i MSN Messenger, od kojih nijedan ne šifrira svoj tok.[29]

4.2.3 Uskraćivanje usluge

Postoji mnogo načina na koje haker može pokrenuti napad uskraćivanjem usluge (DoS) na korisnika instant messengera. Djelomični DoS napad uzrokuje zaustavljanje rada korisnika ili iskorištava veliki dio CPU resursa uzrokujući nestabilnost sustava. Postoji mnogo načina na koje haker može uzrokovati uskraćivanje usluge na klijentu instant messengera. Jedan uobičajeni tip napada je zasipanje određenog korisnika velikim brojem poruka. Popularni klijenti za izravnu razmjenu poruka sadrže zaštitu od flood napada dopuštajući žrtvi da zanemari određene korisnike.

Međutim, postoje mnogi alati koji hakeru omogućuju istovremeno korištenje više računa ili automatsko stvaranje velikog broja računa za izvođenje flood napada. Tome treba pridodati i činjenica da nakon što započne napad i žrtva shvati što se dogodilo, računalo može prestati reagirati. Stoga bi dodavanje napadačkih korisničkih računa na popis zanemarivanja klijenta instant messengera moglo biti vrlo teško. DoS napade vrlo je lako generirati i vrlo ih je teško otkriti pa su stoga privlačno oružje za hakere. U tipičnom DoS napadu napadački čvor lažira svoju IP adresu i koristi više međučvorova da bi zatrpao druge čvorove prometom. DoS napadi obično se koriste za isključivanje važnih poslužitelja na nekoliko sati, što rezultira DoS-om za sve korisnike koje poslužuje poslužitelj. Također se može koristiti za ometanje usluga međuusmjerivača.[30]

[29] Alassouli, H. M., Common Windows, Linux and Web Server Systems Hacking Techniques, https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Common_Windows,_Linux_and_Web_Server_Systems_Hacking_Techniques.pdf

[30] Alassouli, H. M., Common Windows, Linux and Web Server Systems Hacking Techniques, https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Common_Windows,_Linux_and_Web_Server_Systems_Hacking_Techniques.pdf

4.2.4 Phishing

Riječ phishing dolazi iz analogije da internetski prevaranti koriste mamce e-pošte kako bi pridobili lozinke i financijske podatke od internetskih korisnika. Izraz su formirali 1996. godine hakeri koji su krali AOL internetske račune prevarom lozinki od AOL korisnika koji ništa nisu sumnjali. Budući da hakeri imaju tendenciju zamjenjivati "f" s "ph", izveden je izraz phishing.

Phishing je metoda koja iskorištava simpatije ljudi u obliku e-poruka za traženje pomoći: e-mail djeluje kao mamac. Ovi e-mailovi obično traže od korisnika da posjete poveznicu koja naizgled vodi na web stranicu neke dobrotvorne organizacije, ali zapravo povezuje korisnika s web stranicom koja će instalirati trojanski program na računalo korisnika. Stoga, korisnici ne bi trebali prosljeđivati neprovjerene dobrotvorne e-poruke ili klikati na nepoznate poveznice u e-pošti. Ponekad poveznica može biti vrlo poznata poveznica ili često posjećena web stranica, ali ipak bi bilo sigurnije da korisnici upišu adresu kako bi izbjegli povezivanje s lažnom web lokacijom.[31]

Phisher obmanjuje ljude korištenjem sličnih e-mailova koje šalju poznata poduzeća ili banke. Ove e-pošte često traže od korisnika da dostave osobne podatke ili rezultiraju gubitkom njihovih osobnih prava. Obično sadrže krivotvoreni URL koji vodi do web stranice na kojoj korisnici mogu ispuniti tražene podatke. Ljudi često budu obuhvaćeni phishingom zbog nepažnje.[32]

Većina metoda phishinga koristi se nekim oblikom tehničke prijevare osmišljene kako ne bi poveznica u e-poruci (i lažirana web stranica do koje vodi) izgledala kao da pripada lažiranoj organizaciji. Pogrešno napisani URL-ovi ili korištenje poddomena uobičajeni su trikovi koje koriste krađe identiteta, kao što je ovaj primjer URL-a, http://www.yourbank.com.example.com/. Još jedan uobičajeni trik je učiniti da se tekst sidra za vezu čini važećim kada veza, zapravo, vodi na web-mjesto phishinga. Ranija metoda lažiranja koristila je poveznice koje su sadržavale simbol '@', izvorno zamišljen kao način uključivanja korisničkog imena i lozinke (suprotno standardu). Na primjer, veza http://www.google.com@members.tripod.com/mogla bi korisnika navesti da

[31] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017) Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), str. 3629-3654.
[32] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017) Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), str. 3629-3654.

povjeruje da će otvoriti stranicu na www.google.com, a, zapravo, se usmjerava preglednik na stranicu na members.tripod.com, koristeći korisničko ime www.google.com: stranica se otvara normalno, bez obzira na navedeno korisničko ime.

Daljnji problem s URL-ovima je u rukovanju internacionaliziranim nazivima domena (lDN) u web-preglednicima, koji mogu omogućiti da vizualno identične web-adrese vode do različitih, moguće zlonamjernih, web-mjesta. Phisheri su iskoristili sličan rizik, koristeći otvorene URL preusmjerivače na web stranicama pouzdanih organizacija kako bi prikrili zlonamjerne URL-ove s pouzdanom domenom. Phisheri koriste slike umjesto teksta kako bi filtrima protiv krađe identiteta bilo teže otkriti tekst koji se obično koristi u e-porukama za krađu identiteta.[33]

4.2.5 Pharming

Po prirodi sličan phishingu, Pharming je hakerski napad čiji je cilj preusmjeriti promet web stranice na drugu, lažnu web stranicu. Pharming se može provesti ili promjenom host datoteke na žrtvinom računalu ili iskorištavanjem ranjivosti u softveru DNS poslužitelja. DNS poslužitelji su računala odgovorna za pretvaranje internetskih imena u njihove stvarne adrese - oni su "putokazi" interneta. Ugroženi DNS poslužitelji ponekad se nazivaju "otrovani". Izraz pharming je igra riječi o farmingu i phishingu. Izraz phishing odnosi se na napade društvenog inženjeringa za dobivanje vjerodajnica za pristup kao što su korisnička imena i lozinke. Posljednjih godina farmacija se koristi za krađu podataka o identitetu.[34]

Pharming je postao glavna briga za tvrtke koje hostiraju web stranice za e-trgovinu i internetsko bankarstvo. Tehnika koja se koristi za dobivanje neovlaštenog pristupa računalima uključuje da haker šalje poruku računalu s IP adresom koja pokazuje da poruka dolazi od pouzdanog hosta. Da bi se uključio u lažiranje IP-a, haker prvo mora upotrijebiti razne tehnike kako bi pronašao IP adresu pouzdanog hosta, a zatim modificirati zaglavlja paketa tako da se čini da paketi dolaze s tog hosta. Pojam usko povezan i često poistovjećivan s phishingom i

[33] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017) Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), str. 3629-3654.

[34] FDIC, Guidance on How Financial Institutions Can Protect Against Pharming Attacks, https://www.fdic.gov/news/financial-institution-letters/2005/fil6405.pdf

pharmingom je spoofing. "Spoofer", u internetskim terminima, općenito se definira kao "kreker" koji mijenja ili "krivotvori" adresu e-pošte, pretvarajući se da potječe s izvorne adrese različite od one koju on ili ona uistinu ima. Postoji mnogo načina na koje napadač to može učiniti, a postoje i mnoge vrste napada. Napadač to može učiniti kako bi dobio pristup zaštićenoj stranici koja bi prihvatila "otetu" adresu kao jednu od nekoliko dopuštenih adresa ili zlonamjernije, razlog može biti skrivanje izvora bilo koje vrste napada.

4.2.6 Spyware

Spyware softver je računalni softver koji se može koristiti za prikupljanje i uklanjanje povjerljivih informacija s bilo kojeg računala bez znanja vlasnika. Sve što surfer radi online, uključujući njegove lozinke, može biti ranjivo na spyware softver. Spyware softver svakoga može dovesti u veliku opasnost da postane žrtva krađe identiteta. Štoviše, neki oblici spyware softvera mogu se instalirati na računalo s udaljene lokacije bez da kradljivac identiteta ikada ima fizički pristup žrtvinom računalu.[35]

Dok pojam spyware sugerira softver koji potajno nadzire ponašanje korisnika, funkcije spyware softvera proširuju se mnogo dalje od jednostavnog nadzora. Spyware programi mogu prikupljati razne vrste osobnih podataka, ali, također, mogu ometati korisničku kontrolu nad računalom na druge načine, kao što je instaliranje dodatnog softvera, preusmjeravanje aktivnosti web preglednika, pristupanje web stranicama bez nadzora do dovodi do prikupljanja virusa ili preusmjeravanja prihoda od oglašavanja na treća strana. Spyware softver može čak promijeniti postavke računala, što rezultira sporom brzinom veze, različitim početnim stranicama i gubitkom interneta ili drugih programa.

U pokušaju da se poveća razumijevanje spyware softvera, formalnija klasifikacija uključenih vrsta softvera obuhvaćena je pojmom softver koji narušava privatnost. Kao odgovor na pojavu spyware softvera, pojavila se mala industrija koja se bavi 11 anti-spyware softverom. Pokretanje anti-spyware softvera postalo je općepriznat element najbolje prakse računalne sigurnosti za Microsoft Windows osobna računala. Brojne jurisdikcije donijele su zakone protiv

[35] Uomtemp, Spyware, http://uomtemp.uom.ac.mu/CITS/images/tips/spyware/Spyware.pdf

spyware softvera, koji obično ciljaju na bilo koji softver koji je potajno instaliran za kontrolu računala korisnika.

4.2.7 Trojanski konj

Trojanski konj (poznat kao Trojanac) definiran je kao softverski paket koji sadrži zlonamjerni kod koji se čini legitimnim, slično starogrčkom mitu o Odiseji koja je uzrokovala ozbiljnu štetu Troji unatoč bezopasnoj vanjštini. Trojanci su zlonamjerni kod ili softver koji se infiltrira u računalo dok se lažno predstavlja kao pravi program i na kraju preuzme kontrolu nad sustavom, a da korisnik ili IT administrator to ne primijeti. Tehnički, trojanci nisu virusi, već su vrsta zlonamjernog softvera.[36]

Trojanci se mogu koristiti za izvođenje nekoliko štetnih radnji poput brisanja podataka, cenzure podataka, modifikacije podataka, kopiranje podataka i izazivanja smetnji u radu računala ili računalnih mreža.

Trojanski konj, za razliku od računalnih virusa, ne može se manifestirati sam od sebe. Za njezino funkcioniranje korisnik mora preuzeti klijentsku stranu aplikacije. Izvršna datoteka (.exe) mora biti implementirana i softver instaliran da bi trojanac mogao napasti uređaj. Trojanci djeluju lažno predstavljajući legitimne datoteke kako bi prevarili žrtve da ih kliknu, otvore ili instaliraju. Kada se to dogodi, trojanac nastavlja instalirati zlonamjerni softver na uređaj i pokreće se svaki put kada se zaraženi uređaj uključi. Trojanci e-pošte, na primjer, koriste taktiku društvenog inženjeringa da nalikuju bezopasnim privicima e-pošte, zavaravajući korisnika da otvori priloženu datoteku.

Računalo zaraženo trojanskim zlonamjernim softverom, također, ga može prenijeti na druge sustave. Cyberkriminalac transformira sustav u zombi računalo, dajući mu daljinsku kontrolu nad njim bez znanja korisnika. Hakeri tada mogu koristiti zombi računala za širenje zlonamjernog softvera preko mreže uređaja poznatih kao botnet. Zlonamjerni softver će se aktivirati nakon izvođenja određenih radnji korisnika, kao što je pristup određenoj web stranici ili

[36] BasuMallick, C. (2022) What Is a Trojan Horse? Meaning, Examples, and Prevention Best Practices for 2022, https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/

korištenje bankovne aplikacije. Ovisno o vrsti trojanca i njegovoj metodi stvaranja, zaraza se može izbrisati, vratiti u stanje mirovanja ili ostati aktivna čak i nakon što haker izvrši željenu akciju.[37]

[37] BasuMallick, C. (2022) What Is a Trojan Horse? Meaning, Examples, and Prevention Best Practices for 2022, https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/

5 Najpoznatiji hakerski napadi

U ovom poglavlju objašnjeni su neki od najpoznatijih hakerskih napada na globalnoj razini.

5.1 WannaCry Ransomware

Ransomware je vrsta zlonamjernog softvera (malware) koji korisnicima onemogućuje pristup ili im ograničava pristup sustavu ili datotekama, bilo zaključavanjem zaslona ili šifriranjem datoteka, sve dok se ne plati otkupnina. U većini slučajeva ransomware ostavlja korisniku vrlo malo opcija, kao što je samo dopuštanje žrtvi da komunicira s napadačem i platiotkupninu. Najčešće vrste ransomwarea koriste neki oblik enkripcije, uključujući simetrične sheme šifriranja i sheme šifriranja temeljene na javnom ključu.[38]

WannaCry ransomware uočen je tijekom masovnog napada u više zemalja 12. svibnja 2017. godine. Prema brojnim izvješćima dobavljača sigurnosnih sustava, ukupno 300.000 sustava u više od 150 zemalja bilo je ozbiljno oštećeno. Napad je zahvatio širok raspon sektora, uključujući zdravstvo, vlade, telekomunikacije i proizvodnju plina/nafte.[39]

Poteškoće u zaštiti od WannaCryja proizlaze iz njegove sposobnosti širenja na druge sustave pomoću komponente crva. Ova značajka čini napade učinkovitijima i zahtijeva obrambene mehanizme koji mogu reagirati brzo i u stvarnom vremenu. Nadalje, WannaCry ima komponentu šifriranja koja se temelji na kriptografiji s javnim ključem. Tijekom faze zaraze, WannaCry koristi eksploatacije EternalBlue i DoublePulsar koje je u travnju 2017. godine lansirala grupa pod nazivom The Shadow Brokers. EternalBlue iskorištava ranjivost bloka poruka poslužitelja (SMB) koju je Microsoft plasirao 14. ožujka 2017. Godine.[40]

[38] Everett, C. (2016) Ransomware: To pay or not to pay?, Comp. Fraud & Secur., 4, str. 8–12.
[39] What you need to know about the WannaCry ransomware,, https://www.symantec.com/blogs/threat-intelligence/wannacryransomware-attack
[40] Microsoft Security Bulletin MS17-010 – Critical, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Ova ranjivost omogućuje hakerima da izvrše daljinski kod na zaraženim računalima slanjem posebno kreiranih poruka SMB v1 poslužitelju, povezivanjem na TCP portove 139 i 445 nezakrpanih Windows sustava. Konkretno, ova ranjivost utječe na sve nepodržane verzije sustava Windows počevši od Windows XP do Windows 8.1, osim Windowsa 10. Tijekom procesa distribucije, komponenta crva WannaCry koristi EternalBlue za početnu infekciju kroz SMB ranjivost, aktivnim ispitivanjem odgovarajućih TCP portova i, ako je uspješna, pokušava ugraditi DoublePulsar backdoor na zaražene sustave.

Unutar 24 sata zlonamjerni softver WannaCry — kripto-crv koji se sam razmnožava i samoumnožava —uzrokovao je globalnu štetu od 4 milijarde dolara, uglavnom zbog troškova prekida poslovanja. WannaCry je koristio eksploataciju EternalBlue za ciljanje računala s operativnim sustavom Microsoft Windows. Iako je Microsoft službeno objavio zakrpu za ranjivost EternalBlue gotovo dva mjeseca prije napada, većina računala u svijetu još uvijek nije bila zakrpana, što je WannaCryju omogućilo takav globalni utjecaj.

Podaci na zaraženim računalima bili su šifrirani i prikazana je poruka o otkupnini u kojoj se traži Bitcoin u vrijednosti od 300 do 600 dolara za dešifriranje datoteka. Ovako mala otkupnina ukazuje na to da je glavni cilj napadača bio kaos i uništenje umjesto financijske dobiti. Nekoliko sati nakon početka napada, britanski istraživač računalne sigurnosti otkrio je kill switch u WannaCryjevom kodu. Ransomware je šifrirao datoteke na zaraženom računalu samo ako određena tvrdo kodirana domena nije bila registrirana. Iako registracija ove domene nije pomogla već zaraženim računalima, zaustavila je širenje i dala ljudima vremena da rade na svojoj obrani.[41]

Međutim, to nije zaustavilo napad jer su se tijekom sljedećih nekoliko dana pojavile tri varijante WannaCryja s različitim prekidačima za isključivanje. Kada su različiti stručnjaci za kibernetičku sigurnost aktivirali sve prekidače za isključivanje diljem svijeta, napad je prestao. Ipak, nekoliko dana kasnije pojavila se nova varijanta koja je u potpunosti eliminirala funkciju kill switcha. No, do tada je većina sustava već bila zakrpana, ali ipak, čak i dan danas, crv WannaCry

[41] Sokolov, M. (2022) Five years of WannaCry: what has changed in ransomware since 2017?, https://insights.cybcube.com/en/five-years-of-wannacry-ransomware?hs_amp=true&utm_term=&utm_campaign=FY22_Q4_+Brand+Awareness+/+Performance+Max+(EMEA)&utm_source=adwords&utm_medium=ppc&hsa_acc=1114695891&hsa_cam=18997862872&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwzuqgBhAcEiwAdj5dRr3piSzGcuRYTMzhvBD-RGw5Y7K81hU98rYsjJOZozoRDEp07tR1aBoCBwQQAvD_BwE

inficira one računalne sustave čiji vlasnici nisu svjesni da pokreću EternalBlue ranjivost ili je jednostavno još nisu riješili.

Vjerojatno najistaknutija organizacija koja je postala žrtva WannaCryja tijekom njegova četverodnevnog prikazivanja bila je Britanska nacionalna zdravstvena služba (NHS). Tisuće uređaja - uključujući računala, MRI skenere i hladnjake za pohranu krvi - pogođeni su u desecima različitih ustanova NHS-a. Nissan Motor Manufacturing UK i Renault zaustavili su svoju proizvodnju, a španjolska Telefonica, FedEx i Deutsche Bahn bili su pogođeni, zajedno s mnogim drugim zemljama i tvrtkama diljem svijeta.

5.2 Cyber pljačka bangladeške banke

U četvrtak, 4. veljače 2016. u Bangladeškoj središnjoj banci nije radio programirani pisač koji je povezan sa SWIFT softverom, pri čemu je glavni cilj ovog pisača bio ispis transakcija u stvarnom vremenu. Toga dana direktor bangladeške centrale banka je primijetio da ne radi. Pretpostavio je da se radi o kvaru. Ubrzo nakon rješavanja problema s pisačem, transakcije su se počele ispisivati jedna za drugom. Tiskara je ispisivala previše transakcija od očekivanog, a ubrzo je direktor zajedno sa zaposlenicima primijetio da nešto nije u redu. Nakon što su se malo usredotočili, otkrili su 35 sumnjivih naloga za plaćanje enormnih iznosa novca koji su prebačeni s privatnog računa središnje banke Bangladeša na mnoge druge račune u nekoliko drugih zemalja.[42] Nijedna osoba koja radi u bangladeškoj banci nije odobrila te naloge za plaćanje, a ono što je dodatno zabunilo je to što sigurnosni sustav SWIFT nije bilo moguće hakirati, jer ima vojnu sigurnost, ali ni on nije funkcionirao.

Sigurnosni hakeri izdali su 35 lažnih uputa putem SWIFT mreže za ilegalni prijenos blizu jedne milijarde američkih dolara. s računa Federal Reserve Bank of New York koji pripada Bangladesh Bank, središnjoj banci Bangladeša. Pet od trideset i pet lažnih instrukcija uspješno je prenijelo 101 milijun američkih dolara, pri čemu se 20 milijuna američkih dolara pratilo na Šri Lanku, a 81 milijun američkih dolara na Filipinima. Banka saveznih rezervi New Yorka blokirala

[42] Dcham, J. (2016) Congresswoman wants probe of 'brazen' $81M theft from New York Fed, https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/

je preostalih trideset transakcija, u iznosu od 850 milijuna američkih dolara, zbog sumnje izazvane pogrešno napisanom uputom. Sav novac prebačen u Šri Lanku je vraćen. Međutim, vraćeno je samo oko 18 milijuna američkih dolara od 81 milijuna američkih dolara koji su prebačeni na Filipine. Većina novca prebačenog na Filipine otišla je na četiri osobna računa, a ne tvrtkama ili korporacijama.[43]

Kao i mnoge druge nacionalne banke, Bangladesh Bank, središnja banka Bangladeša, ima račun u Banci saveznih rezervi New Yorka za polaganje, održavanje i prijenos deviznih rezervi Bangladeša. Devizne rezerve Bangladeša, rastućeg gospodarstva, često dosežu više milijardi američkih dolara. Mreža SWIFT (engl. *Society for Worldwide Interbank Financial Telecommunication*) koristi se za komunikaciju s bankom koja ima devizni račun radi povlačenja, prijenosa ili polaganja valute. Kibernetički napad na bangladešku banku 2016. godine nije bio prvi napad te vrste. U 2013. godini banka Sonali iz Bangladeša, također, je bila uspješno napadnuta od strane hakera koji su uspjeli povući 250.000 američkih dolara.[44]

5.3 Sony PlayStation Network

Dana 4. travnja 2011. godine hakerska grupa Anonymous srušila je Sony PlayStation Network (PSN) ciljanim napadom distribuiranog uskraćivanja usluge. Anonymous je upozorio Sony na odmazdu nakon što je Sony poduzeo pravni postupak protiv dvoje ljudi: George Hotz, poznat kao GeoHot, i Alexander Igorrenknov, poznat kao Graf_Chokolo. Izjava Anonymousa Sonyju bila je jasna i točna. "Čestitam, Sony. Sada ste dobili nepodijeljenu pozornost Anonymousa. Vaš nedavni pravni postupak protiv naših kolega hakera, GeoHot i Graf_Chokolo, ne samo da nas je uznemirio, već se, također, smatra potpuno neoprostivim. Sada ste zlorabili pravosudni sustav u pokušaju cenzuriranja informacija o tome kako vaši proizvodi rade. Viktimizirali ste vlastite klijente samo zbog posjedovanja i dijeljenja informacija i nastavljate ciljati na svaku osobu koja traži te informacije. Time ste povrijedili privatnost tisuća ljudi. Ovo su informacije koje su bili spremni

[43] Cabalza, D. (2016) Ex-RCBC branch manager free on bail, https://newsinfo.inquirer.net/807690/ex-rcbc-branch-manager-free-on-bail
[44] Cabalza, D. (2016) Ex-RCBC branch manager free on bail, https://newsinfo.inquirer.net/807690/ex-rcbc-branch-manager-free-on-bail

besplatno predati svijetu. Upravo one informacije koje želite potisnuti radi korporativne pohlepe i potpune kontrole nad korisnicima. Sad ćete iskusiti gnjev Anonymousa. — Morate se suočiti s posljedicama svojih postupaka, u stilu Anonymousa. Znanje je besplatno. Anonimni smo. Mi smo Legija. Mi ne opraštamo. Ne zaboravljamo. Očekuju nas."[45]

Godine 2011. Sony je doživo sigurnosnu provalu koju je napravio samo jedan haker. Haker se infiltrirao kroz Sony PlayStation Network i dobio pristup osjetljivim podacima 77 milijuna kupaca. Podaci su uključivali korisnička imena kupaca, sigurnosna pitanja, lozinke i druge osobne podatke.

Sonyjev glavni informacijski direktor (CIO), Shinji Hasejima, izašao je u javnost kako bi rasvijetlio što je pošlo po zlu i kako je mreža bila ugrožena. Prema Sonyjevom CIO-u, Sonyjeva mreža slijedi tipični troslojni arhitekt koji uključuje web poslužitelj, poslužitelj web aplikacija i poslužitelj baze podataka. Hasejima je smatrao da je najslabija karika aplikacijski poslužitelj te da je napadač iskoristio ranjivosti pronađene na web aplikacijskom poslužitelju i da je na taj način dobio pristup poslužitelju baze podataka koji je sadržavao vrijedne osobne i korporativne podatke.[46]

Anonymousi su bili uzrujani Sonyjevim "potpuno neoprostivim" pravnim postupcima protiv PS3 jailbreakera Georgea "Geohot" Hotza. U očima Anonymousa, informacije koje je Geohot otkrio - kako pokrenuti piratske igre, kako pokrenuti homebrew softver - sada su bile u javnoj domeni, a ako ništa drugo, Hotz je Sonyju učinio uslugu razotkrivši vlastitu rupu u zakonu. Grupa je na kraju zaustavila svoje napade, prihvaćajući da samo štete Sonyjevim krajnjim korisnicima: igračima.

[45] Garcia, D. M. (2021) EntertainmentScience & Tech The 2011 PlayStation Network Hack – What Actually Happened?, https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/

[46] Ateskalabs, The Security Vulnerability That Puts Millions of Application Backends at Risk. Yours Included, https://teskalabs.com/blog/security-vulnerability-put-millions-of-application-backends-at-risk

6. Sigurnosne mjere

Sigurnosne mjere su ključne u suvremenom internetskom vremenu jer upravo navedene mjere mogu smanjiti da pojedinci, poduzeća i društva u cjelini budu žrtve hakerskih napada. Za zaštitu od računalnih virusa važno je na računalu imati instaliran pouzdan antivirusni softver, ažurirati operativni sustav i softver najnovijim sigurnosnim zaštitinim sustavima, biti oprezan pri otvaranju privitaka e-pošte ili preuzimanju datoteka s nepoznatih izvora te redovito vraćati do važnih podataka. Osim toga, prakticiranje navika sigurnog pregledavanja i vođenje računa o sumnjivim poveznicama ili web-mjestima može pomoći u sprječavanju virusnih napada.

6.1 Vrste sigurnosnih mehanizama

Od velike je važnosti ostati informirani o najnovijim prijetnjama na mreži i najboljim praksama za sigurnost na mreži.

Mjere koje se moraju primjenjivati u svrhu zaštite uključuju razne mehanizme i procese koji svojom implementacijom osiguravaju detekciju, prevenciju i mogući oporavak sustava, te servisa.

Jedna od mogućih podjela sigurnosnih mehanizama jest: fizička zaštita, zaštita ostvarena sučeljem prema korisniku, unutarni zaštitni mehanizmi i komunikacijski zaštiteni mehanizmi.

Fizička je zaštitia najosnovniji aspert. Predstavlja sigurnost opreme unutar prostorija u kojima se oni nalaze. To je bio prvi oblik zaštite informacije i podatakakoje su se nalazile na uređajima.

Zaštita ostarena sučeljem prema korisniku predstavlja jednu vrstu autorizacije. Sa Prilikom autorizacije potvrđuje se identitet korisnika. U ovim vrstama zaštite samo ovlaštene osobe imaju rpistup podacima i informacijama. Nakon ispravne autorizacije korisnik može pristupiti samom sutavu.

U svrhu osiguravanja sigurnije komunikacije i razmjenu podataka, koristi se kriptografija. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.[47]

6.2 Zaštita poslovnih subjekata

Cyber sigurnost važno je pitanje u infrastrukturi svake tvrtke i organizacije. Tvrtka ili organizacija koja se temelji na kibernetičkoj sigurnosti može postići visok status i nebrojene uspjehe jer je taj uspjeh rezultat sposobnosti tvrtke da zaštiti privatne i korisničke podatke od hakerskih napada. Tvrtka ili organizacija prije svega mora pružiti ovu sigurnost na najbolji način kako bi se uspostavila i razvila. Kibernetička sigurnost uključuje praktične mjere za zaštitu informacija, mreža i podataka od unutarnjih ili vanjskih prijetnji. Stručnjaci za kibernetičku sigurnost štite mreže, poslužitelje, intranete i računalne sustave. Kibernetička sigurnost osigurava da samo ovlaštene osobe imaju pristup tim informacijama. Za bolju zaštitu potrebno je poznavati vrste cyber sigurnosti. Slika 5 prikazuje različite vrste kibernetičke sigurnosti.[48]

[47] PMF, Klasična kriptografija, http://documents.tips/documents/informacijski-sustavi-skripta.html
[48] Aghajani G., Ghadimi N. (2018) Multi-objective energy management in a micro-grid Energy Rep., 4, str. 218-225.

Slika 5. Vrste kibernetičke sigurnosti

Izvor: Aghajani G., Ghadimi N. (2018) Multi-objective energy management in a micro-grid Energy Rep., 4, str. 218-225.

Sigurnost mreže štiti računalnu mrežu od ometača koji mogu biti zlonamjerni softver ili hakiranje. Sigurnost mreže skup je rješenja koji organizacijama omogućuje da računalne mreže drže izvan dohvata hakera, organiziranih napadača i zlonamjernog softvera.[49] Korištenje hardvera i softvera (kao što su antivirusni programi, enkripcija i vatrozidi) štiti sustav od vanjskih prijetnji koje mogu ometati razvoj aplikacija. Informacijska sigurnost štiti fizičke i digitalne podatke od neovlaštenog pristupa, otkrivanja, zlouporabe, neovlaštenih promjena i brisanja. Operativna sigurnost uključuje procese i odluke donesene za kontrolu i zaštitu podataka. Na primjer, dopuštenja korisnicima prilikom pristupa mreži ili procesima koji određuju kada i gdje se

[49] Zhao Z. i sur. (2021) Control-theory based security control of cyber–physical power system under multiple cyber-attacks within unified model framework Cogn. Robot., 1, str. 41-57

informacije mogu pohraniti ili dijeliti. Sigurnost u oblaku štiti informacije u oblaku (na temelju softvera) i prati kako bi se uklonili rizici od napada na licu mjesta.[50]

Nažalost veliki je broj podzeća koji zaštitiu svojih podatak shvaća suviše olako. Mnogi se bore sa problemom manjka resursa i adekvanih kadrova za borbu protiv ovog velikog problema. Sigurnost i zaštita se postiže jačinom i razinom obuke samih djelatnika poduzeća.

Neka poduzeća smatraju da ulaganje u informacijsku sigurnost nije potrebno sve dok potencijalni hakerski napad nema značajnost gubitak za dobrobit tvrtke. Tu je bitno dobro promotriti odluke o poslovanju, kako bi se osigurala sigurnost bez velikih gubitaka.

Obuka korisnika odnosi se na nepredvidive aspekte kibernetičke sigurnosti, odnosno pojedince. Svatko može slučajno unijeti virus u sigurnosni sustav. Poučavanje korisnika da ukloni sumnjive privitke u e-pošti, ne spajanje na anonimne USB-ove i druga kritična pitanja trebala bi biti dio korporativnog sigurnosnog plana bilo koje tvrtke.

Jako veliku ulogu u hakerskim napadima imaju korisnici. Oni nesvjesno omogućavaju pristup virusima i hakerima u podatke i uređaje. Upravo zbog toga poduzeća moraju pravilno i redovito educirati svoje zaposlenike o vrstama napada, pristupima u sustave, te ispavnim postupcima sprječavanja napada. Edukacije trebaju biti redovne, te je potrebno fokusirati njihovu pozornost na aktualne probleme u cyber prostorima.

Nužno je osigurati adekvatne radnike, te radna mjesta za stručnjake koji bi svoju pozornost i rad u poduzeću usmjerili upravo na cyber sigurnost.

6.3. Uloga korisnika u sigurnosti i načini zaštite

Uloga korisnika u samoj sigurnosti je velika. Naime, u današnje vrijeme kvaliteta usluge je ta koja osigurava prednost pred konkurencijom stoga sve vodeće kompanije poduzimaju različite mjere kako bi njihove usluge bile što pouzdanije, a samim time i kvalitetnije. Navedeno podrazumijeva

[50] Alkatheiri M.S., Chauhdary S.H., Alqarni M.A. (2021) Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications Sustain. Energy Technol. Assess., 45, Article 101219

aktivnosti kao što je primjerice nadzor sustava ili pak redovna testiranja. Aplikacije moraju biti redovno ažuriranje kako bi se eventualne greške irpacile, a njihova implementacije, odnosno njihovih novih mogućnosti, bila još kvalitetnija i pružala najbolju prednost i usluge.

Sve veća pozornost u poduzećima mora biti usmjerena na cyber sigurnost. Mnoga poduzeća ne provode dovoljnu kontrolu i zaštitu svoje digitalne sigurnosti, više od pola malih poduzeća na području Velike Britanije vjeruje da takve napade na njihovu sigurnost neće doživjeti. Napadima se gubi puno više od podataka. Napadima poduzeća gube povjerenje korisnika u poduzeće.[51]

Učestala edukacija i obrazovanje zaposlenika i kadrova o trenutnim cyber napadima i prepoznavanju prijetnji je najbolji način za prevenciju mogućih napada na sustave poduzeća.

Aktiviranje antivirusni softver koristi se za uočavanje virusa i potencijalnih napada na sustave. Poduzeća bi svojim podzetnicima trebali osigurati antivirusne sustave koji omogućavaju sigurnost u njihovom radu.

Veliku ulogu u zašititi od hakerskih iskorištavanja ima upravo redovito ažuriranje softvera. Tu se smanjuje mogučnost iskorištavanja sigurnosnih zapreki.

Kao posebno stavku potrebno staviti važnost upravo na poslovanje u različitim poduzećima koje za svoje poslovanje koriste različite aplikacije u svojim sustavima. Razvoj informacijske tehnologije donio je mnoga olakšanja za različite tipove poslova, no sam razvoj omogućio je i veću izložnost kroz poslovanje.

Pouzdane internet aplikacije su aplikacije koja prolaze različite grupe testiranja prije nego li krenu u konačnu upotrebu. Potrebno je naglasiti kako je problem i onih najsigurnijih internet aplikacija korisnik. Socijalni inženjering je ona grana znanosti koja se temelju na tezi kako je upravo čovjek, točnije njegovo ljudsko razmišljanje, najveći sigurnosni propust cjelokupnog sustava. Naime, razlog tome je vrlo jednostavan. Ljudska ograničenost, predvidljivost i subjektivno razmišljanje su ti koji ostavljaju čovjeka ranjivim na moguće manipulacije.

Svaka osoba mora biti svjesna koliko je izložena mogučim napadima koji se mogu desiti u svakom trenutku njegova korištenja internetskih aplikacija. Čovjek na taj način postaje žrtva, a

[51] VpnMentor (2022) Istražitelj Internet sigurnosti, https://hr.vpnmentor.com/blog/kako-sprijeciti-cyber-napade-vodic-za-mala-i-srednja-poduzeca/#section-4

sve infomracije mogu biti zloupotrijebljeni na mnoštvo načina čime on sam može biti na različite načine oštećen.[52]

6.3.1 Jedinstvene lozinke

Svaki korisinik mora pronaći i korisitit jedinstvene i snažne lozinke. Nužno je da se izbjegava korištenje istih lozinki za različite račune, a različitim mjestima. Poželjno je i korištenje duplih lozinki, odonosno stavljanje autentifikacijskuh pitanja, kao dadatna provjera.

6.3.2 Sigurnosne stijene

Sigurnosne stijene jedna su vrsta tehnike od napada. Sigurnosne stijene (engl. firewall) uređaji su ili aplikacije kojima se upravlja sa samim pristupom resursa računalnog sustava. Naime, resurs računalnog sustava odnosi se na cjelokupni sustav računala ili pak na samo jedno računalo unutar sustava. Radi li se o implementaciji na jedno ili više računala obje vrste rade na takav način da se prilikom njihove konfiguracije definiraju pravila pristupa računalnome resursu. Ona se mogu definirati različitim parametrima poput protokola, stanja TCP veze ili pak smjera prometa. Nakon što je konfiguracija pravilno izvršena definiraju se sve one akcije koje će se obaviti onda kada se dogodi pokušaj pristupa na računalni resurs. Akcije mogu biti primjerice dopuštanje pristupa ili pak blokiranje pristupa, obavijest admistratoru o događaju i sl. Iako sigurnosne stijene izgledaju kao vrlo moćni sustavi riječ je o sustavima koji nikada ne bi trebali biti jedina metoda zaštite računalnih sustava.[53]

Poželjno je da svaki korisnik redovnito izrađuje sigurnosne kopije važnih datoteka. Na taj način osigurava se manja šteta od mogućih napada.

6.3.3 Antivirusni sustavi

Slijedeći tip obrane su antivirusni program. Pomoću njih se identificiraju, te omogućavaju eliminiranje zlonamjerne programe. Kod svoga rada koriste dvije tehnike identifikacije, a to su

[52] Alkatheiri M.S., Chauhdary S.H., Alqarni M.A. (2021) Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications Sustain. Energy Technol. Assess., 45, Article 101219
[53] Cao J. i sur. (2021) Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548

neutralizacija i uklanjanje zloćudnih programa.[54] Instaliranje antivirusnih sustava je odlična opcija u zaštiti i stvaranju online sigurnosti. Može spriječiti gotovo sve napade na naše uređaje i podatke. Ovi sustavi mogu osigurati zaštitu i od *spam* poruka, koje u svom radu često primamo. Sustav će kroz redovne kontrole osigurati nesmetano upravljanje uređajima i jamčiti sigurnost.

6.3.4 Vatrozid

Danas, vrlo učinkovitu ulogu imaju i sustavi za otkrivanje napada. Riječ je o mogućnosti pronalaska napada u stvarnom vremenu. Ovi sustavi zaštite reagiraju na virus već prije njegovog doticaja s računalom. U online aktivnostima nesvijesno se šalje velika količina podataka. Vatrozid omogućava limitiranje podataka koji se šalju te omogućava zaštitu i spriječavanje štete. Ovaj sistem zaštite funkcionira samo u tranzitu podataka te nema zaštitnu svrhu ukoliko sam virus stigne do računala. Kroz nadziranje pronalaze se određeni uroci znakova ili okreta. Oni su indikatora nepoželjnog ponašanja u unutar infrastrukture. Pronalazak uzoraka, obavlja se pretraživanjem unaprijed, već definirane baze podataka. Ona sadrži apsolutno sve detalje o poznatim napadima pomoću kojih se lakse otkriva napad koji je u tijeku.

6.3.5 Sustavi za sprkečavanje napada

Postoje i sustavi koji su namijenjeni sprječavanju napada. To su tehnološki napredniji sustavi. Blokiranje napada provode na dva načina. Prvi od njih je mijenjanje sadržaja paketa koji je uzrokovao otkrivanje napada dok je drugi ubacivanje RST paketa unutar TCP veze kojima se provodi napad. U drugom slučaju veza se nasilno prekida te se samim time zaustavlja napad koji je u tijeku.[55]

6.3.6 VPN

VPN ili virtualna privatna mreža predstavlja kodirane poveznice između korisnika i pružatelja VPN usluge. Ovisno o VPN-u koji se koristi omogućavaju se ograničenja koja hakerima

[54] Cao J. i sur. (2021) Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548
[55] Cao J. i sur. (2021) Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548

ne dozvoljavaju pristupe podacima. Ova mreža štiti od prisluškivanja te omogućava pristup podacima koje su u nekim geografskim područjima blokirani ili limitirani.

7. Zaključak

Više od dva desetljeća internet ima značajnu ulogu u globalnoj komunikaciji i sve se više integrira u živote ljudi diljem svijeta. Inovacije i niski troškovi u ovom području značajno su povećali dostupnost, korištenje i performanse interneta, tako da internet danas ima velik broj korisnika. Internet je stvorio ogromnu globalnu mrežu koja godišnje velike količine novca. Trenutačno se većina gospodarskih, komercijalnih, kulturnih, društvenih i vladinih aktivnosti i interakcija zemalja, na svim razinama, uključujući pojedince, nevladine organizacije te institucije i poduzeća odvija u online okruženju.

Hakiranje je čin identificiranja i zatim iskorištavanja slabosti u računalnom sustavu ili mreži, obično za dobivanje neovlaštenog pristupa osobnim ili organizacijskim podacima. Hakiranje nije uvijek zlonamjerna aktivnost, ali izraz ima uglavnom negativne konotacije zbog povezanosti s kibernetičkim kriminalom. Hakeri koriste razne tehnike kako bi postigli svoje ciljeve.

Danas je hakiranje velika prijetnja kako na nacionalnoj tako i na profesionalnoj i individualnoj razini. Iako sigurnosni sustavi sve više napreduju, može se reći kako su sustavi koje koriste hakeri uvijek korak unaprijed te oni uvijek pronalaze načina kako pronaći manjkavosti sigurnosnih sustava. Na takve okolnosti nisu imune ni velike korporacije ni oni informacijski sustavi koji koriste najnovija zaštitna skredstva u smislu informacijske sigurnosti. Međutim, bez obzira na navedeno, području sigurnosti u online okruženju treba pridati veliku pažnju te je potrebno poduzeti korake koji mogu smanjiti ugroženost u online okruženju. Ljudi su najčešća meta cyber napada zbog izostanka vještina obrana. Danas je od velike važnosti očuvati fizički integritet podataka, te tajnost informacija. U poslovanju se bilježe različiti podaci koji su od velike važnosti za poduzeće. Svako poduzeće mora zaštititi te podatke, te osigurati što sigurnije poslovanje. U zaštiti osobnih, financijskih i profesionalnih podataka vrlo je bitna osviještenost pojedinaca i poslovnih subjekata o važnosti kibernetičke sigurnosti, stoga je jedna od primarnih smjernica u

očuvanju kibernetičke sigurnosti podizanje svijesti i promjena stava o zaštiti te investicija u resurse koji omogućavaju uspješnu obranu od kibernetičkih napada i smanjenje rizika od napada.

Rad je ispunio postavljene ciljeve analiziranjem najčešćih napada na informacijske sustave, Kako dolazi do napada i koju štetu mogu nanjeti ovakve vrste online ugroza također je u ovome radu istraženo. Kroz rad navode se i načini na koje se pojedinci i poslovni subjekti trebaju zaštititi, u očuvanju kontinuiteta poslovanja i zaštite privatnosti u online okruženju.

.

Literatura

1. Aghajani G., Ghadimi N. (2018) Multi-objective energy management in a micro-grid Energy Rep., 4, str. 218-225.
2. Alassouli, H. M., Common Windows, Linux and Web Server Systems Hacking Techniques, https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Common_Windows,_Linux_and_Web_Server_Systems_Hacking_Techniques.pdf 22.4.2023.
3. Alkatheiri M.S., Chauhdary S.H., Alqarni M.A. (2021) Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications Sustain. Energy Technol. Assess., 45, Article 101219
4. Antoliš, K. (2010) Internetska forenzika i cyber terorizam. Policija i sigurnost, 19(1), str. 120-127.
5. Ateskalabs, The Security Vulnerability That Puts Millions of Application Backends at Risk. Yours Included, https://teskalabs.com/blog/security-vulnerability-put-millions-of-application-backends-at-risk 22.4.2023.
6. Avast, Hacker Types: Black Hat, White Hat, and Gray Hat Hackers, https://www.avast.com/c-hacker-types 23.4.2023.
7. Baig Z.A. i sur. (2017) Future challenges for smart cities: Cyber-security and digital forensics Digit. Investig., 22, str. 3-13.
8. BasuMallick, C. (2022) What Is a Trojan Horse? Meaning, Examples, and Prevention Best Practices for 2022, https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/ 22.4.2023.
9. Black Hat. Black Hat Hacker, http://www.blackhat.com 23.4.2023.
10. Brautović, M. (2007) Zaštita privatnosti kod hrvatskih online medija. Medianali – znanstveni časopis za medije, novinarstvo, masovno komuniciranje, odnose s javnostima i kulturu društva, 1(1), str. 20- 31.
11. Cabalza, D. (2016) Ex-RCBC branch manager free on bail, https://newsinfo.inquirer.net/807690/ex-rcbc-branch-manager-free-on-bail 21.4.2023.
12. Cao J. i sur. (2021) Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks Inform. Sci., 548, str. 69-84.

13. Dcham, J. (2016) Congresswoman wants probe of ‘brazen’ $81M theft from New York Fed, https://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/ 23.4.2023.
14. Difference between Virus, Worm and Trojan Horse, https://www.geeksforgeeks.org/difference-between-virus-worm-and-trojan-horse/ 23.4.2023.
15. CIS (2012) Ispitivanje sigunosti web servera, http://www.cis.hr/files/dokumenti/CIS-DOC-2012-02-040.pdf 10.4.2023.
16. Everett, C. (2016) Ransomware: To pay or not to pay?, Comp. Fraud & Secur., 4, str. 8–12.
17. FDIC, Guidance on How Financial Institutions Can Protect Against Pharming Attacks, https://www.fdic.gov/news/financial-institution-letters/2005/fil6405.pdf 10.4.2023.
18. FER, Preljev spremnika, http://sigurnost.zemris.fer.hr/ns/malware/2007_klaric/buffer_overflow.html 23.4.2023.
19. Garcia, D. M. (2021) EntertainmentScience & Tech The 2011 PlayStation Network Hack – What Actually Happened?, https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/ 11.4.2023.
20. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017) Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), str. 3629-3654.
21. Iwugo, D. (2022) What are White Hat, Black Hat, and Red Hat Hackers? Different Types of Hacking Explained, https://www.freecodecamp.org/news/white-hat-black-hat-red-hat-hackers/ 19.4.2023.
22. Jovanović, N. (2003) Računarske mreže. Viša poslovna škola, https://www.researchgate.net/profile/Nenad-Jovanovic-4/publication/323538579_Racunarske_mreze/links/5a9ac56ca6fdcc3cbacb3d2a/Racunarske-mreze.pdf 23.4.2023.
23. Kaspersky, Black hat, White hat, and Gray hat hackers – Definition and Explanation, https://www.kaspersky.com/resource-center/definitions/hacker-hat-types 20.4.2023.

24. Martins, A. (2023) Cyberattacks and Your Small Business: A Primer for Cybersecurity, https://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html 20.4.2023.
25. Microsoft Security Bulletin MS17-010 – Critical, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 20.4.2023.
26. Motsch W. i sur. (2020) Approach for dynamic price-based demand side management in cyber-physical production systems Procedia Manuf., 51, str. 1748-1754.
27. PMF, Klasična kriptografija, http://documents.tips/documents/informacijski-sustavi-skripta.html 03.07.2023.
28. Robinson M., Jones K., Janicke H. (2015) Cyber warfare: Issues and challenges Comput. Secur., 49, str. 70-94.
29. ROUSE, M. Script Kiddy, http://searchmidmarketsecurity.techtarget.com/definition/script-kiddy 20.4.2023.
30. SBIT STTR, Introduction to cyberthearts, https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial2.pdf 23.4.2023.
31. Sokolov, M. (2022) Five years of WannaCry: what has changed in ransomware since 2017?, https://insights.cybcube.com/en/five-years-of-wannacry-ransomware?hs_amp=true&utm_term=&utm_campaign=FY22_Q4_+Brand+Awareness+/+Performance+Max+(EMEA)&utm_source=adwords&utm_medium=ppc&hsa_acc=1114695891&hsa_cam=18997862872&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=CjwKCAjwzuqgBhAcEiwAdj5dRr3piSzGcuRYTMzhvBD-RGw5Y7K81hU98rYsjJOZozoRDEp07tR1aBoCBwQQAvD_BwE
32. Solomon R. (2017) Electronic protests: Hacktivism as a form of protest in Uganda Comput. Law Secur. Rev., 33 (5), str. 718-728.
33. Sudar–Kulčar, M. (2006) Zaštita privatnosti i sigurnosti pohranjenih podataka s osvrtom na izravni marketing. Politička misao, 2(4), str. 89-99.
34. Techtarget, https://www.techtarget.com/searchsecurity/definition/spyware 10.06.2023
35. Telekomunikacija I računalne mreže, http://www.unizd.hr/portals/1/primjena_rac/brodostrojarstvo/predavanje_5.pdf 19.4.2023

36. Toth, T. (2000) Od hostova do web-servera: jesu li nam informacije dostupnije danas nego jučer? U: Upravljanje informacijama u gospodarstvu i znanosti : zbornik radova = Information management in industry and science : proceedings / [Konferencija] CROinfo 2000, Dubrovnik, 16.- 18. X. 2000. ; [organizatori = organizers Nacionalna i sveučilišna knjižnica, Zagreb [i] PLIVA] ISBN 953600089X / Stipanov, Josip - Zagreb : Nacionalna i sveučilišna knjižnica, str. 160-173.
37. Uomtemp, Spyware, http://uomtemp.uom.ac.mu/CITS/images/tips/spyware/Spyware.pdf 19.4.2023.
38. Quigley K., Burns C., Stallard K. (2015) 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection Gov. Inf. Q., 32 (2), str. 108-117.
39. What you need to know about the WannaCry ransomware,, https://www.symantec.com/blogs/threat-intelligence/wannacryransomware-attack 19.4.2023.
40. Zhao Z. i sur. (2021) Control-theory based security control of cyber–physical power system under multiple cyber attacks within unified model framework Cogn. Robot., 1, str. 41-57.

Popis slika