SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

ZAVRŠNI RAD

SIGURNOST PODATAKA NA INTERNETU

Mentor: dr. sc. Željko Garača

Student: Andrea Okmažić

Split, srpanj 2019.

SADRŽAJ

1. UVOD

Pojava Interneta kao elektroničkog medija je označila ogromnu promjenu u načinu života. Do tad, život je u mnogočemu bio kompliciraniji - nije bilo online komunikacije, e-bankarstva, lake dostupnosti svih podataka, ali život je bio mnogo 'sigurniji' (navodni znakovi u ovom kontekstu označavaju zaštitu osobnih podataka, ne opću sigurnost). Mnogo teže se dolazilo do osobnih podataka, lokacije, pa nije trebalo voditi računa o sigurnosti u mjeri u kojoj se to danas mora raditi. Jedan od glavnih problema današnjice je upravo ta dostupnost podataka, posebice onih koje sami korisnik ne želi dijeliti, ili pak nije svjestan da su dostupni. Imajući to na umu, globalizacija i pojava Interneta se gledaju dvojako, sa svojim brojnim pozitivnim i negativnim stranama.

S tim u svezi, u ovom radu istražit će se i iznijeti činjenično stanje i pregledati određena istraživanja koja će ukazati na ljudsku svijest o sigurnosti podataka, ali i načine i izvore kojim se može doći do nečijih podataka, kao i zakonske okvire koje se mora poštovati da bi se poslovalo s nečijim podatcima.

Obzirom na to da je pravo na privatnost jedno od temeljnih ljudskih prava koje je zajamčeno Ustavom, potrebno je u svakom trenutku osigurati korisniku privatnost i ne kršiti ga, ali i s pozicije korisnika utvrditi kako s pozicije korisnika zaštititi svoje pravo uz nepromijenjeno, ispravno korištenje mogućnosti koje svijet Interneta pruža. To se postiže obostranom edukacijom u području informatičkog obrazovanja s naglaskom na mlađim generacijama koje su nositelji budućnosti i tehnologije kao glavnog stupa te budućnosti, čime se otvaraju vrata napretku u toj sferi.

U uvodu će se također dati i kratak pregled onoga što će biti tema ovog rada.

U drugom poglavlju analizira se cyber-sigurnost, uključujući : statistike o napadima na sigurnost u svijetu, vrstama napadača, kanalima i sredstvima napada kao i načinima prepoznavanja napada.

U trećem poglavlju analizira se djelovanje hardverskih i softverskih rješenja na sigurnost, pri čemu će se analizirati učinkovitost i djelovanje alata zaštite sigurnosti dostupnih širim masama kao i objasniti kako korisnik savjesnim djelovanjem može zaštititi sigurnost vlastitih podataka, kao i uređaja.

Četvrto poglavlje donosi analizu zaštite privatnosti, analizirajući definiciju osobnog podatka, vrste napada na privatnost osobnih podataka, načine zaštite privatnosti, kao i pravne

okvire unutar Hrvatske kao članice Europske unije. Na kraju poglavlja se predstavlja jedan od mnogobrojnih primjera napada na korisničku privatnost te kako se incident riješio.

Zaključak donosi finalna razmatranja o temi privatnosti i sigurnosti podataka.

2. SIGURNOST UREĐAJA

2.1. OSNOVNE POSTAVKE CYBER-SIGURNOSTI

Cyber-sigurnost označava zaštitu uređaja, procesa. infrastrukture i organizacijskih komponenti od neovlaštenog pristupa, krađe podataka, cyber-napada, ucjene i sl.[1] Rastom i razvojem tehnologije i povećanjem međuovisnosti organizacijskih sustava, učinkovit sustav zaštite sigurnosti postaje nužan korak za sve tipove i veličine organizacija. Stoga su i ulaganja proporcionalna, te se očekuje porast investicija u područje cyber-sigurnosti na 170 milijardi američkih dolara do 2020. godine.[2] Potražnja za stručnjacima u tom području je sve veća, te se istovremeno i potiče obrazovanje i dodatna izobrazba u spomenutom polju. Uz kvalitetna, visokotehnološka rješenja, potrebna je i ljudska svijest o zaštiti sigurnosti, bez koje sama fizička rješenja nemaju snagu.

Cyber-sigurnost nije jednoznačna i sa sobom obuhvaća više tipova sigurnosti. Ti tipovi su :

- aplikacijska sigurnost
- informacijska sigurnost
- oporavak u slučaju štete
- mrežna sigurnost
- zaštita web-stranica
- zaštita krajnjih točaka

Zaštita aplikacijske sigurnosti se odnosi na mjere i poteze kojima bi se rješavale opasnosti i prijetnje pri samim početcima razvoja aplikacija, kao što su dizajn aplikacija, razvoj, održavanje, nadogradnja i sl. Neke tehnike su provjera valjanosti ulaznih parametara, upravljanje sesijama, autentifikacija i autorizacija korisnika itd.

Informacijska sigurnost se odnosi na zaštitu informacija i podataka od krađe, neovlaštenog pristupa, kršenja pravila o upravljanju podatcima da bi se zaštitio identitet korisnika i očuvala privatnost.

[1] Different Types of Cyber Security, 2018. https://www.youthkiawaaz.com/2018/07/different-types-of-cyber-security/ (13.7.2019.)
[2] ibid

Oporavak u slučaju štete podrazumijeva planiranje i stratešku organizaciju koja bi omogućila organizacijama da se nastavi poslovanje i minimizira šteta u slučaju neke vrste cyber-napada. Uključuje procjenu rizika, analitiku, postavljanje prioriteta i uspostavljanje odgovora na napad kao i mehanizama za oporavak.

Zaštita mrežne sigurnosti se odnosi na kombinaciju hardverskih i softverskih rješenja kojima bi se onemogućila eksploatacija i neovlašteni pristup podatcima interne mreže organizacije. Tu spadaju antivirusni i anti-spyware softveri, VPN, IPS, vatrozid i slične tehnologije koje se koriste da bi se osigurala sigurna, pouzdana i uporabljiva interna mreža.

Web sigurnost se odnosi na zaštitu web stranica od cyber-napada. Obuhvaća baze podataka web stranica, aplikacije, izvorne kodove i dokumente. U današnje vrijeme napad na zaštitu web sigurnosti je u konstantnom porastu te je potrebno posebnu pažnju obratiti upravo na to područje, čemu je uzrok općeprihvaćeno mišljenje javnosti da je web stranica zaštićena od svog davatelja usluga. Kao posljedicu takvog (pogrešnog) mišljenja bilježi se stalan porast krađe identiteta, financijskih gubitaka, rušenja stranica i/ili dugog vremena čekanja na odgovor te na koncu gubitak kredibiliteta same web stranice. Neke od metoda zaštite sigurnosti web stranica su real-time skeniranje web stranica i uklanjanje malwarea, mrežni vatrozid, testiranje aplikacijske sigurnosti itd.

Sigurnost krajnjih točaka (eng. Endpoint security) se odnosi na zaštitu samih servera, terminala i mobilnih uređaja od lokalnih napada, kao i onih na daljinu. Uređaji na mreži su povezani te su samim tim i podložni prijetnjama i napadima. Djelovanje ove vrste cyber-sigurnosti se ogleda u tom da sprječava pokušaje pristupa ka navedenim uređajima i mjestima, na način da se konstantno i sistematično prati integritet datoteka, uz korištenje antivirusnog i anti-malware softvera kao najprepoznatijih metoda.

2.2. CYBER-SIGURNOST U SVIJETU - SADAŠNJOST I BUDUĆNOST

Napadi na Internetu i prijevare su nažalost postali učestala, svakodnevna stvar. Statistički podatci iz 2018. kažu da se napad hakera događa svakih 39 sekundi, zahvaćajući u prosjeku trećinu Amerikanaca svake godine.[3] Nisu svi napadi u cilju financijskog profita - o

[3] 12 Alarming Cyber Security Facts and Stats, 16.3.2018. https://www.cybintsolutions.com/cyber-security-facts-stats/ (20.9.2018.)

tom govori podatak da gotovo polovina svih hakerskih napada su napadi na mala poduzeća, s tim da se 95% svih podataka odnosi na podatke iz oblasti politike, tehnologije i maloprodaje[4].

Posljedica krađe podataka je prosječan trošak u iznosu od 150 milijuna dolara[5], kao rezultat sve veće povezanosti poslovne infrastrukture. U zdravstvu je 75% sustava bilo zaraženo malwareom[6] kao i 1 od 131 primljenog e-maila[7], što je ogroman postotak i ogroman udarac na sigurnost podataka. Čak 3/4 aplikacija je palo na običnom testu sigurnosti jer nije imalo pravu enkripciju podataka[8], a iako je 77% korisnika smatralo da je mobilna tehnologija ključ budućnosti, samo polovina te brojke je znala kako se pravilno zaštititi od napasti[9]. Radi svih ovih podataka, tekućih i budućih, je mnogo novca predodređeno upravo za zaštitu sigurnosti u Internet svijetu te se predviđa da će se u 5 godina (u periodu između 2017. i 2021.) izdvojiti 1 trilijun dolara radi svjetske zaštite sigurnosti[10]. S obzirom na to da se predviđa da će do 2020. biti preko 200 milijardi spojenih uređaja, i da prosječan američki građanin ima bar 4 uređaja s internetskom vezom[11], nude se i poslovi povezani s internetskom sigurnosti te se otvara čak 3.5 milijuna slobodnih radnih mjesta u tom području[12]. Ta mjesta zahtijevaju iznimno obrazovane, sposobne i inovativne stručnjake koji će biti korak ispred hakera.

2.3. KANALI NAPADA

Napadi na Internetu se mogu odnositi na tri područja invazije na sigurnost : napad na podatke (npr. brojevi kartica, potvrde pristupa, zapisnik aktivnosti), napad na identitet (krađa identiteta u svrhu lažnog predstavljanja) i napad na uređaj (sprječavanje normalnog funkcioniranja uređaja kao rezultat napada na uređaj).

Napadi se događaju putem više kanala. Kanali napada su :

---

[4] ibid
[5] ibid
[6] ibid
[7] Mason, John. Cyber Security Statistics, 27.2.2018. https://thebestvpn.com/cyber-security-statistics-2018/ (20.9.2018.)
[8] Six Shocking Facts About Enterprise Mobile Security And How to Avoid Them,14.10.2015. https://www.infragistics.com/community/blogs/b/mobileman/posts/six-shocking-facts-about-enterprise-mobile-security-and-how-to-avoid-them (20.9.2018.)
[9] ibid
[10] 12 Alarming Cyber Security Facts and Stats, ibid
[11] ibid
[12] Cyber Security Statistics, ibid

- komunikacijski kanali (SMS-om, MMS-om, e-mailom)
- komunikacijske mreže (GSM, Wi-Fi, Bluetooth)
- softverske aplikacije (web browseri, operativni sustavi)
- hardverski propusti (rootanje uređaja, USB kabel, slušalice)

Komunikacijskim kanalima se napadi događaju privitcima putem MMS ili mail poruka kao i DDoS napadima putem SMS-a[13]. Komunikacijskim mrežama napad se odvija hakiranjem algoritama GSM mreže, kao i korisničkih imena i lozinki raznih Wi-Fi mreža čime se presreće promet i tako prikupljaju podatci. Također, još jedan od načina je korištenje Bluetooth mreže za slanje inficiranih datoteka[14].

Hardver i softver kao temelji računala, kako mobilnih tako i ostalih, podložni su napadima na sigurnost privatnosti korisničkih podataka ali jednako tako i napadom na samo računalo i njegove performanse. Napadom putem softverskih aplikacija se nagomilavaju podatci u memoriju adrese i kreiraju se važeći potpisi iz nevažećih čime se krade identitet korisnika i njegovi podatci koriste za razne nedopuštene aktivnosti kojih korisnik nije svjestan[15]. Hardverski propust je vidljiv putem hakerskih napada u sistem uređaja, pa se uređaj roota te se instaliraju aplikacije koje se pokreću u pozadini i potajno kradu podatke. Isto tako, jedna od neočitih i 'novijih' verzija krađe podataka je instaliranje malwarea na adapterima uređaja za punjenja, na javnim mjestima i slično, kao i upravljanje uređajem i podatcima radiofrekvencijama preko slušalica[16]. Korisnik te opasnosti nije svjestan jer u ogromnom postotku slučajeva korisnik nije ni upoznat s ovim načinom krađe podataka, a dodatna oprema je svakodnevno korištena i naprosto očekivanja krađe podataka na takav način su gotovo nepostojeća.

2.4. TIPOVI NAPADAČA NA SIGURNOST

Hakiranje podataka nije nužno loša aktivnost, iako sa sobom nosi negativnu konotaciju. Hakiranje može biti i dobar čin, ako je usmjeren na otkrivanje nekog od gore prikazanih propusta i kanala napada. Stoga među hakerima prepoznajemo 'white hat' hakere,

[13] Gladshyev, Pavel i Rodgers, Marcus K. : Digital Forensics and Cyber Crime, 2011, str. 40/41
[14] ibid, str. 41, 46
[15] ibid, str. 42
[16] Greenberg, Andy. Great. Now Even Headphones Can Spy On You, 22.11.2016.https://www.wired.com/2016/11/great-now-even-headphones-can-spy/ (20.9.2018.)

koji su upravo usmjereni na tu aktivnost[17]. Koriste ih uglavnom firme, koje su dužne čuvati podatke klijenata i zaposlenika. Na suprotnom kraju spektra imamo 'black hat' hakere, kojima je cilj napad i krađa podataka i identiteta u maliciozne svrhe[18]. Između te dvije krajnosti nalaze se 'grey hat' hakeri, koji su unajmljeni, povremeno ruše zakone i krše pravila da bi otkrili propuste ali za razliku od 'white hat' hakera koji će objasniti nadređenima kako propust zakrpati, te će, ne čekajući ponudu treće strane za popravak, ponuditi popravak uz zaračunatu naknadu[19]. Samim tim su na granici legalnog i ilegalnog, zakona i ilegale. 'Blue hat' hakeri su savjetničke kuće koje su unajmljene s ciljem da testiraju sistem prije njegovog puštanja u prodaju, pronalazeći sigurnosne 'rupe'. Primjer je Microsoft[20] koji koristi takav tip stručnjaka za provjeru svog operativnog sustava Windows.

Hakiranje ne moraju nužno otkrivati zarad firmi i njihovih klijenata. Često Vlada i vojska 'upadaju' u sigurnost i vrše invaziju na podatke, posebice u slučaju sumnji na ilegalno i štetno djelovanje pojedinca ili grupe. Ponekad se to praćenje odnosi na praćenje čak i običnih građana. Time se nameće pitanje etičnosti, ako je u pitanju skriveno praćenje običnih građana, kojima je Ustavom zajamčeno pravo na privatnost, čak i ako je u pitanju praćenje građana radi očuvanja njihove sigurnosti.

2.5. VRSTE ZLONAMJERNIH SOFTVERA

Načini krađe podataka, odnosno konkretna sredstva kojima se hakeri služe su razne verzije štetnih softvera koji mogu kompromitirati računalne funkcije, izvršiti krađu podataka, presresti kontrolu uređaja i dopuštenja kao i ugroziti računalo na druge načine. Takve štetne softvere nazivamo malware (skraćeno od eng. malicious software). Vrste takvih softvera navedeni su u nastavku[21] :

[17] Hoffman, Chris. Hacker Hat Colors Explained : Black Hats, White Hats and Grey Hats, 20.4.2018. https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/ (20.9.2018.)
[18] ibid
[19] What is the Difference Between Black, White and Grey Hat Hackers? https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (20.9.2018.)
[20] Who Are Blue Hat Hackers. https://medium.com/@hackersleague/who-are-blue-hat-hackers-aeb443b90c29 (20.9.2018.)
[21] DuPaul , Neil. Common Malware Types : Cybersecurity 101, 12.10.2012. https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101 (20.9.2018.)

- Adware (Advertising-supported software) : tip štetnog softvera koji bez želje korisnika predstavlja razne reklame. Tipičan primjer su pop-up reklame ili reklame u softverskih alata koji se ugrađuju u 'free' verziju. Oni sami po sebi stvaraju korisničko nezadovoljstvo jer su neželjeni, no osim toga ne nose štetu u sebi izuzevši ako u sebi imaju ugrađenog spywarea (o njemu više u nastavku) koji prati korisničku aktivnost i preuzima informacije koje korisnik svjesno ili nesvjesno pruža
- Bot : softverski programi koji su kreirani da automatski pokreću određene aktivnosti. Mnogi dođu ugrađeni bez ikakvih štetnih namjera (na primjer ugrađuju se u video-igrice, koriste ih i 'blue hat' hakeri za testiranje operativnih sustava), ali u porastu je korištenje botova u štetne aktivnosti (neki od primjera su već spomenuti DDoS napad, dijeljenje malwarea preko download linkova, spamovi reklamama na web stranicama itd.) Iz tog razloga koristi se CAPTCHA test, kojim se potvrđuje da je korisnik ljudsko biće te njegovo djelovanje nije automatizirano
- Bug : greška koja je napravljena s ciljem nepravilnog djelovanja programa. Najčešće su rezultat ljudske pogreške pri programiranju. U blažim slučajevima program samo ne radi kako je potrebno. Nadalje, u težim situacijama program se ruši ili se dogodi 'smrzavanje ekrana'. U najtežim situacijama bug je smišljen s ciljem krađe podataka i pristupa, tako da haker presretne korisnikovu autorizaciju i koristi ju za štetna djelovanja
- Ransomware : tip štetnog softvera koji ucjenjuje korisnika. Na računalo dospijeva putem zaražene datoteke, a prenosi se kao obični računalni (o njima više u nastavku). Potom ograniči korisniku pristup računalu te ga ucjenjuje da plati određenu sumu novca, da bi zauzvrat ponovo dobio ovlasti nad svojim računalom
- Rootkit : daljinski upravlja računalom bez korisničkog znanja. Preuzima na sebe udaljeno upravljanje datotekama, pristup/krađu podataka, modificiranje sistemskih postavki te instaliranje štetnih softvera. Kako je teško pronaći ovaj tip malwarea, potrebno je voditi veliku brigu o ažuriranju antivirusnih programa, preuzimanju programa s valjanim potpisom, popravcima softvera i operativnih sustava i čestom i detaljnom pretraživanju sustava
- Spyware : 'špijun' koji prati korisničko djelovanje u vidu praćenja aktivnosti, praćenja unosa (keyloggeri kao podvrsta spywarea koji prati koje tipke je korisnik pritisnuo pri autorizaciji i tako otkriva šifre dokumenata, osobnih računa i PIN brojeve kartica).

Njegovo djelovanje se širi putem propusta u softveru, tako što se instalacijom legitimnog programa prenese na računalo ili se udruži s trojanskim konjem

- Trojanski konj : najpodmukliji tip štetnog programa 'prerušen' u običnu datoteku s ciljem prevare korisnika i instalacije na računalo. Njegovom instalacijom osoba koja ga je programirala dobiva dopuštenje za apsolutni nadzor nad korisničkim podatcima, unosom, instalacijom i računalom u potpunosti
- Virus : tip štetnog softvera sposoban da se sam replicira i širi na računalo, ali i s jednog na druga računala. Prenosi se inficiranim datotekama i pokretanjem takvih, pokreće se lančana reakcija replikacije. Njegovo djelovanje je nalik na djela prethodnih tipova, odnosno krađa informacija, kreiranje botova, 'spammanje' reklamama i štetno djelovanje na računalima na koja se replicira
- Računalni crv (eng. Worm) : među najčešćim tipom zlonamjernog softvera, širi se računalnom mrežom preko propusta u operativnim sistemima. Djeluju tako da preopterećuju web servere, a kako nose dio štetnog koda na sva povezana računala mrežom raspršuju kod koji napada podatke, briše datoteke i kreira botove na svim računalima. Po tom djelovanju nalik su na viruse, ali ih razlikuje to što se virusi šire ljudskom aktivnosti (pokrećući program), dok se crvi šire automatizirano. Često se nalaze u privitcima e-maila, koji se šalju i korisnikovim kontaktima.

2.6. KAKO PREPOZNATI NAPAD NA SIGURNOST I POSLJEDICE KOJE NAPAD NOSI

Opisani načini i objekti napada su često neminovni, no kao i svaka šteta, što se prije prepozna, veće su šanse za oporavak i spašavanje korisničkih podataka i zaštite sigurnosti. Neki od pokazatelja štetnih aktivnosti su[22] :

- preopterećenje centralne jedinice
- spora internetska veza i/ili računalo
- poteškoće pri spajanju na mrežu
- 'smrzavanje' i rušenje sustava
- modificiranje i brisanje datoteka

[22] Rijnetu, Ioana. 13 Warning Signs That Your Computer is Malware Infected., 18.12.2017. https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/ (20.9.2018.)

- pojava nepoznatih datoteka i programa (onih za koje korisnik zna da ih nije svojevoljno prebacio na računalo)
- nepravilan rad programa (paljenje/gašenje bez ljudske aktivnosti, rekonfiguracija)
- neovlašteno slanje e-maila (bez korisnikovog znanja)

3. DJELOVANJE HARDVERSKIH I SOFTVERSKIH RJEŠENJA ZAŠTITE SIGURNOSTI

3.1. DJELOVANJE ALATA ZAŠTITE SIGURNOSTI

3.1.1. HTTPS PROTOKOL

Protokol definiramo kao skup pravila koja koristimo za neku specifičnu namjenu, u konkretnom primjeru riječ je o komunikacijskom protokolu[23]. Za krajnje korisnike, neprepoznatljivija su dva internetska protokola – HTTP i HTTPS.

HTTP (eng. Hypertext transfer protocol) označava protokol kojim se neka riječ, rečenica ili poruka prenosi putem browsera (koji ju prevodi). Kako računalo funkcionira na princip nula i jedinica, upravo na taj način se prevodi neka riječ/rečenica/poruka, da bi ju računalo shvatilo i nama prikazalo rezultat.

HTTPS (eng. Hypertext transfer protocol secure) je sigurna verzija HTTP protokola, gdje postoji enkripcija između browsera i web stranice, koja omogućuje privatnost pretrage. Posebice je to korisno pri korištenju online bankinga, kupovine putem Interneta i sl., gdje se privatni podatci korisnika izlažu potencijalnom napadu i neovlaštenom pristupu. Enkripcija podataka se obavlja na dva načina – 128-bitnom ili 64-bitnom enkripcijom. Prva, naprednija verzija, je vrlo teška za dekripciju te u slučaju posrednika koji želi iščitati podatke koji se šalju, posrednik dobiva niz besmislenih (kriptiranih) podataka koje ne može uporabiti, jer mu je ključ za dešifriranje nepoznat.

Ono gdje leži prednost korištenja HTTPS pored HTTP protokola je stoga vrlo jasna – pri korištenju HTTPS protokola postoji enkripcija podataka gdje, čak i u slučaju neovlaštenog

[23] Easy Understanding of Web Protocols – HTTP and HTTPS. https://www.izooto.com/blog/understanding-http-https-protocols (13.7.2019.)

pristupa treće osobe, je teško (gotovo nemoguće) iščitati poruku koja je poslana između web stranice i browsera. Samim time, korisnički podatci, kao i njegova privatnost, su sačuvani.

Zadaća protokola je sljedeća : nakon što korisnik upiše URL stranice, protokol pronalazi IP adresu servera koji je zadužen za domenu tražene web stranice te prikuplja tražene podatke i prikazuje ih u browseru korisničkog računala. Potom se očekuje konkretizacija korisničkog zahtjeva (na primjeru domene 'google.com', u browseru će pisati 'google.com/s=', što označava zahtjev servera za konkretizacijom upita). Nakon korisnikovog unošenja konkretnog zahtjeva, ovisno o korištenju HTTP ili HTTPS protokola, u svojoj čistoj ili enkriptiranoj formi se zahtjev šalje na obradu serveru, koji po obradi server vraća protokolom kao rezultat pretrage[24].

Uz korištenje HTTPS protokola, nadovezuje se i uporaba SSL certifikata (eng. koje stranica nosi sa sobom i povezuje domenu sa imenom i lokacijom organizacije. Osigurava sigurnu sesiju između browsera i servera. Kad je certifikat uspješno instaliran na server, tad HTTP prelazi u HTTPS protokol[25].

Dvije su verzije valjanih SSL certifikata[26] :

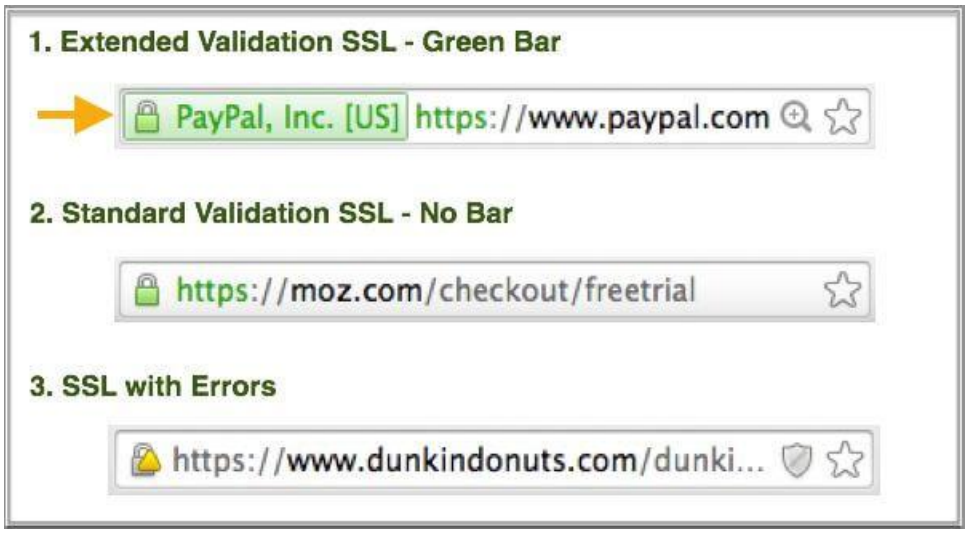
1. Extended Validation (EV) SSL certifikat : prepoznatljiv je po zelenoj adresnoj traci (ili po zelenom pravokutniku sa lokotom unutar adresne trake) koji označava da je certifikat aktivan i da je sigurna veza putem HTTPS protokola uspostavljena. Tvrtka/organizacija koja koristi EV SSL certifikat je jasno označena na adresnoj traci i samo putem korištenja ove verzije SSL certifikata je osigurano da je njeno ime jasno prikazano. Primjeri nekih od tvrtki/organizacija koje koriste ovaj certifikat su DigiCert, Inc. [US], Comodo Security Solutions, Inc. [US] i PayPal Inc. [US].

2. Standard SSL certifikat : prepoznatljiv po zelenom lokotu, adresna traka je bijele boje

SSL certifikat može biti i s greškama, što se prepoznaje po sivom lokotu i žutom trokutiću ispred njega. Najčešći uzrok je da je sadržaj stranice omogućen i preko HTTP i preko HTTPS protokola. Da bi se omogućila potpuna enkripcija i samim time ojačala sigurnost pri korištenju stranice, potrebno je prevesti sadržaj koji je dotad bio omogućen

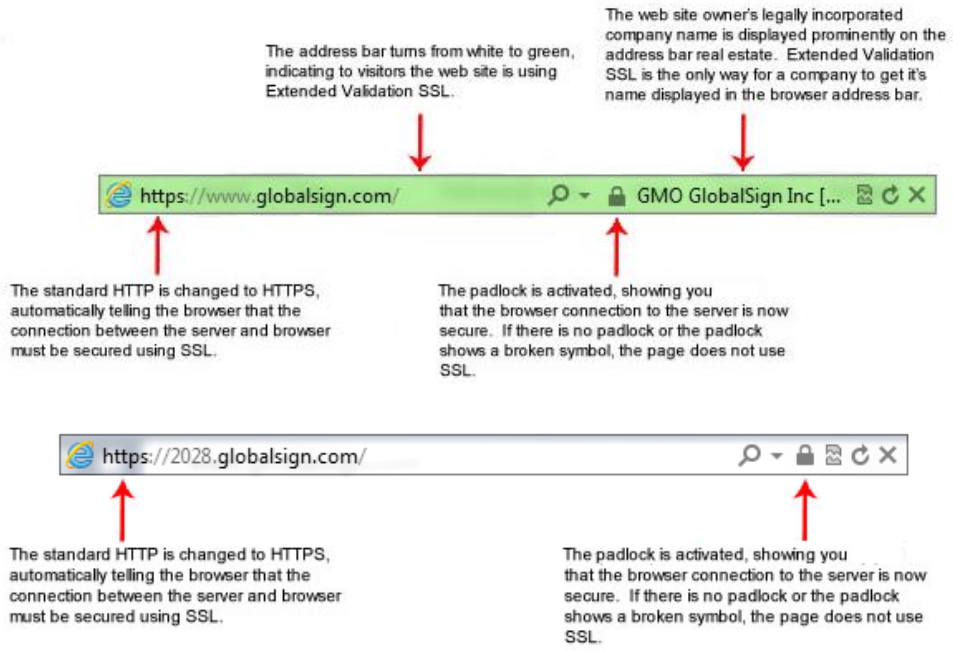
[24] ibid
[25] ibid
[26] What is an SSL certificate? https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/ (13.7.2019.)

preko HTTP protokola, na onaj koji se prenosi preko HTTPS protokola. Ponekad to nije moguće i sadržaj se tad ne može ispravno prikazati. Stranica se može u cijelosti resetirati, ali to bi zahtijevalo ponovnu izradu stranice, stoga je ponekad najjednostavnije rješenje ostati pri mješovitim protokolima.



Slika 1. Prikaz vrsta SSL certifikata

Izvor : https://www.izooto.com/blog/understanding-http-https-protocols



Slika 2. i 3. Prikazi adresnih traka web stranica koje koriste EV SSL certifikat (Slika 2) i SV SSL certifikat (Slika 3)

Izvor : https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/

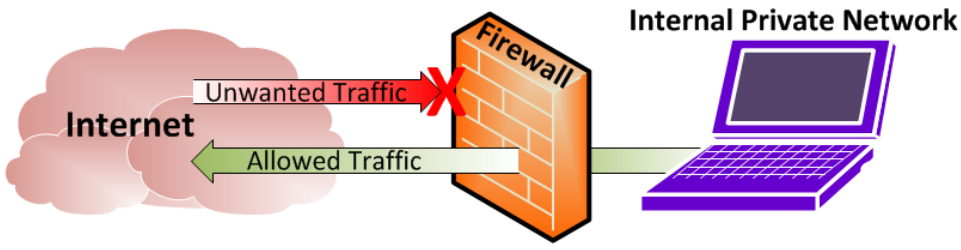
Neki od manjih nedostatka korištenja HTTPS protokola u odnosu na HTTP protokol su dulje vrijeme procesiranja traženih podataka, kao i više hardverskog kapaciteta što sa sobom nosi dodatne troškove. Kao što je vidljivo, u odnosu na prednosti koje HTTPS protokol nudi, nedostatci su zanemarivi i korisnik ne bi trebao imati nedoumica pri donošenju odluke koji protokol koristiti.

3.1.2. VATROZID

Vatrozid (eng. Firewall) je mrežni sigurnosni uređaj koji prati dolazni i odlazni promet i po potrebi blokira podatkovne pakete ukoliko su prijetnja sigurnosti računala.

Način na koji vatrozid djeluje je da filtrira dolazni i odlazni podatkovni promet koji dolazi sa sumnjivih i/ili nesigurnih izvora i ima u cilju prevenciju napada. Svoju funkciju obavlja na ulaznim točkama (eng. port), odakle prati razmjenu informacija između IP adresa servera i domaćina (eng. host).

Vatrozid može biti softversko ili hardversko rješenje, iako se preporučuje uporaba oba. Softverski se instalira na računalo i prati podatkovni promet preko portova i aplikacija, dok se fizički (hardverski) vatrozid instalira kao dio opreme između mrežnog pristupnika i same mreže i često sa sobom nosi i neke dodatne mogućnosti (kao npr. VPN mreža, anti-virus, cloud management i sl.)



Slika 4. Djelovanje vatrozida

Izvor : https://www.tunnelsup.com/what-is-a-firewall/

Pet je vrsta vatrozida[27] :

- paketno-filtrirajući vatrozidi (eng. Packet-filtering firewalls)
- vatrozidi nove generacije (eng. Next-generation firewalls, NGFW)
- proxy vatrozidi (eng. Application-level gateways)
- vatrozid uspostavljen putem poveznika (eng. Circuit-level gateway)
- vatrozidi višerazinske provjere (eng. Stateful multilayer inspection, SMLI)

Najstariji, tradicionalni tip vatrozida je paketno-filtrirajući tip, koji proučava izvor i IP adresu podatkovnog paketa. Ukoliko je na odobrenoj, 'allowed' listi, paketu se omogućava prijenos. U suprotnom, njegov prijenos se blokira. Može biti 'stateful' i 'stateless' vrste. 'Stateless' vrsta proučava pakete nezavisno jedan od drugog i ne povezujući s prethodnim rezultatom ispitivanja, pa je laka meta za hakere. Nasuprot njemu, 'stateful', pametnija verzija pamti prethodno proučene pakete i mnogo je sigurniji za korištenje. Osnovni nedostatak paketno-filtrirajućeg tipa vatrozida je što je previše ograničene zaštite – npr. ne može procijeniti hoće li sadržaj zahtjeva koji je poslan imati utjecaj na računalo na koje je poslan (jer štetan zahtjev sa 'allowed' liste izvora može imati itekako poguban utjecaj na računalo i rezultirati primjerice gubitkom podataka, a ovaj tip vatrozida ga ne može prepoznati). Stoga su druge verzije vatrozida preporučljivije za korištenje.

Vatrozidi nove generacije kombiniraju tradicionalnu tehnologiju s dodatnim funkcionalnostima, kao što je npr. anti-virus, sustav prevencije upada, provjera enkriptiranog prometa i sl. Karakterizira ga detaljna provjera paketa (eng. Deep packet inspection, DPI), koja uključuje ne samo provjeru IP adrese I izvora, već i provjeru podataka unutar paketa, kojim se lako identificira, kategorizira ili blokira prijenos podataka štetnog sadržaja.

Proxy vatrozidi filtriraju mrežni promet na aplikacijskoj razini, tako što djeluju kao posrednici između dva krajnja komunikacijska kanala. Klijent šalje zahtjev vatrozidu, gdje ga vatrozid evaluira putem niza sigurnosnih pravila i tad biva odobren ili blokiran. Proxy vatrozidi djeluju i na HTTP i FTP protokolima, te uključuje 'stateful' način provjere, kao i detaljnu provjeru paketa, čime čini kombinaciju prva dva tipa vatrozida.

Idući tip vatrozida je tip 'Circuit level gateway-ja' koji omogućuje većem broju uređaja koji imaju nezavisne mrežne adrese da se povežu na Internet koristeći jednu IP

[27] The Different Types of Firewall Architecture, 18.5.2018. https://www.compuquip.com/blog/the-different-types-of-firewall-architectures (13.7.2019.)

adresu, čuvajući njihove individualne IP adrese skrivenima. Kao rezultat toga, napadači skenirajući mrežnu IP adresu ne mogu otkriti detalje svakog uređaja zasebno, čime je osigurana veća zaštita od napada. Po principu rada slični su proxy tipu vatrozida, jer djeluju kao posrednik između grupe računala i vanjskog prometa.

Posljednji tip je vatrozid višerazinske provjere, koji filtrira pakete na mrežnoj, transportnoj i aplikacijskoj razini, uspoređujući ga sa pouzdanim paketima. Kao i vatrozidi nove generacije provjeravaju čitav paket i dopuštaju mu prolaz samo u slučaju da je svaka razina zadovoljila sigurnosne kriterije. Ovaj tip vatrozida putem provjere paketa određuje stanje komunikacije i osigurava da se komunikacija održava samo sa pouzdanim izvorima. Nedostatak je da usporava prijenos podataka i zauzima mnogo računalnih resursa, ali prednost je da omogućava veliku razinu zaštite.

3.1.3. ANTI-MALWARE PROGRAM

Anti-malware program je tip softvera koji je razvijen u svrhu skeniranja, identifikacije i uklanjanja štetnog programa (eng. malware) sa računala ili računalne mreže. Osigurava zaštitu sustava od različitih verzija štetnih programa (virusa, računalnih crva, ransomwarea, rootkita, spywarea, keyloggers i sl.)[28]. Može biti uspostavljen na korisničkom računalu, na poslužitelju ili na mrežni pristupnik (router). Učinkovit anti-malware program je višeslojan, te tako omogućava potpunu sigurnost pri korištenju računala.

Najčešći način na koji anti-malware program funkcionira je da pretražuje datoteke uspoređujući identificirane štetne potpise (koje anti-malware ima spremljene u svojoj bazi prepoznatih prijetnji) i ukoliko prepozna takav potpis u nekoj datoteci na računalu (ili u paketu pri mrežnom prijenosu), označava je kao prijetnju[29]. Većina anti-malware programa djeluje upravo na ovakav princip, jer je jednostavan i učinkovit. Stoga je potrebno redovno ažurirati bazu potpisa, kako bi se osiguralo pravovremeno prepoznavanje štetnih datoteka i programa.

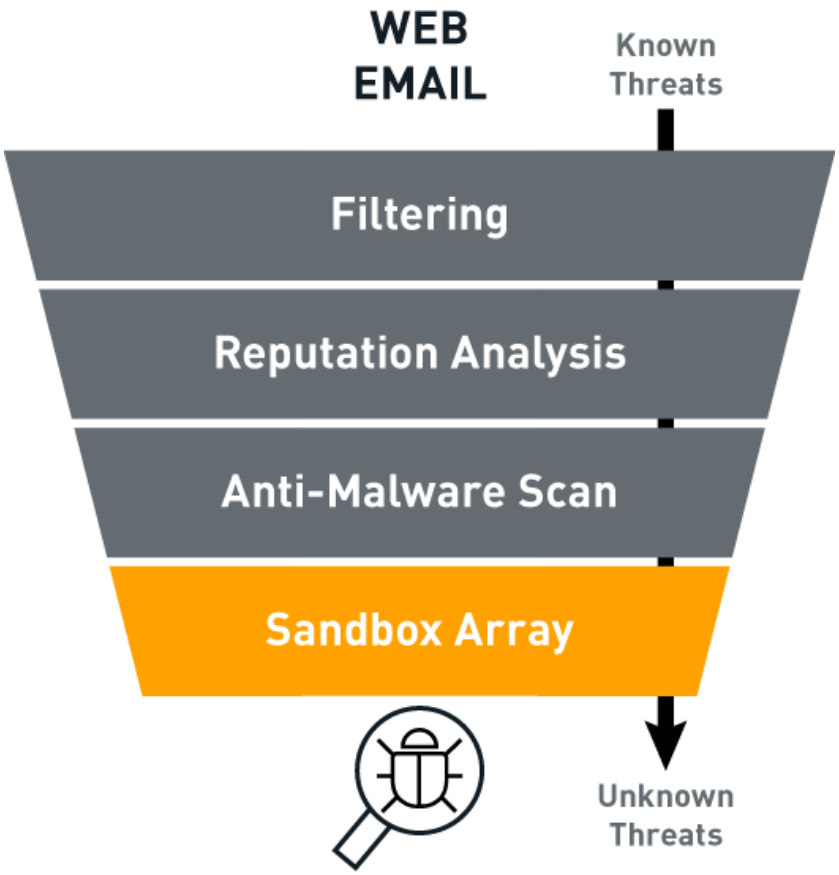
Heuristika (eng. Heuristics) je iduća metoda koja je implementirana u većini anti-malware programa, a služi da prepozna štetnu datoteku ne po principu uspoređivanja s bazom, već provodeći na njoj niz bihevioralno-analitičkih radnji prepoznaje potencijalno

[28] vidi poglavlje 2.5.
[29] What is Antimalware? 2.8.2018. https://enterprise.comodo.com/blog/what-is-antimalware/ (13.7.2019.)

štetno djelovanje koje datoteka može imati na računalo[30]. Jedan od primjera je da datoteka (ili program) u sebi sadrži kod kojim bi se omogućilo brisanje bitnih i osjetljivih sistemskih datoteka, u kojem slučaju bi anti-malware program tu datoteku (ili program) označio kao štetnu. Međutim, nerijetko se dogodi da se ponekad legitimni programi proglase štetnim, kao i da se neke datoteke i programi proglase lažno pozitivnim, čime ova metoda ne spada u sami vrh pouzdanosti.

Hibridna metoda, poznata kao Sandboxing, je metoda kojom se prepoznaju i poznate i (dotad) nepoznate prijetnje. Djeluje na način da ukoliko se neka datoteka proglasi štetnom, miče se u izolirani prostor (karantenu), gdje se na njoj vrši niz postupaka kojima se utvrđuje je li uistinu štetna za samo računalo. Ukoliko se datoteka uistinu pokaže štetnom, anti-malware program je uklanja s računala, čime se ne utječe na korisnikovo iskustvo na računalu, a računalne operacije se izvode neometano[31].

[30] ibid
[31] ibid



Slika 5. Sandboxing princip pretrage sumnjivih datoteka

Izvor : https://www.cyren.com/products/cloud-sandboxing

Potrebno je naglasiti da anti-virusni program nije isto što i anti-malware program. Anti-virusni program se bavi virusima, dok se anti-malware program bavi sa svim skupinama zlonamjernih softvera (uključujući i viruse). Stoga je potrebno obratiti pažnju pri instaliranju da, ukoliko se instalira anti-virusni program, da se osigura da uz njega i anti-malware zaštita u vidu nekog drugog programa[32]. Danas su uglavnom anti-malware programom obuhvaćeni i anti-virusni programi, pa iako se preporučuje imati minimalno dva anti-malware programa, mora se osigurati da samo jedan radi konstantno, u pozadini, a da se drugi po potrebi koristi za dodatnu provjeru. Razlog leži u tome da istovremeno korištenje dva ili više anti-malware programa može prouzročiti usporen rad na računalu, kao i nepravovremeno prepoznavanje

[32] One or Two Anti-Malware? Spector, Lincoln. 25.2.2010. https://www.pcworld.com/article/189245/1_or_2_AV.html (13.7.2019.)

prijetnje radi međusobne ‘borbe za prvenstvo’ anti-malware programa pri čemu se može nepovratno naštetiti računalu.

3.2. KAKO KORISNIK SVOJIM UTJECAJEM MOŽE OSIGURATI ZAŠTITU SIGURNOSTI?

Računalo kao fizičko mjesto gdje korisnik pristupa Internetu i predaje svoje podatke, mora se čuvati jednako kao i sami podatci pri sklapanju virtualnih ugovora, online komunikacije, bankovnih transakcija i tako dalje. Sigurnost korisnikovih podataka i očuvanje identiteta je, kao što je prethodno spomenuto, aktivnost koja zahtjeva ljudsku svijest ali i korištenje tehnoloških rješenja. Korisnik treba imati razvijenu svijest o opasnostima koje vrebaju te, kao i u slučaju zaštite podataka, ne dijeliti osobne podatke ako nije nužno, a koristiti enkripciju za zaštitu onih koje dijeli. Jedna od metoda zaštite je gašenje svih funkcija na računalima koje se ne koriste (Bluetooth, Wi-Fi, podatkovni promet, GPS lokacija) i nekorištenje javnih mreža (posebice se to koristi na nezaštićene, javne Wi-Fi mreže čiji pristup ne zahtijeva lozinku)[33]. Lozinke za pristup korisnicima, kao i za Wi-Fi mrežu, potrebno je periodično mijenjati[34]. Još jedna od metoda je korištenje HTTPS protokola, verzije HTTP protokola s dodatnom sigurnosti, kad god je to moguće. Korisnik treba na računalo instalirati i pokrenuti anti-malware program i vatrozid. Vatrozid je mrežni sigurnosni sistem koji prati i kontrolira mrežni promet kao zaštita od neovlaštenog upada putem internetske mreže. Vatrozid najčešće dolazi ugrađen u operativnom sistemu (iako, ovisno o vrsti vatrozida, to ne mora biti isključivo), a anti-malware program je najčešće potrebno instalirati. Pritom treba paziti da instalirani program dolazi od ovlaštenog izvora, s valjanim certifikatom. Neki od primjera su Avast, AVG, Nod32 i sl. Softvere treba redovito ažurirati, također s ovlaštenih mjesta jer se svakim novim ažuriranjem povećava antivirusna baza i rješavaju problemi pronađeni u prethodnim verzijama. Tako se računalo može izboriti s novokreiranim vrstama malwarea, koji su sve podmukliji i teže prepoznatljivi od ranijih verzija.

[33] 10 Ways To Protect Your Android Phone, 28.3.2018. https://blog.malwarebytes.com/101/2018/03/10-ways-to-protect-your-android-phone/ (20.9.2018.)
[34] 10 Ways to Prevent Cyber Attacks. https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/ (13.7.2019.)

4. ZAŠTITA PRIVATNOSTI

4.1. VRSTE ZAŠTITE PRIVATNOSTI

Dijeljenjem svojih podataka na različitim profilima društvenih mreža, korištenjem internet usluga ili pak jednostavnim klikovima po stranicama bilježe se korisnički podatci i skladište u bazi podataka koju posjeduje upravo ta društvena mreža/stranica koja se koristi. Način napada na podatke može biti cyber-kriminal (krađa podataka koje korisnik ne pristaje dijeliti (nedopuštenim pristupom, širenjem virusa, pranjem novca, krađom identiteta)), ali i ne mora biti. Korisnik nedovoljnim poznavanjem informatičke pismenosti i pravila pri dijeljenju podataka može prepustiti podatke na korištenje osobama kojima su ponekad ti podatci relevantni (npr. cookies - 'kolačići' koji pamte posjećene stranice i mogu korisniku predložiti stranice prema njegovim interesima) a ponekad im ti podatci ne služe poboljšanju korisničkog iskustva, no ipak ih skladište što je vid nenasilnog ali ne i bezazlenog prikupljanja podataka o korisniku.

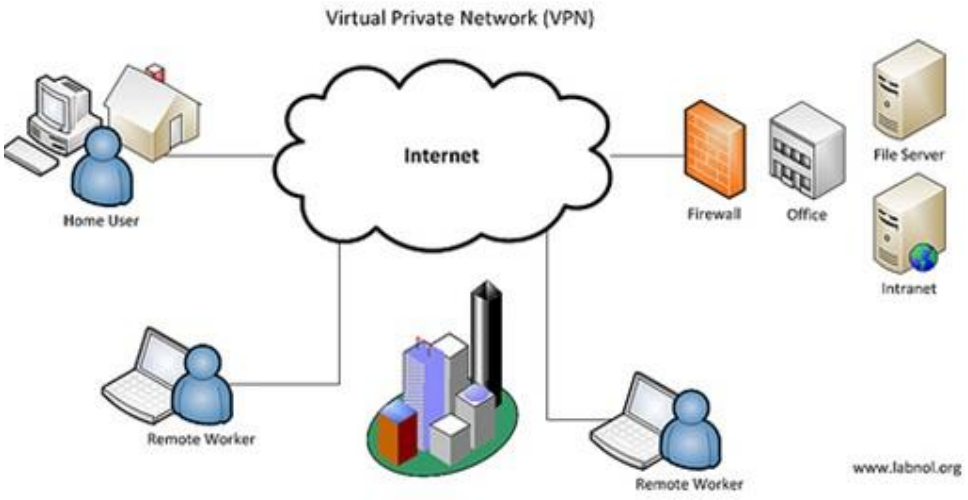
Potonji način se najčešće i najuspješnije rješava obrazovanjem u području informacijske sigurnosti i edukacijom o informatičkoj pismenosti, a prvi je vrlo ozbiljan problem i uz veliku svijest korisnika, potrebno je koristiti i mnoge računalne alate o kojima će biti više riječi kasnije.

Prema jednom istraživanju provedenom u Sjedinjenim Američkim državama čak 80% mladih korisnika Interneta smatra da je svjesno opasnosti i rizika na Internetu. Isti postotak ispitanika smatra da je sposobno nositi se s tim[35]. To upućuje na preveliko samopouzdanje korisnika koji, kao što se utvrdilo, u najvećoj mjeri koriste internetske usluge jer opasnosti se ne smanjuju a štete su iz dana u dan sve veće. Posebice su djeca ta koja su u opasnosti od krađe identiteta, slika i privatnih podataka te su izložena ogromnom postotku neprikladnih sadržaja, te su roditelji ti koji bi trebali pomno pratiti aktivnosti svoje djece i pobrinuti se za to da iskoriste sve mogućnosti koje Internet pruža. Jedna od tih je i 'roditeljski nadzor' : opcija kojom se automatski filtriraju i miču stranice i sadržaji koje dijete ne smije gledati te se surfanje Internetom podiže na veću razinu sigurnosti. Roditelji moraju educirati kako sebe, tako i djecu i poučiti ih sigurnom i ispravnom korištenju mogućnosti koje Internet pruža.

[35] Justament, D. : Zaštita privatnosti na internetu (2017.)

4.2. OPCIJE ZAŠTITE PRIVATNOSTI

Opcije zaštite su da se korisnik osloni na sebe, na tehnološka rješenja ili, najučinkovitije, na oboje. Korisnik se sam može zaštititi pomnim praćenjem kome dijeli osobne podatke putem Interneta (najboljom opcijom se smatra apsolutno nedijeljenje podataka) no ako je to nemoguće, podatke poput adrese stanovanja, podataka bankovnih računa, osobnih identifikacijskih brojeva bi bilo pametnije zadržati za sebe ili ih šifrirati tako da samo primatelj zna točnu informaciju te, ako netko presretne poruku, da ne može na jednostavan način dešifrirati ili ukrasti podatak. Neželjenu i poštu sumnjivih ili nepoznatih pošiljatelja ne bi trebalo otvarati niti na nju odgovarati. 'Kolačići' sami po sebi nisu nužno loša stvar, no korisnik bi trebao proučiti koje 'kolačiće' preglednik prima i postaviti preglednik da svaki put korisnika obavijesti o kolačićima. Jedna od najmodernijih i najboljih metoda je korištenje VPN mreže, kako bi se osigurala potpuna anonimnost. VPN mreža (eng. Virtual private network) predstavlja privatnu mrežu unutar javne, te omogućava korisnicima te mreže dijeljenje podataka sigurno, bez dijeljenja istih ostalim korisnicima mreže[36]. VPN tehnologija koristi enkripciju podataka, virtualne tunele kojim 'paketi' podataka putuju te mrežu samo onih korisnika koji podatke šalju/primaju.



Slika 6. Prikaz VPN mreže

Izvor : https://tweakyourbiz.com/technology/the-different-pros-and-cons-of-using-a-virtual-private-network-vpn

[36] What is a VPN? Virtual Private Network. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html (20.9.2018.)

Na slici je prikaz jedne VPN mreže, koja je predstavljena 'oblakom' Interneta koji povezuje različita računala, pri čemu mogu koristiti IP adresu druge države i pristupati stranicama koje možda imaju nametnutu državnu restrikciju. Ona se plaća po maloj mjesečnoj rati, a sami pružatelj usluga može brinuti o konfiguraciji i administraciji VPN mreže (ako korisnik VPN mrežu preuzme od davatelja usluga a ne odabere self-monitoring (samostalno praćenje))[37]. Postoje i negativne strane VPN mreže (potencijalno se može smanjiti brzina mreže, problemi s povezivanjem na wireless mrežu i 'ovisnost' o pružatelju usluga i njegovoj ažurnosti pri monitoringu i ažuriranju VPN mreže), no one su malobrojne i manje štete u odnosu na koristi.

Zaštita tehnološkim rješenjima se odnosi na zaštitu identiteta 'slijepim potpisom' i biometrijskim šifriranjem. 'Slijepi potpis' je produkt Davida Chauma, a odnosi se na elektronički ekvivalent vlastoručnog potpisa kojim se osigurava anonimnost pošiljatelja[38]. Biometrijsko šifriranje je danas široko rasprostranjeno, a odnosi se na tehnologiju skeniranja otiska prsta ili zjenice. Potonje još ima neke mane i u razvoju je, no otisak prsta se u moderno nalazi na mnogim mobilnim uređajima čime se štiti i uređaj, kao i podatci na samom uređaju.

4.3. PRAVNI ASPEKTI ZAŠTITE PRIVATNOSTI

"Osobni podatak je svaka informacija koja se odnosi na identificirani fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu : ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet."[39]

Obradom podataka smatra se radnja ili skup radnji nad osobnim podatcima. U to spadaju prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, brisanje itd.[40] Voditelj zbirke osobnih podataka je ovlaštena osoba koja u skladu sa zakonom mora djelovati nad tim podatcima, ne u osobne svrhe i isključivo u skladu s korisnikovim

[37] Scheck, Steven.The Different Pros and Cons of Using a Virtual Private Network (VPN), 25.7.2017.. https://tweakyourbiz.com/technology/the-different-pros-and-cons-of-using-a-virtual-private-network-vpn (20.9.2018.)
[38] Chaum, David. Advances in Cryptology,1984. https://link.springer.com/book/10.1007/978-1-4684-4730-9 (20.9.2018.)
[39] Zakon o zaštiti osobnih podataka, NN 106/12, čl.2, točka 1
[40] ibid, točka 2

dopuštenjima za njihovo korištenje. Ključna riječ je 'dopuštenje', koje korisnik daje onda kad je upoznat sa svrhom u koju se njegovi podatci koriste te kad je ta svrha nedvojbeno i jasno izražena, najčešće u pisanom obliku[41]. Uz suglasnost obje strane (korisnika i voditelja), korisnički podatci se mogu prikupljati u npr. znanstveno-istraživačke, marketinške svrhe, u svrhu zaštite voditelja zbirke osobnih podataka, zaštite života ispitanika ili druge osobe i sl. [42] Podatci koje korisnik daje moraju biti točni, ažurirani i potpuni[43], a izvršitelj je dužan korisnika pravovremeno (odnosno prije korisnikovog ustupanja podataka) informirati ga o svrsi u koju daje podatke, njegovih prava za izmjenom i brisanjem podataka, primateljima podataka i radi li se o obveznom ili dobrovoljnom davanju podataka[44]. Nadalje, izvršitelj se mora obvezati na čuvanje tajnosti podataka, dostavljanju podataka samo osobi koja te podatke i treba, te da se podatci uredno i organizirano preuzmu od korisnika[45]. Voditelj je obvezan imati pravni temelj za prikupljanje i korištenje osobnih podataka te točno određenu vrstu podataka koju će koristiti za naznačenu namjenu i smiju se koristiti samo u vremenu u kojem je nužno za ostvarenje svrhe[46]. Agencija za zaštitu osobnih podataka vodi zbirke podataka koje izvještavaju voditelji te su iste zbirke javno dostupne na njenim web stranicama[47].

4.4. KORISNIČKA PRAVA ZA ZAŠTITU PODATAKA

4.4.1. PRAVA KORISNIKA DO 25.05.2018.

Prema Zakonu o zaštiti osobnih podataka, svaki korisnik ima pravo na uvid u podatke koji su o njemu preuzeti i dostavljeni za evidenciju. Prema imenovanom zakonu koji je vrijedio do 25.5.2018., svaki korisnik je mogao dobiti potvrdu koriste li se njegovi podatci za obradu ili ne, koji su izvori prikupljenih podataka, evidencija u zbirku osobnih podataka, potvrdu pravnog temelja prikupljanja, obrade i korištenja podataka, ime osobe zadužene za

[41] ibid, točka 8
[42] ibid, čl. 8
[43] ibid, čl. 6
[44] ibid, čl. 9
[45] ibid, čl. 10
[46] ibid, čl. 11
[47] ibid, čl. 17

korištenje podataka po pravnim temeljima te obavijest o logici automatske obrade podataka koja se koristi za podatke korisnika[48].

Isto tako, korisnik ima pravo usprotiviti se obradi osobnih podataka u svrhe marketinga i u tom slučaju voditelj zbirke osobnih podataka ne smije koristiti korisnikove podatke za tu svrhu[49].

U slučaju kršenja korisničkih prava, korisnik se može žaliti Agenciji za zaštitu osobnih podataka, koja odgovara Hrvatskom saboru. Žalba drugog stupnja nije dopuštena ali se može pokrenuti upravni spor[50]. Ako Agencija pri provjeri zaključi da se krše korisnička prava, može novčano kazniti izvršitelja obrade i/ili voditelja zbirke osobnih podataka u iznosu od 20 000 do 40 000 HRK[51].

4.4.2. PRAVA KORISNIKA UVOĐENJEM GDPR REGULACIJE

Prava korisnika na zaštitu privatnosti osobnih podataka su od 25.5.2018. podignuta na novi nivo stupanjem na snagu 'Opće uredbe o zaštiti podataka'. Popularnije znan kao GDPR (eng. General Data Protection Regulation), donesena je direktiva od strane Europske unije za ujednačeno mijenjanje pravila za ophođenje s korisničkim podatcima. Neke od stavki tog zakona donose se u nastavku[52] :

1. Veliki i među stanovnicima najprepoznatiji pomak se dogodio u području kažnjavanja za voditelje obrade podataka koji bi za nestručno ophođenje s podatcima stanovnika EU mogli platiti čak 20 milijuna eura (ili 5% ukupnog godišnjeg prometa na svjetskoj razini), što ih je prisililo na čvrsti ustroj kvalitetnih mjera zaštite podataka. Podatci se kriptiraju (posebice oni osjetljivi) i čuvaju uz visoku razinu sigurnosti, dok se oni manje bitni smiju čuvati uz nižu razinu sigurnosti. Ono što dijeli rizične od manje rizičnih podataka je koliku štetu njihovo otkrivanje ima po korisnika - ako bi korisnik mogao pretrpjeti zdravstvene teškoće, gubitak društvenog ugleda, imovine ili čak smrt, tad se ti podatci smatraju visokorizičnima.

[48] ibid, čl. 19
[49] ibid, čl. 21
[50] ibid, čl. 25
[51] ibid, čl. 36
[52] Načini zaštite podataka u GDPR-u. 24.1.2018. https://gdprinformer.com/hr/gdpr-clanci/nacini-zastite-podataka-u-gdpr-u (20.8.2018.)

2. Podatci nižeg rizika se ne kriptiraju, no postoji više verzija prikrivanja identiteta korisnika. Za podatke srednjeg i višeg rizika koristi se pseudonimizacija, koju bi se moglo definirati kao 'postupak 'čišćenja' osobnih podataka tako da se pojedinac ne može identificirati iz skupa podataka'. Kako ti podatci nisu anonimni, ali ne sadrže posebna obilježja, za identificiranje pojedinaca potrebni su vanjski podatci. Ovaj primjer podataka je i dalje koristan poglavito pri istraživanjima i marketinškim aktivnostima. U slučaju povrede podataka tvrtka ne mora obavijestiti one kojima je privatnost podataka narušena jer, u suštini, nije. Pseudonimizacijom ni sama tvrtka ne zna čiji su podatci uzeti pa ni napadač ni ona ne mogu identificirati osobu, no svakako je potrebno zaštititi druge, vanjske izvore odakle bi se moglo doći do identificiranja.
3. Pristup podatcima se ograničava na one kojima je prijeko potrebno, a broj tih osoba sveden je na minimum. Zaposlenicima koji rukuju takvim podatcima potrebno je pružati što učestalije edukacije za ispravno ophođenje s tim podatcima (minimalno na godišnjoj razini), dok se politike ophođenja zaštitom podataka trebaju ispitivati bar dva puta godišnje.
4. S tim u svezi, kontrola pristupa za sve koji se bave podatcima treba imati neki vid autorizacije (PIN-ovi koji se mijenjaju redovno, kartice, biometrijski otisci...) i trebaju sadržavati minimalno dva koraka.
5. Redovno se rade sigurnosne kopije podataka kako bi se u slučaju uništenja originalnih podataka omogućilo neometano poslovanje, s tim da se i u ovom dijelu vodi računa o razini sigurnosti i vrsti enkripcije kao i o mjestu pohrane.
6. Kao i sa svim, treba uz opasnost neispravnog ponašanja ljudskog faktora obratiti pažnju i na računalo, pa je potrebno provoditi redovno ažuriranje antivirusnog softvera kao i operativnog sustava. Preporučuje se i korištenje kriptografskih protokola. Ne smiju se koristiti vanjske jedinice za pohranu podataka poput CD-ova, DVD-ova, USB-ova i slično. Pri uništavanju podataka fizički uništiti medij (posebice kod visokorizičnih podataka) je ponekad najbolja opcija, dok se za nisko rizične skupine podataka može koristiti jednostavno brisanje. Oboje bi se trebalo odvijati na lokaciji voditelja obrade podataka.

U Hrvatskoj je dotadašnja Opća uredba o zaštiti podataka stavljena izvan uporabe, a na snagu je stupio Zakon o provedbi Opće uredbe o zaštiti podataka koju je donio Europski parlament i Vijeće. Ona je dovedena s ciljem ispunjavanja Uredbe EU o 'zaštiti pojedinca u

vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka'[53]. Agencija za zaštitu osobnih podataka je nadležno, neovisno, državno tijelo i obavlja poslove iz članka 6., kao što su sudjelovanje u kažnjavanju neovlaštenog ophođenja s podatcima, određivanja visine naknade, prati primjenu Direktive EU itd.

Novotarije koje donosi ovaj zakon je da je obrada podataka zakonita ako osoba ima iznad navršenih 16 godina[54]. Obrada biometrijskih podataka je nužna ako je za zaštitu pojedinca i isključivo mora biti u skladu sa zakonom[55], dok je obrada genetskih podataka zabranjena radi izračuna izgleda bolesti i drugih zdravstvenih stanja ispitanika da bi se sklopio ugovor o životnom osiguranju i čak ni uz privolu korisnika, dozvola nije legalna[56]. Video-nadzor je dopušten za zaštitu imovine i/ili pojedinca, na uvid se daje samo ovlaštenim osobama i ne smije biti za privatne potrebe (bez privole i znanja korisnika). Videosnimke se čuvaju najviše šest mjeseci[57].

Mjere koje donosi GDPR su mjere koje smanjuju troškove, osiguravaju zaštitu bitnih podataka i povećavaju korisnikovo povjerenje. Jedini problem koji je upitan dolazi pri klasificiranju razine rizičnosti podataka gdje je potrebno angažiranje usluge educiranih stručnjaka ako se takav ne nalazi u poduzeću što iznosi privremeni trošak ali dugoročno se isplati.

4.5. SUVREMENI PRIMJER NAPADA NA SIGURNOST PODATAKA NA PRIMJERU FACEBOOK-A

Kroz povijest se protežu razni primjeri kršenja privatnosti (jedan od razvikanijih je bio Wikileaks 2010. godine kad je američki politički vrh priznao curenje vrlo povjerljivih priopćenja kojim su ugroženi i obični građani koji rade za njih)[58]. Nažalost, od tog nemilog događaja, izuzevši uhićenja odgovornih nije napravljeno mnogo napretka u području zaštite podataka. Pravila se nisu mnogo promijenila. Ono što je posebno uzdrmalo javnost je nešto što koriste i odrasli, ali i djeca, a to su društvene mreže te je skandal s podatcima na

[53] Zakon o provedbi Opće uredbe o zaštiti podataka, NN 42/18, čl. 1
[54] ibid, čl. 19
[55] ibid, čl. 21
[56] ibid, čl. 20
[57] ibid, čl. 29
[58] Evans, Jeffrey. Top 5 Privacy Violations of 2010. https://www.huffingtonpost.com/jeffrey-evans/top-5-privacy-violations-_b_802615.html?guccounter=1 (20.8.2018.)

Facebooku doveo u svijest koje sve podatke korisnici 'ispuštaju' putem a o nama se skladište, kao i koje sve podatke korisnik ne želi dati na uvid, ali se o njemu prikupljaju.

Povijest s rušenjem privatnosti seže od 2005. godine (Facebook je osnovan 2003. godine). Jedan od novijih je iz 2013. godine gdje je greška unutar aplikacije prouzrokovala da pri prebacivanju dokumenta o korisnikovoj povijesti aktivnosti na internetu, korisnik ne dobije samo svoje podatke, već i osobne informacije (e-mail adrese, brojeve mobitela itd.) od svojih prijatelja, čak i od onih koji nisu te informacije vidljivo objavili. Način na koji je Facebook te informacije dobio je primjer velike ugroze privatnosti - on je prikupio te podatke iz liste kontakata trećih osoba, 'prijatelja' korisnikovih 'prijatelja' [59].

Informacije i količinu istih koje je Cambridge Analytica, britanska konzultantska firma koja se bavi analizom podataka u kombinaciji sa strateškom komunikacijom tijekom političkih izbora, uspjela prikupiti je nešto što je obilježilo Facebook u 2018. godini. Cambridge Analytica se godinama bavi prikupljanjem informacija o profilu korisnika, njegovom ponašanju, osobnosti i tako modificiraju političko mišljenje i sudjeluju u kampanjama pri izborima. Putem jednostavnog kviza osobnosti su prikupili karakteristike korisnika OCEAN modelom osobnosti (akronim za otvorenost, svijest, ekstrovertnost, sposobnost prihvaćanja i neurotičnost)[60]. Samim prihvaćanjem i povezivanjem tog testa sa svojim Facebook računom došli su u posjed imena i prezimena, svih informacija na profilu, proteklih objava te svih prijatelja s kojima je korisnik povezan na toj društvenoj mreži. Ono gdje nastaje problem je činjenica da Cambridge Analytica nije kreator kviza - kreator je Alexandr Kogan, psiholog i analitičar podataka, koji je prepustio prikupljene podatke Cambridge Analytici, bez znanja i dopuštenja korisnika. Jedna od zanimljivosti je njegovo posjedovanje privatnih poruka korisnika na Facebook platformi. Kao objašnjenje nudio je razlog da 'prati korištenje emojia', ali negira da je privatne poruke predao na uvid Analytici[61]. S obzirom na to da se Cambridge Analytica sličnim aktivnostima bavi od 2015., došli su u posjed privatnih podataka od 87 milijuna korisnika Facebook platforme. Sve ovo je otkriveno u ožujku 2018., kad je novinar na tajnom zadatku otkrio malverzacije pri mijenjanju

[59] Newcomb. Alyssa. A timeline of Facebook's privacy issues – and their responses, 2018. https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651 (20.8.2018.)

[60] Grassegger, Hannes i Krogerus, Mikael. The Data That Turned The World Upside Down, 2017. https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (20.8.2018.)

[61] Hern, Axel i Cadwalladr, Carol. Revealed : Alexandr Kogan collected Facebook users' direct messages., 13.4.2018. https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages (20.8.2018.)

političkog mišljenja u zemljama u razvoju[62], u isto vrijeme kad je otkriven problem s Facebook privatnosti. Isto tako, korisnici koji su se ulogirali preko Android uređaja su primijetili da je Facebook prikupio podatke o njihovim pozivima i porukama. Radi svega ovog Facebook platforma je pretrpjela pad na tržišnoj vrijednosti dionica, istragu i promjenu postavki privatnosti.

U travnju 2018. otkriveno je tko stoji iza tih prljavih radnji te su u roku 14 dana promijenjena Pravila o privatnosti pa je u skladu s GDPR zakonom stanovnicima Europske unije poslan zahtjev za revizijom podataka koje dijele te promjenom dopuštenja koja daju (npr. žele li dati dopuštenje za predlaganje stranica na temelju njihovih 'likeova')[63]. Isto tako mogu u svakom trenutku prebaciti na računalo dokument koji im prikazuje koje sve podatke Facebook ima o njima. Time je situacija glede privatnost stišana, no nije u potpunosti razriješena i dug je put pred osnivačem Markom Zuckerbergom da se iskupi za ovaj sigurnosni propust.

5. ZAKLJUČAK

Značaj sigurnosti i privatnosti korisničkih podataka nije potrebno naglašavati. Očuvanje privatnosti omogućava neometano obavljanje svih potrebnih zadaća koje korisnik ima, pa tako i surfanje bespućem Interneta uz istovremeno osiguravanje onog što mu se jamči Ustavom.

Tehničke aspekte zaštite potrebno je prepustiti stručnjacima, koji se svakodnevno bore s poteškoćama kojima žrtve budu prosječni korisnici Interneta. Visoke kriterije koje društvo samo po sebi nameće iz dana u dan informatički stručnjaci dosežu i nadmašuju, stoga je potrebno usmjeriti svu pažnju, ali i resurse, u razvoj tehničko-tehnoloških aspekata našeg društva. Ponajprije se to odnosi na obrazovanje i dodatna usavršavanja u svijetu informatike i tehnologije, potom na financijske izvore kojim će se poticati istraživanja i obrazovanja stručnjaka, te naposljetku implementacija istog u školama

[62] Ingram, David. Factbox : Who is Cambridge Analytica and what did it do?, 20.3.2018. https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F (20.8.2018.)

[63] Egan, Erin. Complying with new privacy laws and offering new privacy protections for everyone, no matter where you live, 17.4.2018. https://newsroom.fb.com/news/2018/04/new-privacy-protections/ (20.8.2018.)

počevši od najmlađih generacija kojima je informatičko obrazovanje ključ za njihovu budućnost.

Potrebno je naglasiti da je ljudski faktor pogreške u sigurnosnim aspektima uglavnom velik i da ga je moguće izbjeći, a sve uz edukaciju i ispravnu implementaciju sigurnosnih pravila kojima će se proširiti svijest o rizicima, a isti će se svesti na minimum.

LITERATURA

Knjige:

1. Garača, Ž. (2007.), *Informatičke tehnologije*. Drugo dopunjeno izdanje. Sveučilište u Splitu, Ekonomski fakultet Split , str. 189
2. Radić, D. : Informatička abeceda (poglavlje 7.4.)
3. Justament, D. (2017.) : Zaštita privatnosti na internetu (poglavlje 4.1.)
4. Chaum, D. (1984.) : *Advances in Cryptology*, (poglavlje Blind Signature System. URL : https://link.springer.com/chapter/10.1007/978-1-4684-4730-9_14)
5. Gladyshev, P., Rodgers, Marcus K. (2011.) : *Digital Forensics and Cyber Crime,* str. 40, 41, 42, 46. URL : https://books.google.hr/books?id=g_W5BQAAQBAJ&pg=PA41&lpg=PA41&dq=cyber+attack+by+sms+mms+e-mail&source=bl&ots=7SV9sdZJSH&sig=D60o9RpIAjkFWSDH1y6qinxNd3A&hl=hr&sa=X&ved=2ahUKEwiZr4LXqc_dAhXMBcAKHX8NCqEQ6AEwC3oECAIQAQ#v=onepage&q=cyber%20attack%20by%20sms%20mms%20e-mail&f=false

Izvori s interneta:

Anti-malware program, raspoloživo na :

https://blog.malwarebytes.com/101/2015/12/how-does-anti-malware-work/

https://enterprise.comodo.com/blog/what-is-antimalware/

https://www.pcworld.com/article/189245/1_or_2_AV.html

https://www.geeksonsite.com/computer-security/what-does-virus-scan-do-how-antivirus-software-works/

Cambridge Analytica, raspoloživo na:
https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07FF

https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

Društvene mreže, raspoloživo na:

https://www.britannica.com/topic/social-network#ref1073275

Facebook-ov prijestup u zaštiti podataka, raspoloživo na:

https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages

https://newsroom.fb.com/news/2018/04/new-privacy-protections/

HTTP/HTTPS protokoli i SSL certifikati, raspoloživo na :
https://www.globalsign.com/en/ssl-information-center/what-is-an-ssl-certificate/

https://www.izooto.com/blog/understanding-http-https-protocols

Kanali invazije na sigurnost, raspoloživo na:
https://www.wired.com/2016/11/great-now-even-headphones-can-spy/

Načini zaštite podataka po GDPR-u, raspoloživo na:

https://gdprinformer.com/hr/gdpr-clanci/nacini-zastite-podataka-u-gdpr-u

Načini zaštite uređaja, raspoloživo na:
https://blog.malwarebytes.com/101/2018/03/10-ways-to-protect-your-android-phone/

Podjela hakera, raspoloživo na :

https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

https://medium.com/@hackersleague/who-are-blue-hat-hackers-aeb443b90c29

Statistike o sigurnosti, raspoloživo na :

https://www.cybintsolutions.com/cyber-security-facts-stats/

https://thebestvpn.com/cyber-security-statistics-2018/

https://www.infragistics.com/community/blogs/b/mobileman/posts/six-shocking-facts-about-enterprise-mobile-security-and-how-to-avoid-them

Top 5 prijestupa u 2010. godini, raspoloživo na :

https://www.huffingtonpost.com/jeffrey-evans/top-5-privacy-violations-_b_802615.html?guccounter=1

Vatrozid, raspoloživo na :

https://www.compuquip.com/blog/the-different-types-of-firewall-architectures

VPN mreže, raspoloživo na :

https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

https://tweakyourbiz.com/technology/the-different-pros-and-cons-of-using-a-virtual-private-network-vpn

Zlonamjerni softveri, raspoloživo na :

https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Znakovi upozorenja na zlonamjerne softvere, raspoloživo na :

https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/

Zakoni:

Narodne Novine (2012). Zakon o zaštiti osobnih podataka (NN 106/2012). Preuzeto sa https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html (20.8.2018.)

Narodne Novine (2018). Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18). Preuzeto sa https://www.zakon.hr/z/1023/Zakon-o-provedbi-Opće-uredbe-o-zaštiti-podataka (20.8.2018.)

SAŽETAK

Tehnologija kao primjena znanstvenih i inženjerskih spoznaja radi postizanja praktičnih rezultata obilježava sadašnje doba i stvara temelje budućnosti. Internet kao njezina posljedica povezuje svijet i pomaže njegovom daljnjem razvoju i napretku, širenju znanja i promicanju jednakosti.

Osobni podatci i njihova privatnost oduvijek su bili predmeti zlonamjernih napada, te se na razne načine pokušava spriječiti njihova eksploatacija u neželjene svrhe. Korisnici kao vlasnici tih podataka dužni su svoju pozornost usmjeriti na zaštitu i poznavati pravne okvire u kojima mogu djelovati.

Sigurnost uređaja na kojima se podatci čuvaju, obrađuju i skladište su podložni napadima čak i kad sami korisnik pazi na način kako ih dijeli te koje podatke objavljuje javno. Stoga je bitno voditi računa o tome da se korisnici pravovremeno upute o mogućem napadu, točnije o kanalima napada, vrstama napadača, kakva je moguća šteta i kako se obraniti u slučaju da se prepozna napad na sigurnost uređaja.

Ključne riječi: podatci, sigurnost, Internet

SUMMARY

Technology as an application of scientific and engineering knowledge to achieve practical results marks the present time and creates the foundations for the future. The Internet as its consequence connects the world and helps further its development and progress, the spread of knowledge and the promotion of equality.

Personal data and their privacy have always been the subject of malicious attacks and in various ways people are trying to prevent their exploitation for unwanted purposes. Users as owners of such important data are required to focus their attention on protection and to know the legal framework in which they can act.

Security of devices on which data is being kept, processed, and permanently stored is a subject prone to attack even when user is being cautious on how he shares his personal dana and is keeping an eye on what kind of information he shares publicly. Therefore, it is important to keep in mind how to prepare users for a security attack, which means about different ways of attack, attackers, what is a possible damage and how to defend yourself in case of aknowledged security attack.

Key words: data, security, Internet

POPIS SLIKA