Sigurnost baza podataka

Speranza, Roberto

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

ROBERTO SPERANZA

SIGURNOST BAZA PODATAKA

ZAVRŠNI RAD

Rijeka, 2023.

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

SIGURNOST BAZA PODATAKA
DATABASE SECURITY

ZAVRŠNI RAD

Kolegij: Baze podataka
Mentor: Izv. prof. dr. sc. Jasmin Ćelić
Student: Roberto Speranza
Studijski smjer: Elektroničke i informatičke tehnologije u pomorstvu
JMBAG: 0112069501

Rijeka, Svibanj 2023.

Student: Roberto Speranza

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112069501

IZJAVA O SAMOSTALNOJ IZRADI ZAVRŠNOG RADA

Kojom izjavljujem da sam završni rad s naslovom SIGURNOST BAZA PODATAKA izradio/la samostalno pod mentorstvom izv. prof. dr. sc. Jasmina Ćelića.

U radu sam primijenio metodologiju izrade stručnog/znanstvenog rada i koristio literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u završnom radu na uobičajen, standardan način citirao sam i povezao s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Student 

(potpis)

Roberto Speranza

Student: Roberto Speranza

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112069501

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Izjavljujem da kao student – autor završnog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Student - autor Speranza Roberto

(potpis)

SAŽETAK

Baza podataka je najsloženiji oblik strukture i organizacije podataka te ju možemo definirati kao jedinicu u koju se skladište sve informacije i podatci u svrhu jednostavnog pristupanja i upravljanja istima. Zbog povećanja količine podataka s kojom raspolažu tvrtke i organizacije, raste i važnost očuvanja sigurnosti baza podataka kako bi se spriječio neovlašteni pristup od strane zlonamjernih korisnika. Ugrađivanje sigurnosnih elemenata u Sustave za upravljanje bazama podataka predstavlja važan način za povećanje njene sigurnosti. Razinu sigurnosti informacijskog sustava, tehnologije i informacija koje informacijski sustav sadrži određuje sigurnosna politika. U ovom završnom radu cilj je prikazati koje sigurnosne prijetnje postoje, te koji su mogući načini sprječavanja napada i zaštite podataka.

Ključne riječi: *baza podataka, načini zaštite podataka, sigurnosne prijetnje, sustav za upravljanje bazama podataka, zlonamjerni korisnici*

SUMMARY

Database is the most complex form of data structure and organization, which can be defined as a unit in which all information and data are stored for the purpose of easy access and management. Due to the increase in the amount of data that companies and organizations posses, it is important to maintain the security of databases in order to prevent unauthorized access by malicious users. Incorporating security elements into Database Management Systems is an important way to increase its security. The level of security of the information system, technology, and information that the information system contains is determined by the security policy. In this final paper, the aim is to present what security threats exist, as well as possible ways to prevent the attack on the database or how to protect data.

Keywords: *database, data protection methods, database management system, malicious users, security threats*

SADRŽAJ

SAŽETAK ..... **I**
SUMMARY ..... **I**
SADRŽAJ ..... **II**
1. UVOD **1**
2. BAZE PODATAKA **2**
2.1. POVIJEST BAZA PODATAKA 2
2.2. SIGURNOSNA POLITIKA 3
3. SIGURNOSNE PRIJETNJE BAZAMA PODATAKA **4**
3.1. SQL UMETANJE 4
3.1.1. Klasično SQL umetanje *5*
3.1.1.1. SQL umetanje temeljeno na grešci 5
3.1.1.2. SQL umetanje korištenjem operatora UNION 6
3.1.2. Slijepo SQL umetanje *7*
3.1.2.1. SQL umetanje temeljeno na vremenskom odzivu 8
3.2. DOS NAPADI 8
3.2.1. Razlika između DOS-a i DDOS-a *11*
3.2.2. Zaštita protiv DOS napada *13*
3.3. ZLONAMJERNI PROGRAM 13
3.4. NEREGULIRANOST I ZLOUPOTREBA PRIVILEGIJA 16
3.5. PRISTUP SIGURNOSNOJ KOPIJI 16
3.6. „PHISHING“ I „SPOOFING“ – PRIJEVARE PUTEM ELEKTRONIČKE POŠTE 17
3.7. RANJIVOST AUTENTIFIKACIJA 19
4. ZAŠTITA BAZA PODATAKA **21**
4.1. KONTROLA PRISTUPA 21
4.1.1. Načela i načini izvođenja kontrole pristupa *22*
4.1.2. Mehanizmi kontrole pristupa *22*
4.1.2.1. Diskretna kontrola pristupa - DAC 23
4.1.2.2. Obavezna kontrola pristupa - MAC 23
4.1.2.3. Kontrola pristupa temeljena na ulogama - RBAC 24
4.2. AUTENTIFIKACIJA 24
4.3. ŠIFRIRANJE PODATAKA 26
4.4. SIGURNOSNA KOPIJA 27

4.5. SUSTAV ZA OTKRIVANJE I SPRJEČAVANJE PROVALA 29
4.6. VATROZID 31
5. DODATNI NAČINI ZAŠTITE BAZA PODATAKA 32
5.1. FIZIČKA ZAŠTITA BAZE PODATAKA 32
5.2. EDUKACIJA O INFORMACIJSKOJ SIGURNOSTI 33
6. ZAKLJUČAK 35
7. LITERATURA 36
8. POPIS SLIKA 42
9. POPIS KRATICA 43

1. UVOD

Podatci su najvažnija imovina koju jedna tvrtka ili organizacija može posjedovati. Kako bi se velika količina podataka i informacija organizirala i prikupila na jednome mjestu, stvorene su baze podataka. Podatci koji se nalaze unutar baza podataka opisuju stanje u realnom svijetu, npr. količinu robe na zalihi u pojedinoj trgovini, dostupne knjige u knjižnici ili informacije o pojedinoj osobi u gradskoj upravi.

Budući da se u današnje vrijeme baze podataka većinom nalaze u obliku digitalnih zapisa te s obzirom na to da je upotreba interneta dio svakodnevice potrebno je obratiti pozornost na računalnu sigurnost i računalne sigurnosne mehanizme, te time i zaštitu podataka.

Cilj rada je prikazati najčešće oblike sigurnosnih prijetnji bazama podataka uključujući SQL umetanja, DOS i Malware napade, nereguliranost i zloupotreba privilegija u sustavima, neadekvatno sigurnosno kopiranje, Phishing i Spoofing prijevare te ranjivost mehanizama autentifikacije, a uz to i definirati glavne načine zaštite baze podataka koji trebaju biti neizostavni dio svakog sustava. Neki od njih su kontrola pristupa, autentifikacija, šifriranje podataka, kontinuirano stvaranje sigurnosne kopije, korištenje sustava za otkrivanje i sprečavanje provale te upotreba vatrozida.

2. BAZE PODATAKA

Baze podataka (eng. *Database*) su po definiciji međusobno povezani skup informacija i podataka, najčešće zapisanih u digitalnom obliku [1]. Dakle, riječ je o organiziranoj zbirci informacija za jednostavnije upravljanje, u svrhu njihovog uređivanja, bilježenja, brisanja i dodavanja pomoću posebnih programskih alata. Možemo ih klasificirati prema sadržaju na bibliografske, tekstualne, numeričke i multimedijske te prema načinu pohrane na digitalne i fizičke baze podataka [1, 2]. Digitalne baze podataka se obično čuvaju na vanjskoj memoriji računala ili poslužitelja. Baza podataka može biti pohranjena i u fizičkom obliku kao dokumenti koji se pohranjuju u arhivama [1]. Programski alati kojima se može upravljati bazama podataka nazivaju se SUBP – Sustavi za upravljanje bazama podataka (eng. DBMS-Database Management System), a jedni od najpoznatijih danas su: Oracle, MySQL, Microsoft SQL server [1, 2].

2.1. POVIJEST BAZA PODATAKA

Povijest baza podataka seže u 1960-e, kada su se pojavile prve baze podataka koje su bile fizički čuvane na magnetskim vrpcama i disketama. Početkom 70-ih godina prošlog stoljeća, informatičar i znanstvenik Edgar. F. Codd objavio je akademski rad pod nazivom „Relacijski model podataka za velike banke“ (eng. „A Relational Model of Data for Large Shared Banks“). U radu je naveo novi način konstruiranja podataka gdje bi se u međusobno povezane tablice omogućavala pohrana bilo kojeg podatka samo jednom. Na taj način se mogao dobiti odgovor na bilo koje pitanje ukoliko je odgovor bio pohranjen unutar baze. 80-ih i 90-ih godina baze podataka postale su sveprisutne zahvaljujući indeksima koji su omogućili bolju obradu upita. SQL (eng. *Structured Query Language*) je postao programski jezik baza podataka. Ondašnje relacijske baze podataka bile su namijenjene za korištenje na samo jednom računalu te je količina podataka koju mogu stvoriti milijarde ljudi bila prevelika za jedan poslužitelj. Jedini način za obradu svih podataka bio je umrežvanje i povezivanje poslužitelja baza podataka. Početkom 20. stoljeća SQL baze su bile i dalje popularne, ali za korisnike kojima je bilo potrebno procesiranje,fleksibilnost i snažne performanse u obliku obrade podataka počeo se koristiti NoSQL. Ove baze podataka optimizirane su za aplikacije i proizvode koje obrađuju velike količine podataka, na primjer: društvene mreže, internet aplikacije i internet trgovine. Karakteristika ovih baza je ta da se tip i broj atributa nekog entiteta može promjeniti bez utjecaja na ostale podatke. [4–7].

2.2. SIGURNOSNA POLITIKA

Informacijski sustavi brojnih tvrtki i institucija danas pohranjuju velike količine povjerljivih i osjetljivih podataka koje je potrebno zaštititi od neovlaštenog pristupa i zlonamjernih aktivnosti. Tvrtke i institucije ili oni koje sadrže velike količine povjerljivih podataka, moraju svojim korisnicima omogućiti pristup željenim podacima. Međutim, dostupnost interneta u današnje vrijeme te lakoća i jednostavnost pristupa podatcima predstavlja prijetnju koja može ugroziti korisnike i podatke. Stoga je potrebno obratiti pažnju na sigurnost cijelog sustava.

Sigurnosna politika je skup pravila i postupaka kojima se određuje razina sigurnosti jednog informacijskog sustava, istovremeno pridajući pažnju sigurnosti tehnologije i informacija koje informacijski sustav sadrži. Potrebno je poštovati pravila koja su definirana sigurnosnom politikom, a u suprotnom, moguće su sankcije i kazne od strane nadležnih institucija. Sigurnosnu politiku unutar jedne tvrtke ili organizacije potrebno je dati na uvid svakom korisniku prije korištenja računalne opreme. Implementacijom iste, korisnicima se određuju pravila ponašanja i korištenja opreme. Sigurnosna politika baza podataka može sadržavati pravila o obaveznoj provjeri identiteta korisnika prilikom povezivanja, potrebu za šifriranjem podataka u svrhu zaštite od neovlaštenog pristupa, potrebu za redovnom izradom sigurnosne kopije u svrhu očuvanja podataka u slučaju kvara ili greške u sustavu, te druge sigurnosne značajke [8].

3. SIGURNOSNE PRIJETNJE BAZAMA PODATAKA

Baze podataka često sadrže osjetljive podatke poput financijskih podataka koji se moraju zaštititi od neovlaštenog pristupa. Korištenje sigurnosnih protokola i mjera zaštite, poput šifriranja, dvofaktorske autentifikacije i sigurnosnog nadzora od velike je važnosti za sprječavanje gubitka podataka te za očuvanje privatnosti korisnika. Proces osiguranja i zaštite baza podataka nije jednostavan te može predstavljati problem za korisnike koji nisu informatički educirani i/ili upućeni u njihov rad i način funkcioniranja. Unatoč tome što mogućnost pristupanja bazama podataka putem interneta pojednostavljuje korištenje istih sa računala na udaljenoj lokaciji, s druge strane može imati veliki nedostatak u pogledu zaštite i sigurnosti. Jedan od načina zaštite baze podataka je taj da se napadačima onemogući fizički pristup računalu na kojem se podatci pohranjuju. Uz fizičku zaštitu postoji i programska zaštita baza podataka kojom se korisnicima daje definirano ovlaštenje koje im omogućuje pristupanje putem svojih računa, koristeći korisničko ime i lozinku. Tu dolazi do značaja uloga „Administratora“ baza podataka koji ima funkciju odrediti razinu prava i pristupa koju će svaki korisnik imati. Nažalost, jedna od najčešćih grešaka jesu upravo neregulirane privilegije unutar baza podataka. Jedan od nedostataka programske zaštite koji se klasificira kao ljudska greška je upotreba jednostavnih, odnosno predvidljivih lozinki. Osim toga, pohranjivanje lozinki u obliku tekstnog dokumenta na računalu ili na više računala može predstavljati opasnost za sigurnost baze u slučaju pojave računalnog virusa (malware) koji takve podatke može preuzeti i napraviti štetu samoj bazi podataka i njenim korisnicima [4, 9].

3.1. SQL UMETANJE

SQL je programski jezik namijenjen za komunikaciju i pristup bazama podataka. SQL umetanje (eng. *SQL injection*) može se definirati kao kibernetički napad u kojem napadač, odnosno neovlašteni korisnik zlonamjerno ubacuje određeni SQL kod u polja koja su predviđena za unos podataka koje koristi aplikacija baze podataka, a sve u svrhu neovlaštenog pristupa određenim podatcima iz baza podataka. Napad je moguće izvesti ukoliko se podatci koje korisnik unosi ne provjeravaju na ispravan način. Sam napad nije namjenjen direktnom pristupu SUBP, već je namijenjen promjeni upita koji se šalje Internet aplikaciji koja potom mijenja SQL upit koji se šalje bazi podataka. Ukoliko napadač dobije pristup bazi podataka ima mogućnost modificirati, brisati te pregledavati podatke iz baze. Ovaj tip napada je naveden na „Open Web Application Security Project“ (OWASP) top 10 listi najučestalijih sigurnosnih rizika za internet aplikacije [10, 11].

Primjer SQL umetanja gdje napadač pokušava zaobići sustav autentifikacije prikazan je na sljedeći način:

```
SELECT id FROM users
WHERE username = 'user' AND password = 'pass'
```

U gore navedenom SQL upitu provjerava se ukoliko baza podataka sadrži korisničko ime s imenom „user“ koji ima lozinku „pass“. Ukoliko korisnik postoji i lozinka je točna, odobrava mu se pristup u aplikaciju.

Ukoliko napadač na kraju SQL upita doda “OR 5=5“, upit će izgledati ovako :

```
SELECT id FROM users
WHERE username = 'user' AND password = 'pass' OR 5=5'
```

Zbog toga što je izraz 5=5 istinit, cijeli WHERE uvijet postaje istinit bez obzira na upisano korisničko ime i lozinku. WHERE uvijet će dati rezultat prvog korisnika unutar tablice „users“ što je nerjetko račun od administratora baze podataka ili aplikacije [12].

3.1.1. Klasično SQL umetanje

Klasično (eng. *In-band*) SQL umetanje je tip napada koji zlonamjerni korisnik koristi kako bi mogao manipulirati SQL upitom (eng. *Query*) koji se izvršava unutar baze podataka. Karakteristika ovog napada je da napadač prima rezultat izravno, koristeći isti komunikacijski kanal, što znači da ukoliko napadač izvršava SQL umetanje putem internet preglednika, rezultati napada odnosno podatci iz baze podataka će biti prikazani unutar istog internet preglednika. Klasično umetanje može se podjeliti na SQL umetanje koje se temelji na grešci i ono koje se temelji na korištenju operatora UNION [13].

3.1.1.1. SQL umetanje temeljeno na grešci

Jedan od načina klasičnog SQL umetanja je ono temeljeno na grešci. Greške kao rezultati unutar internet aplikacija su dobre značajke jer daju programerima informacije na što treba obratiti pažnju prilikom izrade aplikacije, ali unatoč tome greške kao rezultat ne bi trebale biti vidljive svim korisnicima. Zlonamjerni korisnik namjerno izaziva grešku baze podataka koja potom daje informacije odnosno rezultat o grešci koju napadač koristi za daljnji napad. Na temelju greške napadač može otkriti vrstu, verziju i strukturu baze podataka što mu može pomoći pri izvođenju i planiranju daljnjeg napada. Dodavanjem posebnih SQL znakova u polje za pretraživanje unutar internet preglednika ili internet

aplikacije izaziva se greška unutar baze podataka, a ukoliko baza podataka nije zaštićena od ove vrste napada, unutar internet preglednika odnosno interent aplikacije pokazat će se informacije o grešci [14].

Primjer URL-a internet stranice kojoj pristupamo izgleda ovako:

http://example.com/page.php?id=5

Dodavanjem jednog od posebnih SQL znakova „ ' „ na kraju URL-a provjeravamo ako je internet stranica podložna SQL umetanju:

http://example.com/page.php?id=5'

Ukoliko se unutar Internet preglednika pokaže informacija o grešci, baza podataka je podložna SQL umetanju [15].

Primjer greške koju takva vrsta napada može izazvati prikazana je na slici 1.

Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"@`%>![]*$;:?^<.{}+-=~\#' AND password='' at line 1
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username=""@`%>![]*$;:?^<.{}+-=~\#' AND password=''

Slika 1 Primjer greške koju izaziva napad SQL umetanje

Izvor: Napravljena slika zaslona iz ***SQL injection lesson 1 - error based injection***, NFE Systems Ltd, https://www.youtube.com/watch?v=5ulehtDTuvE (06.03.2023.)

3.1.1.2. SQL umetanje korištenjem operatora UNION

Drugi način klasičnog SQL umetanja zasniva se na korištenju operatora UNION. Operator UNION se koristi u SQL-u kako bi se kombinirali rezultati više SELECT upita u jedan skup rezultata. Pomoću operatora UNION moguće je dobiti dodatne podatke koji nisu bili predviđeni za prikaz. Za primjer možemo uzeti Internet stranicu koja svojim registriranim korisnicima omogućuje čitanje knjiga.

```
SELECT * FROM knjige

WHERE imeKnjige = '[Smogovci]';
```

Upit pretražuje sve redove u tablici „knjige“ naziva „Smogovci“. Ukoliko napadač unese “ ' ' UNION SELECT , userID, password FROM korisnici – „ dobiva se upit koji izgleda na sljedeći način:

```
SELECT * FROM knjige

WHERE imeKnjige = ' '

UNION SELECT , userID, password FROM korisnici --';
```

U ovom slučaju UNION spaja dva upita, prvi upit ispisuje sve knjige iz tablice „knjige“, a drugi upit ispisuje sve lozinke i korisnička imena iz tablice „korisnici“. Dvije crtice u SQL kodu obično označuju komentar što znači da se ostatak upita, ukoliko postoji nakon dvije crtice, predstavlja kao komentar. Korištenjem ovog upita napadač može uklanjati podatke iz baze, ukrasti ili promijeniti neke podatke [14].

3.1.2. Slijepo SQL umetanje

Slijepo SQL umetanje (eng. *Blind SQL injection*) je napad gdje napadač šalje upite bazi podataka u tipu *Boolean* (točno ili netočno, 1 ili 0) i na temelju toga napadač zaključuje ako je upit ispravan u odnosu na ono što internet aplikacija daje kao rezultat. U ovom slučaju podatci se ne prenose napadaču direktno kroz aplikaciju baze podataka kao kod klasičnog umetanja, ali zbog toga ova vrsta napada nekad može biti i veća opasnost zato što je sustav ne detektira kao grešku. Ovaj tip napada koristi se uglavnom nakon pokušaja klasičnog umetanja kada internet aplikacija baze podataka ne daje rezultat koji predstavlja grešku u SQL upitu. Primjer takvog napada može se prikazati na Internet trgovini koja ima određene proizvode u prodaji [16–18].

https://www.webshop.org/item.php?id=14

SQL upit za prikaz iznad navedene stranice i proizvoda izgleda ovako:

```
SELECT * FROM table_name WHERE id = 14
```

Napadač može pokušati Slijepi SQL napad tako što će postaviti „lažan“ *Boolean* upit.

https://www.webshop.org/item.php?id=14 and 1=2

SQL upit za prikaz ove stranice izgleda ovako:

SELECT * FROM table_name WHERE ID = 2 and 1=2

U ovom slučaju ukoliko je baza podataka podložna Slijepom SQL umetanju, na stranici se neće prikazati ništa što će nam dati do znanja da je izraz „lažan“. Napadač potom počinje sa umetanjem „točnog“ *Boolean* upita.

https://www.webshop.local/item.php?id=14 and 1=1

SQL upit izgledati će ovako:

SELECT * FROM table_Name WHERE ID = 14 AND 1=1

Ukoliko dobijemo drugačiji odgovor od strane internet aplikacije za ovaj upit u odnosu na „lažan“ upit, napadač može zaključiti kada je upit koji je poslao točan ili netočan [17].

3.1.2.1. SQL umetanje temeljeno na vremenskom odzivu

Ova vrsta napada radi tako što napadač unutar upita postavlja takozvano „vrijeme čekanja“ gdje onda na temelju vremena čekanja doznaje ukoliko je SQL upit koji je poslan, točan ili lažan.

Primjer takvog upita u obliku URL-a izgleda ovako:

https://www.webshop.org/item.php?id=34 and if(1=1, sleep(10), false)

Ukoliko se od strane aplikacije i baze dobije odgovor nakon 10 sekundi, stranica je podložna SQL umetanju [18].

3.2. DOS NAPADI

DOS (eng. *Denial of service*) ili napad s uskraćivanjem usluge je uz SQL umetanja jedan od najpoznatijih i najčešćih napada na internet usluge i aplikacije, a samim time i baze podataka. U odnosu na SQL umetanje gdje je cilj samog napada doći do povjerljivih informacija iz baze podataka te na taj način napraviti štetu vlasniku usluge, kod DOS napada je cilj učiniti uslugu nedostupnu normalnom korisniku te shodno tome nanijeti štetu pružatelju usluge. DOS napad se postiže slanjem velikog broja zahtjeva u istom trenutku u kojem poslužitelj (eng. *server*) ne može obraditi sve zahtjeve što dovodi do preopterećenja

sustava u obliku usporavanja i na kraju nedostupnosti usluge za normalne korisnike [19]. Za lakše razumjevanje, ova vrsta napada se može objasniti i na primjeru iz stvarnog života. Za primjer se može uzeti jedna fizička trgovina koja se bavi prodajom računalne opreme. Osoba ili u ovom slučaju napadač koji želi ostalim kupcima onemogućiti kupnju u trgovini može unajmiti drugu osobu (napadač može biti i sama ta osoba) koja će biti u trgovini dovoljno dugo te zadržavati prodavača što će rezultirati odlaskom ostalih kupaca (u ovom slučaju, normalnih korisnika) zbog predugog čekanja i nedostupnosti same usluge. U pravilu kupac odlazi u drugu trgovinu koja pruža sličnu uslugu.

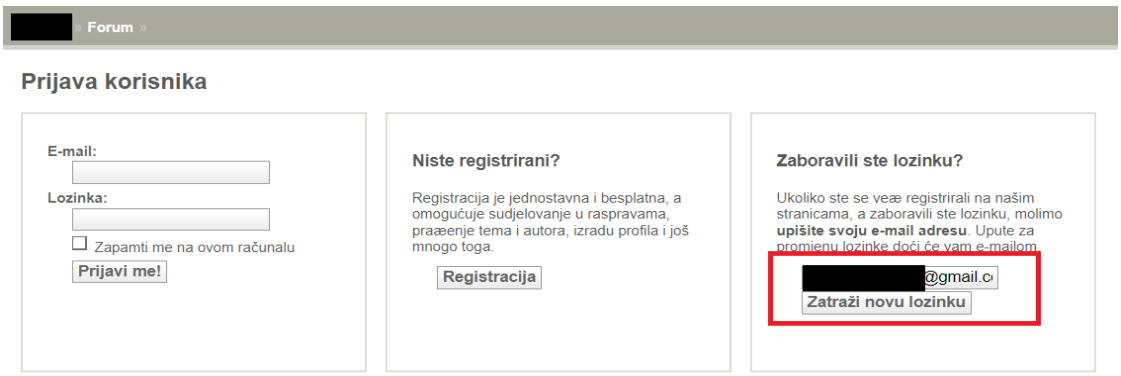
DOS napadi na baze podataka mogu se podijeliti na:

1. Zloupotreba funkcija

   Ovaj napad funkcionira prema logici Internet aplikacije gdje se koriste vlastite sposobnosti i mogućnosti aplikacije, ali u ovom slučaju dolazi do prekomjerene upotrebe istih što dovodi do opterećenja sustava. Najjednostavniji tip ovog napada u slučaju neke internet aplikacije jest upotreba „zaboravljena lozinka“ kao inače normalne funkcije. Ukoliko ograničenja nisu dobro izvedena u sustavu može biti poslano nebrojeno puno upita „zaboravljena lozinka“ što na kraju dovodi do opterećenja sustava [20, 21].

   Primjer napada prikazan je na slikama 2 i 3.

   Zahtjev za potražnjom nove lozinke poslan je na email, što je normalna radnja na bilo kojoj vrsti Internet aplikacije gdje postoji prijava korisnika.



Slika 2 Primjer napada "Zloupotreba funkcije"

Izvor: Izradio student pomoću opcije slikanja zaslona na vlastitom primjeru napada “Zloupotreba funkcije”

U sljedećem koraku ponovno postoji mogućnost zatražiti novu lozinku bez ikakvog vremenskog ograničenja između zahtjeva. Na primjeru je vidiljvo da je zahtjev za promjenom lozinke poslan dva puta u jednoj minuti.

Slika 3 Primjer napada "Zloupotreba funkcije" (nastavak)

Izvor: Izradio student pomoću opcije slikanja zaslona na vlastitom primjeru napada "Zloupotreba funkcije"

U slučaju napadača to bi bilo puno više kroz jednu minutu jer zaštita nije ispravno izvedena. Kada bi Internet aplikacija imala sustav da radi tako da ukoliko se pošalje jedan upit za promjenom lozinke te da isti nije više moguće poslati unutar idućih 24 sata, tada se taj tip napada nebi mogao izvesti.

2. Napad upotrebom kompleksnih upita

   Ovaj napad funkcionira na kompleksnom procesiranju i iscrpljivanju resursa poslužitelja baze podataka. Ciljano se šalju kompleksni upiti bazi podataka čime se opterećuje procesorska jedinica i memorija poslužitelja što dovodi do opterećenja cijelokupnog sustava. Za lakše shvaćanje, ovaj napad može se također predočiti na primjeru taxi službe koja raspolaže svojim vozačima. Napadač može naručiti 100 taxi vožnji što će dovesti do opterećenja unutar taxi službe i uz to ni jedna od tih vožnji neće donijeti financijsku profit taxi službi niti će biti dostupan taxi prijevoz korisnicima kojima to stvarno treba [21].

3. Greške unutar koda

   Napadači u ovom slučaju ciljaju i koriste greške unutar baza podataka. Pomoću posebnih zlonamjernih skripti moguće je napraviti beskonačnu petlju koja će cijelo vrijeme koristiti grešku (eng. *bug*) baze podataka te ju na taj način preopteretiti.

4. Aplikacijski napadi

   Aplikacijski napadi predstavljaju najkompleksniji tip napada koji je zbog svoje kompleksnosti težak za detekciju. Težina detekcije proizlazi iz toga što se u slučaju ovog tipa napada ne koristi velika količina mrežnih resursa te ih je u usporedbi sa ostalim napadima gdje se koriste velike količine mrežnih resursa teže detektirati [21, 22].

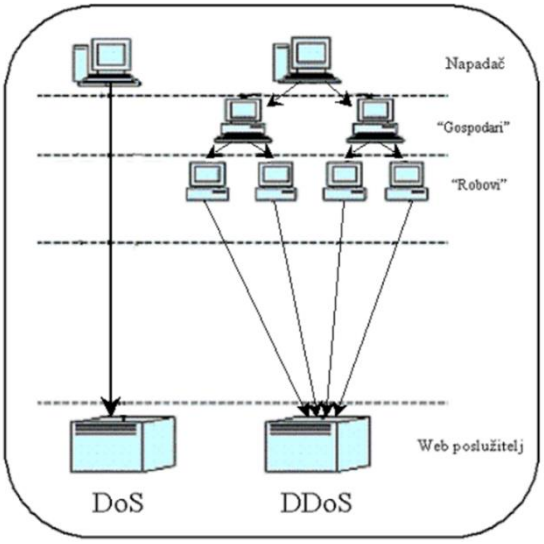
Najčešći razlozi DOS napada su:

1. Financijske prirode gdje kriminalne organizacije putem ilegalnih Internet stranica nude svoje DOS usluge u zamjenu za novac, a plaćanje se u današnje vrijeme najčešće izvršava u obliku kriptovaluta. Također, jedan od načina postizanja financijske dobiti je kada se napadne određena Internet stranica ili aplikacija, ali se ne sruši u potpunosti nego se samo pokaže „moć“ napada tako što se na kratko uspori rad iste. U tom slučaju, vlasnici Internet stranica i aplikacija moraju platiti kriminalnoj organizaciji određenu količinu novaca u zamjenu za prestanak napada.
2. Pojedinci provode napade iz zabave, a većina zbog stjecanja slave i statusa unutar pojedinih grupa u društvu. U današnje vrijeme, ilegalnim forumima koji sadržavaju pojedine programske skripte, može pristupiti bilo tko što osobama koje nemaju prevelikog znanja u sklopu mreža olakšava izvršavanje napada. Takva skupina napadača naziva se još i „script kiddies“.
3. Nezadovoljni korisnici određenih usluga također mogu biti razlog DOS napada. Sama usluga ne mora biti cilj napada pojedinog korisika već njegov cilj može biti neki drugi korisnik iste usluge. Vrsta napada gdje korisnik nad drugim korisnikom iste usluge želi izvršiti napad, najčešće zbog neke vrste osvete se odnosi na mrežne odnosno „multiplayer“ video igre. Napad izgleda tako da se šalju Internet paketi prema korisnikovoj IP adresi koju je napadač pridobio koristeći IP Grabber. IP Grabber je aplikacija koja napadaču šalje podatke o korisnikovoj IP adresi nakon što korisnik klikne na određenu poveznicu misleći da je otvarao nešto normalno poput informativnih članaka i slično.
4. Politički razlozi također su jedni od razloga za napad na pojedine tvrtke i organizacije, pri čemu im cilj nije novac nego politička ideologija. Najpoznatija organizacija koja stoji iza najvećih hakerskih napada u 21. stoljeću koja uključuju i DOS napade je grupa „Anonymous“ [23].

3.2.1. Razlika između DOS-a i DDOS-a

DOS i DDOS (eng. *Distributed denial of service*) kao napadi imaju isti cilj, međutim riječ „Distributed“ ili raspodjeljeno uskraćivanje usluge nam ukazuje na bitnu razliku između ove dvije vrste napada. U slučaju DOS napada, napadač šalje veliku količinu zahtjeva u obliku upita sa samo jednog računala (Slika 4). Takav napad je lako izolirati i spriječiti jer se u slučaju pojave velikog broja zahtjeva sa jednog računala ili jedne IP adrese

ono blokira i ne daje mu se više mogućnost slati zahtjeve što olakšava servisu i sustavu da nastavi raditi normalno. U slučaju DDOS napada, napadač šalje veliku količinu zahtjeva, ali ovog puta to nije sa samo jednog računala nego sa puno više računala istovremeno sa više različitih lokacija (Slika 4). Sama činjenica da se zahtjevi šalju sa više računala, a ne samo sa jednog govori nam da je ovakav napad puno teže izolirati i blokirati jer sustav mora prepoznati koji su zahtjevi ispravni, a koji zahtjevi zlonamjerni. Računala koja se koriste u ovom tipu napada najčešće su zaražena određenom vrstom računalnog virusa koji je neaktivan (eng. *standby*) sve do trenutka DDOS napada. Ukoliko vlasnik računala nema adekvatnu zaštitu u obliku antivirusa na računalu, u pravilu ne može znati da je ono zaraženo. Za lakše razumjevanje razlike između ova dva napada također se može navesti jedan primjer iz stvarnog života gdje je internet aplikacija ili usluga zapravo trgovina koja se bavi prodajom računalne opreme. U ovom slučaju nećemo imati unajmljenu jednu osobu koja će „zagušavati“ promet trgovine nego više osoba istovremeno što će naravno, kao i u digitalnom svijetu, biti teško izolirati. U slučaju jedne osobe ista se jednostavno udalji iz trgovine [24]. Prema izvoru [24] najveći DDOS napad na Hrvatskog mrežnog poslužitelja Hrvatski Telekom (HT) zabilježen je 21. travnja 2021. godine.



Slika 4 Razlika između DoS i DDoS napada.

Izvor: ***DDoS napad CCERT-PUBDOC-2008-09-240***, CARNet CERT LS&S, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf (14.03.2023.)

3.2.2. Zaštita protiv DOS napada

Zaštita protiv DOS napada je jako kompleksna te zahtjeva veliku pozornost od strane osoblja zaduženog za zaštitu aplikacije ili baze podataka. Zaštita se može podijeliti na tri dijela, a to su:

1. Prevencija od napada i implementiranje adekvatne zaštite
2. Otkrivanje napada u zadano vrijeme
3. Ispravna reakcija u određenom vremenu.

Kompleksnost zaštite proizlazi iz toga što postoji više podvrsti DOS napada koji se kroz godine mijenjaju i unapređuju te zbog toga nema jedinstvenog i trajnog riješenja za zaštitu te se ista mora redovito održavati. Sama priprema sustava protiv ovakve vrste napada je jedna od najbitnijih stvari za obranu sustava, ali se nažalost nekad sama priprema zanemaruje što je velika greška te se istoj pridodaje značaj tek nakon određenog sigurnosnog propusta. U ovom slučaju potrebno je držati se izreke „Bolje spriječiti nego liječiti“. Bitno je procjeniti koji dio sustava bi mogao biti cilj napada te istome dati ograničene ovlasti u obliku Internet prometa. Ukoliko se u određenom dijelu sustava koji ima ograničeni Internet promet otkrije nešto sumnjivo, osoba ovlaštena za zaštitu može provjeriti radi li se o napadu te adekvatno reagirati. Rezervni resursi popust proširenja Internet prometa i proxy poslužitelja moraju biti stalno dostupni u slučaju detekcije napada. Jedan od načina zaštite i blokiranja napada je postavljanjem „filtera“ na mrežu prije nego se podatci pošalju Internet poslužitelju. Filter služi kao zaštita tako što štiti mrežu od nepotrebnog prometa koji se šalje prema poslužitelju. Može biti namješten tako da blokira promet s određenih lokacija ili sa određenih IP adresa koje su već klasificirane kao „Bot“ adrese. Naravno, sam poslužitelj mora redovito biti provjeravan od strane nadležne osobe u slučaju pojave neželjenog aplikacijskog programa [25, 26].

3.3. ZLONAMJERNI PROGRAM

Zlonamjerni program ili „Malware“ je štetni računalni program napravljen s ciljem da napravi štetu unutar cijelog sustava, uključujući i bazu podataka. Pojava „Malware-a“ na računalu nije rijetka pojava te je najčešće greška samog korisnika ili ovlaštene osobe koja se koristi računalom. Napadač pomoću zlonamjernih programa može pristupiti „Admin“ privilegijama te učiniti štetu unutar baze podataka bez znanja i dozvole ovlaštene osobe.

Pojedini zlonamjerni programi ne moraju davati nikakav znak da su prisutni. Također, pojedini mogu biti „korisni“ i izvršavati stvari normalno, bez da ovlaštena osoba koja se koristi računalom posumnja na mogući propust. Najčešće se pokreću sami, bez korisničke dozvole te služe za krađu podataka na sustavu, za udaljeni pristup računalu, za slanje bezvrijednih Internet poruka (eng. *spam messages*) ili za sudjelovanje u DDOS napadima.

Prema načinu rada i izvođenja, zlonamjerni programi mogu biti:

1. Računalni virusi

   Zlonamjerni program koji se razmnožava kad je pokrenut tako što zarazi određene datoteke ili operativni sustav na računalu na način da im dodaje svoj vlastiti kod. Ukoliko je zaražen operativni sustav, prilikom pokretanja računala pokrenut će se i virus. Može se koristiti za krađu podataka, neovlašten udaljen pristup računalu, iscrpljivanje procesorske jedinice računala ili memorije. Najčešće je u tipu .exe datoteke ili je zlonamjerni kod smješten unutar nekog dokumenta. Dakle, preuzimanje određene zaražene .exe datoteke neće samo po sebi aktivirati virus već će se virus aktivirati nakon što se pokrene .exe datoteka. Jedni od simptoma zaraze virsom su sporiji rad računala, rušenje sustava prilikom otvaranja pojedinih programa ili datoteka te pojavljivanje novih ikonica na radnoj površini ili nedovoljno radne memorije na računalu. Naravno, ovi simptomi ne moraju uvijek značiti da je riječ o virusu, ali je bitno obavijestiti nadležnu osobu o navedenim problemima [27].

2. Trojanski konj (eng. *Trojan*)

   Jedan od najčešćih i najpoznatijih zlonamjernih programa koji na prvi dojam nije štetan program jer korisniku koji ga je pokrenuo omogućuje normalan rad programa. Primjer ovog tipa virusa može biti preuzimanje programa kojem je potrebna plaćena licenca za rad. Korisnik preuzme određenu datoteku (najčešće u tipu crack.exe) koja mijenja potrebu za tom licencom i omogućuje korisniku normalno korištenje programa bez plaćanja. U ovom slučaju korisnik normalno koristi program, ali se u pozadini mogu odvijati radnje kojih korisnik nije svjestan. U odnosu na računalne viruse i crve, trojanski konj ne ubacuje svoj kod u ostale datoteke i ne razmnožava se [28, 29].

3. Računalni crv (eng. *Worms*)

   Zlonamjerni program koji se samostalno razmnožava kao i računalni virus, ali ne mora biti pokrenut od strane korisnika da bi se aktivirao i proširio. U usporedbi sa računalnim virusom koji za primjer mora imati pokrenutu .exe datoteku kako bi se pokrenuo i razmnožavao, računalni crv to ne mora. Ima mogućnost zaraziti ostala računala na mreži na način da traži greške u kodu operativnog sustava te to radi automatski bez potrebe za prebacivanjem datoteka sa računala na računalo ili otvaranjem određene Internet pošte. Operativni sustavi se zbog toga moraju redovito održavati. Crv je jedan od virusa koji se koristi za dodavanje računala u „Botnet" mrežu koja se kasnije koriste za DDOS napade [30].

4. Program za špijunažu (eng. *Spyware*)

   Zlonamjerni program koji bez dozvole korisnika sustava može „špijunirati" i promatrati što se odvija na računalu te podatke slati na određenu lokaciju koja nije smještena na računalu.Najpoznatija podvrsta „spyware-a" je takozvani „Keylogger" koji zapisuje u određenu datoteku sve što se pritišće na tipkovnici, odnosno, upisuje na računalo u tom trenutku i te podatke prosljeđuje na računalo ili poslužitelj napadača. „Adware" ili program za prikaz reklama je također jedna vrsta „Spyware-a" koja služi za prikaz reklama unutar određenih aplikacija. Najčešće dolazi u sklopu besplatnih aplikacija kod kojih programeri i vlasnici aplikacija zarađuju na temelju otvaranja određenih reklama [31].

5. Ucjenjivački program (eng. *Ransomware*)

   Zlonamjerni ucjenjivački program koji radi tako da šifrira i zaključava datoteke u računalu. Ukoliko korisnik želi da se datoteke dešifriraju, odnosno otključaju, mora napadaču učiniti uslugu, obično korisnik mora uplatiti određenu količinu novaca napadaču, danas najčešće u obliku kriptovaluta. Najčešći način širenja ove vrste programa je putem bezvrijedne Internet poruke. Za primjer se može uzeti određena banka koja svojim korisnicima na mjesečnoj bazi šalje izvod računa. Takva vrsta Internet poruke koja sadrži dokument u PDF formatu je sasvim normalna. U slučaju ove vrste napada, napadač napravi sličnu ili praktički istu Internet adresu s koje šalje Internet poruku (umjesto xxxbanka.hr > xxxbanka.co), za koju prosječan korisnik neće uopće primjetiti razliku. Naravno, Internet poruka napadača sadržu također datoteku koja je u PDF formatu, ali uz to sadrži i zlonamjerni program za ucjenjivanje

korisnika. Nakon što korisnik, sa željom da pročita izvod iz banke, otvori datoteku koja je zaražena, datoteke na računalu će postati zaključane i kriptirane. Nerijetko cijeli operativni sustav bude kriptiran i zaključan [32].

3.4. NEREGULIRANOST I ZLOUPOTREBA PRIVILEGIJA

Neregulirane privilegije mogu na više načina dovesti do propusta i do narušavanja sigurnosti baza podataka. Ukoliko previše korisnika ima veće ovlasti unutar pojedine baze podataka nego što je to stvarno potrebno, postoji veća mogućnost za narušavanje njene sigurnosti. Najveći problem za bazu podataka je kada napadač dobije pristup računu koji ima administratorskih ovlasti u sklopu baze. Naravno, za napadače je puno lakše izvršiti „Phishing“ prevaru ili bilo koju drugu vrstu napada ukoliko ima više korisnika sa većim ovlastima. U slučaju jednog ili dva korisnika s većim ovlastima, vjerojatnost za propustom je mala, ako se uzme u obzir da su oba korisnika dovoljno educirana o sigurnosti baza podataka. Zloupotreba privilegija se može odnositi na osobe koje iz vlastitog ili tuđeg interesa izvršavaju promjene unutar baza podataka, bez dozvole nadređene osobe. Također, postoji mogućnost prodavanja informacija iz baza podataka radi stjecanja financijske koristi. U današnje vrijeme, nažalost zbog ne educiranosti i nepažnje, najčešći razlog upada u baze podataka jest ljudskom greškom [33].

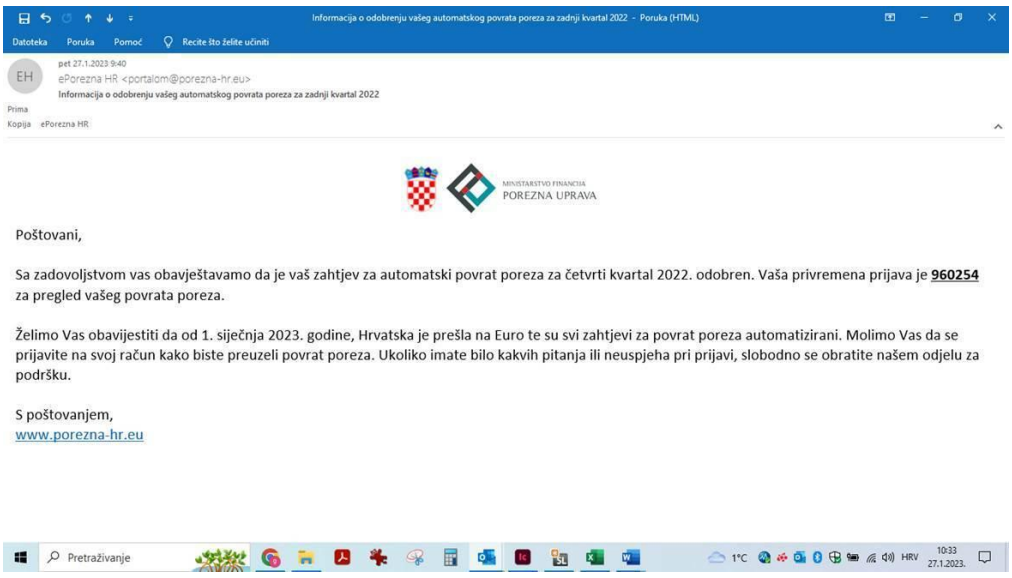
3.5. PRISTUP SIGURNOSNOJ KOPIJI

Redovita izrada i ažuriranje sigurnosne kopije baze podataka iznimno je važna za očuvanje njene sigurnosti u slučaju katastrofe. Sama kopija mora biti u svakom trenutku dostupna za pristup i zaštićena od neovlaštenog pristupa. Nažalost, često se sigurnosna kopija čuva na neadekvatnim i nesigurnim mjestima bez ikakve zaštite što je čini lakom metom za napadače. U slučaju napadača, pristup bazi podataka preko sigurnosne kopije najčešće rezultirati krađom povjerljivih podataka unutar baze. Također, napadač može trajno obrisati određene podatke iz sigurnosne kopije. U slučaju napada, korištenjem zlonamjernih programa, napadač može zaraziti sigurnosnu kopiju te time zaraziti i originalnu bazu podataka. Današnji zakoni i regulative su veoma strogi te ukoliko dođe do „curenja“ povjerljivih podataka, kompanija može biti kažnjena. Prema istraživanju tvrtke Sansec, 12% Internet trgovina pohranjuje svoje sigurnosne kopije u javnim mapama koje se naknadno zaborave zbog ljudske greške i nepažnje [34].

3.6. „PHISHING“ I „SPOOFING“ – PRIJEVARE PUTEM ELEKTRONIČKE POŠTE

„Phishing“ je vrsta prijevare koja se odvija putem elektroničke pošte u kojoj napadač pokušava prevariti korisnika i pribaviti osjetljive informacije poput korisničkih imena, lozinki i bankovnih informacija. „Spoofing“ je usko vezan uz „Phishing“, a također je vrsta prijevare gdje napadač nastoji pribaviti osjetljive informacije o korisniku ili tvrtki putem elektroničke pošte. U ovom slučaju, adresa elektroničke pošte je praktički jednaka pravoj adresi s koje se inače šalje isti legitimni sadržaj, kao i sam sadržaj koji je gotovo jednak pravom sadržaju. Od žrtve se najčešće traži da popuni obrazac unutar elektroničke pošte koji izgleda jako uvjerljivo. Nakon toga žrtvu se najčešće preusmjerava na određenu Internet stranicu u cilju pribave više informacija. Pri tome, stranice najčešće koriste identičan logo kao i prava legitimna stranica te koriste gotovo isti, ali ne i identičan sadržaj unutar stranice. Kod ovakvih vrsta prevare neće biti zatražene osobne i povjerljive informacije odmah u prvom koraku, već u nekom od idućih koraka, kako žrtva ne bih brzo posumnjala na prevaru [35].

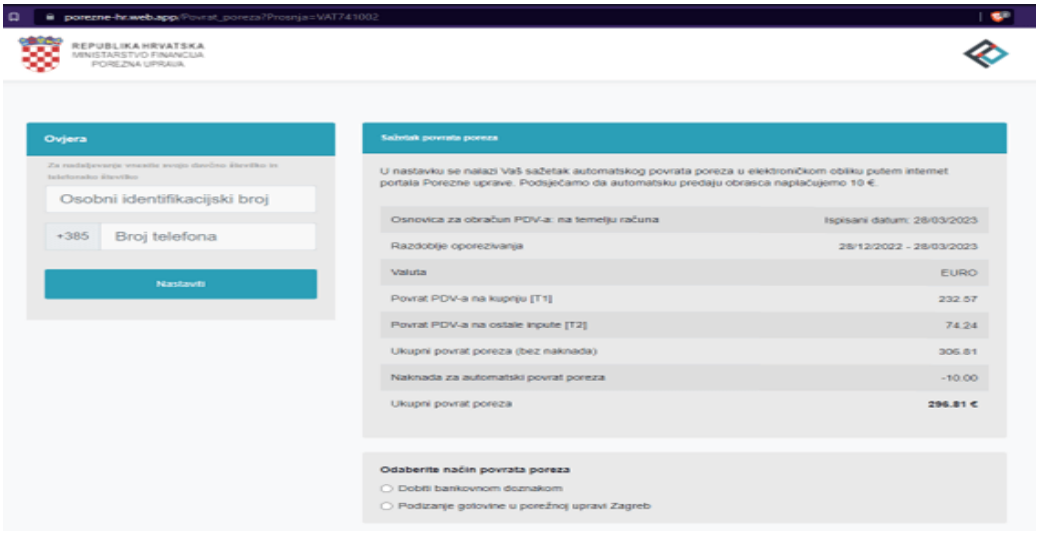
Jedan od najnovijih „Phishing“ napada na području Republike Hrvatske u 2023. godini bio je od strane napadača koji se putem elektroničke pošte pretvarao da je Porezna Uprava RH (slika 5).



Slika 5 Primjer „Phishing“ napada.

Izvor: ***Oprez: Na mail počele stizati lažne (phishing) poruke Porezne uprave***, Lider, https://lidermedia.hr/financije/oprez-na-mail-pocele-stizati-lazne-phishing-poruke-porezne-uprave-148421 (21.03.2023.)

Sadržaj unutar pošte izgleda vrlo uvjerljivo. Adresa elektroničke pošte s koje je poslan sadržaj je : *portalom@porezna-hr.eu*. U sadržaju pošte je navedeno da napadač nudi povrat poreza. Klikom na poveznicu, žrtva je preusmjerena na adresu „*porezne-hr-web.app*“ (slika 6). Nakon upisa OIB-a i broja telefona, navedeno je da se automatska predaja obrasca naplaćuje 10€ što napadaču daje priliku da korisnicima pošalje upit vezan za bankovnu karticu.

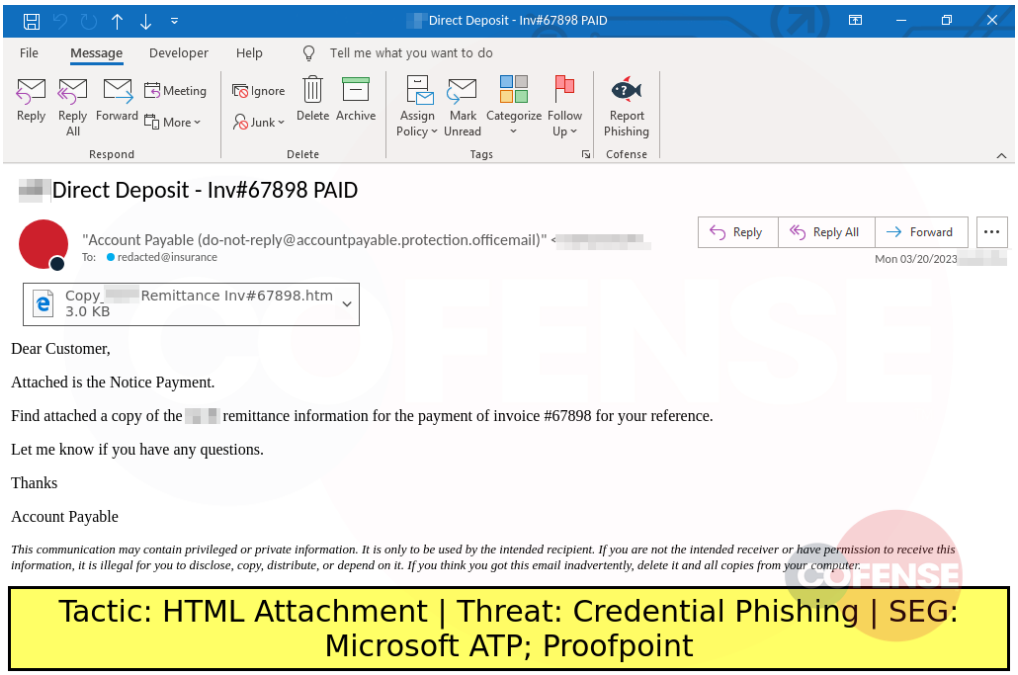


Slika 6 Primjer zlonamjerne stranice

Izvor: ***Upozorenje! U tijeku je prijevara na temu povrata poreza!***, CERT.hr, https://www.cert.hr/upozorenje-u-tijeku-je-prijevara-na-temu-povrata-poreza/ (21.03.2023.)

Iako je ova vrsta napada usmjerena građanima koji su najčešće i najlakša meta, često se za napad biraju i velike svjetske kompanije. U slučaju većih kompanija, najčešće se koristi dodatan dokument u sklopu sadržaja elektroničke pošte koji sadrži zlonamjeran program pomoću kojeg napadač može doći do kontrole unutar sustava i krađe podataka.

Na primjeru sa slike 7 vidljiv je sadržaj koji također sadrži i određeni privitak. Na prvi dojam sve izgleda normalno jer se po sadržaju navedenom u pošti radi o klasičnom računu za određeni proizvod. Detaljnijim pregledom može se uočiti da je datoteka unutar privitka u formatu .html dok se računi najčešće prilažu u formatu .pdf .pdf. Važno je naglasiti da nije rijetkost da i unutar .pdf datoteka može biti smješten zlonamjerni program koji potom može zaraziti određenu bazu podataka ili cjelokupni sustav [36].

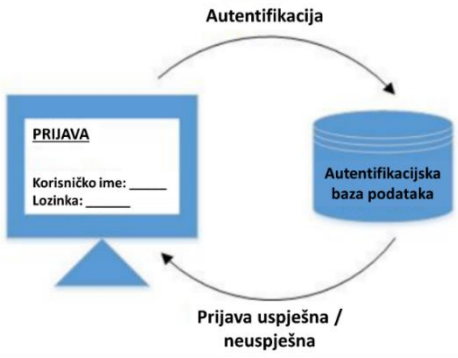


Slika 7 Primjer elektroničke pošte koja sadrži zlonamjernu datoteku.

Izvor: ***Phishing Database: Real Email Phishing Attack Examples & Threats***, Cofense, https://cofense.com/knowledge-center-hub/real-phishing-examples-and-threats/

3.7. RANJIVOST AUTENTIFIKACIJA

Ranjivost autentifikacija se opisuje kao greška unutar mehanizma autentifikacije koju napadač ili zlonamjeran korisnik može iskoristiti za neovlašteni pristup sustavu [37]. Najjednostavniji primjer i provjere i potvrde identiteta (slika 8), odnosno autentifikacije, je prilikom podizanja gotovine na bankomatu gdje se za autentifikaciju i pristup kartici zahtjeva od korisnika da unese četveroznamenkasti PIN, kako bi potvrdio svoj identitet. Jasno je da u slučaju krađe kartice, ista neće moći biti iskorištena ukoliko je PIN nepoznat.



Slika 8 Autentifikacija putem sučelja za prijavu provjerena putem baze podataka

Izvor: Prilagođeno iz J. Blue, E. Furey, i J. Condell, **A novel approach for secure identity authentication in legacy database systems**, 2017 28th Irish Signals Syst. Conf. ISSC 2017, srp. 2017, doi: 10.1109/ISSC.2017.7983624. (21.03.2023)

Problem kod jednostavnih autentifikacija je taj što ukoliko se podatci za prijavu ukradu, u ovom slučaju PIN ili u slučaju baza podataka, korisničko ime i lozinka, lako se dolazi do povjerljivih informacija unutar baza podataka ili krađe sredstava. [38] Jedan od načina upada u račune koji su dio sustava baza podataka može se postići Brute-Force napadom. Ukoliko je napadaču poznato korisničko ime računa u koji želi provaliti, ima mogućnost izvršiti ovu vrstu napada. Napad se vrši pomoću skripte koja, iz određene tekstualne datoteke koja je ispunjena raznim lozinkama, isprobava hoće li se jedna od lozinki podudariti sa računom te na taj način dobiti pristup sustavu. Također, ukoliko sustav nema dovoljno dobro definirano pravilo za korisničko ime i lozinku koju korisnik sustava osobno izabere, može se naći na meti napada. Napadači danas najčešće dolaze do podataka za prijavu putem „Phishing“ prevare gdje korisnik baze podataka nenamjerno preda podatke za prijavu. Također, jedan od načina dobivanja podataka za prijavu unutar baze podataka je „pogađanjem“ korisničkog imena te koristeći brute force metodu probijanja lozinke [37].

4. ZAŠTITA BAZA PODATAKA

Sigurnost baza podataka postala je vrlo važna tema u posljednjih nekoliko desetljeća zbog povećanja količine podataka koje organizacije prikupljaju i obrađuju. Razvoj internet tehnologija doveo je do toga da su baze podataka, odnosno njihovi serveri, javno dostupni što korisnicima daje mogućnost pristupiti bazi podataka putem internet aplikacija koristeći samo internetski preglednik. U pogledu sigurnosti same baze podataka, veliki značaj je taj da se spriječi bilo koji neovlašteni pristup od strane zlonamjernih korisnika koji bi rezultirao krađom podataka, narušavanjem privatnosti te financijskim gubicima. Ugrađivanje sigurnosnih elemenata u SUBP jedini je pravi način za povećanje njene sigurnosti.

Privatnost i zaštita od neovlaštenog pristupa bazi podataka od velikog je značaja u svim korporacijama koje za primjer, u bazi mogu imati pohranjene informacije o klijenatima i korisnicima, njihove bankovne informacije, i slično. Programeri samih baza podataka imaju veliku odgovornost zaštiti privatnost pojedinaca čiji se zapisi nalaze kao podatci u bazi. Privatnost je danas pravo svakog pojedinca da ima kontrolu nad vlastitim podatcima. Države EU imaju Opću uredbu o zaštiti podataka (eng. *General Data Protection Regulation, GDPR*) te su sve organizacije unutar EU koje prikupljaju i pohranjuju podatke i informacije dužne postupati u skladu s uredbom.

Jedan od osnovnih modela zaštite baza podataka je zasnivan na povjerljivosti, integritetu i dostupnosti, poznato kao CIA model. Povjerljivost (eng. *Confidentialty*) osigurava da samo određeni korisnici imaju pravo i mogućnost pristupiti informacijama o pojedincu ili tvrtki. Integritet (eng. *Integrity*) zahtijeva da samo određeni korisnici imaju pravo i mogućnost mijenjati podatke kako bi se očuvala pouzdanost i integritet podataka. Dostupnost (eng. *Availability*) omogućava da podatci budu dostupni određenim korisnicima samo kada je to potrebno [39].

4.1. KONTROLA PRISTUPA

Prema CIA modelu, povjerljivost je navedena kao prva stavka modela zaštite baza podataka. Svaka baza podataka sastoji se od subjekata i objekata. Subjekte možemo smatrati korisnicima koji koriste bazu podataka, dok objekte možemo smatrati podatcima, primjerice tablice unutar baze podataka kojima korisnici pristupaju. Metoda kojom se osigurava povjerljivost jest upravo kontrolom pristupa unutar baze podataka, na način da se samo

određenim korisnicima dopusti pristup osjetljivim podatcima, a istovremeno zabrani pristup neovlaštenim korisnicima. Također, pored same zabrane od neovlaštenog pristupa, kontrola pristupa ima zadatak ograničiti mogućnosti i radnje koje ima ovlašteni korisnik. Način na koji korisnici pristupaju objektima unutar baze podataka je određen privilegijom pristupa. Kontrola pristupa je definirana postupkom kojim se potvrđuje točnost unesenih podataka potrebnih za pristup sustavu, ukoliko su podatci točni korisniku se dopušta čitanje odnosno pristup određenim podatcima unutar baze [39].

4.1.1. Načela i načini izvođenja kontrole pristupa

Načela na kojima se temelji kontrola pristupa:

1. Minimalne i maksimalne privilegije – korisnicima se dodjeljuju minimalne mogućnosti odnosno privilegije unutar baze dovoljne za izvođenje određenih zadataka. Suprotno tome, maksimalne privilegije dopuštaju korisicnima dostupnost svih mogućnosti i podataka unutar baze podataka.
2. Privilegije unutar zatvorenog i otvorenog sustava – u slučaju otvorenog sustava, svi korisnici imaju sve privilegije osim onih koje su zabranjene. U slučaju zatvorenog sustava, privilegije korisnika su dostupne samo uz prethodnu potvrdu.
3. Privilegije unutar centraliziranog i decentraliziranog sustava – u centraliziranom sustavu, jedan korisnik kontrolira sve sigurnosne dijelove sustava dok u decentraliziranom više korisnika ili grupa korisnika kontrolira različite sigurnosne dijelove sustava [40].

Načini za izvođenje kontrole pristupa [2]:

1. Autentifikacijom korisničkog imena i lozinke
2. Posebnim privilegiranjem objekata unutar baze podataka

4.1.2. Mehanizmi kontrole pristupa

Prema načelima sigurnosti, nitko unutar jednog sustava baze podataka nebi trebao imati slobodan pristup svim mogućnostima i resursima. Odabir određene metode kontrole pristupa ovisi ponajprije o vrsti napada na koju je baza podataka najranjivija. Administrator se mora pobrinuti da pravilno rasporedi i dodjeli prava i pristup određenim korisnicima i eliminira mogućnost dodjele pristupa korisnicima kojima to nije potrebno.

Mehanizmi kontrole pristupa mogu se podjeliti na tri grupe [33]:

1. DAC – Diskretna metoda kontrole pristupa
2. MAC – Obavezna metoda kontrole pristupa
3. RBAC – Kontrola pristupa temeljena na ulogama.

4.1.2.1. Diskretna kontrola pristupa - DAC

Diskretna kontrola pristupa zasniva se na dozvoli pristupa korisniku određenom objektu unutar baze podataka ili datoteci unutar sustava na temelju odluke administratora baze podataka koji upravlja određenim objektima ili na temelju odluke vlasnika datoteke unutar sustava. Sama metoda primjenjuje se na razini korisnika što ju čini dinamičnom metodom.

Za primjer se može uzeti jedan „word“ dokument koji je javno dostupan određenim korisnicima putem Internet preglednika. Vlasnik dokumenta dodjeljuje dozvolu za pristup, odnosno pregled dokumenta 10 različitih korisnika. Od 10 korisnika, samo jednom korisniku vlasnik daje pravo na uređivanje i spremanje dokumenta. Od ostalih 9 korisnika, vlasnik četiri korisinka daje pravo na ispisivanje dokumenta uz prethodnu dozvolu vlasnika. Ostalih 5 korisnika imaju pravo samo na pregled dokumenta bez mogućnosti uređivanja i ispisa. Pri tome, u ovom slučaju vlasnik dokumenta u bilo kojem trenutku može povećati ili smanjiti prava određenog korisnika, odnosno dodijeliti ili ukloniti mogućnosti uređivanja i ispisa dokumenta, što objašnjava dinamičnost ove metode kontrole pristupa [40].

4.1.2.2. Obavezna kontrola pristupa - MAC

MAC je vrsta kontrole pristupa kod koje sustav ograničava mogućnost korisnika odnosno subjekta da pristupi ili napravi neku vrste promjene unutar objekta odnosno datoteke. Sustav ima unaprijed određena pravila koja upravljaju kontrolom pristupa. Administrator postavlja pravila kontrole pristupa unutar sustava te se svakom objektu i subjektu dodjeljuje sigurnosna oznaka koja označuje njegovu sigurnosnu osjetljivost. Korisnicima se pristup dodjeljuje na temelju potrebe za informacijom, odnosno, korisnici moraju dokazati potrebu za informacijom prije nego im je dozvoljen pristup. U odnosu na DAC metodu, ovdje vlasnik same datoteke nije u mogućnosti davati ovlasti ostalim korisnicima, već to radi sam sustav. MAC se smatra najsigurnijim modelom kontrole pristupa, a najčešća upotreba jest u vojnim, bankarnim i vladinim sustavima gdje je potrebna maksimalna strogoća u pogledu sigurnosti [40, 41].

4.1.2.3. Kontrola pristupa temeljena na ulogama - RBAC

Uloga se može smatrati skupinom privilegija, što znači da svaki korisnik kojemu je dodijeljena određena uloga posjeduje unaprijed dodijeljene privilegije. Pomoću uloga jednostavnije je skupini korisnika dodijeliti ili ukinuti određene privilegije unutar sustava. Administrator određuje uloge i privilegije za svaku od njih te ih dodjeljuje korisniku. Svaki korisnik može imati više uloga koje mogu imati više različitih privilegija. Korisniku unutar jednog sustava može biti istovremeno pridodano više različitih uloga te isto tako više različitih korisnika može imati istu ulogu. Prednost RBAC metode u odnosu na ostale navedene je ta što je jednostavnija za upravljanje jer se korisnicima ne dodijeljuju privilegije temeljem njihovog identiteta već ovisno o njihovoj odgovornosti unutar sustava [42].

4.2. AUTENTIFIKACIJA

Autentifikacija je proces u sklopu sustava baza podataka ili operativnog sustava pomoću kojeg se korisniku provjerava i potvrđuje identitet na temelju unesenih podataka, te ukoliko su podatci ispravni, korisniku se dopušta ulaz u sustav odnosno u bazu podataka. Administrator zajedno sa sigurnosnim timom zaduženim za sigurnost baza podataka određuje koja će se vrsta autentifikacije koristiti [39].

Postoje tri glavne vrste autentifikacije (slika 9) koje se različito izvode te od kojih svaka ima svoje prednosti i nedostatke:

1. Autentifikacija temeljena na onome što korisnik zna – ovo je najčešće korištena vrsta autentifikacije gdje korisnik za prijavu koristi korisničko ime i zaporku. Dugi period je ova vrsta autentifikacije bila najčešće korištena zbog svoje jednostavnosti. Danas se i dalje većinski koristi, iako se zbog pravila o zaštiti podataka i opasnosti od krađe podataka konstantno unapređuje. Dužnost administratora baze podataka je onemogućiti korisniku da odabere jednostavnu zaporku [43]. Unazad desetak godina uobičajeno je bilo da se od korisnika traži da odabere lozinku od najmanje 7 znakova. U današnje vrijeme od korisnika se traži da odabere lozinku od najmanje 8 znakova gdje je potrebno koristiti barem jedno veliko slovo, jedan broj te jedan interpunkcijski znak. Naravno, pored svojih prednosti ovaj način autentifikacije ima i svojih nedostataka. Zbog korištenja kompliciranijih zaporki, većina korisnika se odlučuje na skladištenje istih u obliku fizičkog ili digitalnog zapisa. Najčešći primjer fizičkog zapisa zaporke je na papir koji se nalazi na radnom stolu gdje je smješteno

računalo. Zapis u obliku digitalnog oblika može biti unutar tekstualne datoteke na računalu. Oba načina su loš primjer čuvanja zaporke. U slučaju fizičke kopije, korisnik koji nije ovlašten za pristup sustavu može ukrasti podatke ukoliko dođe u kontakt sa, na primjer, papirom na kojem je zapisana zaporka. U slučaju digitalne kopije, pojavom računalnog virusa na računalu zlonamjeran korisnik može pristupiti tekstualnoj datoteci i pristupiti sustavu.

2. Autentifikacija temeljena na onome što korisnik posjeduje – ova vrsta autentifikacije temelji se na korištenju dodatnog uređaja kojeg korisnik posjeduje za provjeru i potvrdu identiteta za pristup sustavu. Najčešće je taj uređaj pametna kartica, pametan telefon ili token za autentifikaciju koji generira jedinstveni kod. U slučaju prijave u sustav gdje se kao uređaj za autentifikaciju koristi mobilni telefon, prilikom unosa broja telefona, na isti dolazi jednokratni kod koji se potom upisuje u aplikaciju koja dopušta korisniku da pristupi sustavu. Prednost ove vrste autentifikacije je ta što je krađa samog uređaja primjetljiva što će korisniku i administratoru dati do znanja da poduzmu potrebne mjere kako bi se spriječio neovlašteni pristup sustavu. Sama činjenica da je broj koji se generira putem mobilnog telefona jednokratan, koristi se samo za jednu prijavu i traje određeno vrijeme, upućuje na to da ga je teško ukrasti. Nedostatak može biti taj da se uređaj koji se koristi za autentifikaciju može pokvariti ili uslijed neopreznog korištenja i oštetiti što ga čini neupotrebljivim.

3. Autentifikacija temeljena na onome što korisnik jest – najnovija vrsta autentifikacije koja je postala popularna razvitkom industrije i tehnologije pametnih telefona [44].Ova vrsta autentifikacije jedna je od najsigurnijih metoda pored OTP (eng. *One-Time-Password*) i kontinuirane autentifikacije. Za potvrdu identiteta koriste se fizičke karakteristike korisnika koje su za svakog korisnika jedinstvene te ih je teško ukrasti, a najčešće su to otisak prsta i prepoznavanje lica. Skeniranjem otiska prsta biometrijski podatak se registrira i pohranjuje u bazu podataka. Prilikom prijave korisnika u sustav, uspoređuje se otisak prsta korisnika sa registriranim otiskom prsta u bazi podataka te ukoliko se otisak prsta podudara, korisniku je omogućen pristup sustavu. U nekim slučajevima ova vrsta autentifikacije nije pouzdana zbog mogućnosti kvara uređaja ili fizičke ozljede korisnika.

Slika 9 Tri najčešća načina autentifikacije

Izvor: **Zašto koristiti višefaktorsku autentifikaciju?**, Ventex, https://ventex.hr/hr/novosti/Zasto-koristiti-visefaktorsku-autentifikaciju/ (27.03.2023.)

4.3. ŠIFRIRANJE PODATAKA

Šifriranje (eng. *Encryption*) je postupak kojim se podatci odnosno izvorni tekst pretvara u šifrirani tekst u svrhu njegove zaštite od neovlaštenog pristupa, a izvodi se pomoću posebnog algoritma. Tekst se može dešifrirati samo pomoću odgovarajućeg ključa. Postoje dvije vrste algoritma za šifriranje, simetrični sustav i asimetrični sustav. Kod simetričnog sustava ključ koji se koristi za zaključavanje odnosno šifriranje podataka, koristi se i za otključavanje odnosno dešifriranje podataka. Kod asimetričkog sustava koriste se dva različita ključa, jedan za šifriranje, a drugi za dešifriranje podataka. Postupak šifriranja izvodi se kada podatci iz baze podataka miruju ili se ne koriste. Prilikom slanja zahtjeva bazi podataka za čitanjem određenih podataka oni se dešifriraju. Budući da danas većina baza podataka koristi Internet kao sredstvo komunikacije između poslužitelja baze i korisnika postoji mogućnost da zlonamjeran korisnik pristupi podatcima dok nisu šifrirani odnosno dok se isporučuju korisniku. Kako bi se to spriječilo koristi se SSL (eng. *Secure Socket Layer*) protokol koji šifrira podatke prilikom njihovog slanja korisniku na čitanje. Ključevi koji služe za dešifriranje šifriranih podataka moraju biti pohranjeni na sigurnoj lokaciji [45]. Prema Oracle, najbolji način zaštite samih ključeva je taj da se ključevi pohranjuju odvojeno od šifriranih podataka, odnosno da se ne spremaju na istoj lokaciji [46].

Šifriranje podataka u mirovanju se može odvijati na tri razine:

1. Na razini pohrane podataka – šifriraju se podatci u podsustavu za pohranu podataka te je korisno za šifriranje cijelih direktorija u sklopu operacijskog sustava. Također,

šifriranje na ovoj razini je dobra vrsta zaštite protiv zlonamjernih korisnika za slučaj da žele ukrasti podatke ili tvrdi disk na kojem su pohranjeni podatci. Podsustav pohrane podataka nema znanja o strukturi same baze podataka pa se ne može primijeniti djelomično šifriranje određenih dijelova podataka. Podatci se dešifriraju na poslužitelju baze podataka u toku izvođenja.

2. Na razini baze podataka – šifriranje na razini baze podataka omogućava sigurnost i privatnost podataka prilikom unosa ili čitanja istih. Način šifriranja može biti dio same baze podataka te može biti ovisan o osjetljivosti podataka. U odnosu na šifriranje na razini pohrane, u ovom slučaju moguće je primijeniti djelomično šifriranje određenih podataka kao što su određene tablice ili stupac unutar određene tablice.
3. Na razini aplikacije – smatra se najsigurnijim načinom zaštite podataka. Kad su podatci šifrirani na razini aplikacije postaju zaštićeni gdje god se nalazili. U ovom slučaju podatci se šifriraju prilikom generiranja ili izmjene te su zaštićeni prije nego napuste aplikaciju. Podatci su šifrirani prije nego se pohrane u bazu podataka. Osim toga, ovaj način omogućuje da se odredi koji će podatci biti i za koje korisnike šifrirani [45].

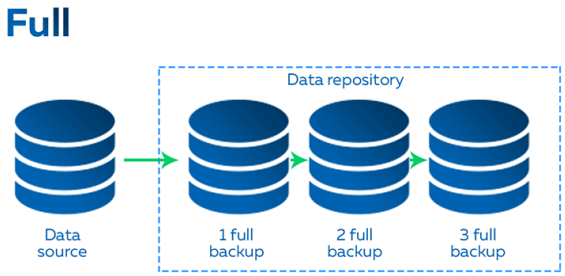
4.4. SIGURNOSNA KOPIJA

Jedan od glavnih zadataka administratora baze podataka je da osigura dostupnost i očuvanje podataka u slučaju kvara opreme ili greške unutar baze podataka i operativnog sustava. Sigurnosna kopija je skup podataka ili datoteka koji se izrađuju u svrhu očuvanja podataka.Vrlo je važno da se prije same upotrebe baze podataka izvede i implementira plan za sigurnosno kopiranje i oporavak. Sigurnosne kopije se obično pohranjuju na tvrdom disku na drugoj lokaciji u odnosu na onu gdje je instalirana baza podataka [47]. Danas se često baze podataka poslužuju sa virtualnih računala te je također vrlo česta pojava da se sigurnosne kopije također pohranjuju i u oblaku što daje dodatnu razinu dostupnosti u slučaju kvara fizičke komponente poput tvrdog diska. Sigurnosno kopiranje se mora izvoditi u redovitom vremenskom intervalu, a ono može biti automatski gdje sustav u svako zakazano vrijeme pokreće sigurnosno kopiranje. Osim toga, administrator ili osoba zadužena za sigurnost, može svojevoljno pokrenuti sigurnosno kopiranje. Nedostatak automatskog kopiranja je da može doći do greške u automatskom procesu te da, na primjer, sigurnosno kopiranje pojedinih podataka bude neuspješno. U tom slučaju je potrebna intervencija

odgovorne osobe. Najčešće proces sigurnosnog kopiranja cijele baze podataka može usporiti rad čitave baze stoga je najčešća praksa da se ono izvodi dok je baza podataka najmanje opterećena [47, 48].

U odnosu na njihov sadržaj i način kreiranja postoje tri vrste sigurnosnih kopija:

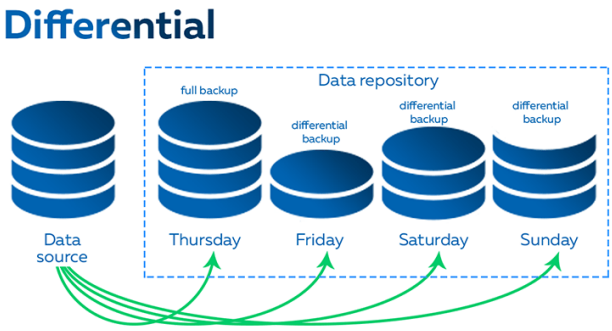
1. Potpuna sigurnosna kopija (eng. *Full backup*) – u ovom slučaju kopiraju se svi podatci iz baze podataka bez obzira na njihovu promjenu od posljednje izrade sigurnosne kopije (slika 10). Obično se ova vrsta kopije izvodi rijeđe, na primjer jednom tjedno, jer zahtjeva puno vremena za izvođenje te zauzima više prostora. Ova vrsta kopija preduvjet je za stvaranje diferencijalne kopije ili kopije temeljene na promjenama zapisa.



Slika 10 Princip funkcioniranja potpune sigurnosne kopije

Izvor: **Full vs Differential SQL Backup**, Handy Backup, https://www.handybackup.net/full-vs-differential-sql-backup.shtml#close (03.04.2023.)

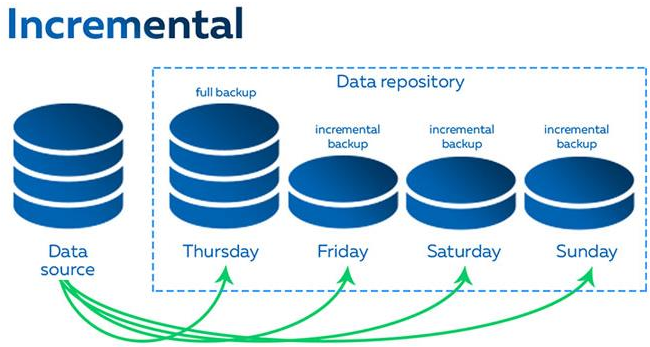
2. Diferencijalna sigurnosna kopija (eng. *Differential backup*) – u ovom slučaju kopiraju se samo oni podatci koji su se dodali ili promjenili od posljednje izrade potpune sigurnosne kopije (slika 11). Ovaj način izrade je neusporedivo brži u odnosu na potpuno sigurnosno kopiranje te zahtjeva manje prostora na disku za skladištenje kopije [49, 50].



Slika 11 Princip funkcioniranja diferencijalne sigurnosne kopije

Izvor: **Full vs Differential SQL Backup**, Handy Backup, https://www.handybackup.net/full-vs-differential-sql-backup.shtml#close (03.04.2023.)

3. Sigurnosna kopija temeljena na promjenama (eng. *Incremental backup*) – u ovom slučaju kopiraju se podatci koji su se promjenili ili dodali u odnosu na posljednju sigurnosnu kopiju, bila ona potpuna ili diferencijalna (slika 12). Veličina ove sigurnosne kopije je puno manja u odnosu na potpunu i diferencijalnu kopiju te se izvodi neusporedivo brže. Ovaj način kopiranja se izvodi češće u odnosu na ostale vrste, na primjer svakih 24 sata. U slučaju potrebe za oporavkom cijele baze podataka potrebno je sadržavati zadnju sigurnosnu kopiju i sve kopije temeljene na promjenama kako bi se u potpunosti povratila baza podataka [50].



Slika 12 Princip funkcioniranja sigurnosne kopije temeljene na promjenama

Izvor: **Full vs Differential SQL Backup**, Handy Backup, https://www.handybackup.net/full-vs-differential-sql-backup.shtml#close (03.04.2023.)

4.5. SUSTAV ZA OTKRIVANJE I SPRJEČAVANJE PROVALA

Sustav za otkrivanje provala (eng. *Intrusion detection system, IDS*) je alat koji služi za nadzor aktivnosti unutar baza podataka, a cilj mu je otkriti pokušaj zlonamjerne radnje unutar sustava. Zlonamjerna radnja se u ovom slučaju može opisati kao bilo koji čin kojem je cilj nanijeti štetu sustavu, u ovom slučaju povjerljivosti, integritetu i dostupnosti baze podataka.

Način na koji se vrši detektiranje provala se može podjeliti u dvije grupe:

1. Detekcija temeljena na potpisu – ova vrsta detekcije sadrži bazu podataka poznatih vrsta napada u sustav, odnosno njihovih potpisa. Potpis se može smatrati detaljem određenog napada po kojem je on prepoznatljiv. Prilikom pokušaja provale, sustav će uzeti trenutnu aktivnost koja se dešava te ju usporediti sa vrstama napada odnosno potpisima koje se nalaze u bazi podataka. Ukoliko se pokaže da je aktivnost ista kao određeni potpis iz baze podataka, sustav će alarmirati i obavjestiti administratora.

Problem kod ove vrste detekcije je taj da će često davati lažno pozitivne rezultate za pojedine radnje, ali isto tako ukoliko se pojavi nova inačica napada čiji potpis još nije smještena unutar baze podataka postoji vrlo velika vjerojatnost da će napad proći neopaženo bez alarmiranja.

2. Detekcija temeljena na anomalijama – ova vrsta detekcije umjesto korištenja baze podataka sa poznatim napadima koja se mora često osvježavati kako bi ostala djelotvorna, traži anomalije u sustavu odnosno traži nešto što ne izgleda ispravno. U ovom slučaju, IDS ima pohranjen primjer kako izgledaju normalne radnje unutar sustava. U svakom trenutku, ukoliko uoči da radnje koje se odvijaju previše odskaču od normalnih, alarmirati će administratora. Izrada ovog sustava se sastoji od dva dijela. Prva je trening faza u kojoj se IDS uči o programu odnosno koje se radnje obično izvode u sklopu sustava, kako bi znao raspoznati što je normalno, a što nije. Nakon trening faze dolazi faza testiranja u kojoj se odvijaju radnje koje se prethodno nisu odvijale kako bi se uvidjela reakcija sustava na nove anomalije. Ova vrsta detekcije će imati prednost u odnosu na onu sa potpisom jer će biti sposobna otkriti nove ili nepoznate vrste napada. Međutim, ova vrsta detekcije često može stvarati lažno pozitivne alarme za aktivnosti koje nisu zlonamjerne [51].

Uz sustav za otkrivanje provala, postoji i sustav za sprečavanje provala (eng. *Intrusion prevention system, IPS*). IPS je mrežni alat koji može biti izveden kao aplikacija ili kao hardver koji konstantno kontrolira promet na mreži na kojoj se nalazi baza podataka te ukoliko otkrije zlonamjerne prijetnje poduzima potrebne korake kako bi se to spriječilo. Ovaj sustav je napredniji u odnosu na IDS koji ima mogućnost samo obavijestiti administratora o problemima, a ne može provesti potrebne radnje za eliminiranje problema [52].

Vrste sustava za sprječavanje provala su:

1. Mrežni IPS – djeluje na mreži i prati i konstantno analizira mrežni promet kako bi se utvrdila zlonamjerna aktivnost, često je dio vatrozida ili rutera .
2. IPS na glavnom računalu (eng. *Host based*) – implementira se na glavnom računalu te koristi aplikacijske slojeve koji služe za komunikaciju aplikacije i operacijskog sustava kako bi se otkrili pokušaji zlonamjernih aktivnosti [2].

4.6. VATROZID

Vatrozid je mrežni sigurnosni sustav koji može biti izveden aplikacijski ili fizički, a kojemu je cilj spriječiti neovlaštene pristupe mreži i zaštititi sustav od zlonamjernih aktivnosti te u isto vrijeme propustiti ovlaštene pristupe mreži. Svrha vatrozida je napraviti „zid“ između privatne mreže na kojoj je smještena baza podataka i javne mreže kako bi se spriječio napad na bazu podataka kojem je cilj pristupiti podatcima. Funkcionira na temelju sigurnosnih pravila koja su postavljena unutar uređaja ili aplikacije. Sistemski ili mrežni administrator unutar organizacije je zadužen za implementaciju sigurnosnih pravila. Sigurnosna pravila unutar vatrozida su zapravo liste kontrole pristupa. Kontrola pristupa se može vršiti filtriranjem IP adresa, protokola, priključaka i slično. Vatrozid može biti implementiran prije poslužitelja baze podataka ili blizu mrežnog pristupnika ukoliko se na mreži nalazi više poslužitelja baza podataka [53].

5. DODATNI NAČINI ZAŠTITE BAZA PODATAKA

S napretkom tehnologije napreduju i načini na koji se baze podataka štite od zlonamjernih napada. Pored glavnih načina zaštite baze podataka koji su neizostavni dio svakog sustava postoje i dodatni načini kojima se može dodatno osigurati privatnost i sigurnost podataka [54]. Vrlo je česta pojava da se unajme specijalizirane kompanije koje potom vrše testiranje baza podataka na nedostatke i ranjivosti. Nakon odrađenog testiranja, sigurnosnom timu dostavlja se izvještaj o nedostatcima u sustavu baza podataka te na koji način se to može riješiti.

U pogledu zaštite i očuvanju podataka iz baze jako je bitno imati dobar plan pohrane sigurnosnih kopija. Ukoliko se sigurnosna kopija pohranjuje samo na jednom mjestu, za primjer se može uzeti lokalni ili vanjski tvrdi disk, postoji mogućnost da se disk uništi odnosno prestane ispravno funkcionirati što dovodi do gubitka sigurnosne kopije. Zbog dostupnosti, bitno je imati sigurnosne kopije pohranjene na više od jednog mjesta, ali isto tako ta mjesta na kojima se čuva sigurnosna kopija moraju biti zaštićena od neovlaštenog pristupa [55].

Pored svih ostalih načina zaštite, baze podataka se dodatno mogu osigurati izbjegavanjem korištenja „osnovnih“ priključaka (eng. *Port*). MySQL server baze podataka obično sluša ulazne konekcije na priključku 3306. Većina napada koji se izvode na baze podataka su automatski kako bi mogli pokušati napasti više baza podataka u istom trenutku, ali ih se ovom metodom eliminira i smanjuje rizik od propusta [56].

5.1. FIZIČKA ZAŠTITA BAZE PODATAKA

Pored opisanog aplikacijskog dijela zaštite baze podataka, postoji i ona fizička. Fizička zaštita se odnosi na zaštitu računalnog dijela sustava sa kojeg se sama baza podataka poslužuje ili pohranjuje te sa kojeg je moguć pristup samoj bazi podataka. Ukoliko ova vrsta zaštite nije adekvatno izvedena postoji mogućnost narušavanja sigurnosti. Računalni sustav mora biti smješten na sigurnom mjestu, najčešće u posebnoj prostoriji koja je osigurana ključem. Prostorije moraju biti adekvatno hlađene kako nebi došlo do pregrijavanja komponenti i pada sustava. Pristup prostoriji mogu imati samo određene osobe koje održavaju sustav, odnosno računalni dio sustava. Za primjer, zaposlenik kojemu je posao u sklopu kompanije izrada financijskih izvještaja nebi trebao imati pristup ovoj prostoriji. Također je značajno da prostorija u kojoj se računalo nalazi bude osigurana video nadzorom

ili alarmnim sustavom u slučaju pokušaja provale. Osim toga, računalo unutar prostorije mora biti osigurano u posebnom ormaru sa sigurnosnim lokotom kako se komponente, npr. tvrdi disk u slučaju provale nebi mogle otuđiti [2]. Ukoliko se baza podataka pruža sa udaljene lokacije od strane druge kompanije, potrebno je uvjeriti se da je pružatelj usluge primjenio potrebne mjere za fizičku zaštitu.

Primjer dobre vrste fizičke zaštite je ona koju provodi Google kompanija, a izvodi se u 6 slojeva. Prvi sloj je sam ulaz u područje zgrade koji je zaštićen sigurnosnom ogradom i rampom gdje osoba koja želi pristupiti u to područje mora imati odobrenje za pristup. Drugi sloj se sastoji od kamera koje se nalaze izvan zgrade te zaštitara koji nadziru i pokrivaju cijeli posjed. Treći sloj je pristup samom objektu. Za ulazak u objekt potrebno je predočiti iskaznicu koja potvrđuje identitet korisnika. Ulaz u prostorije unutar objekta dostupan je samo uz skeniranje iskaznice na vratima. Četvrti sloj je detaljan nadzor unutarnjeg dijela objekta. Svaki korak unutar objekta se prati od strane sigurnosnog tima. Peti sloj se odnosi na pristup strogo čuvanom dijelu objekta. Samo 1% zaposlenika ima pristup tom dijelu, odnosno samo tehničari i inžinjeri koji se bave održavanjem sustava. Bitno je napomenuti kako tehničari i inžinjeri imaju pristup uređajima za pohranu podataka, ali nemaju mogućnost čitanja podataka unutar uređaja jer su podatci šifrirani. Šesti sloj je dio objekta na kojem se uređaji za pohranu koji ne prođu određene testove, a sadrže povrjeljive podatke uništavaju. Pristup tom području ima tek par zaposlenika unutar cijelog objekta. Proces izlaska iz objekta je također osiguran kako se iz objekta nebi otuđili povjerljivi uređaji [57].

5.2. EDUKACIJA O INFORMACIJSKOJ SIGURNOSTI

Jedan od načina zaštite je izvođenje posebnih treninga i edukacija za zaposlenika u sklopu kompanije, kako bi ih se osvjestilo o opasnosti koje postoje u vidu informatičke sigurnosti [58]. Prema istraživanju Ponemon instituta, ispitano je 600 zaposlenika kompanija gdje se provodi trening o informatičkoj sigurnosti. 66% ispitanika reklo je da su zaposlenici najslabija karika stvaranja sigurnosnog „zida“. 55% zaposlenika reklo je da je njihova kompanija bila žrtva napada zbog zlonamjernog ili nemarnog zaposlenika [59]. Također, prema istraživanju IBM-a, 23% „curenja“ podataka odnosno sigurnosnih propusta u kompanijama su razlog ljudske greške i nemarnosti. Iz tog razloga, zaposlenike prolaze posebne obuke na kojima uče o najnovijim vrstama napada i propustima. Zaposlenici su najčešće ti koji svojim postupcima i znanjem mogu ispravno reagirati u pravom trenutku i

spriječiti napad. Podizanjem svjesnosti o napadima i njihovom izvođenju, ukoliko je dovoljan broj zaposlenika upućen u sigurnosne propuste, smanjuje vjerojatnost da će se desiti „curenje“ podataka [58, 60].

6. ZAKLJUČAK

Na temelju svega prikazanog možemo zaključiti da je sigurnost baza podataka neiscrpna tema te područje koje se svakodnevno mijenja. Brojne tvrtke i organizacije, kao na primjer pomorske agencije ili farmaceutske kompanije oslanjaju se na baze podataka u kojima čuvaju povjerljive podatke od izuzetne važnosti. Upravo je zbog toga vrlo važno dobro zaštititi baze podataka te njima pravilno upravljati.

Do danas su razvijene i otkrivene brojne vrste mogućih napada koji mogu narušiti sigurnost baza te otkriti povjerljive podatke. Uspješnost nekih napada je rezultat nedostataka programskih sustava zaštite poput onih koji pogađaju SUBP, dok su drugi napadi rezultat faktora ljudske greške kao što su nemarnost administratora pri upravljanju ulogama ili nepravilno i nesigurno čuvanje lozinki za različite sustave i internetske stranice.

Uz razvoj različitih vrsta napada, razvijeni su i brojni načini osiguranja baza podataka kojima je cilj spriječiti i predvidjeti moguće napade kao i pravovremeno reagirati prije nastajanja velike štete. Neke od glavnih preporuka za čuvanje sigurnosti baze podataka su šifriranje podataka s naglaskom na šifriranje pri transferu, kontinuirana nadogradnja programskih paketa, odvajanje baze na višestruke sigurne mreže, korištenje autorizacije autentifikacije te dodjeljivanje uloga. Glavni cilj je razviti napredne sigurnosne mehanizme koji se konstantno i samostalno programski nadograđuju.

Budući da je internet i informacijske tehnologije u kontantnom razvoju predviđam da će istovremeno nastajati nove vrste napada kao i metode zaštite. Svakako je iznimno važno pridržavati se već postojećih metoda očuvanja sigurnosti te time spriječiti uspješnost zlonamjernih korisnika.

7. LITERATURA

[1] F. Zaman, B. Raza, A. Kamran, i A. Anjum, „Self-Protection against Insider Threats in DBMS through Policies Implementation“, *Int. J. Adv. Comput. Sci. Appl.*, sv. 8, izd. 3, 2017, doi: 10.14569/IJACSA.2017.080334.

[2] „Zaštita baza podataka“, *Cent. Inf. sigurnosti*, izd. CIS-DOC-2012-08-059, 2012.

[3] „Most popular database management systems“, *Statista*. https://www.statista.com/statistics/809750/worldwide-popularity-ranking-database-management-systems/ (pristupljeno velj. 25, 2023).

[4] T. Kramberger, S. Duk, i R. Kovačević, *Baze podataka*. Zagreb: Tehničko veleučilište u Zagrebu, 2018.

[5] F. Keith D, „A Brief History of Database Management“, 2021. https://www.dataversity.net/brief-history-database-management/# (pristupljeno velj. 27, 2023).

[6] „A Timeline of Database History & Database Management“, *Quickbase*. https://www.quickbase.com/articles/timeline-of-database-history (pristupljeno velj. 27, 2023).

[7] D. Kelly, „A brief history of databases: From relational, to NoSQL, to distributed SQL“. https://www.cockroachlabs.com/blog/history-of-databases-distributed-sql/ (pristupljeno velj. 28, 2023).

[8] „Sigurnosna politika CCERT-PUBDOC-2009-05-265“, *CARNet CERT LS&S*, [Na internetu]. Dostupno na: https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf.

[9] „What is Database Security | Threats & Best Practices“, *Imperva*. https://www.imperva.com/learn/data-security/database-security/ (pristupljeno ožu. 02, 2023).

[10] „OWASP Top Ten“, *Open Web Application Security Project (OWASP)*, 2022. https://owasp.org/www-project-top-ten/ (pristupljeno ožu. 04, 2023).

[11] „Napadi umetanjem SQL koda“, *Cent. Inf. sigurnosti*, 2011, [Na internetu]. Dostupno na: www.CIS.hr.

[12] C. T. Wang Yong, Jinsong Xi, „SQL Injection Attack: Real Life Attacks and Code Examples“, 2021. https://brightsec.com/blog/sql-injection-attack/ (pristupljeno ožu. 04, 2023).

[13] F. Q. Kareem *i ostali*, „SQL Injection Attacks Prevention System Technology: Review“, *Asian J. Res. Comput. Sci.*, str. 13–32, 2021, doi: 10.9734/AJRCOS/2021/V10I330242.

[14] K. Ahmad, „Classification of SQL Injection Attacks“, *VSRD Tech. Non-Technical J.*, sv. 1(4), str. 235–242, 2010, Pristupljeno: ožu. 04, 2023. [Na internetu]. Dostupno na: https://www.researchgate.net/publication/262536173_Classification_of_SQL_Injection_Attacks.

[15] „Error Based SQL Injections“, *GeeksforGeeks*. https://www.geeksforgeeks.org/error-based-sql-injections/ (pristupljeno ožu. 06, 2023).

[16] „Blind SQL Injection“, *Open Web Application Security Project (OWASP)*. https://owasp.org/www-community/attacks/Blind_SQL_Injection (pristupljeno ožu. 09, 2023).

[17] N. Besic, „Blind SQL Injection: How it Works, Examples and Prevention“, 2021. https://brightsec.com/blog/blind-sql-injection/ (pristupljeno ožu. 09, 2023).

[18] „What Are Blind SQL Injections“, *Acunetix*. https://www.acunetix.com/websitesecurity/blind-sql-injection/ (pristupljeno ožu. 09, 2023).

[19] „Što je DDoS napad?“, *Microsoft / Microsoft security*. https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-ddos-attack (pristupljeno ožu. 10, 2023).

[20] R. Auger, „Abuse of Functionality“. http://projects.webappsec.org/w/page/13246913/Abuse of Functionality (pristupljeno ožu. 13, 2023).

[21] „Dealing with Database Denial of Service“, *Securosis*.

[22] „Napadi uskraćivanjem resursa CCERT-PUBDOC-2006-07-162“, *CARNet CERT*

LS&S, [Na internetu]. Dostupno na: https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-07-162.pdf.

[23] E. Chou i R. Groves, „Distributed Denial of Service (DDoS) Practical Detection and Defense“, *O'Reilly Media*, 2018, [Na internetu]. Dostupno na: https://www.a10networks.com/wp-content/uploads/A10-TPS-EB-Distributed_Denial_of_Service_DDoS_Practical_Detection_and_Defense.pdf.

[24] „DDoS napad CCERT-PUBDOC-2008-09-240“, *CARNet CERT LS&S*, [Na internetu]. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-09-240.pdf.

[25] A. Householder, A. Manion, L. Pesante, i G. M. Weaver, „Managing the Threat of Denial-of-Service Attacks“, *Carnegie Mellon Univ. CERT® Coord. Cent.*, 2001, [Na internetu]. Dostupno na: http://www.cert.org/reports/dsit_workshop.pdf.

[26] D. K. Bhattacharyya i J. Kumar Kalita, *DDoS Attacks*. Boca Raton: CRC Press Taylor & Francis Group, 2016.

[27] A. P. Namanya, A. Cullen, I. U. Awan, i J. P. Disso, „The World of Malware: An Overview“, *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud, FiCloud 2018*, str. 420–427, ruj. 2018, doi: 10.1109/FICLOUD.2018.00067.

[28] Y. Wang, J. Xi, i T. Cheng, „The Overview of Database Security Threats' Solutions: Traditional and Machine Learning“, *J. Inf. Secur.*, sv. 12, izd. 01, str. 34–55, 2021, doi: 10.4236/JIS.2021.121002.

[29] Z. Akhtar, „Malware Detection and Analysis: Challenges and Research Opportunities“, str. 1–10, 2021, [Na internetu]. Dostupno na: http://arxiv.org/abs/2101.08429.

[30] P. Divya, Midhunchakkaravarthy, Ganapathi, „Computer Network Worms Propagation and its Defence Mechanisms: A Survey“, *J. Netw. Comput. Appl.*, 2014, [Na internetu]. Dostupno na: https://www.researchgate.net/publication/299468348_Computer_Network_Worms_Propagation_and_its_Defence_Mechanisms_A_Survey.

[31] M. Boldt, B. Carlsson, i A. Jacobsson, „Exploring Spyware Effects“, *Privacy-*

Invasive Softw., 2014, [Na internetu]. Dostupno na: https://www.researchgate.net/publication/30499314_Exploring_Spyware_Effects.

[32] A. K. Maurya, N. Kumar, A. Agrawal, i R. A. Khan, „Ransomware Evolution, Target and Safety Measures“, *Int. J. Comput. Sci. Eng.*, sv. 6, izd. 1, str. 80–85, sij. 2018, doi: 10.26438/IJCSE/V6I1.8085.

[33] M. Malik i T. Patel, „DATABASE SECURITY-ATTACKS AND CONTROL METHODS“, *Int. J. Inf. Sci. Tech.*, sv. 6, izd. 1, 2016, doi: 10.5121/ijist.2016.6218.

[34] B. Toulas, „Over 12% of analyzed online stores expose private data, backups“. https://www.bleepingcomputer.com/news/security/over-12-percent-of-analyzed-online-stores-expose-private-data-backups/ (pristupljeno ožu. 20, 2023).

[35] P. Hoonakker, P. Carayon, i N. Bornø, „Spamming , spoofing and phishing E-mail security : A survey among end-users“, *Int. Ergon. Assoc. 2009 17th World Congr. Ergon.*, izd. August, str. 1–7, 2009, [Na internetu]. Dostupno na: https://www.researchgate.net/profile/Plt-Hoonakker/publication/268412871_Spamming_spoofing_and_phishing_E-mail_security_A_survey_among_end-users/links/54ee8e2c0cf2e28308651168/Spamming-spoofing-and-phishing-E-mail-security-A-survey-among-end-users.pdf.

[36] V. Bhavsar, A. Kadlak, i S. Sharma, „Study on Phishing Attacks“, *Int. J. Comput. Appl.*, sv. 182, izd. 33, str. 27–29, pros. 2018, doi: 10.5120/IJCA2018918286.

[37] J. Blue, E. Furey, i J. Condell, „A novel approach for secure identity authentication in legacy database systems“, *2017 28th Irish Signals Syst. Conf. ISSC 2017*, srp. 2017, doi: 10.1109/ISSC.2017.7983624.

[38] A. Magnusson, „11 Common Authentication Vulnerabilities You Need to Know“, *StrongDM*, 2022. https://www.strongdm.com/blog/authentication-vulnerabilities (pristupljeno ožu. 21, 2023).

[39] E. H. Highland, „Introduction to database security“, *Comput. Secur.*, sv. 7, izd. 3, str. 329, 1988, doi: 10.1016/0167-4048(88)90104-6.

[40] K. Indu Kashyap, „Database Security & Access Control Models: A Brief Overview“, *Int. J. Eng. Res. Technol.*, sv. 2, izd. 5.

[41] „Mandatory (MAC) vs Discretionary Access Control (DAC) Differences“, *Ekran System*. https://www.ekransystem.com/en/blog/mac-vs-dac (pristupljeno ožu. 22, 2023).

[42] S. Jajodia i M. Gertz, *Handbook Of Database Security - Applications and Trends*. 2008.

[43] „How to Make a Strong Password“, *Technology Solutions*. https://www.techs.co.nz/how-to-make-a-strong-password/ (pristupljeno ožu. 27, 2023).

[44] R. Sandra, „3 Most Secure Authentication Methods“, *Best Reviews*. https://password-managers.bestreviews.net/3-most-secure-authentication-methods/ (pristupljeno ožu. 30, 2023).

[45] L. Bouganim i Y. Guo, „Database Encryption“, *Encycl. Cryptogr. Secur.*, str. 307–312, 2011, doi: 10.1007/978-1-4419-5906-5_677.

[46] V. Samar, „Securing the Oracle Database A technical primer“, *4th Ed. Oracle*, str. 147, 2021.

[47] N. Paul, „Database Backups in the Cloud for Disaster Recovery“, *Severalnines*. https://severalnines.com/blog/database-backups-cloud-disaster-recovery/ (pristupljeno tra. 02, 2023).

[48] A. Romero i L. Ashdown, „Backup and Recovery Basics“, *Oracle Database Backup Recover. Basics*, izd. 10.1.

[49] D. Gotseva, V. Gancheva, i I. Georgiev, „DATABASE BACKUP STRATEGIES AND RECOVERY MODELS“, *Challenges High. Educ. Res.*, sv. 9, 2011.

[50] S. Salam i M. Hamad, „Implementation of Backup and Recovery methods in Oracle Database“, 2004, doi: 10.13140/RG.2.2.31565.90089.

[51] A. Khraisat, I. Gondal, P. Vamplew, i J. Kamruzzaman, „Survey of intrusion detection systems: techniques, datasets and challenges“, *Cybersecurity*, sv. 2, izd. 1, str. 1–22, pros. 2019, doi: 10.1186/S42400-019-0038-7/FIGURES/8.

[52] „What is Intrusion Prevention System?“, *VMware Glossary*. https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

(pristupljeno tra. 05, 2023).

[53] K. Scarfone i P. Hoffman, „Guidelines on Firewalls and Firewall Policy“, *Natl. Inst. Stand. Technol.*, 2009, doi: 10.6028/NIST.SP.800-41r1.

[54] „What Is Database Security Testing - Complete Guide“, *Software testing help*. https://www.softwaretestinghelp.com/database-security-testing/ (pristupljeno tra. 10, 2023).

[55] „How to Perform Database Backups“, *Rubrik*. https://www.rubrik.com/insights/how-to-perform-database-backups (pristupljeno tra. 10, 2023).

[56] J. C. Villanueva, „Port Confusion - Is Security Through Obscurity Bad?“, *JSCAPE*. https://www.jscape.com/blog/using-nonstandard-ports-is-security-through-obscurity-really-bad (pristupljeno tra. 10, 2023).

[57] „Google Data Center Security: 6 Layers Deep“, *Youtube*. https://www.youtube.com/watch?v=kd33UVZhnAA (pristupljeno tra. 13, 2023).

[58] „Data Security and Management Training: Best Practice Considerations“, *Protecting Student Privacy*. https://studentprivacy.ed.gov/resources/data-security-and-management-training-best-practice-considerations (pristupljeno tra. 13, 2023).

[59] Y. Josh, „Why is Data Security Training for Employees Important?“, *EVERFI*. https://everfi.com/blog/workplace-training/why-is-security-awareness-training-important (pristupljeno tra. 16, 2023).

[60] „Cost of a Data Breach Report“, *IBM Secur.*, 2022, Pristupljeno: tra. 20, 2023. [Na internetu]. Dostupno na: https://www.ibm.com/downloads/cas/3R8N1DZJ.

8. POPIS SLIKA

Slika 1 Primjer greške koju izaziva napad SQL umetanje 6
Slika 2 Primjer napada "Zloupotreba funkcije" 9
Slika 3 Primjer napada "Zloupotreba funkcije" (nastavak) 10
Slika 4 Razlika između DoS i DDoS napada. 12
Slika 5 Primjer „Phishing“ napada. 17
Slika 6 Primjer zlonamjerne stranice 18
Slika 7 Primjer elektroničke pošte koja sadrži zlonamjernu datoteku. 19
Slika 8 Autentifikacija putem sučelja za prijavu provjerena putem baze podataka 19
Slika 9 Tri najčešća načina autentifikacije 26
Slika 10 Princip funkcioniranja potpune sigurnosne kopije 28
Slika 11 Princip funkcioniranja diferencijalne sigurnosne kopije 28
Slika 12 Princip funkcioniranja sigurnosne kopije temeljene na promjenama 29

9. POPIS KRATICA

DOS	Napad uskraćivanja usluga (eng. *Denial of service*)
DDOS	Napad raspodjeljenog uskraćivanja usluge (eng. *Distributed denial of service*)
IDS	Sustav za otkrivanje provala (eng. *Intrusion Detection System*)
IPS	Sustav za sprječavanje provala (eng. Intrusion Prevention Systems)
SUBP	Sustavi za upravljanje bazama podataka
SQL	Strukturni programski jezik (eng. *Structured Query Language*)