VODIČ:

OSNOVE DIGITALNE BEZBED-NOSTI

SHARE FOUNDATION - 2015

vodič

"VODIČ: OSNOVE DIGITALNE BEZBEDNOSTI"
SHARE FOUNDATION
MART 2015
UREDNICI: Vladan Joler, Đorđe Krivokapić
TEKSTOVI: Andrej Petrovski
LEKTURA: Bojan Perkov
DIZAJN I PRELOM: Olivia Solis Villaverde

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ : 200

PODRŠKA PROJEKTU:

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

Kingdom of the Netherlands

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
004.738.5.056(036)
ПЕТРОВСКИ, Андреј
Osnove digitalne bezbednosti : vodič / [tekstovi Andrej Petrovski]. - Novi Sad : Share fondacija, 2015 (Novi Sad : NS press). - 36 str. : ilustr. ; 16 cm
Tiraž 200.
ISBN 978-86-89487-01-5
a) Интернет - Безбедност - Водичи
COBISS.SR-ID 295461383

UVOD

ZAŠTO SU INTERNET PRIVATNOST I BEZBEDNOST BITNI?

KONCEPT PRIVATNOSTI JE RELATIVNO JASAN U NE-DIGITALNOM OKRUŽENJU. SVAKA OSOBA JE SVESNA SVOJE PRIVATNOSTI I TRUDI SE DA JE ZAŠTITI DO MERE KOJA JOJ ODGOVARA.

Situacija je malo drugačija u digitalnom okruženju. Ljudi nisu svesni kada su sami, a kada nisu dok su online, pa samim tim često ne znaju da li se zna šta su oni radili online i ko može to da sazna. Sa druge strane, digitalna bezbednost je dosta širi koncept, koji obuhvata privatnost, ali i neke dodatne stvari. Preciznije, digitalni sistem koji nije bezbedan ne može se smatrati privatnim, dok samim tim što sistem ima obezbeđenu privatnost, ne znači da je potpuno bezbedan.

Postoji čitav niz faktora koji utiču na to da li će sistem biti bezbedan ili ne. Pre svega, to su tehnološki faktori, tj. da li je sistem tehnološki kompromitovan ili ranjiv i koji je nivo bezbednosti koji sami uređaji i programi koji su instalirani pružaju. Zatim, postoje i ne-tehnološki faktori, odnosno određene navike korisnika, koji su takođe veoma bitni. Opšte pravilo jeste da bezbednost nije urođena karakteristika digitalnih sistema, te da bi sistem bio bezbedan moraju se preuzeti određene aktivnosti.

Svaki korisnik tokom svojih online aktivnosti ostavlja određene tragove, "senku" koja ga prati dok se kreće kroz sajber prostor. U digitalnom okruženju, slično kao i u ne-digitalnom, ove senke daju određene karakteristike vlasnika senke. Analizom senke može se doći do određenih informacija koje su od važnosti napadačima koji imaju za cilj da uđu u određeni sistem. Prednost digitalne sredine je to što korisnici donekle mogu da kontrolišu oblik svoje senke ukoliko povedu računa o određenim stvarima, što je i tema ovog vodiča.

KLJUČNI TERMINI

INTERNET PRIVATNOST je oblik lične privatnosti koji se odnosi na čuvanje, reprodukciju, deljenje sa trećim licima i prikazivanje informacija koje pripadaju određenoj osobi, preko Interneta.

INTERNET BEZBEDNOST je zaštita online naloga, računara, datoteka i sistema od napada spoljnih subjekata.

SAJBER PROSTOR je apstraktna sredina u kojoj se odvija komunikacija između računarskih mreža.

INFORMACIONI SISTEM (IS) je sistem koji se sastoji od ljudi i računara u kome se obrađuju i tumače određene informacije.

OPERATIVNI SISTEM (OS) je programski sistem koji korisnicima računara omogućava rad, odnosno koji prenosi korisničke komande uređaju koji izvršava određene operacije.

HAKER (HACKER) je osoba koja nalazi, iskorišćava nedostatke i prilagođava IS i kompjuterske mreže svojim potrebama.

KRAKER (CRACKER) je haker koji nalazi i iskorišćava bezbednosne nedostatke u IS i kompjuterskim mrežama zbog malicioznosti ili lične dobiti. (Ergo, nisu svi hakeri loši)

KLIJENT ili korisnik u tehničkom smislu je računar koji se koristi za pristup Internetu.

SERVER je vrsta računara, koji ima znatno jaču specifikaciju od klijenta i na njemu se čuvaju (hostuju) sadržaji različite vrste, web strane, datoteke (fajlovi), e-mail poruke itd.

WWW (WORLD WIDE WEB) je IS međusobno povezanih web sajtova koji su dostupni preko Interneta.

WEB PREGLEDAČ (WEB BROWSER) je program čija je namena pregledanje sadržaja sa WWW (npr. Firefox, Chrome, Internet Explorer, Opera, Safari itd)

WEB PRETRAŽIVAČ (SEARCH ENGINE) je web servis koji je deo WWW i koji omogućava lakše pretraživanje po WWW (npr. Google, Bing, DuckDuckGo itd)

URL (UNIFORM RESOURCE LOCATOR) je referenca na IP adresu web sajta. Standardni URL ima oblik http://www.example.com

IP (INTERNET PROTOCOL) adresa je osnovna ćelija Internet adresiranja. Svaki uređaj koji je povezan na Internet mora da ima bar jednu javnu IP adresu. Postoje dve verzije IP adresa koje se koriste: IPv4 i IPv6.

Primer IPv4 adrese:
98.139.180.149

Primer IPv6 adrese:
FE80:0000:0000:0000:0202:B3FF:-FE1E:8329

METAPODACI (METADATA) su podaci koji se automatski generišu od strane programa i uređaja koji se koriste za povezivanje na Internet. Metapodaci podrazumevaju lokaciju, datum, vreme, vrstu uređaja koji je korišćen itd.

MALWARE (MALICIOZNI SOFTVER) je opšti termin za softver koji se koristi za ometanje rada računara, prikupljanje osetljivih informacija ili dobijanje pristupa zaštićenom IS.

OPEN SOURCE je vrsta softvera čiji je izvorni kod (tekstualni fajl koji određuje funkcionisanje softvera) javno dostupan i svaki korisnik ima mogućnost da vrši reviziju i da ga prilagodi svojim potrebama. Open source softver je u najvećem broju slučajeva besplatan.

CLOUD TEHNOLOGIJA (CLOUD COMPUTING) je jedna od najnovijih Internet tehnologija koja se bazira na korišćenju resursa (protok podataka, prostor za skladištenje, radna memorija itd) na daljinu i njihovo deljenje između više aplikacija i korisnika. Cloud može biti privatan, javan ili hibridan.

KAKO NAVIKE KORISNIKA UTIČU NA NJIHOVU BEZBED-NOST?

ENKRIPCIJA

ENKRIPCIJA JE KRIPTOGRAFSKI KONCEPT KODIRANJA PORUKA ILI INFORMACIJA ČIME SE OSIGURAVA DA ĆE JEDINO OSOBE KOJE IMAJU NAČIN DA JE DEKODIRAJU (DEKRIPTUJU) MOĆI DA JE PROČITAJU.

Enkripcija kao koncept nije nova, postojala je još u starom Rimu. Tada su korišćeni primitivni algoritmi koji se uglavnom odnose na kreiranje novih slovnih skorišćenjem postojećih postojeće time što se redosled slova modifikuje na određeni način.

Savremena digitalna enkripcija proizlazi iz ovog koncepta, ali je toliko razvijena da se izdvojila kao potpuno novi i drugačiji pravac u kriptografiji. Izvorno, većina informacionih sistema nije enkriptovana, što znači da enkripcija mora da se postavi da bi postojala.

Veliki broj korisnika koji nema edukaciju o digitalnoj bezbednosti zanemaruje enkripciju i time izlažu rizicima sebe, ljude sa kojima komuniciraju i organizaciju u kojoj rade. Enkripcija se implementira na više nivoa, tj. enkripcija veze i enkripcija diska.

LOREM IPSUM ORIGINALNI TEKST

ERSPZHEBBZP73Z7YMBFFSA== ENKRIPTOVANO

BEZBEDNO PRETRAŽIVANJE

ZA PRETRAŽIVANJE INTERNETA KORISTE SE PROGRAMI KOJI SE ZOVU INTERNET PREGLEDAČI. TEHNIČKO PRETRAŽIVANJE PREDSTAVLJA PRISTUPANJE SADRŽAJU NA INTERNETU POMOĆU HTTP INTERNET PROTOKOLA.

Postoje različita komercijalna rešenja i svi na neki način obavljaju istu funkciju, ali da bi pretraživanje bilo bezbedno, potrebno je podesiti dodatne parametre i instalirati dodatne programe (plugins).

Osnovni nivo bezbednosti podrazumeva korišćenje SSL-a ili TLS-a. Ove tehnologije enkriptuju komunikaciju između klijenta i servera i tako efikasno štite od MitM napada. Na ovaj način je omogućen bezbedan prenos osetljivih podataka preko Interneta kao što su korisnička imena, šifre, poverljivi lični podaci (JMBG), podaci o platnim karticama, brojevima bankovnih računa itd. SSL se instalira na serveru, što znači da ne postoji kao opcija za svaki web sajt. Web sajtovi koji koriste SSL u URL adresi imaju ''https'' umesto standardnog ''http''.

Prilikom pretraživanja na Internetu, pored sadržaja koji se šalje i preuzima sa servera voljom korisnika, razmenjuju se i metapodaci. Logičkim mapiranjem metapodataka i njihovom analizom moguće je otkriti dosta značajnih informacija o korisniku, npr. sa kim, kada i sa koje geografske lokacije je

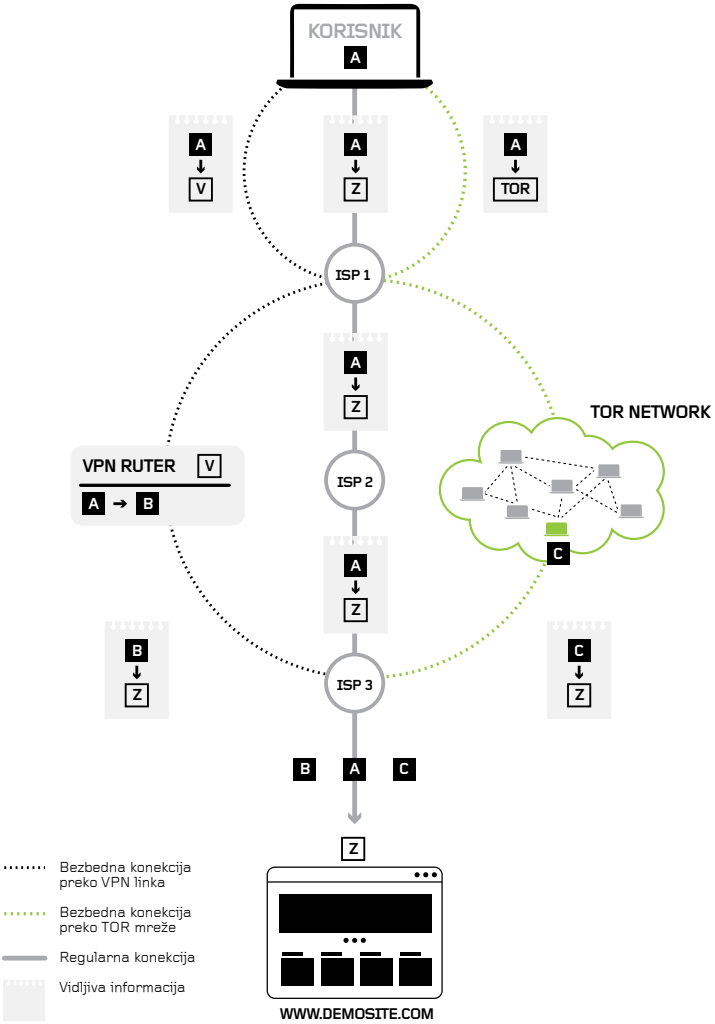
TOOL BOX:

Korišćenjem plugin-a **''HTTPS EVERYWHERE''** pregledač će automatski uvek učitavati bezbednu verziju web stranice. Plugin je dostupan na sledećem linku: https://www.eff.org/https-everywhere

PLUGIN ADBLOCK PLUS je dodatak za Internet pregledače koji blokira sadržaje trećih strana. Plugin je dostupan na sledećem linku: https://adblockplus.org/

DUCKDUCKGO je pretraživač koji prikuplja jako malo podataka o klijentima. Pretraživač je dostupan na sledećeg linku: https://duckduckgo.com/

Postoji posebna verzija Mozilla Firefox pregledača koja je podešena tako da koristi **TOR MREŽU** za pregledanje sadržaja na Internetu. Pregledač se može preuzeti sa sledećeg linka: https://www.torproject.org/download/download-easy.html.en


KORISNIK
A
A
V
A
Z
A
TOR
ISP 1
A
Z
TOR NETWORK
VPN RUTER
V
A → B
ISP 2
C
A
Z
B
Z
ISP 3
C
Z
B
A
C
Z
WWW.DEMOSITE.COM
Bezbedna konekcija preko VPN linka
Bezbedna konekcija preko TOR mreže
Regularna konekcija
Vidljiva informacija

korisnik komunicirao, koje sadržaje je pretraživao itd. Ovaj svojevrsni bezbednosni "nedostatak" se koristi za ciljano reklamiranje, pa zbog toga korisnici često prilikom pretraživanja dobijaju reklame koje su tematski slične nnjihovim prethodnim pretraživanjima. Pritom, reklame koje se učitavaju predstavljaju sadržaj trećih strana i one takođe skupljaju metapodatke o korisniku. Postoje dodaci za blokiranje reklama koje se dodaju pregledačima i blokiraju celokupan sadržaj trećih strana.

Ipak, konvencionalni pregledači ne rešavaju do kraja "problem" sa metapodacima. Trenutno aktuelne su tri tehnologije koje se koriste da bi se korisnicima omogućilo da sakriju deo metapodataka koji se odnosi na geolokaciju i vrstu uređaja koji se koristi. Time ova hardversko - softversko rešenja nude Internet anonimnost. Ove tehnologije su VPN, Proxy i TOR. Iskustvo je pokazalo da je najkonzistentnije rešenje upotreba TOR mreže.

TOR mreža je hibridno hardversko-softversko rešenje koje korisnicima omogućava anonimno povezivanje na Internet. Ova mreža ima karateristike VPN i Proxy-ja, u smislu da može da se koristi i samo u pregledaču, ali takođe postoji mogućnost da se posebnom konfiguracijom računara ceo saobraćaj preusmeri na TOR mrežu.

INFO BOX:

HTTP (HYPERTEXT TRANSFER PROTOCOL) je protokol kroz koji se odvija saobraćaj koji se odnosi na pretraživanje World Wide Web-a (WWW). Ovim protokolom je regulisana komunikacija između korisnika i servera na kom se sadržaj nalazi.

SSL (SECURITY SOCKET LAYER) je poseban sloj zaštite na HTTP Internet protokolu.

TLS (TRANSPORT LAYER SECURITY) je unapređena i novija verzija SSL-a.

MITM (MAN IN THE MIDDLE) napad je vrsta tehničkog napada u kom klijent i server nisu nužno kompromitovani, međutim veza između njih jeste, te napadač koristi nedostatke veze da bi imao pristup komunikaciji kako bi je kompromitovao.

BACKDOOR (SPOREDNI ULAZ) u IS je mehanizam zaobilaženja standardne forme autentifikacije i dobijanje neovlašćenog pristupa zaštićenom IS, pritom je specifično to što upadač ostaje nezapažen.

SADRŽAJ TREĆIH STRANA (THIRD PARTY CONTENT) je sadržaj koji korisnik nije direktno zahtevao, ali mu je prikazan zbog toga što je vlasnik zahtevanog sadržaja ustupio deo svog sajta trećim stranama (Google reklamama, Facebook komentarima itd).

VPN (VIRTUAL PRIVATE NETWORK) je Internet usluga koja omogućava povezivanje na privatnu mrežu kroz javnu mrežu kao što je Internet. VPN omogućava korisnicima da bezbedno šalju i primaju poverljive podatke kroz Internet.

PROXY je servis koji omogućava povezivanje na server na daljinu kroz koji se onda pristupa Internetu. Suštinska razlika između Proxy-ja i VPN-a jeste u tome što Proxy prolazi samo saobraćaj koji se odnosi na pregledač, dok VPN pokriva ceo saobraćaj koji proizilazi iz tog računara (uključujući Skype, e-mail klijente itd)

(Napomena: Ne preporučuje se korišćenje TOR mreža za skidanje velikih datoteka zbog toga što se mreža opterećuje i to utiče na njenu brzinu. Takođe, u slučaju da korišćeni program nije pouzdan, TOR ne može garantovati anonimnost)

AŽURIRANJE SOFTVERA

SVAKODNEVNO SE RAZVIJAJU NOVE VRSTE TEHNOLOŠKIH NAPADA I MALICIOZNOG SOFTVERA, TE ANTI-MALWARE APLIKACIJE SVAKODNEVNO AŽURURAJU SVOJE LISTE ČIME OMOGUĆUJU DA PROGRAM DETEKTUJE NAJNOVIJE VRSTE MALWARE-A.

Ni jedan softverski ili hardverski sistem nije potpuno savršen, odnosno svaki sistem ima nedostatke koji se mogu iskoristiti da bi se ostvario neovlašćeni pristup sistemu. Krakeri konstantno rade na pronalaženju i istraživanju ovih nedostataka čijom bi se eksploatacijom omogućio upad u sistem.

Zbog toga je bitno redovno ažurirati sve vrste aplikacija u okviru sistema, počevši od operativnog sistema, preko anti-malware aplikacija do aplikacija koje korisnik koristi svaki dan. Bitno je napomenuti da se preporučuje jedino in-

TOOL BOX

Windows i iOS korisnici mogu koristiti FileHippo App Manager koji je dostupan na sledećem linku: http://www.filehippo.com/download_app_manager/

Linux korisnici mogu koristiti Synaptic menadžer za update-ove koji je dostupan na sledećem linku: http://www.nongnu.org/synaptic/

staliranje aplikacija pouzdanih proizvođaća zbog toga što mnogi krakeri lažno predstavljaju svoj malware kao ažuriranu verziju programa. Da bi korisnici lakše znali koje aplikacije nisu ažurirane i da bi bili sigurni da će preuzeti prave ažurirane verzije programa, mogu koristiti različite aplikacije. U svakom slučaju preporučuje se da se koriste aplikacije koje samo obaveštavaju korisnika da treba da ažurira određeni softver, a da se ne dozvoljava da automatski preuzimaju ažurirane verzije programa.

(Napomena: Uvek je dobro videti recenzije o određenoj aplikaciji pre njene instalacije)

MALWARE

MALWARE JE NAJJEDNOSTAVNIJE REČENO SOFTVER KOJI KRAKERI KREIRAJU DA BI NAMERNO PRIČINILI ŠTETU NEKOM IS.

Najprepoznatljivija vrsta malware-a su računarski virusi, ali postoje i druge vrste kao što su trojanci, adware, spyware i crvi (''worms''). Svaka vrsta malware-a ima svoj način funkcionisanja, pa je zbog toga šteta koju nanosi svaki od njih različitog stepena.

I pored toga što postoje određene definicije i podele malware-a, kategorije se ne mogu definitivno razgraničiti, pa se često desi da jedan malware obavlja aktivnosti koji su karakteristični za druge vrste malware-a. Malware može raditi različite operacije, počevši od preusmeravanja na lažne web sajtove do destabilizacije čitavog sistema. Posebna vrsta malware-a su key logger-i, koji beleže svaki unos preko tastature i zapise šalju trećim licima. Takođe, postoji vrsta malware-a koja ima mogućnost da šalje i po nekoliko hiljada e-mail poruka sa zaraženog računara.

Malware se distribuira na različite načine. Najčešće korisnici sami preuzmu malware nekom svojm aktivnošću, ali kako instalirani programi komuniciraju na Internetu na različite načine zbog svoje aktivnosti, a svaki od njih ima po neki nedostatak koji napadači mogu iskoristiti, u većini slučaje-

TOOL BOX

Avira je jedan od najboljih besplatnih anti-malware programa. Program je dostupan na sledećem linku: http://www.avira.com/en/avira-free-antivirus

va ovi nedostaci se rešavaju, pa je zato bitno ažurirati programe.

Nije uvek jednostavno prepoznati malware, često se desi da korisnik u početku uopšte nije svestan da je njegov računar/sistem zaražen. Ponekad aktivnost malware-a može da se primeti zbog spontanog pogoršanja performansi sistema. Prosečni korisnici svakako ne mogu sami u potpunosti ukloniti malware bez upotrebe određenog anti-malware programa. Ovi programi vrše monitoring sistema, skeniraju fajlove koje preuzimaju sa Interneta i e-mail poruke, pa ukoliko pronađu neki malware oni ga stavljaju u karantin ili ga obrišu, u zavisnosti od podešavanja.

Ipak, nije dovoljno samo instalirati određeni program koji će da se bori protiv malware-a, bitno je da korisnici ne instaliraju aplikacije koje nisu pouzdane, da ne klikću na sumnjive linkove, ne otvaraju sumnjive e-mail poruke i da ne posećuju nepouzdane web sajtove.

INFO BOX

VIRUS je vrsta malware-a koji se sam umnožava u postojeće fajlove, programe, pa čak i u sam operativni sistem. Najčešće modifikuje sadržaj fajlova ili ih briše, što može da prouzrokuje pad sistema ukoliko virus obriše neki sistemski fajl.

TROJANAC (TROJAN) je vrsta malware-a koji kad se instalira u IS obavlja operacije koje su definisane od strane napadača, najčešće je to brisanje ili modifikovanje podataka, ali često može da dođe i do oštećenja čitavog sistema. Najčešće liče na normalne i korisne instalacione datoteke, pa su tako i dobili ime.

ADWARE (ADVERTISING SOFTWARE) je vrsta malware-a koji kad zarazi IS automatski prikazuje reklame prilikom pretraživanja na Internetu što donosi prihod oglašivaču koji ga je kreirao. (Kompanije plaćaju oglašiva čima prema broju prikazivanja određene reklame)

SPYWARE (SPYING SOFTWARE) je vrsta malware-a koji prikuplja podatke sa zaraženog IS i iste prosleđuje trećem licu (najčešće instanci koja ga je kreirala). Ovim malware-om neovlašćena lica mogu da dođu do šifre, ličnih podataka, korespondencije i sl.

CRV (WORM) je vrsta malware-a koji se sam umnožava. To znači da ukoliko je jedan računar u okviru sistema zaražen, velika je verovatnoća da će svi računari koji su sa njim povezani biti zaraženi posle određenog vremena. Najčešće nanosi štetu mreži i sistemu time što usporava protok podataka u mreži, Crvi su samostalni malware, tj. za razliku od virusa ne moraju da budu povezani za postojeći program da bi se prenosili.

ŠIFRE

KAKO KREIRATI BEZBEDNE I KOMPLEKSNE ŠIFRE KOJE SE LAKO PAMTE?

ŠIFRE SU NAJRASPROSTRANJENIJI METOD AUTENTIFIKACIJE I ZBOG TOGA JE VAŽNO DA BUDU ŠTO KOMPLEKSNIJE.

Osnovno pravilo pri kreiranju šifri jeste da one ne sadrže faktografske podatke o korisniku i cele reči prirodnog jezika, jer se tako mogu lako otkriti metodom pokušaja i pogrešaka. Postoje generatori kompleksnih, nasumičnih šifara, ali se te šifre jako teško pamte. Dobro rešenje je kreirati naizgled nasumične šifre koje se teško pogode, ali se lako pamte. Na primer, sastavi se određena rečenica i uzmu se prva slova svih reči i na taj način se kreira šifra. Takođe, bitno je konfigurisati i dobra sigurnosna pitanja za resetovanje šifre. Treba povesti računa da odgovor na sigurnosno pitanje ne bude opšte-poznat i da takođe bude naizgled nasumičan.

Pored kompleksnih šifri, dobra praksa je aktivirati i autentifikaciju na dva nivoa gde god je to moguće. Autentifikacija na dva nivoa (two step authentication) je način autentifikacije koja pored unosa šifre zahteva i dodatni korak, a to

INFO BOX

Primer naizgled nasumične šifre:

Kad je leti vruće, mogu da popijem 2 litra vode za 1 sat

= **Kjlv,mdp2lvz1s**

je najčešće unos koda koji se dobija putem SMS poruke.

Kvalitet šifre i ostalih mehanizama zaštite je neminovan na putu ka bezbednom sistemu, ali je podjednako bitan i način čuvanja. Nikako se ne preporučuje da se šifre zapisuju u različite sveske, na ceduljice ili da se čuvaju u telefonu i pored toga što su ove prakse jako česte. Bezbedan način čuvanja su softverska rešenja koja čuvaju šifre u bazi podataka u enkriptovanom formatu, tako da i u slučaju da je računar na kom se šifre čuvaju predmet napada, šifre ne gube svoj integritet.

TOOL BOX

Two step authentication se može konfigurisati za sledeće platforme:

GOOGLE: http://www.google.com/landing/2step/

FACEBOOK (Login Approvals): https://www.facebook.com/settings?tab=security&section=approvals

TWITTER: https://support.twitter.com/articles/20170388-using-log-in-verification

DROPBOX : https://www.dropbox.com/en/help/363

LINKEDIN: http://blog.linkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/

Dobar program za čuvanje šifara jeste **KEEPASS**, koji je dostupan na sledećem linku: http://keepass.info/download.html

ENKRIPCIJA DISKOVA

ENKRIPCIJA DISKOVA

ENKRIPCIJA JE GENERALNI KONCEPT KOJI IMA RAZLIČITE IMPLEMENTACIJE, A JEDNA OD NJIH JE ENKRIPCIJA DISKOVA ILI LOKALNA ENKRIPCIJA.

Tehnološki postoje različite vrste diskova, ali su dve opšte grupe relevantne kad je u pitanju enkripcija: to su lokalni diskovi i prenosivi uređaji.

Enkripcija diska podrazumeva stvaranje sloja zaštite koji onemogućava neovlašćenim licima da pristupe sadržaju koji se nalazi na disku. Da bi se pristupilo sadržaju potreban je unos šifre, a ponekad i dodatnih parametara kao što su autentifikacija na dva nivoa, digitalni sertifikat ili biometrijski podaci.

Svaka implementacija enkripcije je različita jer se potrebe razlikuju u zavisnosti od toga kako se koriste podaci koji se enkriptuju, tj. da li se radi o prenosu ili skladištenju podataka. SSL je klasičan primer enkripcije prenosa podataka, dok enkripcija lokalnog diska na računaru je primer enkripcije podataka koji se čuvaju na tom disku.

U pojedinim slučajevima javlja se potreba hibridne enkripcije, na primer kod USB flash memorije, u

TOOL BOX

VERACRYPT je modifikovana verzija ranije popularnog TrueCrypta čiji je razvoj prekinut i samim tim je prestao biti potpuno bezbedan. VeraCrypt je program koji enkriptuje podatke lokalno i dostupan je na sledećem linku: https://veracrypt.codeplex.com/

BOXCRYPTOR je softversko rešenje koje se uglavnom koristi za enkripciju datoteka i fajlova na cloud-u. Dostupan je na sledećem linku: https://www.boxcryptor.com/en/download

jednoj transakciji javlja se potreba da se enkriptuje prenos sa nekog diska do flash memorije i onda se enkripcija vrši na samoj memoriji. Cloud tehnologija sa druge strane takođe uslovljava posebne mehanizme enkripcije jer je sama tehnologija hibrid prenosa i skladištenja.

INFO BOX

DIGITALNI SERTIFIKAT (DIGITAL CERTIFICATE) je poseban sertifikat koji služi za dokazivanje identiteta tokom različite vrste komunikacija u sajber prostoru i izdaju ga organizacije koje imaju ovlašćenje za izdavanje digitalnih sertifikata.

BIOMETRIJSKI PODACI su biološke karakteristike koje mogu da se digitalizuju, kao na primer otisak prsta i šake, sken zenice i retine itd.

ENKRIPCIJA KOMUNIK-ACIJE

EMAIL

E-MAIL JE I PORED RAZVOJA SAVREMENIJIH NAČINA KOMUNIKACIJE OPSTAO KAO KONVENCIONALNO I NAJČEŠĆE KORIŠĆENO REŠENJE U ZVANIČNOJ KOMUNIKACIJI PREKO INTERNETA.

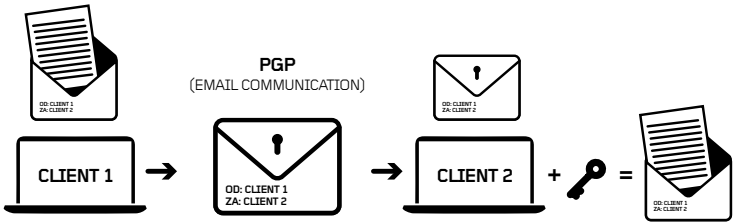
Samim tim i dalje se veliki broj bitnih i osteljivih informacija prenosi e-mail-om. S druge strane, sama tehnologija koja stoji iza e-mail-a nije u potpunosti bezbedna, tj. ima dosta bezbednosnih nedostataka, te korisnik nema kontrolu ko sve može da pristupi metapodacima i sadržaju njegove e-mail komunikacije, naročito kada se koriste javni e-mail servisi poput Gmail, Live, Yahoo Mail i sl.

Delimično rešenje za problem sa metapodacima, jeste naravno korišćenje TOR mreže, kao i blokiranje aktivnog sadržaja kao što su slike i različiti drugi potencijalno rizični elementi u e-mail porukama. U svakom slučaju, sadržaj na ovaj način nije enkriptovan. Jedan od najboljih načina za enkriptovanje sadržaja e-mail poruke jeste PGP. Nedostatak PGP-a je možda njegova implementacija koja nije potpuno orientisana korisničkom iskustvu. Takođe, potrebno je da obe strane u komunikaciji koriste PGP da bi se on mogao uspostaviti kao mehanizam zaštićene komunikacije.

TOOL BOX

THUNDERBIRD je klijent za e-mail koji podržava dodatke za jednostavniju primenu PGP enkripcije, program je dostupan na sledećem linku: https://www.mozilla.org/en-US/thunderbird/

ENIGMAIL je dodatak za Thunderbird koji omogućava jednostavniju primenu PGP enkripcije, dodatak je dostupan na sledećem linku: https://addons.mozilla.org/en-us/thunderbird/addon/enigmail/



INFO BOX

PGP (PRETTY GOOD PRIVACY) je metod enkripcije i dekripcije koji se koristi za end-to-end zaštitu sadržaja.

END-TO-END ENKRIPCIJA (E2EE) je paradigma u kriptografskoj nauci koja označava neprekinutu enkripciju sadržaja od izvora do kraja komunikacije.

CHAT

PORED E-MAIL KOMUNIKACIJE VELIKI DEO KORISNIKA INTERNETA KORISTI I RAZLIČITE CHAT USLUGE.

Ove usluge se uglavnom koriste za neformalnu i ličnu komunikaciju, te su često predmet prepiske poverljive informacije o korisnicima koje ne bi trebalo da budu dostupne trećim stranama. Postoje aplikacije koje omogućavaju enkriptovanu komunikaciju kroz chat usluge.

SMS komunikacija je slična chat komunikaciji, jedina razlika je u

tome što se kao medijum prenosa podataka u chat komunikaciji koristi Internet, dok se kod SMS poruka koristi standardna mreža mobilnih telefona (GSM, 2G, 3G, 4G itd). Zbog toga je mehanizam enkripcije SMS poruka malo drugačiji nego enkriptovanje chat poruka. U oba slučaja se radi o E2EE, tako da je bitno naglasiti da obe strane moraju koristiti enkripciju kako bi sistem bio bezbedan. Postoje posebne aplikacije za sve OS pametnih telefona koje omogućavaju enkripciju komunikacije kroz SMS poruke.

TOOL BOX

PIDGIN je program koji nudi mogućnost enkripcije chat komunikacije, dostupan je na sledećem linku: https://www.pidgin.im/

TELEGRAM je aplikacija za bezbedan chat za pametne telefone i računare. Aplikacija je dostupna na sledećem linku: https://telegram.org/apps

TEXTSECURE je aplikacija za enkriptovanje SMS komunikacije za Android pametne telefone. Aplikacija je dostupna na sledećem linku: https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en

SIGNAL je aplikacija za enkriptovane tekstualne, slikovne i video poruke za iPhone. Aplikacija je dostupna na sledećem linku: https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8

DOBRE I LOŠE PRAKSE INTERNET BEZBEDNO-STI

DOBRE PRAKSE

1. Budite veoma pažljivi sa vašim ličnim podacima.
2. Poštujte privatnost drugih osoba na Internetu.
3. Preuzimajte samo fajlove i instalirajte samo programe čiji su vam izvori poznati i u koje imate poverenja.
4. Ažurirajte sve programe i OS da bi smanjili rizik od napada.
5. Kreirajte kompleksne šifre koje se lako pamte, a teško pogađaju.
6. Aktivirajte autentifikaciju na više nivoa gde god je to moguće.
7. Koristite anti - malware program.
8. Enkriptujte sve što možete enkriptovati.
9. Ukoliko koristite javni računar potrudite se da ne ostavite nikakve tragove za sobom.
10. Ukoliko je vaša USB flash memorija bila u javnom ili nezaštićenom računaru, obavezno je skenirajte anti-malware programom pre nego što je koristite.
11. Preporučuje se da se prenosivi uređaji skeniraju svaki put kad se povežu za računar.
12. Povedite računa o rizicima koje implicira svaki vaš postupak na Internetu, privatnost ne znači manju odgovornost.
13. Makar na brzinu pročitajte uslove korišćenja pre nego što kliknete ''Prihvatam''.

LOŠE PRAKSE

1. Nikad nemojte slati šifre, lične podatke ili finansijske informacije elektronskom poštom.
2. Nemojte pristupati mrežama za koje nemate ovlašćenje, sve i da ste na neki način došli do određenih login detalja (korisničko ime, šifra). To ne znači da ste dobili ovlašćenje.
3. Nemojte instalirati sumnjive dodatke i ažurirane verzije programa.
4. Nemojte da klikćete na sumnjive linkove koje ste dobili putem elektronske pošte, koliko god zanimljivo delovala poruka.
5. Izbegavajte korišćenje javnih i nezaštićenih računara.
6. Izbegavajte korišćenje tuđih mobilnih uređaja.
7. Nemojte pisati svoje šifre na post-it. Ozbiljno, nemojte!
8. Nemojte stavljati imena ili datume rođenja vama bliskih ljudi kao šifre.
9. Nemojte ostavljati vaše uređaje bez nadzora i otključane.
10. Nemojte zanemarivati sumnjive aktivnosti. Ponekad je bolje biti paranoičan.
11. Nemojte koristiti piratski softver. Ukoliko nećete da plaćate za softver, potražite open source varijantu.
12. Nemojte živeti u svojoj zoni komfora. Ponekad vredi uložiti malo vremena i napora i naučiti osnovne stvari o tome kako biti bezbedan na Internetu.

ZANIMLJIVI RESURSI

MYSHADOW:
https://myshadow.org/

Zanimljiva interaktivna platforma koja se fokusira na koncept privatnosti na Internetu. Sadrži dosta edukativnog materijala, ali i interaktivne kvizove pomoću kojih korisnici mogu odrediti koliko su ranjivi na Internetu.

WOLFRAMALPHA FACEBOOK REPORT
http://www.wolframalpha.com/facebook/

Zanimljiv način da korisnici društvene mreže Facebook saznaju koje lične informacije su podelili sa ovom društvenom mrežom i sa celim svetom. Da bi se izveštaj generisao, korisnik mora biti ulogovan u svoj Facebook nalog u okviru istog pregledača.

LIGHTBEAM:
https://addons.mozilla.org/en-us/firefox/addon/lightbeam/

Dodatak za Mozilla Firefox koji prikazuje mrežu sajtova koji prikupljaju podatke o korisniku putem sadržaja trećih strana (third party content).

TERMS OF SERVICE DIDN'T READ

https://tosdr.org/

Zanimljiv dodatak za pregledače, koji analizira uslove korišćenja Internet servisa i izdvaja najbitnije delove, odnosno delove na koje korisnik treba da obrati pažnju.

SHARECONFERENCE.NET

Sajt SHARE fondacije, koristan izvor vesti i informacija o stanju u sajber prostora u Srbiji, regionu i Evropi.

EFF.ORG

Sajt Electronic Frontier Foundation, koristan izvor informacija, softverskih rešenja i različitih uputstava i vodiča u oblasti Internet bezbednosti.

Napomena: SHARE fondacija ne favorizuje određene programe u odnosu na druge. Programi koji se spominju u ovom priručniku su izabrani na osnovu njihovog rejtinga i ocene zajednice. SHARE fondacija neće snositi nikakvu odgovornost ukoliko neka od ovih aplikacija obavlja funkcije koje se od nje očekuju. Preporučujemo odgovorno korišćenje aplikacija.

ODJAVNI TEKST

Ovaj vodič je namenjen svim korisnicima Interneta koji vode računa o privatnosti i bezbednosti svojih podataka. Njegov cilj je da se koncepti privatnosti i bezbednosti na Internetu približe prosečnom korisniku, na način koji je njemu razumljiv i jasan. Da bi se koristio ovaj vodič nisu potrebna dodatna znanja iz oblasti IT-ja, već samo strpljenje i dobra volja.

Tehnologija se razvija brzo, pa samim tim ovaj vodič nije dovoljan da bi se korisnik trajno obezbedio, te su zbog toga navedeni korisni resursi, koji bi korisniku omogućili da prilagođava svoje bezbednosne mehanizme najsavremenijoj tehnologiji. Ipak, vodič pre svega služi kao početna tačka na putu ka bezbednosti i privatnosti na Internetu.