Koncepti informacijske sigurnosti - povjerljivost, integritet i dostupnost

Šindija, Mateo

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Preddiplomski studij računarstva

Završni rad

Koncepti informacijske sigurnosti - povjerljivost, integritet i dostupnost

Rijeka, srpanj 2022.

Mateo Šindija
0069087852

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
Preddiplomski studij računarstva

Završni rad

Koncepti informacijske sigurnosti - povjerljivost, integritet i dostupnost

Mentor: izv.prof.dr.sc. Jonatan Lerga

Rijeka, srpanj 2022.

Mateo Šindija
0069087852

SVEUČILIŠTE U RIJECI
TEHNIČKI FAKULTET
POVJERENSTVO ZA ZAVRŠNE ISPITE

Rijeka, 21. ožujka 2022.

Zavod: **Zavod za računarstvo**
Predmet: **Digitalna logika**
Grana: **2.09.02 informacijski sustavi**

ZADATAK ZA ZAVRŠNI RAD

Pristupnik: **Mateo Šindija (0069087852)**
Studij: Preddiplomski sveučilišni studij računarstva

Zadatak: **Koncepti informacijske sigurnosti - povjerljivost, integritet i dostupnost / Concepts of Information Security - Confidentiality, Integrity And Accessibility**

Opis zadatka:

Potrebno je proučiti, opisati i analizirati osnovne koncepte informacijske sigurnosti - povjerljivost, integritet i dostupnost. Nadalje, potrebno je opisati na koje se načine isti ostvaruju u računalnim aplikacijama, kao i na koje se načine najčešće probijaju. Također, potrebno je objasniti najčešće sigurnosne propuste u razvoju aplikacija kao i mane postojećih sigurnosnih zaštita te minimalnu zaštitu koju bi svaka aplikacija koja prikuplja korisničke podatke trebala imati.

Rad mora biti napisan prema Uputama za pisanje diplomskih / završnih radova koje su objavljene na mrežnim stranicama studija.

Zadatak uručen pristupniku: 21. ožujka 2022.

Mentor:

Izv. prof. dr. sc. Jonatan Lerga

Predsjednik povjerenstva za završni ispit:

Prof. dr. sc. Kristijan Lenac

Izjava o samostalnoj izradi rada

Izjavljujem da sam samostalno izradio ovaj rad.

Rijeka, srpanj 2022.

_____

Ime Prezime

Sadržaj

Popis slika

Popis tablica

Poglavlje 1

Uvod

Od početka razmjene poruka cilj je bio zaštiti informacije od neželjenih očiju. Kako je vrijeme napredovalo tako su i metode za zaštitu informacija. Dolaskom interneta informacije su se počele razmjenjivati u ogromnim količinama i brzinama, ali s time im se počela narušavati sigurnost i povjerljivost. Kao odgovor tomu proizašli su koncepti integriteta, povjerljivosti i dostupnosti informacija koji navode organizacije pri zaštiti informacija, te se smatraju srcem informacijske sigurnosti. Cilj ovog rada je opisati načine na koje ovi koncepti probijaju, koje mjere poduzeti za obranu od takvih napada te kako se implementiranju ovi koncepti.

Poglavlje 2

Što je kibernetička sigurnost?

Za shvatiti pojam informacijske sigurnosti za početak treba shvatiti termin sigurnosti. Biti siguran znači biti zaštićen od gubitka informacija, štete, nepoželjnih modifikacija ili nekih drugih opasnosti. Kibersigurnost se dijeli na više grana, neke od najpoznatijih su mrežna sigurnost, aplikacijska sigurnost, sigurnost web stranica, analiza zlonamjernih programa, informacijska sigurnost i mnoge druge. **Informacijska sigurnost** je definirana kao zaštita informacija i njenih kritičnih karakteristika (integriteta, dostupnosti i povjerljivosti), uključujući sistem i sklopovlje koje se koristi za skladištenje ili prijenos informacija, treniranje osoblja i implementacija sigurnosnih mjera [1].

Za obranu kritičnih infrastruktura i građana države od kibernetičkih napada zadužene su vladine organizacije, na primjer u Hrvatskoj je za to odgovorno Nacionalno vijeće za kibernetičku sigurnost. Osim samih država za kibernetičku sigurnost su zadužene i tvrtke koje, u slučaju proboja baze podataka ili nešto slično tomu, posljedica je veliki gubitak novca i reputacije. Primjer toga je jedna od najvećih krađa informacija 2016. godine kada je tvrtka *Yahoo* objavila da joj je ukradeno 500 milijuna korisničkih računa, što je kao za posljedicu rezultiralo gubitkom od 350 milijuna američkih dolara [2]. Iako države i tvrtke ulažu mnogo novaca u kibernetičku sigurnost to ne znači da su korisnici sigurni i da se nemaju o čemu brinuti. Po Internet Organised Crime Threat Assessment (IOCTA) grupi za vrijeme COVID-19 pandemije desio se znatni porast u internet prevarama i ucjenjivačkim softverima (eng. *ransomware*) [3].

Hakeri često ciljaju prosječne građane, pogotovo one koji nisu oprezni na internetu i one koji su informatički nepismeni, zato svi koji se koriste internetom bi trebali biti upoznati barem s osnovama internet sigurnosti.

Poglavlje 3

Koncepti povjerljivosti, integriteta i dostupnosti

Kako se još sredinom 1980-ih godina počelo širiti jeftino sklopovlje i programska podrška, proboj podataka se znatno uvećao, kao rezultat tomu više se pažnje počelo obraćati na zaštitu podataka umjesto zaštitu samih računala [4]. Saltzer and Schroeder su u svojem radu "The Protection of Information in Computer Systems.", 1975. godine definirali osnovne principe informacijske sigurnosti: povjerljivost, integritet i dostupnost [5]. Ova tri osnovna principa imaju različite zahtjeve i definiraju se kao:

- Povjerljivost: svojstvo koje osigurava da informacije neće biti dostupne neovlaštenim osobama, entitetima ili procesima,
- Integritet: svojstvo koje tvrdi da se informacijama može vjerovati i da ih uređuju samo ovlaštene osobe.
- Dostupnost: svojstvo koje jamči da će informacije biti dostupne kada budu zatražene od ovlaštenog korisnika.

S ova tri temeljna principa razvili su se razni modeli informacijske sigurnosti, kao što su: CIA, Parkerian Hexad, International Organization for Standardization Model (ISO) Model i razni drugi. Tablica 3.1 prikazuje neke sigurnosne modele i njihova svojstva.

Tablica 3.1 Primjeri nekih sigurnosnih modela [4]

Svojstva modela	CIA Model	Parkerian Hexad Modele	7ISO principles
Povjerljivost	•	•	•
Integritet	•	•	•
Dostupnost	•	•	•
Autentičnost		•	•
Ne poricanje			•
Posjed		•	
Korisnost		•	
Pouzdanost			•
Odgovornost			•

3.1 CIA Model

Koristeći principe povjerljivosti, integriteta i dostupnosti Clark i Wilson 1987. godine su predstavili takozvani Confidentiality, Integrity and Availability (CIA) model. Ovaj model je jedan od osnovnih modela informacijske sigurnosti, pomaže pri razvoju sigurnosnih politika za organizacije. Pri razvijanju novog proizvoda ili tehnologije model pomaže sigurnosnim timovima za vođenje politika informacijske sigurnosti [4]. Jedan od problema CIA modela jest taj da je definicija na nekim mjestima preširoka, a na nekim preuska, to jest definira nesigurna stanja kao sigurna i sigurna kao nesigurna [6].

3.2 Parkerian Hexad Model

Kao nadogradnju na CIA model Donn B. Parker je dodao tri nova principa posjed, autentičnost i korisnost. Posjed označava kontrolu ili vlasništvo nad informacijom, autentičnost se odnosi na ispravno označavanje ili pripisivanje informacije i korisnost se odnosi na samu korist informacije [4].

3.3 International Organization for Standardization Model

Godine 2004. ISO je predstavila model za informacijsku sigurnost, poznatiji kao "7 ISO principles", ili točnije pod nazivom ISO/IEC 13335-1. Sastoji se od sedam principa: povjerljivosti, integriteta, dostupnosti, ne poricanja, odgovornosti, autentičnosti i pouzdanosti. Svojstvo ne poricanja označava mogućnost dokazivanje nastanke radnje na taj način da se radnje kasnije ne može odbaciti, odgovornost osigurava da se identitet osobe koja radi akcije nad sustavom sa informacijama može pratiti, pouzdanost označava konzistentnost u namijenjenom ponašanju i rezultatu [4].

Poglavlje 4

Opasnosti za povjerljivost podataka

Cilj povjerljivosti jest zaštiti informacije od neovlaštenih korisnika. U suštini informacija treba dostupna samo onim korisnicima koji imaju potrebnu autorizaciju.

4.1 Prisluškivanje

Prisluškivanje ili poznatiji kao *Eavesdropping attack*, je kada hakeri se spoje na nezaštićene kanale za komunikaciju i kradu podatke. Kako bi se ovaj napad izveo potreban je samo program koji se nalazi bilo gdje na putu između klijenta i poslužitelja koji hvata sve relevantne podatke koji putuje mrežom. Napadač ne treba imati direktan pristup programu za prisluškivanje, već ga može samo instalirati na neki uređaj u ciljanoj mreži i zatim se vratiti nakon nekog vremena da bi dohvatio podatke. Teško ga je za otkriti pošto se na kanalu za komunikaciju ne očitiju neki čudni događaji [7]. Posljedica ovog napada može biti katastrofalna, povjerljive informacije mogu postati javne (npr. podatci o kreditnoj kartici) kao i privatni razgovori.

4.1.1 Prisluškivanje mrežnog kanala

Kako podatci prolaze kroz ogroman broj usmjerivača (eng. *router*) moguće se smjestiti na nekom od tih usmjerivača i pratiti promet, ujedno podatci mogu prolaziti i kroz neke medijske posrednike (eng. *media proxy*) koji služe za prijenos medijskih

podataka sa jednog mrežnog segmenta na drugi. Ako napadač uspije probiti usmjerivač, vatrozid (eng. *firewall*), Session Border Controller (SBC) ili medijskoga posrednika onda može prisluškivati promet koji prolazi kroz te točke. Za prisluškivanje prometa koji putuje kroz Wide Area Network (WAN) potrebno je znati kojim putem paketi putuju, što je jako teško pošto paketi ne moraju putovati uvijek istim putem. Iako je jako teško ne znači da je nemoguće, kako se komunikacija između dvije krajnje točke stalno širi tako se povećava i broj čvorova, to jest povećava se broj mogućih točka proboja [7].

4.1.2 Prisluškivanje lokalne mreže

Češći oblik ovog napada jest taj da napadač prisluškuje neku od lokalnih mreža koje sadrže krajnje točke. Ovo se često dešava na nezaštićenim *Wi-Fi* mrežama gdje se jednostavno može iskoristi neki od programa za analizu mrežnih paketa (npr. *Wireshark*). Postoji i mogućnost da se napadač fizički spoji na *Ethernet* port da bi ukrao podatke koje putuju mrežom [7].

4.1.3 Prisluškivanje uređaja

Drugi način za prisluškivanje jest da napadač ugrozi sigurnost nekog od uređaja koji služi kao krajnja točke veze. Instaliranjem zloćudnog programa na taj uređaj koji bi ugrozio sigurnost sustava, napadač će biti u mogućnosti instalirati program za prisluškivanje direktno na taj uređaj. Tada se sva komunikacija kroz neko vrijeme može proslijediti na neki vanjski poslužitelj [7].

4.1.4 Zaštita od prisluškivanja

Otkrivanje *eavesdropping* napada je jako teško, zato je najbolja praksa koristiti preventivne mjere kako se kanal uopće mogao prisluškivati. Neke od tih mjera su: šifriranje podataka, autentifikaciju dolaznih paketa, razdvajanje mreža i Virtual Private Network (VPN).

Šifriranje podataka - jedna od najvažnijih stavki jest šifriranje podataka i internet mreže. Za zaštitu *Wi-Fi* mreža preporučeno je koristiti Wi-Fi Protected Access 2 (WPA2) ili Wi-Fi Protected Access (WPA3) zaštitu. Sva komunikacija koja se odvija na web-u trebala bi koristiti Hypertext Transfer Protocol Secure (HTTPS) protokol koji nam osigurava šifrirani prijenos podataka između intenetskog preglednika i web stranice.

Autentifikacija dolaznih paketa - *spoof* je napad gdje se napadač predstavlja kao neka legitimna organizacija ili neki pouzdani izvor informacija, često se koristi za ostvarenje *eavesdropping* napada. Za zaštitu od *spoof* napada treba implementirati autentifikaciju nadolazećih paketa. Internet Protocol (IP) *spoofing* je jedan od napada gdje napadač lažira izvornu IP adresu kako bi je neki sistem prihvatio, slično se može izvesti i s modificiranjem Media Access Control Address (MAC) adrese. Kriptografski protokoli kao što su Transport Layer Security (TLS), OpenPGP i Internet Protocol Security (IPsec) imaju implementiranu neku vrstu autentifikacije.

Razdvajanje mreža - dobra praksa za tvrtke je odvajanje kritičke infrastrukture od ostalih. Na primjer podijeliti mrežu na IT, financijski i marketinški dio, tako da zaposlenici svakog sektora imaju pristup samo svojoj mreži. Ako neka od mreža bude ugrožena druge i dalje mogu nastaviti s normalnim radom.

VPN - VPN može biti jako koristan kao zaštita od prisluškivanja, VPN funkcionira na način da maskira našu IP adresu i djeluje kao posrednik preusmjeravajući naš promet, također implementira i šifriranje podataka.

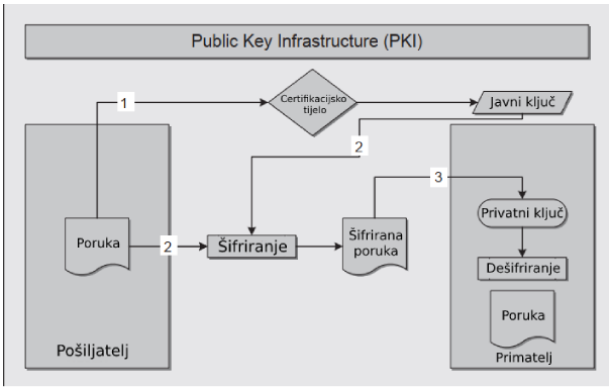
Najbolje sigurnosne prakse - korištenjem jakih lozinki, pažnji pri otvaranju linkova, preuzimanju datoteka i izbjegavanjem javnih Wi-Fi mreža dodatno otežavamo posao napadaču da instalira neki zločudni program na naš uređaj.

4.2 Enkripcija

Enkripcija ili šifriranje je stvoreno s ciljem zamaskiranja poruke tako da je ne može nitko razumjeti osim onoga za koga je namijenjena. Šifriranje se koristi još od drevnih vremena a u posljednje vrijeme je našla ogromnu upotrebu u digitalnoj komunikaciji. Public Key Infrastructure (PKI) je set sklopovlja, programa, politike i procedura potrebnih za kreiranje i upravljanje digitalnim certifikatima i javnim ključevima, danas se masovno koristi za šifriranje internet komunikacije. Da bi bili sigurni da dokument koji smo poslali nije promijenjen na putu i da je stvarno kreiran od strane pošiljatelja, PKI koristi kriptografsku operaciju zvanu digitalni potpis. Podatci se šifriraju uz pomoć javnog ključa a dešifrira ih primatelj koristeći privatni ključ (Slika 4.1). PKI koristi dvije vrste šifriranja, asimetrično i simetrično šifriranje. Asimetrično šifriranje koristi različite ali povezane ključeva za šifriranje i dešifriranje, dok simetrično koristi iste ključeve za obje radnje. Mrežni sigurnosni protokoli koriste simetrično šifriranje jer asimetrično zahtjeva više proračunskog vremena, energije i šifrirani podatci su veće veličine. Postoje dvije vrste simetričnog šifriranja, blok šifriranje i stream šifiranje. Blok šifriranje podijeli poruku u više dijelova fiksne dužine i svaki dio šifrira zasebno. Advanced Encryption Standard (AES) koristi blok šifriranje, AES koriste mrežni protokoli kao što su HTTPS, WPA2 i File Transfer Protocol Secure (FTPS). Stream šifriranje tretira poruku kao kontiunirani tok podataka koje se šifrira i dešifira bit po bit, korisiti se u Rivest Cipher 4 (RC4) i u mrežnim protokolima kao što su Wired Equivalent Privacy (WEP) i Wi-Fi Protected Access (WPA) [8].

4.2.1 Napad uzastopnim pokušavanjem

Napadi uzastopnim pokušavanjem pokušavaju dešifrirati poruku tako da iskoriste sve moguće ključeve kako bi probili šifriranje. Ovi napadi su u praksi jako neučinkoviti jer da bi se izvrtile sve moguće kombinacije potrebno je jako puno vremena čak i sa jako dobrim sklopovljem.



Slika 4.1 Primjer toka rada PKI pri slanju emaila [8]

4.2.2 Rođendanski napad

Napad baziran na teoremu iz teorije vjerojatnosti koji tvrdi ako su u sobi 23 ljudi šansa da dvoje ima isti rođendan je oko 50%. Ako se pronađu dva različita ulaza koja su identična nakon šifriranja, to znači da postoje hash (rezultat šifriranja) kolizije i onda je moguće otkriti na koji način algoritam šifrira podatke. Algoritam koji pretvara poruku u hash fiksne duljine m ima 2^m mogućih hasheva. Ako se uzme k kao broj nasumičnih poruka koje se šifriraju, koliki mora biti k da bi postojala 50 postotna šansa duplikata hasha? Pomoću formule: $1.174\sqrt{n}$, koja govori da za vrijednost n treba 1.174 pomnožiti sa korijenom od n da bi postojala 50 postotna šansa da se ponovi hash. U ovom slučaju $k = \sqrt{2^m}$ tada je konačna formula: $k = 1.174\sqrt{2^m}$. Ako uzmemo za primjer 2^{16} bitova to znači da postoji 65,536 mogućih hasheva, ako iskoristimo formulu $k = 1.174\sqrt{2^{16}}$ dobiti ćemo da u 300 pokušaja postoji 50% šanse da će se hash ponoviti. Tablica 4.1 prikazuje koliko treba pokušaja ako se koristi veći broj bitova [9].

Najbolji način za spriječiti ovaj napad jest koristiti hash funkciju koja kao izlaz daje vrlo dugačak niz bitova tako da pronalazak duplikata postane računski neizvediv.

Tablica 4.1 Vjerojatnost kolizije ako je hash 2^n bitova dug [9]

Bitovi	**Broj mogućih izlaza**	**Pokušaji za željenu vjerojatnost kolizije**	
		50%	**75%**
16	65,536	300	430
32	4.3×10^9	77,000	110,000
64	1.8×10^{19}	5.1×10^9	7.2×10^9
128	3.4×10^{38}	2.2×10^{19}	3.1×10^{19}
256	1.2×10^{77}	4.0×10^{38}	5.7×10^{38}
384	3.9×10^{115}	7.4×10^{57}	1.0×10^{58}
512	1.3×10^{154}	1.4×10^{77}	1.9×10^{77}

4.2.3 Napad degradiranjem

Prilikom svake inicijalizacije TLS sesije uređaji biraju kriptografske algoritme i odlučuju koje će koristiti prilikom procesa rukovanja (eng. *handshake*). Česti način ostvarivanja ove vrste napada je koristeći *Man-In-The Middle* (MITM) napad. Ovo omogućuje napadaču da se umiješa u proces dogovaranja kriptografskog algoritma i forsira poslužitelje da koriste starije verzije TLS protokola. U nastavku su neki od glavnih vrsta napada degradiranjem.

- **POODLE** - (Padding Oracle On Downgraded Legacy Encryption) funkcionira na način da prevari korisnika na pokretanje zlonamjernog *JavaScript* programa u web pregledniku. Pokretanje tog koda omogućuje napadaču slanje zahtjeva za uspostavu TLS veze, napadač zatim odustaje od pokušaja za uspostavu veze. Poslužitelj će ove neuspješne zahtjeve za uspostavu veze protumačiti kao poruku da se prebaci na SSL 3.0 umjesto TLS. Jednom kada je uspostavljena SSL 3.0 veza potrebno je samo iskoristiti ranjivost Cipher Block Chaining (CBC) šifriranja koja se koristi u SSL 3.0.
- **FREAK** - (Factoring RSA Export Keys) umjesto da forsira korištenje starijih verzija protokola, FREAK će iskoristiti svoju poziciju da forsira prebacivanje sa RSA šifranja na algoritme šifriranja niske kvalitete. Ovo se događa u TLS

rukovanju, točnije za vrijeme *Hello message*-a prema poslužitelju.

- ***LogJam*** - slično kao i u prijašnim napadima LogJam iskorištava MITM napad. Napad se izvršava na poslužiteljima koji koriste *Diffie-Hellman* razmjenu ključeva forsirajući ih da koriste 512 bitni *Diffie-Hellman export-grade* algoritam za razmjenu ključeva. Kada promijeni verziju protokola napadač može probiti enkripciju i dobiti kontrolu nad vezom.

Jedna od preventivnih mjera napada degradiranjem jest maknuti podršku za *export-grade* šifriranja (algoritmi za šifriranje niske kvalitete) i drugih algoritma za šifriranje sa poznatom greškom. Druga bitna stavka jest uspostavljanje sigurne i stabilne TLS veze, ovo podrazumijeva omogućiti podršku samo snažnim protokolima kao što su TLS 1.2 i 1.3, potrebno je i koristiti dobre enkripcijske protokole bez znanih propusta. Ako je jedan od zahtjeva imati omogućeno korištenje protokola nižih verzija trebalo bi konfigurirati TLS_FALLBACK_SCSV signal, naime taj signal omogućava korištenje protokola viših verzija ako klijent zahtjeva niže verzije a ima instalirane i više verzije [10].

4.3 Mrežna krađa identiteta

Mrežna krađa identitata ili poznatiji pod engleskim nazivom *phishing*, možda jedan od najpoznatijih i najuspješnijih napada. Prema Proofpoint-ovom istraživanju provedenom u 2020. godini od ispitanih organizacija gotovo 88% njih je bilo na meti *phishinga* [11]. Mrežna krađa identiteta je najuspješnija kod ljudi s manjom informatičkom pismenošću. U principu izvedba napada nije previše sofisticirana, jedan način je kreirati lažnu web stranicu koja izgleda identično kao neka legitimna web stranica koja je možda često posjećivana (npr. Facebook, Gmail itd.). Dajući lažni osjećaj sigurnosti žrtva ispuni formu koja na primjer može zahtijevati korisničko ime, lozinku ili informacije o kreditnoj kartici. Predajom tih informacije otvara se stvarna web stranica i sa velikom vjerojatnošću žrtva neće biti svjesna da je upravo predala povjerljive informacije hakeru. Mrežna krađa identiteta se može podijeliti u više kategorija neke od njih su:

- ***Spear phishing*** - vrsta *phishinga* gdje se cilja individualna osoba ili grupa

ljudi. Može ciljati zaposlenika neke tvrtke s ciljem da upadne njihovu mrežu.

- ***Whaling*** - se najčešće provodi na nekim izvršni pozicijama u ciljanoj tvrtki, kao što je direktor, neki član odbora i slično.
- ***Smishing*** - je napad koji koristi tekstualne poruke ili SMS za izvršenje napada. Uobičajena tehnika je isporuka poruke na mobitel putem SMS-a koji sadrži poveznicu na koju se može kliknuti ili povratni telefonski broj koji se može nazvati.
- ***Vishing*** - za razliku od drugih vrsta *phishinga* ovaj se provodi koristeći glasovni poziv. Napadač se može predstavljati žrtvi kao lažni zaposlenik neke tvrtke i tvrditi da je njegov račun ugrožen te da on može pomoći sa instalacijom nekog programa, ti programi su najčešće zlonamjerni.

4.3.1 *Pharming*

Pharming je oblik mrežne krađe identiteta ali umjesto mamca on preusmjerava promet sa originalne stranice na zlonamjerno kreiranu web stranicu. Ove zlonamjerne stranice kao kod mrežne krađe identiteta imaju cilj ukrasti naše osjetljive podatke. Postoje dva načina kako preusmjeriti promet na zlonamjernu stranicu. Prvi način je da napadač instalira virus na računalo kako bi promijenio Domain Name System (DNS) host datoteku i tako osigurao da iako se upiše točno ime u web pretraživač on neće otvoriti legitimnu stranicu već njenu krivotvorenu verziju. Drugi način je takozvano DNS trovanje gdje je cilj napasti DNS poslužitelja i tako ugroziti više ljudi.

4.3.2 Zaštita od mrežne krađe identiteta

Mrežna krađa identiteta spada pod socijalni inženjering što znači da je cilj prevariti čovjeka a ne nužno probiti sigurnost mreže ili uređaja. Neke stavke koje bi mogle sugerirati da je poštu namijenjena za krađu identiteta:

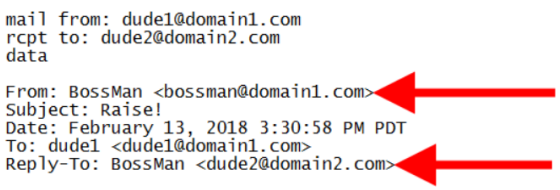
Hitni poziv - poruke koja pozivaju na hitno djelovanje, tipa: “vaš račun je ugrožen otvorite poveznicu u nastavku kako bi potvrdili identitet”, moguć su pokušaj

prevare i ne bi trebalo direktno otvarati njihovu poveznicu. Lebdenjem iznad poveznice u kutu ili direktno ispod miša bi se trebala pokazati stvarna adresa te poveznice.

Loša gramatika - obratiti pažnju na gramatiku, velike kompanije imaju posebne uredničke timove zadužene za održavanje profesionalizma i kvalitete elektroničke pošte. Greške u pisanju ili gramatici mogući su znak *phishinga*.

Ne personalizirani pozdravi - većina kompanija danas šalju elektroničku poštu gdje nam se obraćaju s našim imenom, tako da pozdravi kao "Poštovani gospodine ili gospođo" mogu sugerirati da pošiljatelj nije onaj za kojeg se predstavlja.

Pošiljatelj - pri primanju nove pošte treba dobro provjeriti adresu pošiljatelja. Da bi ostvarili lažni osjećaj sigurnosti napadači mogu pokušati predstaviti poštu kao da je došla sa izvora kojem žrtva vjeruje. Ta metoda se zove email lažiranje, to je moguća ostvariti pošto Simple Mail Transfer Protocol (SMTP) poslužitelji nemaju načina za potvrditi da li je adresa stvarna ili lažirana. Jedna od tehnika je korisiti već poznatu domenu ali zamijeniti neka slova da bi izgledala stvarno, npr. umjesto "microsoft" napisati "rnicosoft" ili zamijeniti "o" sa "0". Moguće je i koristiti ne latinična slova koja vizualno izgledaju identična kao latinična, tipa latinično "a" i ćirlično "a" izgledaju vizualno identično ali zapravo nisu, za provjeru najbolje je kopirati adresu u neki *unicode inspector* za potvrdu vrstu znakova. Napadač se može predstaviti sa lažnom domenom, ali najčešće ako je ne posjeduje *reply-to* polje će sadržavati drugačiju adresu (Slika 4.2).



Slika 4.2 Primjer lažne elektroničke poruke [13]

Pri sumnji da je primljena poruka pokušaj *phishinga* najbolje je prijaviti po-

ruku i zatim je odmah izbrisati. Nikako ne otvarati poveznice njihove ili preuzimati priložene datoteke .

Poglavlje 5

Opasnosti za integritet podataka

Integritet podataka nam jamči da su podatci ispravni, kompletni i validni kroz njihov životni ciklus. Postoje više različitih vrsta integriteta podataka kao što su:

- **Fizički integritet** - znači zaštititi točnost, ispravnost i cjelovitost podatka kada se pohranjuju i dohvaćaju. Često je ugroženo prilikom nestanka struje, prirodnim katastrofama i hakerima koji ciljaju funkcije baze podataka.
- **Integritet entiteta** - označava da podatci u relacijskim bazama podataka ne smiju ponavljati i biti prazni.
- **Referentni integritet** - je niz procesa koji osiguravaju da podaci ostaju pohranjeni i korišteni na ujednačen način. Sa definiranim stranim ključevima postoje pravila koja osiguravaju da samo određeni podatci se smiju brisati i uređivati.
- **Integritet domene** - jamči točnost podataka unutar domene. Svaka domena ima skup pravila koje vrijednosti stupci u bazi smiju sadržavati.
- **Korisnički definiran integritet** - znači da pravila i ograničenja za podatke kreira korisnik kako bi uskladili sa njegovim zahtjevima.

5.1 *Man-in-the middle* napad

Slično kao i napada prisluškivanjem (Poglavlje 4.1) MITM se ubaci u komunikaciju između krajnjih točaka (Slika 5.1), ali dok je prisluškivanje pasivno, MITM može utjecati na nju, bilo modifikacijom paketa ili nagovaranjem korisnika na neku radnju. MITM napad se izvodi u dvije faze presretanje i dešifriranje [12].

Slika 5.1 Vizualni prikaz MITM napada [12]

5.1.1 Presretanje

Prvi korak napada je priključivanje u žrtvenu mrežu i presretanje aktivnosti prije nego što paket od cilja stigne do ishodišta. Tu se napadač postavlja kao točka komunikacije između korisnika i poslužitelja. Jedna od najčešćih metoda za ostvarivanje toga jest da napadač otvori javnu Wi-Fi mrežu, po mogućnosti sa slabom šifrom i relevantnim imenom za to područje. Jednom kad se žrtva spoji napadač ima pristup svoj razmjeni podataka što se odvija na toj mreži. Postoje i drugi načini koje napadač može iskoristiti da bi upao u mrežu:

- **Address Resolution Protocol (ARP) lažiranje** - kada se napadač spoji na mrežu na kojoj se nalazi žrtva on i dalje nema pristup njegovoj komunikaciji jer se to odvija između usmjerivača i njega. Zato koristi ARP lažiranje da bi uvjerio žrtvu da je on usmjerivač i usmjerivača da je on zapravo ciljani uređaj. Za ovakvu obmanu često se uz pomoć *Ettercap* programa, pokrene

program i promatra IP i MAC adresu usmjerivača, zatim počne slati ARP pakete kroz LAN mrežu koji sadrže napadačevu MAC adresu i žrtvinu IP adresu, ovo prevari usmjerivača i drugog uređaja da se spoju na napadačev uređaj a ne izravno jedan s drugim. Napadač je sada u sredini komunikacije i ima pristup svim paketima koji namijenjeni za žrtvin uređaj.

- **IP lažiranje** - ovdje napadač mijenja izvorišnu IP adresu u zaglavlju paketa kako bi se predstavio kao netko drugi da bi uvjerio žrtvu da komunicira sa nekim legitimnim sustavom. Od tuda je moguće ukrasti podatke ili odvesti žrtvu na lažnu web stranicu.
- **DNS lažiranje** - kao što je navedeno u 4.3.1 poglavlju moguće je otrovati DNS poslužitelj i tako navesti korisnika da komunicira sa vama umjesto sa stvarnom stranicom [12].

5.1.2 Dešifriranje

Sada kada napadač ima pristup, podaci mu neće biti baš od naročite koristi pošto je velika vjerojatnost da su šifrirana, zato je druga faza napada dešifriranje. Postoje razne metode za dešifrirati podatke:

- **HTTPS lažiranje** - napadač šalje lažni certikfikat prema žrtvinom pretraživaču jednom kad žrtva zatraži uspostavu HTTPS veze. Certifikat će sadržavati lažni digitalni otisak prsta (eng. *thumbprint*) asociran sa ciljanom stranicom. Pretraživač tada potvrdi certifikat ako se nalazi u listi sigurnih stranica. Napadač tada ima pristup podatcima prije nego što se proslijede web stranici.
- **SSL otimanje** - se ostvaruje prilikom Transmission Control Protocol (TCP) rukovanja kada napadač pošalje lažne autentifikacijske ključeve korisniku i web stranici. Klijentu i web stranici će veza izgledati sigurno, dok u stvarnosti onaj tko je u sredini kontrolira sesiju.
- **SSL uklanjanje** - je napad gdje napadač promijeni web vezu sa HTTPS na nesigurniji Hypertext Transfer Protocol (HTTP) protokol. Napadač može izvesti ovaj napad kada primijeti korisnikov HTTP zahtjev za vezu, tada umjesto da proslijedi taj zahtjev prema originalnoj stranici, on ostvari HTTPS vezu sa

stvarnom stranicom dok vezu na klijentu ostavlja na HTTP protokolu. Kako korisnik nije svjestan da razgovara sa napadačem a ne sa stvarnom stranicom on svoje podatke šalje kao čisti tekst [12].

5.1.3 Zaštita od MITM napada

Za zaštiti od MITM napada najbolje je izbjegavati javne Wi-Fi mreže i stranice bez HTTPS zaštite. Svaka stranica bi trebala imati HTTPS zaštitu ne samo ona koja služi za prijavu i registriranje, tako se smanjuje rizik od krađe sesijskih tokena [12].

5.2 Ljudska greška

Može biti implementiran savršen sustav za obranu informacija, ali svejedno informacije nikad nećemo biti 100% sigurne. Ljudska greška odgovorna je za 95% sigurnosnih proboja prema IBM-ovom istraživanju [14]. U računalnoj sigurnosti ljudska greška se odnosi na nenamjerne radnje ili nedostatak radnje što je dovelo do sigurnosnog proboja. Ljudske greške se mogu podijeliti u dvije kategorije: pogreške temeljene na vještini i greške pri donošenju odluka. Greška u vještini se sastoji od propusta pri izvođenju već dobro poznate aktivnosti, neki mogući razlozi bi bili umor, gubitak koncentracije ili multitasking. Pogreške pri donošenju odluka mogu biti uzrokovane nedostatkom znanja ili informacija, ne poduzimanjem nikakvih radnji se također smatra greškom u donošenju odluka. Sve ljudske greške koje bi mogle uzrokovati sigurnosni proboju bilo bi nemoguće nabrojati, ali zato je moguće izdvojiti neke na koje bi trebalo obratiti pažnju.

5.2.1 Slabe loznike

Lozinke kao što su "password" ili "123456" su i dalje često korištene a računalo ih može probiti za manje od sekunde. Lozinke se mogu probijati tako da napravi program koji bi vrtio sve moguće kombinacije dok ne pogodi lozinku, ali takav pristup može trajati mjesecima ili pak godinama u ovisnosti o kompleksnosti lozinke. Puno praktičniji pristup je tako zvani *dictionary* napad, koji vuče iz liste često korištenih lozinka

i radi im preinake dok ne pogodi kombinaciju. Često se u tu listu dodaju osobne informacije o meti kao što je datum rođenja, mjesto stanovanja i slično pošto korisnici ne rijetko to uključe u svoje lozinke. Kako su danas ljudi prijavljeni na velik broj aplikacija koji zahtijevaju lozinku, dosta njih se odluči koristiti istu lozinku za sve. Ako se pronađe jedna lozinka tada se može iskoritii *credential stuffing* napad, to jest napadač će pokušavati iskoristiti istu lozinku ili možda uz neke preinake na drugim web stranicama dok se ne uspije na neku od njih prijaviti. U slučaju otkrivanja provale u račun što prije bi trebalo promijeniti lozinku na način da ima što manje sličnosti sa prijašnjom, korištenje velikih i malih slova uz što više znakova i brojeva je preporučeno.

5.2.2 Ne ažuriranje programa

Hakeri konstantno pokušavaju pronaći sigurnosne propuste u programima i nanijeti što više štete prije nego što se propust zakrpa, ova vrsta napada se zove iskorištavanje nultog dana (eng. *zero day exploit*). Jednom kada se propust otkrije programeri ga pokušavaju što prije zakrpati i omogućiti ažuriranje. Zato ako korisnik koristi stariju verziju programa sa poznatim propustom potencijalna je meta hakera.

5.2.3 Nedostatak znanja o sigurnosti

Napadači uvijek traže najslabiju točku u obrani pa tako ciljaju zaposlenike sa slabijim sigurnosnim praksama. Takvi zaposlenici će lakše biti prevareni u otvaranje sumnjivih poveznica i instaliranje zlonamjernih programa. Stoga je bitno svakog zaposlenika provesti kroz trening o kiber sigurnosti.

5.3 Zaštita integriteta podataka

Postoje razne tehnike za očuvanje integritet podataka, kao što su kriptografski kontrolni zbroj, verifikacija dolaznih podataka, kreiranje sigurnosnih kopija, revizijski tragovi i slično.

5.3.1 Kriptografski kontrolni zbroj

Kontrolni zbroj ili poznatiji pod engleskim nazivom *checksum* se koristi kao provjera da podatci nisu bili promijenjeni prilikom transporta. Kontrolni zbroj je broj bitova u poruci koju želimo proslijediti, postavlja se nakon šifriranja poruke, bilježi se duljina šifirane poruke. Kada poruka stigne na krajnji cilj provjerava se vrijednost kontrolnog zbroja i ako je izračunata vrijednost imalo drugačija od originalne to označava da je poruka oštećena ili potencijalno mijenjana. Postoji više razloga zašto je poruka oštećena od loše veze i problema u sklopovlju, do namjerne promjene podataka uzrokovane hakerima.

5.3.2 Verifikacija dolaznih podataka

Verifikacija dolaznih podatka je proces testiranja podataka koju je aplikacija primila. Postoje dvije vrste verifikacije dolaznih podataka, dozvoljene (eng. *whitelist*) i ne dozvoljene (eng. *blacklist*). Dozvoljena verifikacija provjerava da li primljeni podatak odgovara setu poznatih pravila, dok *blacklist* verifikacija provjerava da li primljeni podatak ne sadrži potencijalno opasne segmente.

Ako je odluka spala na *whitelist* provjeru onda bi trebalo provjeravati slijedeće stavke:

- **Vrstu podatka** - da li vrsta dolaznog podataka odgovara onomu što smo očekivali? Tipa ako se očekuje slika treba provjeriti je li primljeni podatak stvarno slika a ne nekakva skripta ili nešto slično tomu, ako se očekuje broj treba provjeriti da li je onda broj stvarno i primljen.
- **Dužinu podatka** - provjerava se da li primljeni podatak odgovara traženoj dužini, to jest gleda se da li je duži od očekivane maksimalne dužine ili je pak kraći od minimalne dopuštene dužine, ako se očekuje broj gleda se je li u traženom rasponu.

Za *blacklist* verifikaciju provjerava se da li primljeni podatak sadrži poznate zabranjene znakove ili uzorke. Verifikacija podataka može poslužiti i kao prevencija napada poznatog kao Structured Query Language (SQL) injekcija. SQL injekcija je napad gdje napadač unosi zlonamjerni SQL kod u polje za unos kako bi poremetio

bazu podataka.

5.3.3 Sigurnosne kopije podataka

Velik broj kompanija ovisi o podacima da bi poslovali, dogodi li se trajni gubitak podataka to može dovesti uzrokovati zatvaranjem kompanije. Stoga je izrazito bitno imati sigurnosne kopije podataka. Pošto se podatci stalno nadodaju ili mijenjaju potrebno je odrediti period koliko često će se izvršavati kopiranje, ovaj period je poznatiji kao Recovery Point Objective (RPO). Kraći RPO znači češće kopiranje ali ujedno je potrebno i više prostora za pohranu, kompjuterske moći i mrežnih resursa da bi vratili podatke u slučaju gubitka. Još jedan bitan period je vrijeme potrebno za povratak podataka od gubitka, Recovery Time Objective (RTO).

5.3.4 Revizijski tragovi

Revizijski trag je kronološki zapis događaja sa odredištem i izvorom koji pruža dokumentirane dokaze o slijedu aktivnosti nad određenom operacijom. Kao revizijski trag uobičajeno se prate: akcije nad bazom podataka, aplikacijski zapisi, zapisi operacijskih sustava, tko je kada pristupio serveru i njegovu IP adresu, zapise mrežnih uređaja i zapise specifične za aplikaciju 5.2.

Slika 5.2 Skupine revizijskih tragova [15]

Revizijski zapisi su jako korisni za praćenje da li se nešto potencijalno opasno događa, to jest moguće je da napadač ima pristup bazi podataka i da radi akcije nad njom a da to nitko ne primijeti, stoga se često revizijski zapisi provjeravaju u potrazi za čudnim događajima. Ako je već šteta načinjena revizijski zapisi mogu nas odvesti do počinitelja [15].

Poglavlje 6

Opasnosti za dostupnost podataka

Dostupnost podataka jamči da će podatci biti dosljedni i lako dostupni ovlaštenim korisnicima u bilo kojem trenutku.

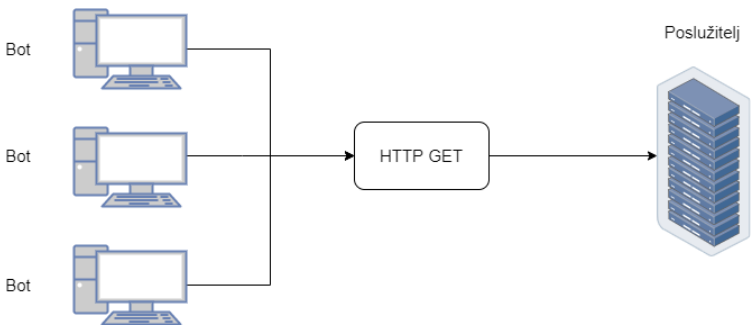
6.1 DDoS napad

Distributed Denial-Of-Service (DDoS) je jedan od često korištenih napada na dostupnost podataka. Cilj napada je zasuti ciljanu metu podacima kako bi se uzrokovao prestanak rada. DDoS se izvršava sa nizom uređaja spojenih u mrežu. Spomenuta mreža se sastoji od računala ili nekih drugih uređaja zaraženih zloćudnim programom koji dozvoljava udaljeno upravljanje. Ti pojedini uređaji zovu se *botovi* dok se mreža zove *botnet*. Pošto je svaki *bot* stvarni uređaj razdvajanje štetnog prometa od normalnog je po prilično teško za izvesti, stoga je DDoS jedan od najvećih problema kiber sigurnosti. Postoje razne tehnike za ostvarenje ovog napada ali više manje sve rade na principu zatrpavanja prometom.

6.1.1 Napad na aplikacijski sloj

Još znan kao napad na sloj 7 koristi HTTP protokol da bi preplavio poslužitelja, HTTP poplava je jedan od DDoS napada na aplikacijski sloj (Slika 6.1). Kako za HTTP zahtjev poslužitelj treba učitati nekakve datoteke i izvršiti funkcije nad bazom,

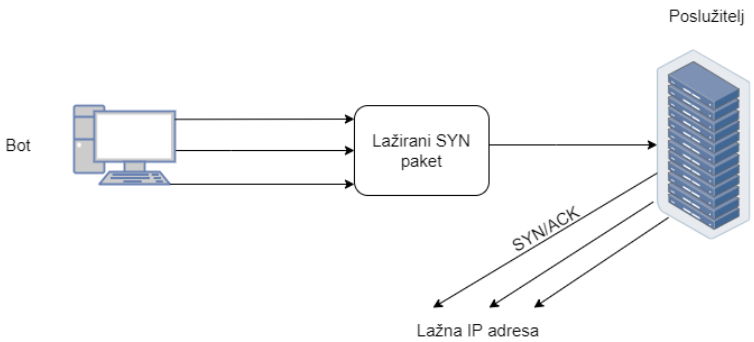
odgovor na HTTP može trajati neko vrijeme. Cilj je napasti funkcije koje zahtijevaju više resursa da bi se izvele, kao što je preuzimanje velikih datoteka ili predaja nekih većih obrasca. HTTP poplava je inače dosta lakša za izvesti od nekih drugih vrsta DDoS-a pošto ne zahtjeva veliku propusnost mreže. Sloj 7 DDoS napadi se inače smatraju "niskim i sporim", to jest nisu toliko efektivni naspram nekih drugih vrsta DDoS-a [16].



Slika 6.1 Primjer HTTP poplave

6.1.2 Protokol napadi

Protokol napadi se fokusiraju na slabosti u internetskim komunikacijskim protokolima specifično u trećem i četvrtom sloju, kako su ti protokoli u globalnoj upotrebi nije tako lako popraviti mane. Synchronize (SYN) poplava je primjer protokol napada, iskorištavajući protokol za uspostavu TCP veze, gdje prvo klijent šalje SYN paket poslužitelju, tada poslužitelj odgovara svojim SYN/Acknowledge (ACK) paketom i na kraju klijent potvrđuje uspostavljenu vezu sa ACK paketom. SYN poplava funkcionira na način da se šalju paketi sa lažnom IP adresom, poslužitelj tada otvara na zahtjev i ostavlja *port* otvorenim neko vrijeme kako bi mogao primiti potvrdu. Kako posljednji ACK paket neće nikad stići i kako napadač stalno šalje SYN pakete to forsira poslužitelja da stalno drži *port*-ove što ometa normalnu funkcionalnost (Slika 6.2) [16].



Slika 6.2 Primjer SYN poplave

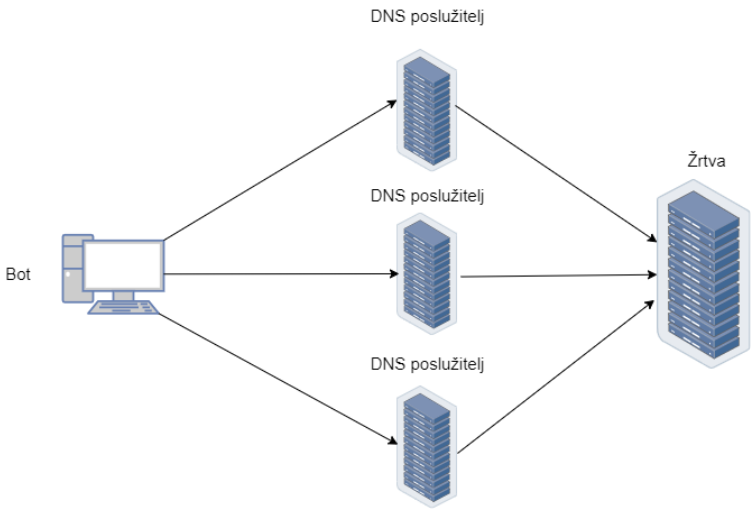
6.1.3 Volumetrijski napadi

Cilj ovog napada je iskoristiti svu propusnost mreže između izvora i cilja. Iskorištavajući razliku u cijeni zahtjeva napadač može slati relativno male upite koji rezultiraju mnogo većim odgovorima. Napad zvan Domain Name System (DNS) pojačanje se česti oblik volumetrijskog napada. Napadač šalje User Datagram Protoco (UDP) pakete DNS poslužitelju sa parametrom "ANY" tako da odgovori sa najvećim mogućim podacima, umjesto da ostavi svoju izvornu IP adresu napadač postavi žrtvinu, žrtva tada primi odgovor od DNS poslužitelja koji zapravo nije tražila (Slika 6.3) [16].

6.1.4 Sprječavanje DDoS-a

DDoS je poprilično problematičan za sprječavanje pošto je teško raspoznati korisnika od napadača. Napad može varirati od jednostavnog napada iz jednog izvora do kompleksnih multi vektorskih napada. Multi vektorski napad mijenja svoje principe napada, na primjer napada može započeti sa HTTP poplavom a zatim se prebaciti na DNS pojačanje. Što je napad kompleksniji to ga je teže raspoznati od stvarnog prometa.

Preusmjeravanje u crnu rupu - jedno riješenje je napraviti takozvanu *crnu rupu* i preusmjeriti sav promet u nju gdje se on ujedno i izgubi. Riješenje nije idealno pošto ako nije dobro implementirano sav dolazni promet se uništi i nitko nema pristup, što



Slika 6.3 Primjer DNS Pojačanja

je ujedno i cilj napadaču.

Ograničenje stope - drugi način je ograničiti broj zahtjeva koji će server prihvatiti kroz neki vremenski period. Funkcionira na način da prati vrijeme između zahtjeva po IP adresi, ako zaključi da zahtjevi dolaze prečesto može mu onda omogućiti slanje novog zahtjeva tek nakon nekog vremena. Ova zaštita je korisna protiv *web scrapper*-a i pokušaja *brute force* prijave.

Vatrozid web aplikacije - je jako koristan protiv DDoS-a koji cilja aplikacijski sloj. Postavljanjem vatrozida između Interneta i poslužitelja može zaštititi ciljani poslužitelj od zlonamjernog prometa. Cilj je postaviti niz pravila koji bi otkrili DDoS aplikacijskog sloja i spriječili ga, još jedna bitna stavka je mogućnost brzog dodavanja novih pravila.

Anycast mrežna difuzija - koristeći Anycast mrežu možemo razbacati pakete kroz mrežu povezanih poslužitelja to te točke da se paketi izgube u mreži. Naime Anycast je metoda mrežnog adresiranja i usmjeravanja gdje se paketi mogu usmjeriti na niz različitih lokacija. Uspješnost obrane sa Anycast mrežom ovisi o veličini napada i o

veličini i sposobnosti mreže.

6.2 Kvarenje opreme

Zakazivanje opreme može dovesti do pada usluge što znači da podatci neće biti dostupni, pri većim kvarovima moguće je da se podatci trajno izgube. Kada se dogode takve situacije iznimno je bitno što prije otkriti problem i popraviti ga. Jedan od najčešćih razloga prestanka rada poslužitelja jest pregrijavanje, ključno je održavati nisku temperaturu u prostoriji i pobrinuti se da oprema ima dobar protok zraka. Drugi česti razlog je preopterećenje, uzrok može biti preveliki promet što dovodi do usporavanja ili potpuno zaustavljanje rada poslužitelja. Preopterećenje se još može desiti ako neke operacije koriste veliku propusnost mreže, procesi koriste previše Random Access Memory (RAM) ili se iscrpi procesorska moć. Prestanak rada poslužitelja ne mora značiti da je uvijek oprema kriva, zastarjeli Operating System (OS) također može zakazati pod zahtjevnim operacijama. Iako je korisno što češće ažurirati programe pri ažuriranju programa koji se nalazi na poslužitelju potrebno je biti oprezan kako nova verzija ne bi prouzrokovala neke nove probleme ili oštetila podatke.

6.2.1 Minimiziranje kvarova

Za minimalizaciju kvara opreme i vrijeme zastoja korisno je implementirati softver preko kojeg se može pratiti stanje kritičnih sistema. Česta inspekcija opreme je obvezna pošto je takvu vrstu zastoja najteže predvidjeti. Korištenjem prediktivne analitike može se predvidjeti kada će se koji dio pokvariti. Za zaštitu od neplaniranih slučajeva prestanka rada potrebno je imati spreman Disaster Recovery Plan (DRP), što može podrazumijevati rezervne poslužitelje, dodatni RAM i sekundarni izvor napajanja.

Poglavlje 7

Implementacija povjerljivosti, integriteta i dostupnosti

U nastavku cilj je navesti neke metode koje se koriste u IT industriji kako osigurali koncepte povjerljivosti, integriteta i dostupnosti, te koje bi stavke obavezno trebalo implementirati u aplikaciji koja koristi korisničke podatke.

7.1 Povjerljivost

Povjerljivost se odnosi na privatnost informacija i ovlaštenja za njihovo dijeljenje i korištenje. Informacije sa niskom povjerljivošću se smatraju ne prijetećim ako se prošire u javnost. Dok informacije sa visokom povjerljivošću trebaju biti tajne, pod te informacije bi spadale lozinke i osobni podaci o korisnicima. Kako kompanija nema apsolutno nikakvog razloga zašto bi trebao znati korisničke lozinke, pri spremanju u bazu sve lozinke bi se trebale šifrirati. Algoritmi za šifriranje kao što su DES, 3DES, SKIPJACK, RC2, RSA (ispod 1024 bita), MD2, MD5 i MD4 se smatraju probijenima te bi ih se trebalo izbjegavati. Preporučeno je koristiti AES (preko 128 bitova), RSA (preko 2048 bitova) i SHA2 (preko 256 bitova) kao trenutno najsigurnije algoritme [18]. Kontrola pristupa podacima također igra važnu ulogu u očuvanju povjerljivosti. Pristup podacima bi trebali imati samo oni korisnici kojima je to izrazito bitno, niži zaposlenici kojima nije potreban pristup cijelo bazi bi trebali imati ograničene

mogućnosti. Za prijavu koristiti što snažnije lozinke (nasumična velika i mala slova sa brojevima i znakovima) i Two-Factor Authentication (2FA). Svako toliko nakon nekog perioda potrebno je proći kroz listu korisnika sa dozvoljenim pristupima te ih ukloniti ako više nisu potrebni. Nisu svi podaci digitalni zato treba obratiti pažnju i na fizičke dokumente te se pobrinuti da su na sigurnom mjestu, isto tako se i treba pobrinuti da neautorizirani korisnici nemaju pristup uređajima. Jednom kad podaci više nisu potrebni ili mediji za pohranu više nisu u opticaju, podatke je potrebno na što sigurniji način uništiti. Jedna od najboljih metoda za uništavanje podataka na tvrdom disku je prepisati podatke, iako je jedna od sigurnijih metoda i dalje nije 100% sigurna. Kod Solid-State Drive (SSD) stvar je drugačija pošto se podaci ne mogu prepisati kao kod optičkih uređaja za pohranu, već se izvodi "ATA sigurnosno brisanje". ATA naredba funkcionira na način da uzrokuje nagle poraste napona na svim blokovima *flash* memorije kako bi izbrisala podatke. Ako želimo biti sigurni da podaci neće nikako moći biti vraćeni onda je najbolja opcija fizički uništiti uređaje. Zaposlenici u ozbiljnijim tvrtkama često potpisuju ugovore o neotkrivanju podataka koji ih zakonski obvezuju da podatke neće širiti izvan dozvoljenih granica.

7.2 Integritet

Očuvanje integriteta podataka je izrazito bitno, većina aplikacija i organizacija temelji svoju funkcionalnost na izmjenama informacija, stoga ako informacije nisu pouzdane i točne to može jako utjecati na organizacije ili aplikacije. Veće organizacije koje se oslanjaju na svoje zaposlenike za unošenje podataka nude treninge za unos podataka kako bi osigurali što manje grešaka. Što su podatci kvalitetniji to će biti i njihov integritet. Kvaliteta podataka se može mjeriti sa: točnošću, potpunosti, konzistentnosti, valjanosti, jedinstvenosti i pravovremenosti. Neke od najboljih i najpopularnijih alata za očuvanje kvalitete podataka su Ataccama, Informatica, Oracle Cloud Infrastructure Data Catalog i Talend Data Catalog. Kao što je navedeno u prijašnjem poglavlju (5.3.2) validacija dolaznih podataka, revizijski tragovi i sigurnosne kopije su bitna svojstva za očuvanje integriteta. Dupliciranje podataka je jedan od najvećih razloga za kršenje integriteta pošto može uzrokovati dvosmislenost. Tvrtke sa većim resursima imaju posebne odjele za rješavanje tog problema, dok se

manje koriste alate poput BleachBit, FSlint, rmlint, GDuplicateFinder i slično. Ako je aplikacija bazirana na web-u Secure Sockets Layer (SSL) certifikat je neizostavan [17]. Prema *Forbes advisoru* jedni od najboljih i najsigurnijih prodavača certifikata trenutno su Comodo, SSL.com, Sectigo, AlphaSSL, Entrust i GlobalSign [19].

7.3 Dostupnost

Ako podatci nisu dostupni u bilo kojem trenutku može doći do zastoja cijele aplikacije. U slučaju nedostupnosti informacija organizacije pokreću svoje planove za oporavak, to može uključivati RTO i RPO. Sigurnosne kopije su rješenje protiv trajnog gubitka podataka, što se više podataka može spasiti i što brže to bolje. Kopije se inače spremaju na drugačijem uređaju od onoga koji služi za prijenos podataka. Redundant Array Of Inexpensive Disks (RAID) polja su jedan od popularnih izbora za stvaranje kopije, RAID 10 se smatra najboljim po performansama i redundanciji ali je zato najskuplji jer mu je potrebno minimalno 4 diskova za pohranu. Ujedno treba i izbjegavati jednu točku kvara (SPOF), to jest grešku u dizajnu gdje bi jedna točka kvara mogla srušiti cijeli sustav. Korištenjem data loss prevention (DLP) alatima može se umanjiti rizik oštećivanja podataka. Neki od najpopularnijih alata su: Google Cloud Data Loss Prevention, Endpoint Protector by CoSoSys, Code42, Barracuda Backup, Arcserve UDP i slični. Još jedan koristan način za oporavak podatka je *erasure coding*, gdje se podatci dijele u fragmente, proširuju i šifriraju suvišnim dijelovima podataka i pohranjuju na niz različitih lokacija ili medija za pohranu. Jednom kad se podatci izgube mogu se rekreirati iz segmenta na drugim lokacijama. U posljednje vrijeme sve više se kompanije odlučuje za spremanje podataka u oblak ili hibridni model gdje su neki podatci spremljeni lokalno a neki u oblaku [20].

Poglavlje 8

Zaključak

U ovom radu su opisani koncepti informacijske sigurnosti: povjerljivost, integritet i dostupnost. Sva tri koncepta imaju zajedničku manu koja može ugroziti podatke: ljudsku grešku. Svi ljudi rade greške neovisno o tome koliko su oprezni, a jedna greška može biti dovoljna da se cijeli sustav ugrozi. Stoga je nemoguće imati neprobojan sistem, ono što jedne organizacije dijeli od drugih jest kad su hakirani koliko im treba za pronaći rupu i što poduzimaju da se to više ne ponovi. Enkripcija je jedan od ključeva zaštite informacija, trebala bi se koristiti u svim trima konceptima sa što modernijim i sigurnijim algoritmima za šifriranje. Metode za obranu koje se danas smatraju sigurnim već sutra mogu biti probijeni, stoga je izrazito bitno biti upućen u najnovije sigurnosne mehanizme. Nažalost ova tri koncepta sama se više ne smatraju dovoljnim za zaštitu informacija već im se nerijetkoj pridodaju koncepti kao što su autentičnost, ne poricanje, posjed, korisnost, pouzdanost i odgovornost.

Bibliografija

[1] Whitman, M.; Mattord, H.: "Management of information security", Cengage Learning, 2013.

[2] Trautman, L.; Ormerod, P.; "Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach", American University Law Review, Vol. 66, No. 5, 2017.

[3] Internet Organised Crime Threat Assessment, "Internet Organised Crime Threat Assessment (IOCTA) 2021", s Interneta, `https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf`, 2021.

[4] Moghaddasi, H.; Sajjadi, S.; Kamkarhaghighi, M.: "Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model", The Open Medical Informatics Journal, 2016.

[5] Smith, R.: "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles", IEEE Security & Privacy, Vol. 10, No. 10, pp. 20-25, 2012.

[6] Lundgren, B.; Möller, N.: "Defining Information Security", Science and Engineering Ethics, Vol. 25, pp. 419–441, 2017.

[7] York, D.: "Seven Deadliest Unified Communications Attacks", Elsevier, 2010.

[8] Vacca, J.: "Computer and Information Security Handbook", Todd Green, 2017.

[9] Gupta, G.: "What is Birthday attack??", s Interneta, `https://www.researchgate.net/publication/271704029_What_is_Birthday_attack`, veljača 2015.

[10] Kiprin, B.:"What is a downgrade attack and how to prevent it", s Interneta, `https://crashtest-security.com/downgrade-attack/`, travanj 2022.

[11] Proofpoint: "State of the Phish", s Interneta `https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical`, siječanj 2020.

[12] Mallik, A.: "MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS?", Jurnal Pendidikan Teknologi Informasi, Vol. 2, No. 2, pp. 109-134, 2018.

[13] Glick, N.: "How Does Email Spoofing Work and Why Is It So Easy?", s Interneta `https://www.proofpoint.com/us/corporate-blog/post/how-does-email-spoofing-work-and-why-it-so-easy`, kolovoz 2018

[14] IBM: "IBM Security Services 2014 Cyber Security Intelligence Index", s Interneta, `https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF`, 2014.

[15] Bozhanov B.: "What is an Audit Trail in IT Context?", s Interneta, `https://logsentinel.com/blog/what-is-an-audit-trail-in-it-context/?cookie-state-change=1655495114443`, ožujak 2019.

[16] CloudFlare: "What is a DDoS attack?", s Interneta, `https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/`

[17] Sharma, A.: "How to Ensure Data Integrity in Your Organization", s Interneta, `https://www.dataversity.net/how-to-ensure-data-integrity-in-your-organization/#`, siječanj 2021.

[18] OpenStack: "Security/Guidelines/crypto algorithms", s Interneta, `https://wiki.openstack.org/wiki/Security/Guidelines/crypto_algorithms`

[19] Watts, R.; Smith, N.: "The Best SSL Certificate Services To Buy From In 2022", s Interneta, `https://www.forbes.com/advisor/business/software/best-ssl-certificate-services/`, siječanj 2022.

[20] Tibco: "What is Data Availability?", s Interneta, `https://www.tibco.com/reference-center/what-is-data-availability`

Pojmovnik

2FA Two-Factor Authentication. 31

ACK Acknowledge. 26

AES Advanced Encryption Standard. 10

ARP Address Resolution Protocol. 18, 19

CBC Cipher Block Chaining. 12

CIA Confidentiality, Integrity and Availability. 5

DDoS Distributed Denial-Of-Service. vi, 25–28

DNS Domain Name System. 14, 19, 27

DRP Disaster Recovery Plan. 29

FTPS File Transfer Protocol Secure. 10

HTTP Hypertext Transfer Protocol. 19, 27

HTTPS Hypertext Transfer Protocol Secure. 9, 10, 19, 20

IOCTA Internet Organised Crime Threat Assessment. 2

IP Internet Protocol. 9, 19

IPsec Internet Protocol Security. 9

ISO International Organization for Standardization Model. 4, 6

Pojmovnik

MAC Media Access Control Address. 9, 19

MITM Man-In-The-Middle. vi, 12, 13, 18, 20

OS Operating System. 29

PKI Public Key Infrastructure. 10

RAID Redundant Array Of Inexpensive Disks. 32

RAM Random Access Memory. 29

RC4 Rivest Cipher 4. 10

RPO Recovery Point Objective. 23, 32

RTO Recovery Time Objective. 23, 32

SBC Session Border Controller. 8

SMTP Simple Mail Transfer Protocol. 15

SQL Structured Query Language. 22

SSD Solid-State Drive. 31

SSL Secure Sockets Layer. 32

SYN Synchronize. 26

TCP Transmission Control Protocol. 19, 26

TLS Transport Layer Security. 9, 12, 13

UDP User Datagram Protoco. 27

VPN Virtual Private Network. 8, 9

WAN Wide Area Network. 8

WEP Wired Equivalent Privacy. 10

WPA Wi-Fi Protected Access. 10

WPA2 Wi-Fi Protected Access 2. 9, 10

WPA3 Wi-Fi Protected Access. 9

Sažetak

U radu se prikazuju česte metode za narušavanje informacijskih koncepta povjerljivosti, integriteta i dostupnosti. Neki od navedenih i objašnjenih napad su: prisluškivanje, mrežna krađa identiteta, man-in-the middle te DDoS. Za svaki od napada navedene su i neke metode zaštita. Ukratko je objašnjeno šifriranje i dešifriranje podataka koji se razmjenjuju putem interneta te načini za probijanje šifriranja. Uz sve to, navedeni su i neki principi koji se koriste za implementaciju ovih triju sigurnosnih koncepta u modernoj IT industriji.

Ključne riječi — **dostupnost, integritet, povjerljivost**

Abstract

This paper shows common methods for violating the information concepts of confidentiality, integrity, and availability. Some attacks that are listed and explained are eavesdropping, phishing, man-in-the-middle, and DDoS. Protection methods for each of these attacks are also presented. We also briefly explained the encryption and decryption of data transferred over the internet and ways to break the encryption. In addition, some principles are listed that are used to implement these three security concepts in the modern IT industry.

Keywords —**availability, integrity, confidentiality**