Kolačići, privatnost i kibernetička sigurnost

Ševo, Ivana

Sveučilište u Zadru

Stručni preddiplomski studij Informacijske tehnologije

Ivana Ševo

Kolačići, privatnost i kibernetička sigurnost

Završni rad

Zadar, 2021.

Sveučilište u Zadru

Stručni preddiplomski studij Informacijske tehnologije

Kolačići, privatnost i kibernetička sigurnost

Završni rad

Student/ica:
Ivana Ševo

Mentor/ica:
izv.prof.dr.sc. Dino Županović

Zadar, 2021.

Izjava o akademskoj čestitosti

Ja, **Ivana Ševo,** ovime izjavljujem da je moj **završni** rad pod naslovom **Kolačići, privatnost i kibernetička sigurnost** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

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

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

Zadar, 6. listopada 2021.

Sadržaj

1 UVOD 1

2 PRIVATNOST NA INTERNETU 2

3 KOLAČIĆI 4

3.1 KAKO KOLAČIĆI RADE? 4

3.2 KOLAČIĆI PRVE STRANE - FIRST-PARTY COOKIES 5

3.3 KOLAČIĆI TREĆE STRANE - THIRD PARTY COOKIES 5

3.4 HTML5 KOLAČIĆ 7

3.5 KOLAČIĆ SESIJE / PRIVREMENI KOLAČIĆ 8

3.6 SUPER KOLAČIĆI 8

3.7 ZOMBI KOLAČIĆI 9

3.8 TRAJNI KOLAČIĆI 10

3.9 EVERCOOKIE 10

3.10 KOJI SU RIZICI KOLAČIĆA 11

3.10.1 HVATANJE KOLAČIĆA PREKO NESIGURNIH KANALA - CAPTURING COOKIES OVER INSECURE CHANNELS 11

3.10.2 FIKSIRANJE SESIJE- SESSION FIXATION 11

3.10.3 CROSS -SITE SKRIPTIRANJE 12

3.10.4 CROSS -SITE KRIVOTVORENJE ZAHTJEVA 12

3.10.5 BACANJE KOLAČIĆA - COOKIE TOSSING 12

3.11 KAKO HAKERI KORISTE KOLAČIĆE 12

3.12 INTERNETSKA SIGURNOST KOLAČIĆA 12

3.13 UPRAVLJANJE KOLAČIĆIMA 13

3.14 PRESTANAK KORIŠTENJA KOLAČIĆA 14

4 KIBERNETIČKA SIGURNOST 15

4.1 TRENDOVI U CYBER SIGURNOSTI 16

4.1.1 AUTOMOBILSKO HAKIRANJE 16

4.1.2 INTEGRIRANJE UMJETNE INTELIGENCIJE SA KIBERNETIČKOM SIGURNOŠĆU 17

4.1.3 RANJIVOST OBLAKA 17

4.1.4 BRUTE FORCE NAPAD 18

4.1.5 INTERNET STVARI POVEZANE NA 5G MREŽU 19

4.1.6 ENKRIPCIJA 19

4.1.7 KAKVU ULOGU IMAJU MEDIJI U CYBER SIGURNOSTI 20

4.2 CYBER NAPADI 20

4.2.1 DENIAL-OF-SERVICE(DOS) I DISTRIBUTED DENIAL-OF-SERVICE (DDOS) NAPADI 21
4.2.2 MAN-IN-THE-MIDDLE (MITM)NAPADI 23
4.3 CYBER NAPAD -KORIŠTENJE SLABE LOZINKE 25
4.4 SLUČAJ UBER 26
4.5 SAVJETI KAKO RIJEŠITI OVAKVE PROBLEME 27
5 POLITIČKA PERSPEKTIVA 28
5.1 EU 28
5.2 PROVEDBE VAN EUROPE 29
6 ZAKLJUČAK 30
7 BIBLIOGRAFIJA 32
8 SUMMARY 35
9 TABLICA SLIKA 36

SAŽETAK

Cilj ovog završnog rada je pobuditi svijest korisnika Internet usluga i upozoriti na sve opasnosti koje vrebaju, a čijeg postojanja vrlo vjerojatno nisu niti svjesni. U prvom dijelu rada predstavljeni su osnovni pojmovi: kolačići, vrste kolačića, privatnosti i kibernetička sigurnost i u kratkim je crtama predstavljena i povijest kolačića i njihova prvotna namjena. Također, podrobno je opisan način djelovanja kolačića te rizici njihovog korištenja.

Osim pojma kibernetičke sigurnosti, nužno je spomenuti i trendove - što hakeri najčešće napadaju, kako se uz pomoć medija lako mogu doznati osobni podaci, ali i moguće posljedice za korisnike. Bitno je prikazati ozbiljnu narav ovakvih napada, stoga su u drugom dijelu rada navedeni primjeri nekih poznatijih cyber napada, prikazana je povezanost cyber napada i kolačića te način na koji kolačići ugrožavaju privatnost.

Završni dio ovog rada posvećen je zaštiti od praćenja i zakonima koje su donijela tijela EU -a, ali i provedbe istih u drugim državama.

KLJUČNE RIJEČI: kolačići, sigurnost, privatnost, cyber napadi i zaštita

POPIS KORIŠTENIH KRATICA:

EU	– Europska Unija
HTTP	- Hypertext Transfer Protocol
HTML,HTML5	-Hyper Text Markup Language
ID	-identification
IP	-Internet Protocol
XSS	-Cross-site scripting
KB	-kilobyte
XML	-Extensible Markup Language
MTV	-Music Television
ESPN	-Entertainment and Sports Programming Network
ABC	-American Broadcasting Company
NBC	-National Broadcasting Company
CSS	-Cascading Style Sheets
URL	-Uniform Resource Locator
SSL	-Secure Sockets Layer
TLS	-Transport Layer Security
SAD	-Sjedinjene Američke Države
IT	-Informacijske tehnologije
ADP	-Automatic Data Processing
DOS	-Disk Operating System
DDOS	-Distributed Denial of Service
MITM	-Man- in- the -middle
WI-FI	-Wireless Fidelity

OMB	-Office of Management and Budget
F12	- Company Configuration.

1 UVOD

Internet je postao neizostavanim dijelom života, ali paralaleno s razvojem Interneta razvijale su se i neke druge tehnologije. Jednu od takvih čine upravo kolačići. Iako će neki možda pomisliti kako je riječ o poslastici koju bi rado pojeli nakon ručka, ipak će ostati razočarani. Internetski kolačići postali su obvezan dio elemenata svake web stranice i svaka tvrtka koja se bavi web razvojem, a želi biti konkurentna na tržištu i ostaviti vjerodostojan dojam koristi kolačiće. Drugim riječima, kolačići su must have, no oni su se sve češće počeli pojavljivati u istom kontekstu sa sigurnosti i zaštitom podataka.

Pretražujući Internet, često se uopće ne razmišlja o presudnoj važnosti kolačića. Za većinu korisnika oni predstavljaju puku formu ili prozorčić koji se pojavi na dnu ili sredini stranice i onemogućava pregled sadržaja stranice dok se ne prihvate svi uvjeti. Velika većina korisnika ne zna čemu kolačići zapravo služe niti što točno prihvaćaju klikom na gumb za dopuštanje njihove upotrebe. Kolačići su danas postali tema mnogih prijepora, a najviše onih o cyber sigurnosti.

Svatko se barem jednom zapitao kako se na web stranicama pojavljuju upravo oglasi čiji su sadržaj pregledavali par dana ranije i nerijetko se na Facebooku može naići na tvrdnje kako nas Google prisluškuje. Kako Google dobiva uvid u naše želje i ima li pristup i nekim drugim podacima? Koji se sve podaci nesvjesno ostavljaju? Tko sve ima pristup tim podacima?

Velikom broju Internet korisnika nije poznato ni značenje kolačića ni činjenica da ih ima više vrsta, stoga će u ovom radu biti prikazane različite vrste i način na koji funkcioniraju.

Najčešće se ne razmišlja o svim opasnostima koje su prisutne na Internetu. One prvenstveno obuhvaćaju cyber napade, a mete hakera su raznolike, od vladinih organizacija do običnih građana pa takve prijetnje nikako ne treba shvaćati olako, već se moraju poduzeti mjere zaštite tamo gdje je to moguće.

Zadiranje u nečiju privatnost bi se moglo klasificirati kao kazneno djelo. To su uvidjele i mnoge države među kojima je i EU. Taj problem se pokušao riješiti propisima i zakonima kako bi se korisnik osjećao što sigurnije.

2 PRIVATNOST NA INTERNETU

Privatnost na Internetu je oduvijek bila jedna od glavnih tema kojom se i dalje bave mnoge države i vlade i svatko od njih imaju svoje vlastito viđenje nadzora protoka informacija. Jedan od nedostataka je svakako nepostojanje jednog jedinstvenog tijela koje bi moglo upravljati internetskim prostorom pod zajedničkim nazivnikom strogih pravila. Prije nego što korisnik ima vremena razmisliti što se događa oko njega, kolačići ga bombardiraju podacima i mame ponudama. Iako mnogi tvrde kako je to naprosto marketinška strategija takvog karaktera, to baš i nije tako jer se korisnika uznemirava sve dok ne popusti pod pritiskom.

Zapravo je riječ o kršenju privatnosti jer većina web stranica ne traži od korisnika dopuštenje za korištenje kolačića, a najvažnije je da se ne daje izjava da se ti podaci koriste za ciljani marketing.

Postoji nešto što se naziva bihevioralno ciljanje kojim se stvaraju profili određenih korisnika, a kako profil odgovara različitim korisnicima, šalju im se različiti oglasi koji bi ih mogli zanimati.[29].

Privatnost na Internetu je podskup privatnosti podataka i glavno ljudsko pravo, a odnosi se na privatnost na koju korisnici imaju pravo kada prikazuju, pohranjuju ili pružaju informacije o sebi na Internetu. To može uključivati i podatke u kojima se otkriva identitet korisnika, ali i kretanje po web stranicama praćenjem kojeg se otkrivaju osobni podaci.[3].

Jedan od glavnih alata koji se koristi za profiliranje korisnika je praćenje njihovog kretanja po internetskom prostoru. Prikupljeni podaci uključuju redoslijed posjećenih stranica i pregledanih stranica te sveukupno vrijeme provedeno na nekoj stranici. Praćenje korisnika nije dopušteno u slučajevima kada informacije sadrže podatke o imenu, telefonskom broju i slično, tj. kada sadrže bilo kakve informacije pomoću kojih se korisnik može identificirati. Praćenje se većinom odvija nadgledanjem IP adresa i upotrebom tehnika kao što su kolačići ili super kolačići.
Iako postoje situacije u kojima su kolačići treće strane korisni i dalje postoje razlozi za zabrinutost po pitanju njihovog korištenja. Web stranice često sadrže izvršne java script datoteke koje korisnik preuzima prilikom posjete stranice. Java script datoteke mogu pristupiti podacima koji su pohranjeni u pregledniku uključujući i povijest posjećenih veza. Na taj način

dobivaju pristup svim informacijama korisnika od IP adrese pošiljatelja preko e-mail adrese do jezičnih postavki. Problematika privatnosti korisnikovih podataka je najviše vezana uz supercookies i evercookies.[29].

3 KOLAČIĆI

Internet kolačići nastali su ne tako davne 1994. godine, a razvio ih je Netscapeov programer Lou Montulli. Prvi su se kolačići koristili isključivo u svrhu spremanja korisničkog imena i lozinke, odnosno kako se korisnik po povratku na stranicu ne bi morao ponovno ulogirati. Prije izuma kolačića u košaricu se nije moglo spremiti više objekata prije kupnje.[1].Lou Montulli je objasnio potrebu za nastankom kolačića rekavši da HTTP Osnovna Autentifikacija nije bila dovoljno prijateljska i trebalo je razviti nešto drugo. Kada je jedan klijent zatražio razvoj web košarice, razvijeno je rješenje koje je omogućavalo stavljanje proizvoda u košaricu prije kupnje. Po Lou Montulliu, kolačići nisu osuđeni na propast niti bi to oglašivači dopustili, a sve kada bi i došlo do toga prebacili bi se na neke druge tehnologije kao što je korištenje JavaScripta za slanje tajnih kodova drugim web preglednicima.[2].

Ubrzo nakon nastanka, kolačići su stekli veliku popularnost, a prvi pretraživač koji je koristio kolačiće je bio upravo onaj firme Netscape, no već godinu dana nakon nastanka i Internet Explorer ih je integrirao u svoj web preglednik.[1].

3.1 KAKO KOLAČIĆI RADE?

Kolačići ili često zvani HTTP kolačići izvorno su nastali kako bi korisnici mogli brže i jednostavnije pristupiti sadržaju koji ih zanima. Umjesto da se svaki put ponovno ulogira, kolačić pamti korisničko ime i lozinku. Današnji kolačići su davno prerasli svoju prvotnu ulogu i postali su jednako bitni kao struja ili HTML.[5].

Kolačić je tekstualni dokument koji se sastoji od identifikatora (ID-a) korištenog za identifikaciju korisnika i sprema se na računalo korisnika. Web stranice žele što više podataka o svojim korisnicima pa im tako nije u cilju da se sve informacije spremaju na korisnikovo računalo, već u bazu na nekom serveru, a na računalu se spremaju samo osnovni podaci što možete i sami provjeriti ukoliko odete na postavke svojeg Internet preglednika pod odjeljak kolačići ili cookies. Na hard disku korisnikovog računala pohranjene su informacije o ID-u, kada je kolačić nastao, kada istječe, koja mu je domena i slično.[6].

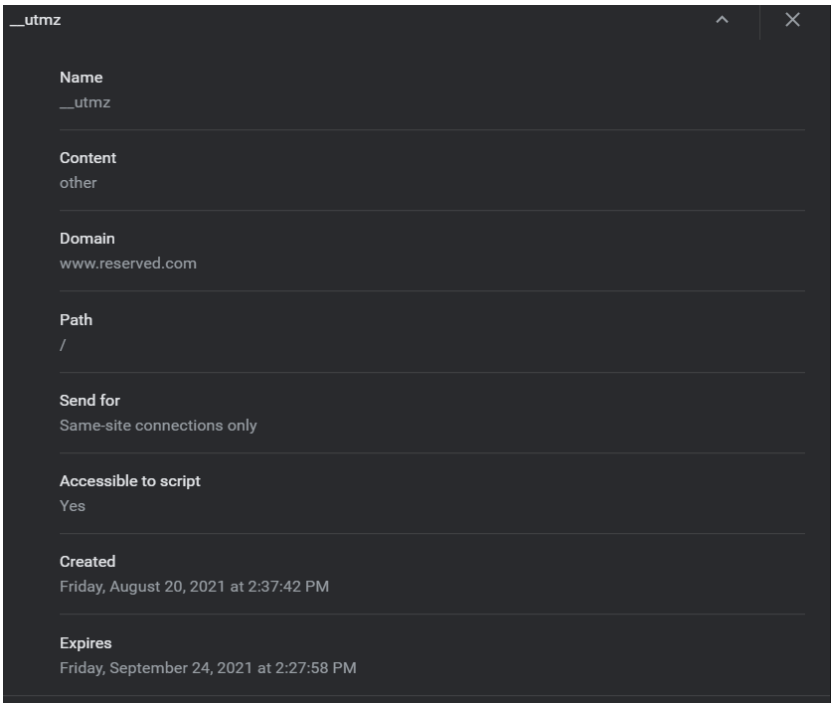
ID na kolačiću ima razne uloge, jedna od njih je prepoznavanje korisnika prilikom pretraživanja sadržaja na Internetu. Jednom kada korisnik upiše URL koji ga zanima, npr. ako je riječ o Amazonu, kada se korisnik ulogira u svoj račun, web preglednik pretraži kolačiće koji su

lokalno spremljeni i ako naiđe na onaj Amazon-ov potrebne podatke šalje Amazon-u koji zatim pregledava korisničko ime i lozinku i nakon nekog vremena dolazi poruka o tome da se korisnik ili uspješno ulogirao ili da uneseni podaci nisu prepoznati, no ako na računalu ne postoji Amazon-ov kolačić, Amazon dobiva obavijest o tome i šalje kolačić sa određenim identifikacijskim brojem.

Iako danas gotovo sve web stranice koriste kolačiće, oni zapravo i nisu nužni. Gotovo ista stvar koja se postiže uz pomoć kolačića može se postići i s upotrebljavanjem skrivenih polja u HTTP formama ili korištenjem klijentove IP adrese, ali to nije bilo dovoljno učinkovito.[7].

3.2 KOLAČIĆI PRVE STRANE - FIRST-PARTY COOKIES

Kolačiće prve strane je stvorila stranica koju korisnik posjećuje npr. NewYork Times ili Amazon. Najčešće se koriste u svrhu logiranja i pamćenja korisnikovih postavki kao što je odabir jezika ili teme. Kolačići su dostupni samo domeni koja ih je stvorila, a korisnik ih ukoliko to želi, može izbrisati.[8].



Slika 1 PRIMJER FIRST PART COOKIE, IZVOR: Autor

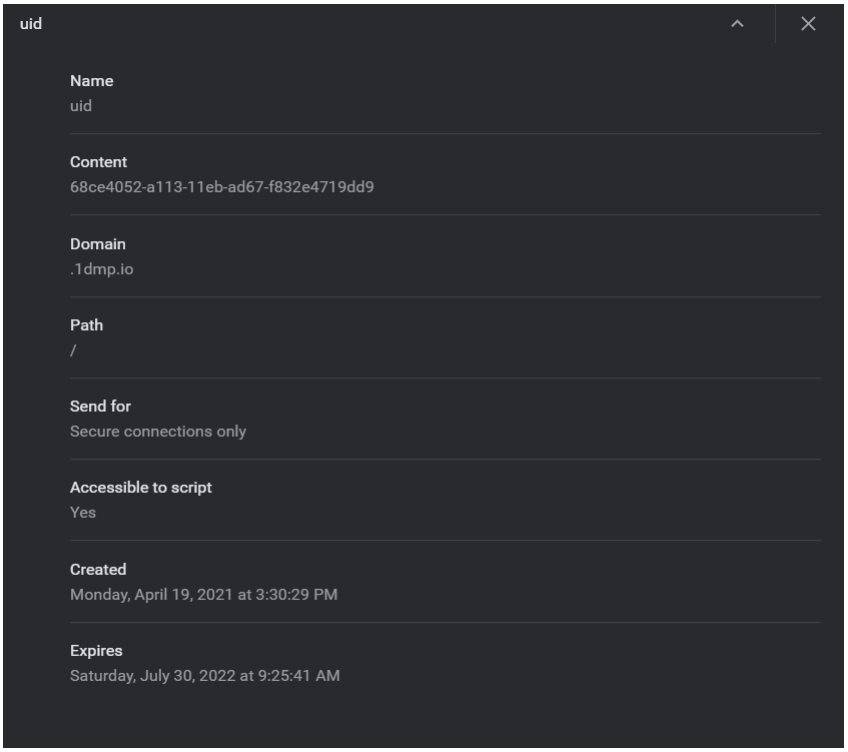
3.3 KOLAČIĆI TREĆE STRANE - THIRD PARTY COOKIES

Godinama se koriste u svrhu oglašavanja, a često se povezuju sa pojmom cross-site tracking. Jedan od primjera korištenja kolačića treće strane su reklame na web stranicama.[4]. Ako npr.

korisnik posjeti stranicu Večernjeg Lista, velika je vjerojatnost da će prilikom pregledavanja članaka naići na reklame koje nude proizvode, koje je sigurno u nekom trenutku pretraživao. Uloga kolačića treće strane je pratiti korisnikovo ponašanje na Internetu na temelju kojeg svatko dobije personalizirani oglas. Moguće je i samostalno provjeriti kolačiće treće strane. Dovoljno je otvoriti željenu stranicu, a klikom na F12 otvori se prozor sa alatima za developere i u dijelu Application s lijeve strane se može uočiti natpis cookies, a klikom na karticu moguće je vidjeti domenu. Ako je vidljiva samo trenutna domena, tada stranica ne koristi kolačiće treće strane. Može se dogoditi da korisnik nije ni svjestan da se nalazi na stranici koja koristi kolačiće treće strane.
Takve stranice se lako prepoznaju po oglasima.[9].
Kada korisnik posjeti neku web stranicu koja sadrži više različitih objekata implementiranih sa različitih poslužitelja, generira se više HTTP zahtjeva za različite poslužitelje. Vrlo često kolačić jest povezan sa svakim od ovih zahtjeva. Poslužitelj postavlja kolačiće na web stranice i često ih koristi za pohranu korisničkih postavki ili za provjeru autentičnosti prilikom zadržavanja ovjerene sesije. Preglednik šalje natrag nepromijenjeni kolačić svaki put kada korisnik pristupi toj stranici, pa ga web stranice često koriste za praćenje korisnika tijekom posjete stranici.

Kolačići se šalju samo stranicama koje su postavile kolačiće, no web stranica može sadržavati slike, poveznice, java script komponente itd. koji su pohranjeni na poslužiteljima druge domene. Tu je riječ o kolačićima treće strane pomoću kojih agencija koja je zadužena za postavljanje i objavu internetskih oglasa može pratiti korisnike preko svih stranica na kojima ima postavljene oglase.

Iako postoje situacije u kojima su kolačići treće strane korisni, sve više je i razloga za zabrinutost po pitanju njihovog korištenja. Web stranice često sadrže izvršne java script datoteke koje korisnik preuzima prilikom posjete stranice. Takve datoteke mogu pristupiti podacima koji su pohranjeni u pregledniku uključujući i povijest posjećenih veza. Na taj način dobivaju pristup korisnikovim informacijama, od IP adrese pošiljatelja preko e-mail adrese do jezičnih postavki.[29].



Slika 2 PRIMJER THIRD PART COOKIE, IZVOR: Autor

3.4 HTML5 KOLAČIĆ

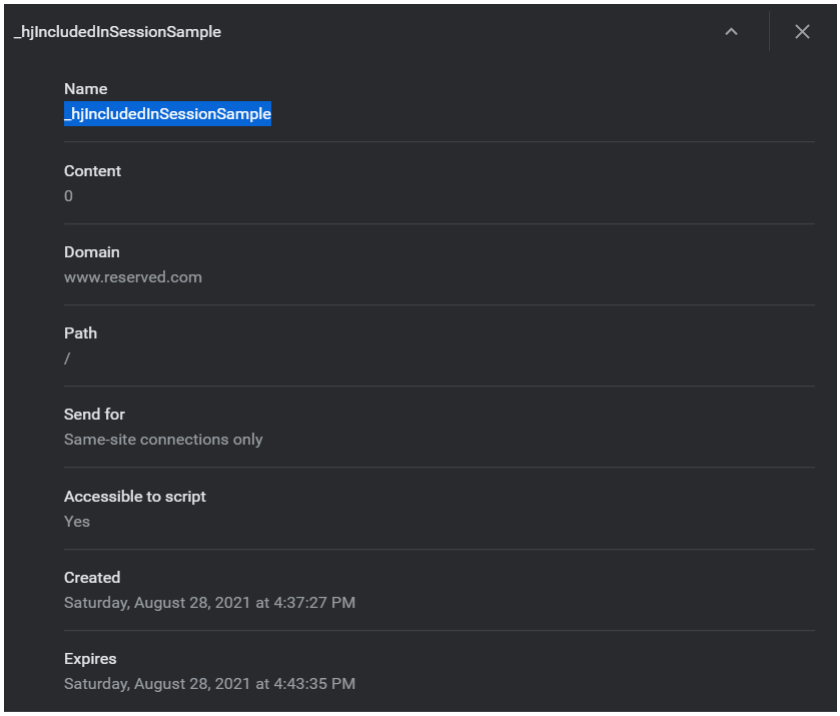
HTML5 kolačić nije standardni tip kolačića kao kolačići prve ili treće strane. Ovdje je riječ o pohranama koje nudi HTML5, a sastoji se od mogućnosti lokalne pohrane i pohrane sesije. HTML5 kolačić je poznat još i kao HTML5 Web storage, a prednosti su mu brzina i sigurnost, ali i veća pohrana.[10].Za razliku od standardnih HTTP kolačića koji istječu nakon nekog vremena, HTML5 pohrana nema rok trajanja osim ako je web stranica ili korisnik ne izbrišu, no puno je polemike oko sigurnosti takve pohrane.[11].

HTML5 nudi developerima mogućnost pohrane velike količine podataka unutar JavaScript koda. Glavna razlika između sesijske pohrane i lokalne pohrane je ta što sesijska briše sve podatke jednom kada korisnik izađe iz web preglednika. Od strane web developera HTML5 nudi zanimljivo i jednostavnije rješenje pohrane podataka. Pozitivna strana korištenja ovakve pohrane je najbolje vidljiva kod izrade statičkih stranica. Za pokretanje takvih aplikacija nije potreban web server za pohranu, no za složenije aplikacije to ipak nije rješenje jer usporavaju aplikaciju. Što se tiče sigurnosti ovo može predstavljati veliki problem. Podaci su u ovom

slučaju najranjiviji na XSS napade tj. cross-site scripting attacks. Ako napadač može pokrenuti JavaScript sa vaše stranice, onda može i vratiti podatke sa lokalne pohrane.[12].

3.5 KOLAČIĆ SESIJE / PRIVREMENI KOLAČIĆ

Ovaj tip kolačića namijenjen je pamćenju korisnikove lozinke i imena, a jednom kada korisnik zatvori web preglednik, kolačić se izbriše.[13].Budući da je kolačić sesije privremen, ne prikuplja informacije s korisnikovog računala. Uobičajeni primjer kolačića sesije je košarica za kupnju koja se nalazi na većini web stranica za online kupovinu ili e-trgovinu. Sesijski kolačić pohranjuje artikle koje je korisnik dodao u košaricu. Bez kolačića sesije, kada bi korisnik otišao na stranicu za naplatu, sve bi nestalo iz košarice.[14].



Slika 3 PRIMJER KOLAČIĆA SESIJE ,IZVOR: Autor

3.6 SUPER KOLAČIĆI

Za razliku od kolačića sesije koji su privremeni, super kolačići će biti trajno pohranjeni na računalo i neće se moći izbrisati. Oni mogu pristupiti povijesti preglednika.[10]. Korisnik može u postavkama svog preglednika blokirati kolačiće, ali ukoliko stranica koju je posjetio koristi super kolačiće, oni će i dalje biti instalirani na računalo, a imaju i mogućnost pristupa informacijama kojima obični kolačići ne mogu pristupiti. Jedna od super moći super kolačića je vraćanje obrisanih standardnih kolačića.[15].Postoje dvije vrste super kolačića, a to su Flash,

koji je razvio Adobe i Silverlight, koje je razvio Microsoft.[16].Glavna razlika između Adobe kolačića i regularnih kolačića je ta da mogu pohraniti više informacija, točnije 100 KB po default-u, a obični HTTP kolačići samo 4KB. Čak i ako se korisnik prebaci na neki drugi web poslužitelj, time problem i dalje nije riješen jer ga Flash kolačići i dalje mogu pratiti. Corey Benninger je 2006. godine slučajno primijetio da se Flash kolačići mogu postaviti bez da se korisnika obavijesti da ih ta stranica koristi, a to je mogao biti veliki sigurnosni problem jer bi se na taj način mogli dijeliti identifikacijski brojevi korisnika. Pitanje sigurnosti Adobe-ovih kolačića nastavilo se kroz njihovu politiku o pravilu više domena. Riječ je o XML dokumentu koji omogućava Flash Playeru pristup podacima iz dane domene, a da pritom ne obavijesti korisnika o tome i ne traži ga pristanak. Jeremiah Grossman je ukazao na ovaj problem 2008. godine rekavši da politika više domena može lako dovesti do curenja podataka te da može dovesti do malicioznih napada, a svi koji imaju pristup korisnikovim podacima ih vrlo lako mogu i izmijeniti. Tijekom 2011. godine provedeno je istraživanje o broju korištenih Flash kolačića na uzorku od 100 web stranica. Rezultati istraživanja su bili 100 kolačića na 100 web stranica, a 2009. godine ih je bilo 281 pri čemu se može uočiti značajan pad. MTV.com je koristio 8 Flash kolačića od kojih su neki pohranjivali 140 vrijednosti.[11].

3.7 ZOMBI KOLAČIĆI

Zombi kolačići tj. kolačići koji se ne mogu izbrisati su se pojavili 2010. godine. Firma za online oglašavanje Quantcast optužena je zajedno s internetskim gigantima kao što su MTV, ESPN, MySpace, Hulu, ABC i NBC za stvaranje i korištenje kolačiće u svrhu praćenja korisnika preko Interneta. Ti kolačići su nastali na temeljima Adobe Flash kolačića, a korišteni su za ponovno rekreiranje kolačića koje je korisnik izbrisao sa web preglednika.[17].Ovakvi kolačići su nazvani zombi kolačićima i preko njih su se izvlačili podaci o vrstama posjetitelja pojedinih web Flash kolačića.[18].Sličan postupak vođen je i protiv jednog Quantcast-ovog rivala 2010. godine. Na korisnikovo računalo bi se instalirao kod za praćenje koji je vraćao izbrisane kolačiće preko widget-a AddThis kojeg su koristile mnoge stranice među kojima su Disney, Playlist, Ustream, Soda Head i Warner Brothers Records. Tužitelji su se koristili istraživanjima na sveučilištu u Kaliforniji prema kojima je 44 od 100 web stranica na kojima je provedeno istraživanje koristilo Flash kolačiće, a samo su 4 to spomenule u svojoj politici privatnosti. Dokazano je da su se gore navedene tvrtke koristile tehnikom instaliranja dvaju kolačića na korisnikovo računalo. Kolačić koji korisnik može izbrisati preko web preglednika i Flash kolačić.[17].

3.8 TRAJNI KOLAČIĆI

To je podatkovna datoteka koja pamti korisnikove odabire i postavke. Svaki put kada korisnik ponovno uđe na istu stranicu, stranica će biti prilagođena njemu u skladu sa njegovim preferencijama. Ovi kolačići najčešće pamte detalje o loginu, odabir teme, autentifikaciju, odabir jezika, najdraže objekte i slično, a istječu nakon jedne ili dvije godine.[19].

3.9 EVERCOOKIE

Samy Kamkar je 2010. godine razvio JavaScript biblioteku kojom su nastali konzistentni kolačići, a na korisnikovo računalo su pohranjivali znatnu količinu podataka. U početku se neiskusni korisnici nisu nikako mogli riješiti takvog kolačića, no s vremenom su se web preglednici razvijali i nudili više privatnosti, a na GitHubu su se pojavile informacije da evercookie ima ograničenja i da neće biti više konzistentni prilikom korištenja privatnog pretraživanja u pregledniku, no počelo se nametati pitanje hoće li se evercooke moći koristiti za praćenje korisnika Internetom.

Sada malo više o tome kako evercookie radi. Prvi korak je slanje kolačića tj. postavljenje kolačića u php skriptu i kao odgovor na taj zahtjev, šalje se skripta sa podacima iz kolačića. Zaglavlje za kontrolu predmemorije govori web pregledniku da uhvati taj dokument. Kako bi evercookie dohvatio podatke iz skripte, ponovno šalje zahtjev za php skriptom, ali bez parametara. Poslužitelj šalje poruku 304 i prisiljava web preglednik da dohvati skriptu iz predmemorije.

Evercookie može pristupiti korisnikovoj povijesti pretraživanja tj. može pristupiti kolačiću sa stranice koju ste nekada posjetili. Provjerava znak po znak i kada dođe do znaka minus, znači da je provjerio i zadnje slovo. Sljedeći dio teksta predstavlja primjer procesa brute force kojim se upravo provjerava povijest korisnikovog pretraživanja.

google.com/evercookie/cache/b
google.com/evercookie/cache/bc
google.com/evercookie/cache/bcd
google.com/evercookie/cache/bcde
google.com/evercookie/cache/bcde-

Naravno cijeli opisani proces je moguć ako je omogućeno spremanje povijesti pretraživanja u predmemoriju. Povijest pretraživanja je lokalno zapisana u JavaScriptu i na kraju svakog URL linka nalazi se znak minus, na temelju kojeg evercookie zna da je došao do kraja. Pretraživanje povijesti pregledavanja je vrlo jednostavno ako se koristi CSS History Knocker .Tko se odluči koristiti privatni način pretraživanja tj. incognito window, nakon njegovog zatvaranja evercookie ne može pristupiti podacima.[20].

3.10 KOJI SU RIZICI KOLAČIĆA

Nije vjerojatno da će kolačić prenijeti virus jer kolačići zapravo predstavljaju jednostavne tekstualne datoteke, ali ovisno o načinu korištenja mogu predstavljati značajan sigurnosni rizik. Jedan od primjera utjecaja na sigurnost kolačića je kada ga napadač hakira i predstavlja se kao korisnik, te time stječe neovlašteni pristup. Neki od načina na koje se to može napraviti su sljedeći: hvatanje kolačića preko nesigurnih kanala, fiksiranje sesije, cross-site skriptiranje, cross-site krivotvorenje zahtjeva i bacanje kolačića.[21].

3.10.1 HVATANJE KOLAČIĆA PREKO NESIGURNIH KANALA - CAPTURING COOKIES OVER INSECURE CHANNELS

Svaki kolačić koji pregledava autentičnost unesenih podataka trebao bi putovati sigurnim protokolima, ali to nije uvijek slučaj. Takav problem predstavljaju kolačići bez sigurnosne zastavice. Svaki kolačić sa znakom za sigurnost daje pregledniku na znanje da se kolačiću može pristupiti samo preko sigurnih SSL i TLS kanala. Ako kolačić nema oznaku za sigurnost to bi omogućilo bilo kome tko prisluškuje promet da lako uhvati kolačić.[21].

3.10.2 FIKSIRANJE SESIJE- SESSION FIXATION

Ovo je još jedan od načina otimanja korisnikove sesije. Ovaj put koristi ograničenja u načinu na koji web aplikacija upravlja ID-em sesije. Takav napad se može izvesti kada napadač korisniku šalje URL sa određenim ID-em sesije u koji su uključeni i korisnikovi podaci. Kada korisnik odluči provjeriti autentičnost preko ovog URL-a, napadač mu lako otme sesiju.[21].

3.10.3 CROSS -SITE SKRIPTIRANJE

Drugi način krađe podataka je korištenje skriptiranja na više web lokacija. Primjer ovakvog napada je kada korisnik klikne na URL koji je postavio napadač i tada žrtvin preglednik šalje žrtvine kolačiće do sustava koje kontrolira napadač. [21].

3.10.4 CROSS -SITE KRIVOTVORENJE ZAHTJEVA

Ovo je primjer napada u kojem se tjera stranicu na izvršavanje neovlaštenih naredbi koje se prenose od korisnika kojem web aplikacija vjeruje. Cilj napadača je natjerati žrtvu da nesvjesno podnese zlonamjerno izrađen web zahtjev web mjestu kojem žrtva ima privilegiran pristup. Do toga može doći kada žrtva klikne na neki URL, ali takvi zlonamjerni zahtjevi se mogu ugraditi i u sliku ili se aktiviraju prilikom samog otvaranja maila. [21].

3.10.5 BACANJE KOLAČIĆA - COOKIE TOSSING

Prilikom ovakvog tipa napada, napadač šalje korisniku zlonamjerni kolačić koji samo prividno izgleda kao da ga šalje poddomena tražene stranice. Ovo postaje problematično kada web stranica omogućava neprovjerenim osobama hostanje poddomene te web stranice. [21].

3.11 KAKO HAKERI KORISTE KOLAČIĆE

Ako hakeri pristupe kolačićima korisnika tada mogu dobiti pristup njegovoj sesiji, lozinkama i drugim povezanim mrežnim aktivnostima. Ponekad hakeri stvaraju zoombie kolačiće i superkolačiće kako bi lakše došli do podataka. Takvih kolačića se teško riješiti jer se umnožavaju i ponašaju poput crva. Još jedan od načina na koji mogu pristupiti vašim podacima je ako dobiju pristup korisnikovoj mreži i poslužitelju web stranice koju on posjećuje. Na primjer hakiranje web stranice preko koje korisnik obavlja kupnju i na taj način dolazi do podataka u kolačiću. [28].

3.12 INTERNETSKA SIGURNOST KOLAČIĆA

Bilo koja web stranica može izdati kolačiće. Sve što se sprema u kolačić se kodira i sprema u obliku teksta tako da se svaki put kada korisnik posjeti web stranicu kolačić promijeni, pa se lako mogu neovlašteno pregledavati i krivotvoriti.

U prošlosti se kolačići nisu koristili za pokretanje koda ili za isporuku virusa jer imaju brojne ranjivosti. Detektirane su tri prijetnje: mrežne prijetnje, prijetnje krajnjem sustavu i prijetnje prikupljanju kolačića.

Mrežne prijetnje predstavljaju podatke u kolačiću spremljene kao tekst pa se kao takvi prilikom komunikacije mogu lako mijenjati. Može se koristiti SSL (Secure Socket Layer) kako bi zaštitili kolačiće dok se prenose putem mreže. Prijetnje krajnjem sustavu predstavljaju lažno predstavljanje i krivotvorenje podataka. Napadač može izvršiti napad na prikupljanje kolačića lažnim predstavljanjem legitimne web stranice i prikupljanjem kolačića od korisnika.[29].

Unutar kolačića se nalaze podaci koji omogućavaju lociranje korisnika i uređivanje postavki i zato je izuzetno važno omogućiti sigurnost takvih podataka. Dva glavna načina gubljenja podataka su migracija i krađa. U sprječavanju toga važnu ulogu ima integritet kolačića. Ako se promijene podaci u kolačićima za autentifikaciju, autentifikacija neće uspjeti. U borbi protiv neovlaštenog pristupa može se koristiti i šifriranje. Radi osiguravanja povjerljivosti, cjelovitosti i vjerodostojnosti podataka koristi se SSL/TLS protokol radi šifriranja podataka.

Provjerava se autentičnost treće strane preko digitalne potvrde i tek se nakon izvršene provjere omogućava komunikacija između korisnika i servera. Svi podaci koji se izmjenjuju između korisnika i servera su šifrirani i na taj se način sprječava nezakonita krađa podataka. Algoritam SSL šifriranja i hash funkcija koriste se za osiguravanje integriteta podataka koji se prenose između web klijenta i poslužitelja.[13].

3.13 UPRAVLJANJE KOLAČIĆIMA

Velika većina web preglednika nudi mogućnost onemogućavanja kolačića i privatno pretraživanje i u tom slučaju se kolačići neće spremati na korisnikovo računalo, ali to nije dovoljna zaštita. Brisanjem kolačića gubi se povezanost između web preglednika i servera, pa svaki sljedeći put kada korisnik posjeti stranice čiji kolačić je izbrisan, server će ga smatrati novim korisnikom i poslat će mu kolačić sa jedinstvenim identifikacijskim brojem. Ako se pak blokira kolačić, u tom slučaju se ne može spremiti na računalo.

Uklanjanje novijih vrsta kolačića kao što su superkolačići ili Flash kolačići, često nije tako jednostavno i potrebni su određeni alati. Tako na primjer Adobe nudi alat za konfiguriranje Flash kolačića. Pomoću njega korisnik može mijenjati postavke pohrane i brisati kolačiće koji

su povezani sa web stranicom. IAB (Europsko trgovačko udruženje digitalnih i interaktivnih marketinških industrija) pruža upute za pristup postavkama kolačića za različite preglednike, kao i poveznice za alate preko kojih se upravlja Flash kolačićima.[29].

3.14 PRESTANAK KORIŠTENJA KOLAČIĆA

Google je 2020. godine najavio planove o prestanku praćenja korisnika korištenjem kolačića. Odlučili su da će na Chrome pregledniku prestati podržavati kolačiće treće strane. Drugi preglednici kao što su Mozilla Firefox i Safari već su ih prestali podržavati. Također, najavili su kako nemaju namjeru razvijati nove alate koji bi zamijenili ulogu kolačića. Ovakva odluka je uslijedila nakon sve većih napora za zaštitu ljudskih prava u Europi i SAD-u.

Google je rekao da se trenutni način internetskog oglašavanja treba promijeniti kako bi se smanjila što veća zabrinutost korisnika po pitanju njihove privatnosti i načina na koji se koriste njihovi identiteti.

Ubrzo nakon toga su Google-ovi planovi postali upitni jer su britanski regulatori konkurencije proveli istragu oko mogućeg monopola oglašavanja na Internetu. Google je optužen za zlouporabu svog dominantnog položaja jer pokušava stvoriti novi način oglašavanja.

U svom posljednjem priopćenju Google je rekao da radi s drugima u industriji na projektu "Sandbox Sandbox", čiji je cilj stvoriti novi sustav koji će zadovoljiti i oglašivače i izdavače, ali su i napomenuli kako ne namjeravaju zamjenu kolačića treće strane s novim tehnologijama. [22].

4 KIBERNETIČKA SIGURNOST

Danas pojedinac može slati i primati poruke samo jednim pritiskom na gumb, no često se ne razmišlja o tome koliko su te informacije sigurno prenesene drugoj strani. Time se bavi kibernetička sigurnost. Više od 60% razmjena vrši se preko Interneta, pa je ova grana postala izuzetno bitna. Kibernetička sigurnost je postala preduvjet za kvalitetnu razmjenu podataka.

Stvaranje sigurnijeg Interneta i zaštita klijenata je postala zakonodavna strategija. U poslijednjih deset godina kibernetička sigurnost je postala bitno pitanje u svijetu IT-a.

U današnjem svijetu svi se suočavaju s istim problemima vezanim uz cyber kriminal. Kako su teme hakerskih napada uglavnom osjetljivi podaci vlade i nekih poduzetničkih organizacija, pojedinci su itekako zabrinuti jer napad na internetsku sigurnost može za sobom povući i druge neželjene radnje, od veleprodajnih prijevara do ucjena velikih tvrtki.[23].

Kibernetička sigurnost je postala područje sve veće važnosti zbog velikog oslanjanja na računalne sustave, povezivanja raznih uređaja na Internet -mobitela, televizora, ali i malih kućanskih aparata. Internet nudi neograničene mogućnosti, ali s njima dolazi i rizik od hakiranja. Koliko god brzo da se razvija sigurnost, jednako brzo se razvija i raste svijet cyber kriminala. Što je uopće kibernetička sigurnost i zašto je potrebna?

Kibernetičku sigurnost čini niz tehnika, procesa i tehnologija kojima se nastoji zaštiti programe i podatke od neovlaštenog pristupa i može je se nazvati i sigurnošću informacijskih tehnologija. Operacije kibernetičke sigurnosti uključuju zaštitu informacija i sustava od glavnih cyber prijetnji koje se pojavljuju u raznim oblicima. Držanje koraka sa cyber napadima često zna biti izazovno, a ponajviše u vladinim i poduzetničkim organizacijama gdje su napadi uvijek inovativni jer za cilj imaju pristup tajnim, vojnim i osjetljivim informacijama. Među najčešćim prijetnjama treba istaknuti :cyber terorizam, cyber ratovanje i cyber špijunažu.

Korištenje cyber sigurnosti može pomoći u sprječavanju cyber napada, kršenja podataka i krađe identiteta te može pomoći u upravljanju rizicima. Na primjer, zaštita krajnjeg korisnika brani informacije i štiti od gubitka ili krađe, a istovremeno skenira računala u potrazi za zlonamjernim kodom.

Organizacija koja trpi kibernetički napad mora se suočiti s gubitkom imovine, poslovne reputacije, a potencijalno i s kaznama i poduzimanjem pravnih radnji i troškovima sanacije. U Velikoj Britaniji je 2017. godine provedeno istraživanje o troškovima sanacije kibernetičkih napada po kojem prosječni trošak za veliku firmu iznosi 19 000 funti, a za mala i srednja poduzeća 1570 funti.[30].

Dakle cyber napadi ne samo da predstavljaju veliki sigurnosni propust i problem, nego i znatan udarac na financije. Bitno je napomenuti da hakiranje i krađa informacija nisu samo gubitak povjerljivih informacija nego i narušavanje odnosa s kupcima na tržištu.

Zbog brzo rastućih tehnologija i trendova nitko nije u mogućnosti adekvatno zaštiti svoje privatne podatke i shodno tome eksponencijalno raste i stopa cyber kriminala. Većina transakcija što osobnih što komercijalnih se odvija putem Interneta, stoga je važno imati stručne osobe koje bi osigurale kvalitetnu sigurnost, a time bi se osigurala i bolja transparentnost. Tehnologije kao što su usluge u oblaku, e-trgovine ili Internet bankarstvo zahtijevaju visoke sigurnosne standarde, a svi alati i tehnologije koje su uključene u te transakcije sadrže vrlo osjetljive podatke.[23].

4.1 TRENDOVI U CYBER SIGURNOSTI

Zaštita podataka je u današnje vrijeme postala otežana. Uprave i organizacije poduzimaju razne korake kako bi smanjili cyber napade, no bez obzira na to kibernetička sigurnost i dalje predstavlja izazov. Glavni trendovi u cyber sigurnosti su: automobilsko hakiranje, integriranje umjetne inteligencije sa kibernetičkom sigurnošću, ranjivost oblaka (cloud-a), Internet stvari povezane na 5G mrežu i enkripcija.[39].

4.1.1 AUTOMOBILSKO HAKIRANJE

Jedan od uzlaznih trendova u svijetu cyber kriminala je automobilsko hakiranje. Suvremena vozila su opremljena automatiziranim softverima koji utječu na tempomat, zračne jastuke, upravljaju motorima i naprednim sustavima koji osiguravaju sigurniju i udobniju vožnju, a često koriste i WiFi i Bluetooth tehnologije za komunikaciju. Stručnjaci za cyber sigurnost očekuju da će preuzimanje kontrole nad vozilom i korištenje mikrofona za prisluškivanje značajno porasti u narednim godinama.[39]

4.1.2 INTEGRIRANJE UMJETNE INTELIGENCIJE SA KIBERNETIČKOM SIGURNOŠĆU

Umjetna inteligencija je najznačajnija u izgradnji automatiziranih sigurnosnih sustava, prepoznavanje glasa i lica, ali sve češće se počela koristiti i za izradu zlonamjernih softvera i provođenje napada kojima je cilj zaobići najnovije sigurnosne sustave.

Umjetna inteligencija i strojno učenje može biti korišteno za smanjenje površine napada umjesto jurnjave za zlonamjernim aktivnostima, ali kako je to grana koja je još u procesu sazrijevanja, treba biti svjestan nedostataka :

- Hakeri mogu koristiti umjetnu inteligenciju za razvoj mutirajućeg softvera, a posljedica toga su krivi podaci
- Ako manipulacija podacima ostane neotkrivena, organizacije će nastojati oporaviti takve podatke[39].[42].

4.1.3 RANJIVOST OBLAKA

Potrebno je ažurirati sigurnosne mjere kako ne bi došlo do curenja podataka. Neki od najčešćih napada su :

1. Phising tj. krađe identiteta- korisnika se usmjerava na nesigurnu web stranicu kako bi mu napadač ukrao ID sesije
2. Keylogger -program koji bilježi tipke korisnika uključujući i lozinke
3. Brute force napadi- napadač pogađa lozinku dok ne dobije pristup podacima

U prvoj polovici 2019. godine je zabilježeno 3800 povreda podataka, a to je dovelo do gubitka milijuna dolara. Prema istraživanjima koja su provedena te godine, 43% žrtava su bile male tvrtke. Razlog za tako visok postotak je razina zaštite koja nije na razini zaštite koju pružaju velike tvrtke, pa su time i lakša meta napada.[40].

4.1.3.1 PHISING

Ovo je vrsta napada kojom se hakeri koriste kako bi došli do raznih korisničkih podataka uključujući vjerodajnice za prijavu i brojeve kreditnih kartica. Žrtvu se često pokušava namamiti e- mail porukom koja sadrži zlonamjernu vezu, klikom na nju se može instalirati zlonamjerni softver, te može zamrznuti sustav što omogućava napadaču da dođe do povjerljivih informacija. Phising može ciljati slučajne korisnike ili određene osobe i poduzeća, a takav tip napada se naziva Spear phishing.[41].

4.1.3.2 KEYLOGGER

Keylogger može biti program ili uređaj koji je namijenjen tajnom nadziranju i praćenju pritisaka na tipke. Postoje legitimni programi kao što su Ninja tipkovnice koje pamte pritisnute tipke koje se kasnije koriste za pozivanje određenih programskih funkcija ili programi koji služe administratorima u svrhu nadgledanja zaposlenika, ali tu se onda nameće razmišljanje da je vrlo tanka granica između špijunaže i opravdanog nadziranja, pa se tako događalo da legitimni softveri postanu alati za krađu lozinki. Keylogger-i se smatraju legitimnima i lako ih je nabaviti. Pozitivno korištenje keylogger-a:

- Roditeljski nadzor
- Ljubomorni supružnici ili partneri mogu pomoću keylogger-a pratiti svoju bolju polovicu
- Tvrtke mogu pratiti računala koje koriste njihovi zaposlenici (koriste li službena računala u poslovne svrhe ili privatne)[37].

4.1.4 BRUTE FORCE NAPAD

Ovakvi napadi se temelje na pogađanju tj. koristi se metoda pokušaja i pogreške kako bi haker došao do podataka za prijavu, lozinke, ključeva za šifriranje i slično. Haker prolazi kroz sve moguće kombinacije u nadi da će jedna biti uspješna. Iako je ova metoda poprilično zastarjela, i dalje je vrlo popularna. Ovisno o duljini lozinke, ovakva metoda može trajati od nekoliko sekundi do mnogo godina. Hakerima su prilikom ovakvih napada korisni automatizirani alati koji imaju koji brzo nagađaju znakove.[38].

4.1.5 INTERNET STVARI POVEZANE NA 5G MREŽU

Komunikacija između više uređaja otvara vrata ranjivosti. Uređaji će postati izloženiji vanjskom utjecaju, napadima i nepoznatim programskim greškama. 5G mreža je nova i potrebno je još uložiti puno vremena i provesti istraživanja kako bi se pokrili svi nedostaci i rupe po pitanju sigurnosti. Proizvođači bi trebali stvoriti sofisticirani 5G softver i hardver koji bi kontrolirao kršenje podataka.[38]

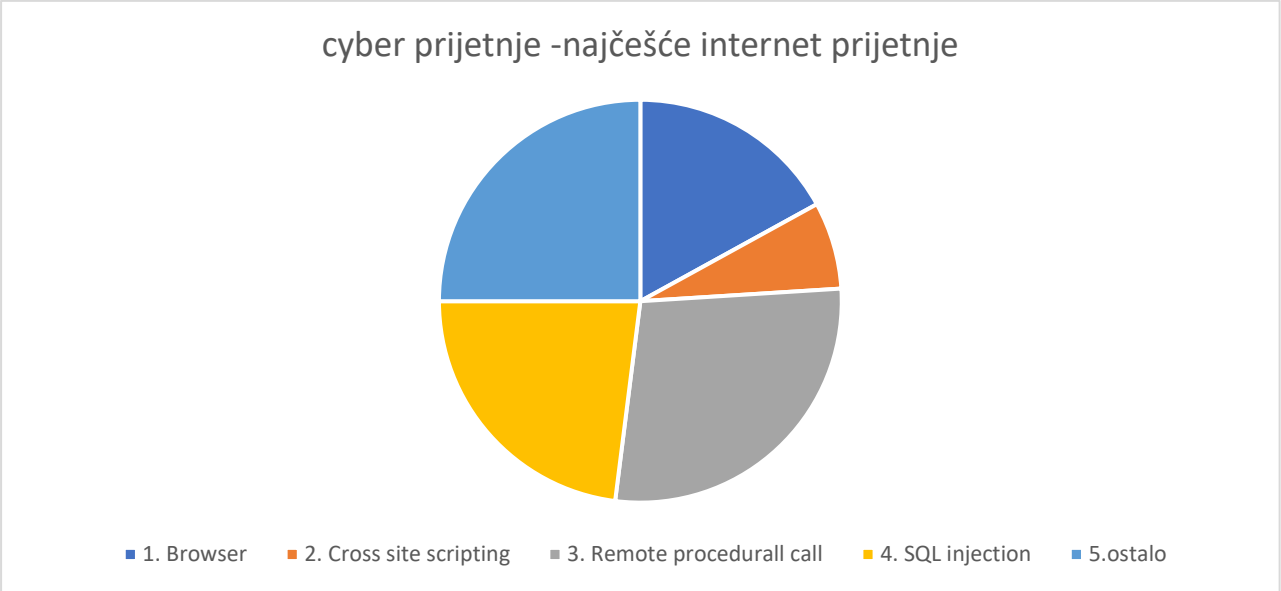
4.1.6 ENKRIPCIJA

To je metoda šifriranja poruka na koju programeri nemaju utjecaj, a najčešće se koristi ključ pomoću kojeg se šifra kodira, ali i dekodira. Šifriranje se koristi za zaštitu podataka prilikom njihovog slanja od točke A do točke B.

The Advanced Persistent Threat ili ADP su sofisticirani napadi od strane kriminalnih organizacija koje za cilj imaju:

1. Pristupiti tajnim, financijskim dokumentima vlade ili pojedinca
2. Održavanje uporišta u tim okruženjima kako bi se omogućila buduća upotreba i kontrola.
3. Izmjenu podataka

Najčešće web prijetnje:[23].



Slika 4 IZVOR: Cyber Security ,sciendo , HOLISTICA Vol 10, Issue 2, 2019, pp. 115-128

4.1.7 KAKVU ULOGU IMAJU MEDIJI U CYBER SIGURNOSTI

Mediji su postali okosnica života bilo da ih se koristi za informiranje, dijeljenje sadržaja, planiranje i/ili održavanje kontakata. Zamijenili su e-mail i poštu. Kao i sve drugo što je vezano za web tako je i ovdje presudno informirati se o opasnostima. Korištenje medija je za mnoge prozor u nečiji tuđi život, a samim time predstavlja i opasnost. Za neke zlonamjerne osobe to lako može poslužiti kao dobar izvor informacija koje se mogu hakirati i iskoristiti u neke sasvim druge svrhe.

Organizacije moraju osigurati brzo detektiranje opasnosti, ali i svaki pojedinac mora poduzeti odgovarajuće mjere kako bi se zaštitio od potencijalne krađe.

No postoji i drugi problem medija. Često se znalo događati da se ukradeni podaci i informacije javno distribuiraju i time bi se načinila neprocjenjiva, a često i nepopravljiva šteta.[23].

4.2 CYBER NAPADI

Za veliku većinu ljudi, terorizam označava usmjeravanje mržnje i agresije prema drugima na temelju vjere, boje kože ili slično, no terorizam postoji i u sektoru IT-a. Iz konvencionalne strukture se razvio cyber terorizam koji je postao vitalno pitanje. Kritično pitanje u cyber

terorizmu je motivacija za dovršavanjem takve akcije na Internetu koja rezultira divljanjem i oštećivanjem ljudi i njihove imovine.[23].

6. Case Study Examples

4.2.1 DENIAL-OF-SERVICE(DOS) I DISTRIBUTED DENIAL-OF-SERVICE (DDOS) NAPADI

Napad uskraćivanjem usluge ili DOS se temelji na preplavljivanju sustava tako da ne može odgovoriti na zahtjeve. DDOS je također napad na sustav tj. na server sustava, ali se pokreće s velikog broja drugih hostova koji su zaraženi zlonamjernim softverom. Postoje napadi kojima je cilj povećati razinu pristupa, a postoje i oni kojima je dovoljno onemogućavanje pristupa. Svrha DOS napada može biti isključivanje sustava kako bi se mogla pokrenuti neka druga vrsta napada. Neki od napada koji ovdje spadaju su flood attack, teardrop attack, smurf attack, ping-of-death attack i botnets.[23].

4.2.1.1 BOTNET ATTACK

Botnet napad izvodi skupina uređaja povezanih Internetom pod kontrolom hakera. Botneti su zapravo mreže uređaja. Napadači se ubacuju u mrežu zlonamjernog softvera kako bi kontrolirali mrežu, a napade reliziraju preko botneta na svojim računalima. Ovi napadi se koriste u svrhu krađe podataka i ugrožavanja povjerljivih informacija. Cyber kriminalci prvo dobiju pristup uređajima tako što ugrožavaju njihovu sigurnost npr. koristeći se trojanskim konjem ili nekim drugim tipom marvela. Ponekad napadači ne koriste botnet za pokretanje napada već prodaju pristup mreži drugim napadačima koji tada koriste botnet kao zombi mrežu za svoje potrebe.[36].

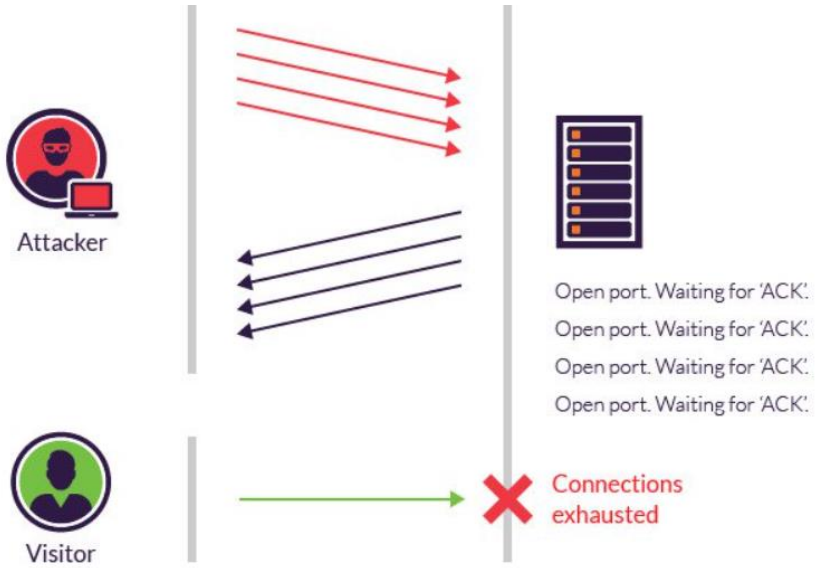
4.2.1.2 FLOOD ATTACK

Ovo je vrsta napada koja se temelji na uskraćivanju usluge. Cilj je iskoristiti TCP protokol kako bi se ciljani poslužitelj natjeralo da ne reagira. Počinitelj šalje zahtjeve za povezivanje toliko brzo da ih ciljani poslužitelj ne može obraditi i nastaje zastoj u mreži. Napad se odvija u tri faze:

1. Klijent zahtijeva konekciju šaljući sinkronizirajuću poruku (SYN)

2. Server na klijentov zahtjev odgovara slanjem potvrde sinkronizacije (SYN- ACK)
3. Klijent potvrđuje serverovu poruku(ACK) i veza je uspostavljena

Napadač zatrpava odabrani poslužitelj porukama koje najčešće šalje sa lažne IP adrese. Poslužitelju svi SYN paketi izgledaju ispravni i klijentu šalje SYN -ACK paket, ali od klijenta nikada ne dobije ACK paket. Tijekom tog vremena server ne može zatvoriti konekciju, a napadač šalje nove pakete što uzrokuje prelijevanje koje dovodi do kvara i zastoja rada servera. [33].



Slika 5 flood attack IZVOR: https://www.imperva.com/learn/ddos/syn-flood/

4.2.1.3 TEARDROP NAPAD

Ovo je tip DOS napada koji za cilj ima učiniti server nedostupnim preplavljujući mrežu zahtjevima. Napadač šalje ciljanom serveru fragmente paketa i u slučaju da je protokol TCP ranjiv, server ne može sastaviti paket i nastaje preopterećenje.

Starije verzije Windowsa i Linuxa imaju grešku pri ponovnom sastavljanju fragmentiranih dijelova TCP -a, a ovakvi napadi nastoje iskoristiti tu slabost. Klijent namjerno šalje fragmente informacija koji se preklapaju što onemogućava ponovno sastavljanje paketa i nastaje greška, a napadom se izaziva pad sustava ili aplikacije.[32].

4.2.1.4 SMURF NAPAD

Smurf je tip DDOS napada, a događa se na mrežnom sloju. Naziv je dobio po zlonamjernom softveru DDoS.Smurf koji je dobio ime po Štrumfovima, a napadi su slični flood napadima. Haker preopterećuje računala echo zahtjevima protokola internetske kontrolne poruke (ICMP), koji su još poznati i kao ping. Uloga ICMP-a je utvrditi da poruke stižu na odredište u pravo vrijeme. Cilj ovog napada je iskoristiti ranjivosti IP i ICMP protokola. Odvija se u tri faze:

1. Proces lažiranja- DDOS.Smurf pridružuje paket lažnoj IP adresi
2. Paket sadrži ICMP ping poruku koja naređuje mrežnim čvorovima da pošalju odgovor
3. Nastaje beskonačna petlja koja zatrpava server zahtjevima [34].

4.2.1.5 PING OF DEATH

Ping of deth (PoD) je podtip DOS napada kojim napadač nastoji destabilizirati ciljano računalo šaljući pakete zaražene malverima i prevelikim paketima koristeći se naredbom ping. Ispravan paket ima veličinu zaglavlja od 65 535 bajta. Mnogi povijesni računalni sustavi nisu mogli upravljati većim paketima pa bi se srušili. Kako slanje paketa većeg od 65 535 bajta krši internetski protokol, napadači bi slali deformirane pakete u fragmentima, a kada sustav pokuša povezati dijelove paketa u jedan dolazi do rušenja sustava. Napadači koji se koriste ovom metodom ne trebaju detaljne podatke osim IP adrese računala kojeg napadaju.[35].

4.2.2 MAN-IN-THE-MIDDLE (MITM)NAPADI

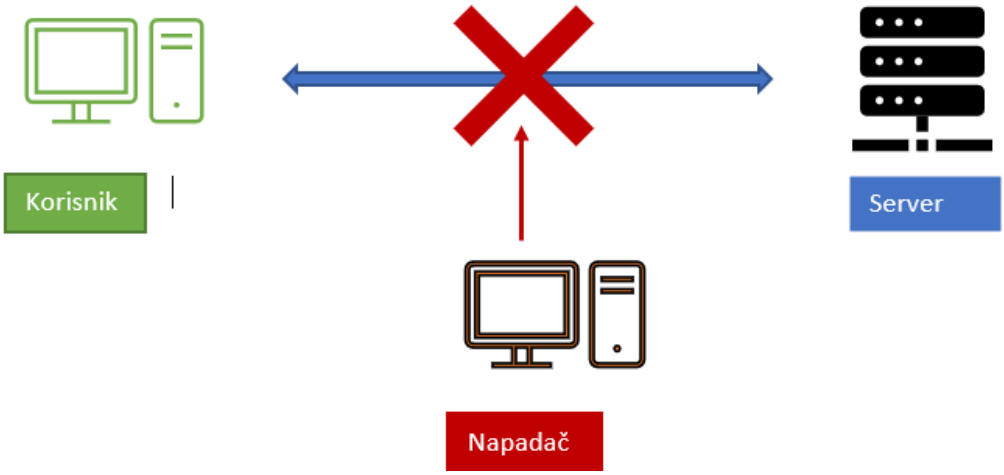
MITM napad se događa kada haker 'uskoči' između komunikacije servera i klijenta. Neki od najčešćih takvih napada su: Session hijacking, IP spoofing i replay. Trenutno ne postoji jedinstvena tehnika kojom bi se moglo odbraniti od svih MITM napada. Šifriranje i digitalni certifikati su poprilično učinkoviti, ali ne u potpunosti.[23].

4.2.2.1 IP SPOOFING

Ovaj tip napada se koristi kako bi se sustav uvjerilo da komunicira sa pouzdanim entitetom i na taj se na taj napadaču osigura pristup sustavu. Napadač izabere host i šalje mu paket sa IP adresom, ali ne svojom nego nekom drugom adresom koja je pouzdana.[23].

4.2.2.2 SESSION HIJACKING

U ovom tipu napada, napadač otme sesiju između pouzdanog klijenta i servera. Napadajuće računalo zamjenjuje svoju IP adresu pouzdanim klijentom dok poslužitelj nastavlja sesiju, vjerujući da komunicira s klijentom. Na sljedećoj slici se može vidjeti primjer jednog takvog napada.



Slika 6 Session hijacking IZVOR: Session Hijacking in Ethical Hacking ,https://www.certiology.com/computing/certified-ethical-hacker/ethical-hacking-study-guide/session-hijacking-in-ethical-hacking.html

Klijet uspostavi kontakt sa serverom, ali napadač sa svog računala nastoji diskonektati korisnika. Napadač uzima korisnikovu adresu i sa svojim računalom nastavi komunicirati sa serverom.[23].

4.2.2.3 REPLAY NAPAD

Replay napad ili ponavljajući napad se događa kada napadač presretne podatke, spremi ih i kasnije ih pokuša ponovno poslati pretvarajući se da je jedan od sudionika. Ovakvi napadi se mogu spriječiti metodom šifriranja.[23].

Kao što je ranije navedeno za cyber napade, šifriranje i certifikati predstavljaju određenu razinu zaštite, ali to ponekad nije dovoljno. U idućem primjeru će biti razmotren slučaj kada šifriranje nije od velike pomoći.

Do replay napada dolazi kada napadač presretne i spremi staru poruku, a kasnije je pokuša ponovno poslati lažno se predstavljajući kao jedan od sudionika. Trenutno nema jedinstvene tehnologije koja bi spriječila sve MITM napade. Enkripcije i digitalni certifikat pružaju povjerljivost i integritet podataka, ali može se dogoditi da se napadač ubaci u sredinu protoka informacija na način da kriptiranje neće pomoći.

Za sigurno komuniciranje između klijenta i servera, koriste se javni i privatni ključevi. Recimo da napadač koji je osoba A presretne javni ključ osobe P i zamijeni ga svojim ključem. Svi koji žele slati poruku će za šifriranje koristiti javni ključ od osobe P koji je sada zamijenjen ključem napadača. U ovom slučaju se može vidjeti da osoba A može čitati i modificirati poruke, a da osoba P toga nije ni svjesna.

Kako riješiti ovaj problem? Postoje posebni certifikati i hash funkcije. Kada osoba 2 (P2) želi poslati poruku P-u, a P želi biti sigurna da A neće pročitati ili izmijeniti poruku i da je poruka zapravo došla s P2, mora se koristiti sljedeća metoda:

Prvo P2 stvara simetrični ključ i šifrira ga P- ovim javnim ključem, a potom P2 šalje šifrirani simetrični ključ P-u. Za poruku se računa hash funkcija koja se digitalno potpisuje. P2 zatim šifrira poruku i potpisuje ju simetričnim ključem i sve to šalje P-u. P prima simetrični ključ od P2 jer samo on ima privatni ključ za dešifriranje. P može dešifrirati poruku jer samo on ima simetrični ključ. Na taj način može se potvrditi da poruka nije bila izmijenjena.[26].

4.3 CYBER NAPAD -KORIŠTENJE SLABE LOZINKE

Za većinu ljudi 2021. godina je i dalje izazovna, no uz pandemiju neki su imali i problema sa cyber napadima. U siječnju ove godine jedan britanski par neugodno se iznenadio kada ih je na vratima njihovog doma dočekala policija. Policija je istraživala teške zločine koji su uključivali istragu nad slikama djece koja su bila zlostavljana, a kasnije su te slike dospjele i online.

Nacionalna krim policija je istragom utvrdila da su slike objavljene prije godinu dana upravo sa njihove IP adrese. Da situacija bude još gora, policija im je oduzela mobitele, tablete i računala, a kako je cijela Engleska bila u to vrijeme u lockdownu, obadvoje su morali raditi od doma, a djeci je nastava bila online. Naravno policija je morala javiti socijalnoj službi da je par osumnjičen za zlostavljanje djece, što po Engleskim zakonima spada pod B kategoriju teških

zločina. Ubrzo je i socijalna služba javila školi u koju idu njihova djeca, pa im je bilo zabranjeno pojavljivati se u blizini škole.

U veljači im je prijatelj koji radi u cyber sigurnosti predložio da provjere router i pokušaju pronaći tragove. Kada su kupili Vodafone router nisu mijenjali lozinku, jer kako i sami kažu nitko im nije rekao da to moraju učiniti. Stručnjak za cyber sigurnost Ken Munro je rekao kako hakerima treba svega nekoliko minuta da probiju takvu šifru, a nakon toga drugi korak je mijenjanje konfiguracije rutera.

U ožujku, kada je slučaj zatvoren, policajac koji im je bio dodijeljen je okrivio neovlaštenu uporabu njihove wi-fi mreže. Par je podnio predmetni zahtjev za pristup Vodafonu kako bi provjerili mogu li pronaći dokaze o neovlaštenoj upotrebi njihovog Wi-Fi-a, ali Vodafone je rekao da nema evidenciju o njihovoj internetskoj aktivnosti.

Problem je zapravo nastao u slaboj lozinci routera, ali i u činjenici da bi provajderi Internet usluga trebali više poticati svoje korisnike na mijenjanje početnih lozinki.[25].

Povijesno gledano, organizacije i vlade zauzele su se reaktivnim pristupom „usmjerenih proizvoda“ u borbi protiv cyber prijetnji, proizvodeći nešto zajedno, pojedinačne sigurnosne tehnologije, jednu na drugu, kako bi zaštitile svoje mreže i vrijedne podatke. Ova metoda je složena i skupa, a i nije postigla željene rezultate jer i dalje dominiraju naslovi o cyber napadima.[34].

4.4 SLUČAJ UBER

Krađa podataka se događa svaki dan, no to sve može utjecati i na ugled tvrtke, što će nanijeti veliku štetu prihodima te tvrtke. Jedan od nedavnih velikih cyber-napada je otkrivanje kršenja osobnih podataka za oko 57 milijuna korisnika Ubera i 600 000 Uberovih vozača. Ovo je primjer kako ne treba postupiti prilikom hakerskih napada.

Dva hakera su 2016. godine uspjela doći do podataka korisnika uključujući njihove mailove, brojeve mobitela i imena. Uspjeli su ukrasti 600 000 podataka o vozačkim dozvolama. Hakeri su preko treće strane uspjeli pristupiti Uberovom Git Hub računu, na kojem su našli podatke koji su im omogućili pristup korisničkim podacima u AWS-u. Uber je tada platio tim hakerima 100 000 dolara da trajno unište sve podatke do kojih su došli. Uber je javio svojim korisnicima

da su podaci uništeni. Prema američkim agencijama za provođenje zakona, svako kršenje treba prijaviti vlastima, a ne plaćati hakere. Kada se saznalo za ovo Uber je morao platiti 20 mil dolara. No ovakvo ponašanje Ubera potaklo je druge hakere na ucjenjivanje Netflixa.[23].

4.5 SAVJETI KAKO RIJEŠITI OVAKVE PROBLEME

Postoje tehnike kojima se može poboljšati cyber sigurnost:

- Kontrola pristupa i zaštita lozinkom korisničkog imena glavna je metoda za osiguravanje podataka
- Antivirusni softveri
- Firewall
- Malware skeneri [23].
- Ne instalirati aplikacije iz nepoznatih izvora
- Ne otvarati nepoznate i sumnjive mailove
- Onemogućiti nepoznate ekstenzije fajlova
- Napraviti backup svih podataka
- Zaključavanje IP adrese

Zaštita računala započinje instalacijom antivirusnog softvera i firewall-a. Bitno je ne zanemarivati ažuriranje softvera, te ne otvarati sumnjive mailove i ne preuzimati nepoznate privitke iz takvih mailova. Nije loša navika isključiti i odspojiti računalo sa Interneta ukoliko ga korisnik ne namjerava više koristiti.[31].

5 POLITIČKA PERSPEKTIVA

5.1 EU

Europska unija je donijela direktivu koja se odnosi na zaštitu privatnosti i obradu osobnih podataka u sektoru elektroničkih komunikacija. Direktiva o privatnosti i elektroničkoj komunikaciji bavi se upotrebom kolačića. Njena uloga je osigurati krajnjim korisnicima povjerenje u tehnologije koje se bave elektroničkom komunikacijom. Dio odredbi se odnosi na neželjenu poštu, pristanak korisnika i instaliranje kolačića.

Kolačići mogu biti legitiman i koristan alat, osobito u analizi učinkovitosti dizajna web stranice i oglašavanja, te u provjeri identiteta korisnika. Po regulativi legitimno korištenje kolačića znači korisnicima pružiti jasne i precizne informacije o svrsi kolačića i sličnih tehnologija. Korisnicima se također mora ponuditi mogućnost odbijanja pohrane takvog uređaja u svojoj memoriji. To je izrazito bitno kada i druge osobe ili tehnologije imaju pristup podacima koji su pohranjeni na uređaju korisnika. Pravo na odbijanje može se jednom ponuditi za različite uređaje i pokriva svako iduće povezivanje i korištenje opreme preko iste veze. Način na koji se korisniku prikazuju informacije ili nuđenje prihvaćanja i odbijanja pristanka treba biti što jednostavnije i razumljivije. Pristup određenim dijelovima web stranice može i dalje biti uvjetovan korištenjem kolačića ako se on koristi u legitimne svrhe.

U direktivi se navodi da treća strana može pohraniti podatke na korisnikovo računalo ili dobiti pristup informacijama koje se već nalaze na računalu, pa je bitno da korisnik dobije jasne i sveobuhvatne informacije prilikom obavljanja neke aktivnosti koja bi za rezultat imala pohranu informacija. Tamo gdje je to moguće, potrebno je u skladu sa odredbama direktive omogućiti korisniku pristanak ili odbijanje obrade podataka u postavkama preglednika.

U izmijenjenoj verziji Direktive stoji da korisnici moraju dati pristanak za pohranjivanje podataka i za pristup već pohranjenim informacijama. Ove odredbe štite korisnikove privatne informacije od zlonamjernog softvera ili virusa, ali to se također odnosi i na kolačiće. Web stranice koje provode oglašavanje ili broje posjetitelje zahtijevaju pristanak korisnika za korištenje kolačića.

I u ovoj deklaraciji postoji niz stavki koje je potrebno razjasniti. Neka od pitanja na koje se traži valjan odgovor su: predstavljaju li postavke preglednika valjani pristanak ili ne, a obrada

podataka bez poznavanja svrhe u koju se obrada provodi ne može dobiti valjani pristanak. Također, uvjet pristanka se po Direktivi odnosi samo na kolačiće koji se bave prikupljanjem osobnih podataka.

Zbog nacionalne prilagodbe, države članice imati će priliku pojasniti i/ili navesti neke aspekte Direktive kao što je npr. Velika Britanija kopirala tekst direktive u nacionalno pravo. ENISA je provela istraživanje u kojem se jasno vidi kako se osobni podaci prenose van EU i to za gotovo polovinu ispitanih. Problem je u tome što su van EU provedbe drugačije.[29].

5.2 PROVEDBE VAN EUROPE

Vlada Sjedinjenih Američkih Država je 2000. godine objavila novi memorandum vezan uz upotrebu kolačića sa svrhom zaštite svojih građana. Zahvaljujući tom memorandumu je ograničena upotreba kolačića.[29].

OMB je 2009. godine počeo preispitivati politiku kolačića kako bi se pronašla ravnoteža između privatnosti građana i korištenja kolačića. U srpnju 2009. godine objavljen je javni poziv za reviziju Politike o tehnologijama praćenja weba za savezne web stranice. U lipnju 2010. godine nakon otvorenog savjetovanja, objavljena su dva memoranduma -Vodič za internetsku upotrebu weba tehnologijom mjerenja i Prilagodbe i smjernice za agencijsku upotrebu web stranica trećih strana. Tim dokumentima su uvedene određene zabrane, razine upotrebe, jasne obavijesti o osobnoj upotrebi, zaštiti privatnosti i ograničenjima zadržavanja podataka.

Nakon što su ažurirane smjernice o korištenju tehnologija poput kolačića, objavljena je i web stranica sa uputama za isključivanje kolačića. Stranica je prilagođena najpopularnijim preglednicima na računalima i mobitelima.

Kanadski ministar financija je 2002. godine izdao smjernice za uporabu kolačića na web stranicama kanadske vlade, a 2010. godine je izdan i Nacrt izvješća o konzultacijama o internetskom praćenju, profiliranju i ciljanju te računalstvu u oblaku. Svrha ovog nacrta je bila analizirati tehnološke trendove sa sigurnosnog aspekta. Između ostalog treba istaknuti i Zakon o zaštiti osobnih podataka i elektroničkim dokumentima, ali i dalje postoji dosta nejasnoća i stavki koje se trebaju razjasniti i doraditi kao što su npr. osobni podaci, određivanje odgovarajućih oblika pristanka i ograničavanje uporabe osobnih podataka.

Centar za zagovaranje javnih interesa je ispitivao stavove kanadskih potrošača. Polovina ispitanika koji koriste Internet nije bila upoznata sa kolačićima, pa je prijeko potrebno povećati svijest o manama i prednostima njihove upotrebe.[29].

6 ZAKLJUČAK

U ovom su radu ukratko prikazani neki od najčešćih vrsta kolačića na koje se može naići pretraživanjem Interneta. Prvotna namjena kolačića bila je pojednostavniti i olakšati proces prijavljivanja. Cilj je bio omogućiti korisniku obavljanj logiranja u par klikova miša, a da pritom ne mora svaki put ponavljati isti postupak. S vremenom su kolačići dobili i mnogo veće uloge koje su uključivale oglašavanje, profiliranje, praćenje itd.

Glavni cilj ovog rada je uputiti korisnike na značenje pojmova sigurnosti, cyber napada, privatnosti i kolačića, načina na koji su oni povezani, kako utječu jedni na druge, ali i istaknuti gdje vrebaju opasnosti te kako se zaštiti i po mogućnosti svesti rizik na minimum.

Industrija oglašavanja je uvelike utjecala na razvoj kolačića. Vremenom su kolačići postajali sve snažniji. Može se reći da su neki od njih kao Flash kolačići postali i neuništivi, no sve više se i kod korisnika pojavljivala zabrinutost o tome kako kolačići i u kojoj mjeri utječu na privatnost. Takvoj zabrinutosti su pridonijeli i mnogobrojni cyber napadi. Neki od njih su obrađeni i objašnjeni u ovom radu.

Kako bi se zaštitilo korisnike, pojedina državna tijela su donijela propise i zakone po kojima svaki korisnik ima pravo znati kako web stranica namjerava koristiti njegove/njezine podatke, te su im omogućili izbor prihvaćanja ili odbijanja kolačića. Velika većina korisnika ima skromno znanje u području IT-a, pa je potrebno što više takvih korisnika osvijestiti o mogućnosti uklanjanja kolačića i mehanizmima kojima se to može postići.

Na preglednicima i razvojnim programerima je da učine što više kako bi korisnici mogli sami kontrolirati razinu na kojoj ih kolačići prate. To je naravno vrlo teško postići jer postoje kolačići nad kojima preglednici nemaju utjecaj kao što su supercookies ili everookies.

Trenutno korisnici nemaju veliki utjecaj nad kolačićima. Često se pristup sadržaju uvjetuje prihvaćanjem kolačića i tako se i korisnicima nude samo dvije mogućnosti ili da prihvate kolačiće ili da ih odbace. Web preglednici su počeli nuditi mogućnosti brisanja, ali to onda

znači i gubljenje povezanosti sa serverom, koji onda pri svakom novom pristupu ponovno zahtijeva ponovni unos podataka.

S razvojem novih tehnologija, ljudi traže nove načine na koje bi mogli zaštiti osobne podatke. Hakeri pak uvijek traže način kako da se domognu takvih osjetljivih podataka i zato je ključno zaštiti računalo instaliranjem firewall-a i antivirusnih softvera. Kolačići nisu napravljeni radi sigurnosti i ne jamče pouzdanost ni integritet.

7 BIBLIOGRAFIJA

1. Beauvisage, Kevin Mellet & Thomas. Cookie monsters. Anatomy of a digital market infrastructure, Consumption Markets & Culture. 2019, str. 116-117, .

2. Kihn, Martin. Cookies, Chaos and the Browser: Meet Lou Montulli. [Mrežno] 6. 2 2018. [Citirano: 14. 6 2021.] https://blogs.gartner.com/martin-kihn/cookies-chaos-and-the-browser-meet-lou-montulli/.

3. Shahid, Haris. PUREVPN. *What Is Internet Privacy & Why It Matters so much in 2021?* [Mrežno] 20. Veljača 2020. [Citirano: 14. 6 2021.] https://www.purevpn.com/blog/what-is-internet-privacy-scty/.

4. CookiePro. [Mrežno] 11. prosinac 2020. [Citirano: 14. 6 2021.] https://www.cookiepro.com/knowledge/whats-the-difference-between-first-and-third-party-cookies/.

5. Hill, Simon. Are cookies crumbling our privacy? We asked an expert to find out. [Mrežno] 29. 3 2015. [Citirano: 14. 6 2021.] https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy.

6. Brain, Marshaill. How Internet Cookies Work. [Mrežno] [Citirano: 14. 6 2021.] https://computer.howstuffworks.com/cookie.htm.

7. David M. Kristol, Bell Labs. HTTP Cookies: Standards, Privacy, and Politics. [Mrežno] 9. 5 2001. [Citirano: 15. 6 2021.] https://arxiv.org/pdf/cs/0105018.pdf.

8. CookiePro. [Mrežno] 11. 11 2020. [Citirano: 15. 6 2021.] https://www.cookiepro.com/knowledge/whats-the-difference-between-first-and-third-party-cookies/.

9. Cookie Script. [Mrežno] 25. 5 2021. [Citirano: 15. 6 2021.] https://cookie-script.com/all-you-need-to-know-about-third-party-cookies.html.

10. Technopedia. [Mrežno] [Citirano: 15. 6 2021.] https://www.techopedia.com/definition/27673/html5-cookie.

11. MIKA D. AYENSON, , DIETRICH J. WAMBACH,ASHKAN SOLTANI,NATHANIEL GOOD,CHRIS JAY HOOFNAGLE. FLASH COOKIES AND PRIVACY II:NOW WITH HTML5 AND ETAG RESPAWNING. [Mrežno] [Citirano: 15. 6 2021.] https://ptolemy.berkeley.edu/projects/truststc/education/reu/11/Posters/AyensonMWambachDpaper.pdf.

12. Degges, Randall. DEV Community. [Mrežno] 30. 1 2018. [Citirano: 15. 6 2021.] https://dev.to/rdegges/please-stop-using-local-storage-1i04.

13. Madushanka, Ruwan. ResearchGate. *Cookies, Privacy and Cyber Security.* [Mrežno] 29. 8 2019. [Citirano: 16. 6 2021.] https://www.researchgate.net/publication/347015177_Cookies_Privacy_and_Cyber_Security.

14. technopedia. [Mrežno] [Citirano: 16. 6 2021.] https://www.techopedia.com/definition/4910/session-cookie.

15. Beckstrom, Matthew. *Protecting Patron Privacy: Safe Practices for Public Computers.* Santa Barbara, California : LIBRERIES UNLIMITED, str. 87.

16. Mitnick, Kevin. *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data.* s.l. : Little Brown and Company, 2019, str. 87.

17. [aut. knjige] Daniel R. Bestor. Eric Hamp. *Northwestern Journal of Technology & Intellectual Property.* s.l. : North Western , 2010, str. 35.

18. WIRED. [Mrežno] 12. 5 2010. [Citirano: 16. 6 2021.] https://www.wired.com/2010/12/zombie-cookie-settlement/.

19. technopedia. [Mrežno] 2. 1 2014. [Citirano: 17. 6 2021.] https://www.techopedia.com/definition/4901/persistent-cookie.

20. Schmidt, Jonathan. [Mrežno] 6. 3 2020. [Citirano: 18. 6 2021.] https://faui1-files.cs.fau.de/public/publications/df/df-whitepaper-18.pdf.

21. Dodt, Claudio. INFOSEC. [Mrežno] 7. 7 2020. [Citirano: 19. 6 2021.] https://resources.infosecinstitute.com/topic/cookies-an-overview-of-associated-privacy-and-security-risks/.

22. Lynn, Bryan. Learning English. [Mrežno] 10. 3 2021. [Citirano: 19. 6 2021.] https://learningenglish.voanews.com/a/will-the-end-of-internet-cookies-bring-more-user-privacy-/5809138.html.

23. Rohit Kalakuntla, Anvesh Babu Vanamala,Ranjith Reddy Kolipyaka. ResearchGate. [Mrežno] 2019. [Citirano: 19. 6 2021.] https://www.researchgate.net/publication/335322600_Cyber_Security.

24. kaspersky. [Mrežno] [Citirano: 19. 6 2021.] https://www.kaspersky.com/resource-center/definitions/replay-attack.

25. *Did weak wi-fi password lead the police to our door?* Wakefield, By Jane. 2021, BBC NEWS.

26. Seemma P.S, Nandhini Sundaresan,Sowmiya M. ResearchGate. [Mrežno] 11. 11 2018. [Citirano: 20. 6 2021.] https://www.researchgate.net/publication/329678338_Overview_of_Cyber_Security.

27. Melnick, Jeff. netwrix. [Mrežno] 15. 5 2015. [Citirano: 20. 6 2021.] https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.

28. rewotech. [Mrežno] 5. 4 2021. [Citirano: 21. 6 2021.] https://revotech-networks.com/everyone-loves-cookies-even-cybercriminals/.

29. enisa. enisa. [Mrežno] 2. 2 2011. [Citirano: 3. 7 2021.] https://www.enisa.europa.eu/publications/copy_of_cookies.

30. P.S.Seemma, , S.Nandhini,M.Sowmiya. [Mrežno] 11 2018. [Citirano: 24.6. 6 2021.] https://ijarcce.com/wp-content/uploads/2018/12/IJARCCE.2018.71127.pdf.

31. Hoster, Planet. *10 Steps to Protect Your Computer from Cyber Threats.* [Mrežno] 15. 10 2020. [Citirano: 14. 8 2021.] https://blog.planethoster.com/en/10-steps-to-protect-your-computer-from-cyber-threats/.

32. F5 GLOSSARY. *What Is a Teardrop Attack?* [Mrežno] [Citirano: 14. 8 2021.] https://www.f5.com/services/resources/glossary/teardrop-attack.

33. imperva. *TCP SYN Flood.* [Mrežno] [Citirano: 14. 8 2021.] https://www.imperva.com/learn/ddos/syn-flood/.

34. FORTINET. [Mrežno] [Citirano: 14. 8 2021.] https://www.fortinet.com/resources/cyberglossary/smurf-attack.

35. imperva. [Mrežno] [Citirano: 14. 8 2021.] https://www.imperva.com/learn/ddos/ping-of-death/.

36. *Botnet Attacks – Everything You Need to Know.* [Mrežno] 17. 5 2021. [Citirano: 15. 9 2021.] https://www.cdnetworks.com/cloud-security-blog/botnet-attacks/.

37. Kaspersky. Securelist. [Mrežno] 29. 3 2009. [Citirano: 22. 9 2021.] https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/.

38. Brute Force Attack: Definition and Examples. *kaspersky.* [Mrežno] [Citirano: 22. 9 2021.] https://www.kaspersky.com/resource-center/definitions/brute-force-attack.

39. Dougal, Nikita. [Mrežno] 14. 6 2021. [Citirano: 22. 9 2021.] https://www.simplilearn.com/top-cybersecurity-trends-article.

40. Staff, Alert Logic. ALert Logic. [Mrežno] 20. 1 2021. [Citirano: 21. 9 2021.] https://www.alertlogic.com/blog/top-cloud-vulnerabilities/.

41. imperva. *Phishing attacks.* [Mrežno] [Citirano: 21. 9 2021.] https://www.imperva.com/learn/application-security/phishing-attack-scam/.

42. Balbix. [Mrežno] [Citirano: 22. 9 2021.] https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.

8 SUMMARY

Cookies, privacy and cyber security

The purpose of this final paper is to raise awareness about the threats lurking on the Internet that most users are not even aware of. Concepts such as cookies, type of cookies, privacy and cyber security, behaviour of the cookies and the risks of their use, as well as the history of the cookies and their original purpose are discussed in the first part of the paper.

In addition to illustrating the concept of cyber security, it is also crucial to depict the trends – what are the most often targets of hackers attacks and what is the role of media in finding out the personal information. It is also important not to forget the consequences for such actions. In the second part of this paper some examples of the most notorious cyber-attacks are mentioned, as well as the connection between such threats and cookies and the way that cookies are threatening the privacy.

The final part is about protection under the laws elected by the EU and other countries, but also showing how these laws are enforced.

KEY WORDS: cookies, security, privacy, cyber-attacks and protection

9 TABLICA SLIKA

Slika 1 PRIMJER FIRST PART COOKIE, IZVOR: Autor 5
Slika 2 PRIMJER THIRD PART COOKIE, IZVOR: Autor 7
Slika 3 PRIMJER KOLAČIĆA SESIJE ,IZVOR: Autor 8
Slika 4 IZVOR: Cyber Security ,sciendo , HOLISTICA Vol 10, Issue 2, 2019, pp. 115-128 20
Slika 5 flood attack IZVOR: https://www.imperva.com/learn/ddos/syn-flood/ 22
Slika 6 Session hijacking IZVOR: Session Hijacking in Ethical Hacking ,https://www.certiology.com/computing/certified-ethical-hacker/ethical-hacking-study-guide/session-hijacking-in-ethical-hacking.html 24