Centar Informacijske Sigurnosti

Zaštita baza podataka

kolovoz 2012.

CIS-DOC-2012-08-059

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Baza podataka (eng. *Database*) je organizirana zbirka informacija, tipično u digitalnom obliku, [1] koje se pomoću specijaliziranih programskih alata mogu uređivati, bilježiti, brisati i dodavati. Baze podataka su informacije koje opisuju stanje nekog sustava u realnom svijetu, bilo da je to broj slobodnih hotelskih soba, rezultati biomedicinskih istraživanja, zapisi filmova na poslužiteljima i sl. Baze podataka mogu se klasificirati prema sadržaju: bibliografske, tekstualne, numeričke i multimedijske. [2] U računarstvu baze podataka se dijele na nekoliko vrsta:

- **relacijsko–tablične** - strukture koje su definirane tako da se informacijama može pomoću logičkih izraza jednostavno pristupiti i izdvojiti tražene informacije,
- **objektno orijentirane** - koriste se pri programiranju, odnosno sadržavanju informacije koje pripadaju objektima, razredima i podrazredima te
- **distribuirane** - baze podataka koje se mogu rasporediti na više točaka u računalnoj mreži ili na Internetu.

Alati za uređivanje, stvaranje i upravljanje bazama podataka objedinjeni su pod jednim nazivom SUBP - sustavi za upravljanje bazama podataka (eng. DBMS- *Database Management System)*. Neki od najpoznatijih SUBP-a su: Oracle, DB2, MySQL, Informix, PostgreSQL i SQL server. Česta pojava od kad postoje baze podataka su napadi zlonamjernih korisnika koji se žele domoći informacija pohranjenih unutar SUBP-a. Posljedice takvog napada mogu rezultirati krađom identiteta, brojeva kreditnih kartica, financijskim gubicima, gubicima privatnosti, narušavanjem nacionalne sigurnosti te drugim brojnim opasnim posljedicama koje su rezultat pristupa osjetljivim podacima.

Kako su se razvijali SUBP-ovi, tako je postajala sve očitija potreba za njihovom sigurnošću. Zbog toga su svakom novom inačicom (kod svih proizvođača) dodavane brojne sigurnosne opcije, kao i sigurnosne nadogradnje koje bi uklanjale ranjivosti. Sve većom uporabom Interneta, privatno i na radnom mjestu, javio se imperativ osiguravanja baza podataka od pristupa iz vanjskog svijeta. Ne samo zaštitom mrežnih resursa na kojima se SUBP nalazi, kao što su postavljanje vatrozida i ažuriranjem programskih paketa na poslužiteljima, nego i zaštitom samog SUBP-a postavljanjem dozvola pristupa i sigurnosnih politika.

Zaštita baza podataka je od ključne važnosti za sigurnost bilo kojeg informacijskog sustava iz razloga što je sama količina osjetljivih informacija pohranjena u tim bazama velika i što o njoj često ovisi jako velik broj ljudi. Prema izvještajima objavljenim na web stranici www.datalossdb.org, broj provala u prvoj polovici 2012. godine samo kod velikih tvrtki iznosi 704, što je gotovo jednako broju provala u 2009. i 2010 zajedno.

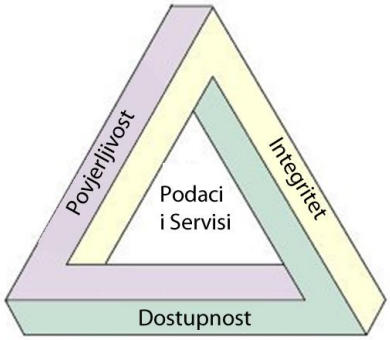
Najveće baze za koje je javno poznato da su provaljene u 2012. su: Zappos (24 milijuna zapisa), Global Payment System (7 milijuna zapisa), South Carolina Health and Human Services (228 435 zapisa) zr Linked In (6.5 milijuna zapisa).

2. Elementi zaštite na razini baze podataka

Kod zaštite vitalnih informacija na razini baze podataka, prema [3] postoje tri ključna elementa, tzv. trijada sigurnosti. Ti elementi (Slika 1) su:

- **povjerljivost** - zaštita podataka od neovlaštenog pregledavanja,
- **integritet** - zaštita od nedozvoljenog pristupa podacima i
- **dostupnost** - mogućnost oporavka od programskog ili sklopovskog zatajenja koje rezultiraju DoS (eng. *Denial of Service*) stanjem SUBP-a ili cjelokupnog sustava.

U vidu tih ključnih elemenata analizirat će se osnovni principi ostvarenja sigurnosti baza podataka i pripadnih SUBP-a.



Slika 1: Trijada sigurnosti podataka
Izvor: blogs.technet.com

2.1. Kontrola pristupa

Najosnovnija metoda zaštite osjetljivih informacija koje se čuvaju u bazi podataka je ograničenje pristupa podacima samo određenoj skupini korisnika. Na ovaj način osigurava se povjerljivost podataka. Kontrola pristupa može se ostvariti na dva načina:

1. Autentifikacijom odnosno ovjeravanjem korisničkog imena ili lozinke.
2. Davanjem posebnih privilegija i prava specifičnim podatkovnim objektima i skupovima podataka. Unutar baze podataka to su obično tablice, pregledi, redci i stupci, a prava koja im se dodjeljuju su čitanja, pisanja ili oboje.

Općenito kontrola pristupa definirana je na tri načina:

1. obvezna kontrola pristupa (eng. *Mandatory Access Contro,* MAC*l*),
2. diskretna kontrola pristupa (eng. *Discretionary Access Control,DAC*) i
3. kontrola pristupa zasnovana na ulogama (eng. *Role Based Access Control* RBAC).

MAC i DAC daju privilegije određenim korisnicima ili grupama koje sadrže korisnike kojima se želi dati pristup. MAC pravila se primjenjuju na razini sustava i smatraju se sigurnijima. DAC pravila se primjenjuju na razini korisnika, smatraju se dinamičkim, a usmjerena su na sadržaj. Primjerice, ako se jednom korisniku pridijeli samo djelomično čitanje ovisno o nekom svojstvu (pr. čitanje samo parnog broja hotelske sobe u registru hotela) radi se o MAC pravilima. MAC i DAC su vrlo moćni alati no RBAC je posebno učinkovit u zaštiti SUBP-a. RBAC je analogan funkcijama na poslu. Primjerice, jedan ured se sastoji od direktora, računovođe, tajnika, i sl. sa različitim ulogama. Svaka uloga, ima svoja vlastita prava te sadrži ograničenja. Prava uključuju naredbe odabira podataka, modificiranje podataka ili manipuliranje strukture baze podataka.

Kontrola pristupa posjeduje i nadogradnju pod nazivom „odobri/povuci odobrenje“ (eng. *grant/revoke*) koja omogućuje dinamično davanje dozvole pristupa određenom korisniku. Problem koji nastaje pri ovakvom pristupu sigurnosti je mogućnost davanja privilegija korisniku koji zapravo nema dobre namjere te može načiniti štetu na sustavu, a korištenje se dodatno komplicira ako korisnici često moraju mijenjati uloge.

Odobrenje prava pristupa administratori obavljaju preko logičkog jezika koji je implementiran na SUBP. Najčešći logički jezik je SQL [1] (eng. Structured Querry Language), razvijen tijekom sedamdesetih godina prošlog stoljeća u IBM-ovim laboratorijima. Naredbe na koje se mogu primijeniti prava pristupa su CREATE, INSERT, SELECT, DELETE i UPDATE. Izgled naredbe za odobravanje i oduzimanje prava pristupa je sljedeći:

```
GRANT privileges
[ON relation]
TO users
[WITH GRANTOPTION]
```

U navedenoj relaciji[2] prvo se nalazi osnovna naredba GRANT koja daje prava pristupa, zatim "privileges" vrsta privilegije koja se daje relaciji (ON relation) koja sadrži neku ili sve spomenute naredbe (CREATE, INSERT, DELETE,...). Na kraju naredbe navodi se ime korisnika ("TO users") kojem se daju prava pristupa te dodatne opcije. Naredba REVOKE uklanja prava korisnicima i njena je sintaksa vrlo slična onoj narebe GRANT.

```
REVOKE privileges
[ON relation]
FROM users
[WITH GRANTOPTION]
```

Razlike su samo leksičke, u riječima REVOKE i FROM, te TO i FROM.

2.2. Ispitivanje (eng. auditing)

Ispitivanje se koristi za praćenje pristupa bazi podataka i aktivnosti korisnika. Također, ispitivanje se može koristiti za identifikaciju korisnika koji pristupa objektima u bazi podataka te koje akcije se obavljaju i koji podaci su promijenjeni. Nažalost, ispitivanje ne donosi obranu od napada ali pridonosi računalnoj forenzici nakon napada kako bi se lakše identificirao propust i način iskorištavanja spomenutog propusta koji se koristio za upad u bazu podataka. Uobičajene kategorije ispitivanja baza podataka uključuju nadgledanje pokušaja ulaza u bazu podataka, aktivnosti upravljačkog jezika za podatke (eng. *data control language,* DCL), aktivnosti definicijskog jezika za podatke (eng. *data definition language* DDL) i aktivnost jezika za manipulaciju podacima (eng. *data manipulation language,* DML). Nadgledanje pokušaja ulaza u bazu podataka obuhvaća sve informacije o uspješnim i neuspješnim pokušajima autorizacije na bazu podataka. DCL ispitivanja bilježe promjene uloga i privilegija korisnika kao i brisanja i dodavanja korisnika. DDL ispitivanja, s druge strane bilježe promjene na shemi baze podataka kao što su izmjena strukture tablice ili atributa tipova podataka. Provjera se implementira preko dnevničkih podataka i ispitnih tablica.

Ispitivanje ima vrlo veliku važnost u cjelokupnom planu za povećanje sigurnosti baze podataka. Primarna slabost procesa ispitivanja je vremenski odmak od izvedene akcije do pregledavanja i analize zapisa o izvedenoj radnji. Posljedično, upadi u baze i druge ne autorizirane aktivnosti se prekasno uočavaju te je gotovo nemoguće na njih promptno reagirati. U novije vrijeme se pokušavaju implementirati rješenja za nadgledanje baze u realnom vremenu tako da se prepoznaju uzorci nelegitimnog manipuliranja bazom podataka te da se o tome odmah obavijeste administratori baze podataka.

[1] Za više detalja o jeziku korisnicima se preporučuje pregled dokumenta [5] u kojem je jezik objašnjen na jednostavnim primjerima.

[2] relacija je naziv za skup naredbi u jeziku SQL

2.3. Autentifikacija i lozinke

Svaka baza podataka ima autentifikacijksu proceduru. Proceduru kroz koju je korisnik primoran dati svoje korisničko ime i lozinku te druge slične identifikacijske i autorizacijske elemente. Jednom kad je korisnik autentificran, baza podataka „zna“ tko je korisnik i dodjeljuje mu pripadne privilegije. Prema SANS rječniku autentifikacija je „proces potvrđivanja ispravnosti predloženog identiteta korisnika“. Metode koje se mogu koristiti pri autentifikaciji korisnika su:

- **elementi koje korisnik zna** - korisničko ime i lozinka (najčešće se koristi),
- **element koje korisnik posjeduje** - pametna kartica (eng. *smart card*) ili certifikat,
- **element koji je atribut samog korisnika** – npr. biometrijska autentifikacija pomoću otiska prsta ili uzorka rožnice.

Većina baza podataka dozvoljava kontrolu administratora nad mogućnostima kako se obavlja autentifikacija. Ukoliko je administrator nepažljiv, vrlo lako bi mogao dovesti bazu podataka u opasnost. Autentifikacija se može provoditi na razini operacijskog sustava ili unutar samog SUBP. Kao primjer uzimamo SUBP DB2 koji ima nekoliko autentifikacijskih mogućnosti. Prva autentifikacijska mogućnost naziva se CLIENT, a korisnicima omogućuje pristup bazi bez autentifikacije na poslužitelju. Sustav pretpostavlja da je autentifikacija već obavljena na strani klijenta te propušta korisnika u bazu s dodijeljenim ulogama. Ova autentifikacijska mogućnost prelazi u sigurnosni propust ukoliko je klijent[3] kompromitiran. U primjeru s DB2 potrebno je koristiti opciju KRB_ENCRYPT_SERVER u kojoj se autentifikacija obavlja na poslužitelju te se dodatno koristi „kerberos“[4] mrežni sigurni protokol.

Kod korištenja lozinki bitno je odabrati lozinku prave duljine koju je teško pogoditi, a poželjno je koristiti i posebne znakove. Administratori bi trebali pri davanju korisničkih računa dati upute za izradu lozinki te unutar SUBP-a zabraniti korištenje jednostavnih lozinki. Postoji niz alata za administratore SUBP-a za provjeru valjanosti (duljine i kompleksnosti) i nadzora lozinki kao na primjer „SQL server auditing tool“[5] ili „Oracle password cracker“. Ovi alati za administratore rade isključivo ako se autentifikacija ne obavlja na operacijskom sustavu nego unutar same baze podataka. Najbolja praksa za čuvanje lozinki za pristup bazi podataka prema [6], je odvajanje lozinki od izvornog koda programa SUBP-a u odvojenu konfiguracijsku datoteku. Konfiguracijsku datoteku potrebno je kriptirati pomoću nekog od poznatih algoritama (Data Encryption Standard, DES ili *Advanced Encryption Standard*,*AES*), tj. nikako se ne bi smjeli ostaviti u tekstualnom formatu čitljivom svim korisnicima (eng. *plaintext*) u proizvoljnom direktoriju. Direktoriju u kojem se nalaze lozinke također bi trebalo ograničiti pristup preko operacijskog sustava. Operacijski sustav bi se trebalo konstantno nadograđivati i održavati sigurnim.

Isto tako, zbog zaštite baze podataka od DoS napada bitno je postavljanje broja pokušaja ovjere korisničkog imena i lozinke (npr. dozvoliti 3 unosa lozinke). U tom slučaju, ukoliko se korištenjem napada sirovom snagom (eng. brute force) pokuša probiti lozinka, sustav će obavijestiti administratora, a te onemogućiti prijavu s navedenim korisničkim imenom.

2.4. Kriptiranje

Element povjerljivosti podataka najbolje se osigurava preko metoda kriptiranja koje se implementiraju na SUBP. Metode su posebno korisne kada se podaci spremaju na sekundarne spremnike podataka kao na primjer pomoćni poslužitelj za kopije (eng. *Backup server*) ili pri transferu podataka kroz mrežu. Kriptiranje bi se trebalo shvaćati kao posljednja linija obrane kad sve ostale sigurnosne mjere zakažu.

Dvije najčešće tehnike koje se koriste pri kriptiranju u bazama podataka su kriptiranje podataka u tranzitu i kriptiranje podataka u mirovanju.

Kriptiranje podataka u tranzitu postala je apsolutnom nužnošću od kad su računala koja sadrže baze podataka spojena na Internet. Preslušavanje podataka u tranzitu mrežom vrlo je jednostavno jer se podaci prenose skupom protokola TCP/IP (eng. Transmission Control Protocol/ Internet Protocol) , preko predefiniranih priključaka (1433 za Microsoft SQL Server,

[3] Izraz klijent odnosi se na bilo koje računalo koje nije poslužitelj: http://en.wikipedia.org/wiki/Client%E2%80%93server_model

[4] Kerberos je protokol otvorenog koda koji se koristi za kriptiranje mrežnog prometa

[5] Alati se mogu pronaći na stranicama: http://www.cqure.net.tools.jsp/?id=10 i http://www.petefinnigan.com/tool.htm

1521 za Oracle, 4100 za Sybase, 50000 za DB2, 3306 za MySQL), a većina informacija se prenosi u tekstualnom obliku čitljivom svima ili uz jednostavniju obradu.

Kriptiranje podataka u mirovanju, prikazano na slici 2, može biti izvedeno na tri razine:

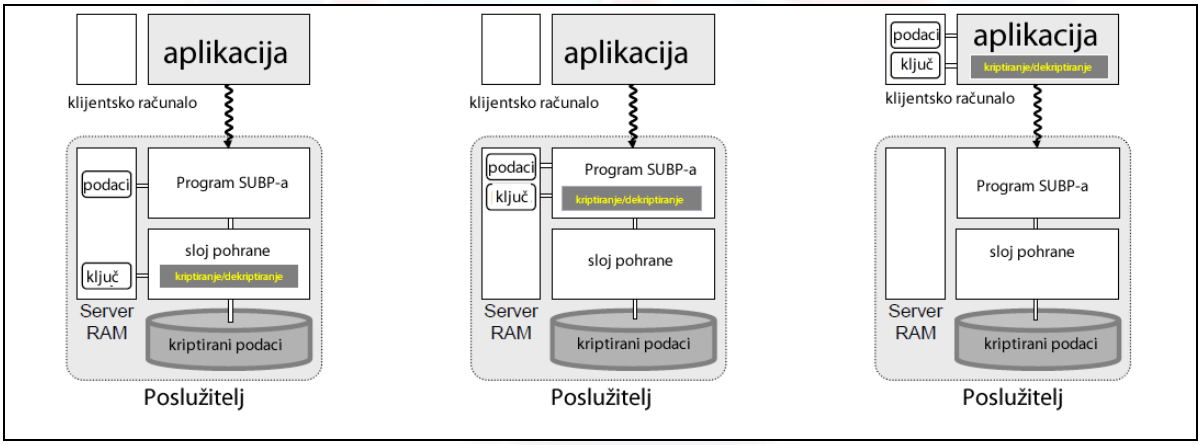
1. na razini skladišta podataka (eng. *storage level encryption*),
2. na razini baze podataka (eng. *database-level encryption*) te
3. na aplikacijskoj razini (eng. *application level encryption*).

Prva razina, razina skladišta podataka kriptira podatke u podsustavu skladišta podataka i štiti čitave datoteke i direktorije. Postoji velika razina transparentnosti te se izbjegavaju promjene na postojećoj aplikaciji. S druge strane, podsustav skladišta podataka nema nikakvog znanja o objektima baze podataka niti o njezinoj strukturi pa se ne može primijeniti kriptiranje isključivo jednog dijela baze niti se može kriptirati dio baze koji pripada korisniku s određenim privilegijama. Smanjenje enkripcijskog viška[6] koji bi se dobio selektivnim kriptiranjem ovisi o granuliranosti datoteka.

Kriptiranje na razini baze podataka omogućava osiguravanje podataka tijekom umetanja ili dohvaćanja podataka iz baze. Strategija kriptiranja može biti dio dizajna baze podataka i može se korelirati s osjetljivošću podataka ili razinom prava korisnika. Moguće je selektivno kriptirati retke, stupce, tablice. Prema nekim logičkim uvjetima,ovisno o razini integracije, kriptiranje može utjecati na neke od aplikacija.

Obje prethodne strategije dekriptiraju podatke u tijeku izvođenja programa te se ključevi kojima se kriptira moraju držati ili na poslužiteljskoj strani ili slati s klijentskog računala. To omogućuje zlonamjerno iskorištavanje od strane administratora ili napadača koji ima administratorske ovlasti.

Kriptiranje na razini aplikacije provodi se unutar same aplikacije koja rukuje podacima u SUBP-u, te se pohranjuje i dohvaća već kriptirana. Tako se odvaja čuvanje ključa za kriptiranje od baze podataka. Aplikacije bi se trebale modificirati da podržavaju ovo rješenje. Isto tako, potrebno je vratiti veću količinu podataka nego što je potrebno (zbog granuliranosti datoteka) što predstavlja određeni sigurnosni rizik. Također, onemogućeni su napredni oblici upravljanja bazama podataka kao što su okidači (eng. *trigger*) i pohranjene procedure.



Slika 2. *Različiti načini kriptiranja podataka,redom: kriptiranje na razini pohrane, kriptiranje na razini baze podataka, kriptiranje na razini aplikacije*
Izvor: *www.inria.fr*

Različite baze podataka omogućuju različite opcije pri odabiru algoritama i načina kriptiranja podataka. U tablici 1 dane su sve mogućnosti kriptiranja i osiguravanja povjerljivosti i integriteta prijenosa podataka za poznatije SUBP.

[6] Pri kriptiranju određenim metodama većeg broja datoteka javlja se i veći redundantni broj bitova.

	Oracle	Microsoft SQL Server	IBM DB2/UDB	Sybase	MySQL
Kriptiranje podataka u pokretu	SSL	SSL	Komercijalno mrežno kriptiranje	SSL	SSL
Kriptiranje pohranjenih podataka	EFS na Windows operacijskom sustavu	EFS na Windows operacijskom sustavu	EFS na Windows operacijskom sustavu	EFS na Windows operacijskom sustavu	EFS na Windows operacijskom sustavu

Tabela 1: Načini kriptiranja u različitim SUBP
Izvor: CIS

Pri kriptiranju informacija u prijenosu iz baze podataka u korisničku aplikaciju većina SUBP koristi SSL (eng. *secure sockets layer*) protokol. SSL kriptiranje odvija se sa 40 ili 128 bita, ovisno o inačici operacijskog sustava koji se koristi kao i protokola koji se koristi za komunikaciju između klijenta i poslužitelja. Problemi koji se javljaju pri kriptiranju SSL protokolom je dodatan zahtjev za računalnim resursima kako bi se obavila enkripcija. To može rezultirati i osjetnim padom performansi cijelog sustava ukoliko je broj simultanih transakcija jako velik pa ovu tehniku treba koristiti s oprezom.

2.5. Kontrola integriteta

Kontrola integriteta osigurava se preko semantičkih ograničenja integriteta. Kad god korisnik pokušava izmijeniti podatke, nakon što mehanizmi kontrole pristupa omoguće korisniku rad, semantički podsustav započinje provjeru jesu li izmijenjeni podaci semantički točni. Semantička točnost podataka se ovjerava preko skupine uvjeta ili predikata koji se moraju uskladiti sa trenutnim stanjem baze. Kako bi se omogućilo otkrivanje zlonamjernog rukovanja podacima, podaci se dodatno digitalno potpisuju.

2.6. Sustav oporavka i sinkronizacije podataka

Ovaj mehanizam zaštite podataka unutar baze osigurava točnost i dostupnost podataka usprkos sklopovskim, programskim i mrežnim greškama. Dostupnost podataka, posebno za podatke dostupne na Internetu, može se poboljšati posebno korištenjem tehnika koje sprječavaju napade uskraćivanjem usluga. Takvi se mehanizmi temelje na strojnom učenju i predviđanju količine upita na bazu podataka.

3. Dodatni elementi zaštite

3.1. Fizička sigurnost

Ukoliko je baza podataka udaljena ili se pruža kao tzv. SaaS (eng. *Software as a service*) , potrebno je provjeriti da li pružatelj takvih usluga (eng. *Application service provider,* ASP) ima dovoljne tehničke uvijete, kao što su: [4]

- dovoljno rashlađivanje prostorija u kojima se drže poslužitelji,
- video nadzor sklopovlja poslužitelja,
- protuprovalne sustave,
- dozvola pristupa samo ključnim djelatnicima ASP-a te
- postojanje redundantnih sustava.

3.2. Baza podataka kao mrežni poslužitelj

Kod sigurnosti baze podataka kao mrežnog poslužitelja vrijede osnovna pravila zaštite kao i kod bilo kojeg aplikativnog mrežnog poslužitelja, kao što su frekventna nadogradnja programskih paketa, korištenje antivirusnih alata, alata za detekciju i prevenciju upada na poslužitelj i drugi.

Dominantni pristup u mrežnoj sigurnosti je baziran na tome da se mrežu pokuša segmentirati na više manjih dijelova, postavljajući na rubnim dijelovima podsegmenata vatrozide koji primjenjuju sigurnosna pravila i politike kako bi onemogućili upadanje iz vanjskih mreža.

3.2.1. Vatrozidi

Vatrozidi su evoliuriali zajedno s razvojem Interneta te dijele mrežu na dijelove kojima možemo i ne možemo vjerovati (eng. *Trusted, untrusted network*). Kod zaštita baza podataka uglavnom se koriste sljedeći vatrozidi:

- **Paketno filtrirani vatrozidi** - nadgledaju izvorne i odredišne IP adrese bilo koje veze i provjeravaju ih prema ugrađenom setu pravila kako bi odlučili da li bi se veza trebala dozvoliti ili ne. Ne provjeravaju sadržaj pa ih je lako zaobići.
- **Aplikacijski usmjernici** (eng. *application proxy)* - zamjenjuju klijenta na poslužiteljskoj strani odnosno poslužitelja na klijentskoj strani. Dozvoljavaju i prekidaju te dvije veze po potrebi, a sav promet prolazi kroz njih.
- **Inspecijski vatrozidi** - procesori paketa koji provjeravaju čitave sjednice. Provjeravaju postoje li protokoli te postoje li zlonamjerno oblikovani paketi. Provjeravaju konzistentnost tablica stanja prometa i provjeravaju stanje TCP veze, adresne translacije i druge. Ovi vatrozidi podržavaju korištenje VPN (eng. *Virtual private network*) veza.

Jedan od najpoznatijih vatrozida za baze podataka je SecuSphere DBF, tvrtke Imperva.[7]

3.2.2. Sustav za detekciju provale

Sustav detekcije provale IDS (eng. *Intrusion detection system*) sakuplja informacije sa brojnih osjetila unutar računala i računalnih mreža, te analizira te informacije kako bi našao indikacije zlonamjernih aktivnosti u računalnoj mreži. Osim detekcije upada, ovakvi alati

[7]Vatrozid sadržava brojne napredne sigurnosne opcije kao što su nadgledanje prometa u realnom vremenu, Više podataka o vatrozidu može se naći na: http://www.imperva.com/products/dsc_database-firewall.html

pružaju širok spektar funkcija kao što su analiza korisničke aktivnosti, statistička analiza abnormalnih aktivnosti, pregled dnevnika operacijskih sustava i brojne druge.

Osjetila su aplikacije na računalu koje prikupljaju podatke te često te podatke bilježe u dnevnike (eng. *logs*). To uključuje dnevnike baza podataka, web poslužitelja, aplikativnih poslužitelja i drugih. Osjetila su isto tako aplikacije koje nadziru mrežni promet, a često su integrirane na samim mrežnim sučeljima NIC (eng. *network interface card*).

Nakon što su podaci skupljeni, analiziraju se ili u intervalnom modu ili u realnom vremenu. Analiza se obavlja bazirano na signaturama, statističkoj analizi, analizi integriteta ili kombinaciji ovih metoda. Analiza bazirana na signaturama se izvodi uspoređivanjem stanja mreže s dosadašnjim poznatim načinima napada na sustav (signaturama). Statistička analiza pokušava otkriti devijaciju od normalnog ponašanja korisnika, a analiza integriteta provjerava konzistentnost svih datoteka.

Nedostatak ovakvog sustava je prilično često lažno alarmiranje korisnika.

3.2.3. Sustav prevencije provale

Sustav prevencije provale IPS (eng. *intrusion prevention system*) izvodi jednaku zadaću kao i IDS, ali s dodatnom mogućnošću blokiranja prepoznatog pokušaja provale. Detekcija je malo ublažena naprema IDS sustavima kako bi se izbjegla učestalost lažne detekcije. Postoje dvije vrste sustava za detekciju provale:

- **IPS na glavnom računalu** (eng. *Host based*) - implementira se koristeći aplikacijske slojeve API (eng.*application programming interface*) koji se koriste za komunikaciju operacijskog sustava i aplikacija. Provjerava se svaki sistemski poziv prema pravilima pristupa koji se automatski generiraju. Svrha ovih IPS-a je blokiranje napada prepisivanjem spremnika(eng. *buffer overflow*), sprečavanje izmjene registarskih vrijednosti i prepisivanja dijeljenih dinamičkih biblioteka (DLL, eng. *dynamic link library*).
- **Mrežni IPS** - izgrađuju se na mreži i služe za dubinsku inspekciju paketa. Točnije, mrežni IPS-ovi provjeravaju pakete na slojevima ispod TCP/IP složaja, koji čini tek 2% paketa. Zbog toga dubinska analiza provjerava i ostalih 98% paketa, a mogu se provjeravati XML(eng. *extensible markup language*) paketi, SQL () paketi i HTTP promet.

3.3. Aplikacijska sigurnost

Upadi u baze podataka prema dosadašnjim saznanjima su do 70% interne naravi, no još veću zabrinutost izazivaju preostalih 30% koji dolaze s Interneta. S velikim razvojem elektroničkog poslovanja i elektroničke trgovine, potreba za visokom razinom sigurnosti baza podataka je sve više rasla kao i broj otkrivenih sigurnosnih ranjivosti web aplikacija. Rješenje ovog problema javlja se u vidu obrazovanja razvojnih inženjera o sigurnosti aplikacija, korištenja sigurnih razvojnih okolina. korištenjem alata za sigurnosno testiranje i sl. Sa strane puštanja aplikacije u pogon (eng. *deployment*), potrebno je paralelno instalirati aplikacijski vatrozid koji provodi URL (eng. *uniform resource locator*) filtriranje te zaštitu protiv napada uskraćivanjem usluge.

4. Poznati napadi i propusti

4.1. Zlonamjerno korištenje privilegija

Kada se korisnicima ili aplikacijama dodjeli veća razina sigurnosti nego što im je potrebna čest je slučaj zlouporabe danih privilegija. Ovaj propust uglavnom je uzrokovan administratorovim nedostatkom vremena da fino granulira zadatke koje pojedini korisnik mora i može obavljati te se vrlo često događa da korisnik dobije velike ovlasti nad bazom podataka nad kojom mu je potrebno pregledati svega par redaka. Rješenje ovog propusta bio bi mehanizam ograničavanja pristupa na razini upita. Tako bi se neke osnovne radnje na negranuliranim podacima mogle obavljati, dok bi se ostale nedozvoljene radnje blokirale i dojavljivale administratoirma. Implementacija ovakvog rješenja trebala bi biti potpuno automatizirana te bi se trebao koristiti programski paket izvan SUBP-a koji nema takvih mogućnosti (u protivnom je posao za administratora vrlo težak ako ne i nemoguć).

Drugi slučaj zlonamjernog korištenja privilegija je korištenje legitimnih privilegija. Primjerice, ako korisnik posjeduje privilegiju čitanja i spremanja podataka na računalo i u slučaju da je to računalo ukradeno, ili korisnik podijeli osjetljive informacije s dugima, tad postoji opasnost od otkrivanja osjetljivih informacija. Rješenje ovakvog problema bilo bi kontekstualna kontrola pristupa, odnosno pod kojim okolnostima se pristupa bazi podataka. Primjeri kontekstualne provjerue su: vrijeme pristupa, izvorišna IP adresa, volumen podataka koji se koristio, aplikacijski klijent i slično.

4.2. Povišene privilegije

Napadači bi mogli iskoristiti ranjivost platforme kako bi prepravili prava pristupa bazi podataka s razine običnog korisnika na razinu administratora baze podataka. Ovakve ranjivosti mogu se naći u pohranjenim procedurama, ugrađenim funkcijama, implementacijama protokola pa čak i u SQL upitima. Sprečavanje ovakvog tipa propusta moguće je pomoću spomenutog ograničenja kontrole pristupa na razini upita te pomoću IPS-a. IPS bi trebao točno odvajati legitimne funkcije od onih koje uključuju napad.

4.3. SQL umetanje

Kod napada umetanjem SQL koda, počinitelj umeće ili ugnježđuje neautorizirane izraze baze podataka u ranjivi SQL podatkovni kanal. Ciljani kanali podataka uključuju spremljene procedure, ali najčešće i ulazne parametre web aplikacije. Napadači iskorištavaju činjenicu da programeri često ulančavaju SQL naredbe sa korisnički unesenim parametrima te tako mogu jednostavno umetnuti SQL izraze. Umetnuti izrazi se šalju na bazu podataka gdje se potom izvršavaju.

Kao primjer uzeta je web aplikacija koja upravlja proizvodima. U jednoj od dinamičkih stranica web aplikacije korisnici mogu unijeti identifikator proizvoda te pregledati ime i opis proizvoda Zahtjev se šalje u obliku sljedećeg izraza:

```
SELECT ProductName, ProductDescription
FROM Products
WHERE ProductNumber = ProductNumber
```

Tipično web aplikacije koriste upite u obliku niza znakova u kojem je sadržan sam upit i njegovi parametri. Aplikativni ASP (eng, *Active server pages*)[8] kod izgleda ovako:

```
sql_query= "
```

[8] Active server pages je Microsoftova tehnologija za izradu Web aplikacija.

```
SELECT ProductName, ProductDescription
FROM Products
WHERE ProductNumber = " & Request.QueryString("ProductID")
```

Vidimo da je SQL kod samo „umotan“ u ASP kod koji prosljeđuje bazi podataka na obradu. Napadač bi mogao iskoristiti navedeni kod tako da na URL postavi dodatni izraz „OR 1=1“ čiji će uvjet biti uvijek zadovoljen (jer je 1=1 točna izjava pa će cijeli izraz, zbog OR operacije, također uvijek biti istinik) primjerice:

```
http://www.mydomain.com/products/products.asp?productid=123 or 1=1
```

A potom bi mogao nadodati i naredbu „drop table“ koja briše cijelu tablicu podataka:

```
http://www.mydomain.com/products/products.asp?productid=123; DROP
TABLE Products
```

Veliki brj modela web aplikacija pretpostavlja SQL upit kao valjanu naredbu, što omogućuje napadačima iskorištavanje SQL upita za zaobilaženje kontrole pristupa. U nekim slučajevima SQL upiti mogu omogućiti pristup naredbama operacijskog sustava preko spremljenih procedura. Za navedeni primjer napadač bi mogao dodati sljedeći kod na URL:

```
123;EXEC master..xp_cmdshell dir--
```

To bi napadaču dalo uvid u kompletan sadržaj direktorija u kojem se izvršava proces SQL poslužitelja.

Napadi umetanjem SQL koda mogu se spriječiti pregledavanjem SQL signatura u dolaznom HTTP (eng. *hypertext transfer protocol*) protokolu. Stoga se savjetuje korištenje alata koji omogućava analizu SQL naredbi sa predviđanjem ispravnosti upotrebe.

4.4. DOS

DoS napad je posljedica propusta koja uzrokuje nemogućnost pristupa resursu. U ovom slučaju radi se o bazi podataka odnosno o web aplikaciji. DoS stanje može se kreirati preko različitih tehnika kao što su korupcija podataka, mrežno preplavljivanje (preopterećenje) i preopterećenje računalnih resursa te iskorištavanjem ranjivosti platforme i/ili okoline na kojoj se baza podataka nalazi. Primjer DoS napada slične izvedbe kao i umetanje SQL koda je korištenje dugih posebno oblikovanih regularnih izraza. Na primjer:

```
_[^|?$%"*[(Z*m1_=]-%RT$)|[{34}\?_]||%TY-3(*.>?_!]_
```

Prevencija DoS napada zahtjeva zaštite na višestrukim razinama kao što su mrežna, aplikacijska i razina baze podataka.

Učinkovita obrana protiv DoS napada na razini mreže ostvaruje se korištenjem dinamičkog poslužitelja, koji pruža višestruke dretve za rukovanje vezama i postavlja ograničenja na vrijeme izvođenja pojedinih naredbi.

IPS i validacija protokola sprječava zlonamjerne korisnike u iskorištavanju programskih ranjivosti kao bi izazvali DoS stanje.

Dinamičko profiliranje automatski pruža kontrolu pristupa na razini upita kako bi detektirao neautorizirane upite, koji bi pak mogli voditi do DoS napada. DoS napadi koji ciljaju ranjivosti na razini platforme mogu izazvati alarmiranje sustava za dinamičko profiliranje.

4.5. Ranjivosti komunikacijskih protokola

Rastući broj mrežnih ranjivosti identificira se u komunikacijskim protokolima baza podataka. Četiri od sedam sigurnosnih zakrpa u dva recentna IBM DB2 paketa za nadogradnju odnosila su se na ranjivosti komunikacijskih protokola. Aktivnosti koje ciljaju na ovakav tip ranjivosti mogu sezati od neautoriziranog pristupa bazi podataka i korupcije podataka pa do izazivanja stanja uskraćivanja usluge. Ranjivosti komunikacijskih protokola mogu se zaobići tehnologijom koja se naziva validacija protokola. Svaki komunikacijski paket se kod te tehnologije rastavlja te se uspoređuje je li u skladu s očekivanjem. U slučaju da stvarni promet ne odgovara očekivanjima on se može blokirati.

5. Komercijalne i baze otvorenog koda

Baze otvorenog koda su one čiji je izvorni kod dostupan svakom korisniku. Dozvoljene su modifikacije i nadogradnje, ali se ne smiju licencirati (naplaćivati). Komercijalne baze podataka nemaju dostupan programski kod, naplaćuje se njihovo korištenje te je uglavnom zabranjena njihova modifikacija od strane krajnjeg korisnika (eng. *End user licence agreement,* EULA).

Svaka od opcija ima svoje prednosti i nedostatke. Na primjer, komercijalne baze podataka obično uključuju i dodatne programske pakete i korisničku podršku kao i korisničke treninge koju pruža proizvođač. Baze otvorenog koda generalno su fleksibilnije i jeftinije pri korištenju i održavanju. Druga prednost baza otvorenog koda je kompatibilnost sa drugim tehnologijama i postojećim sustavima. U 2011. godini zastupljenost baza podataka otvorenog koda kod većih tvrtki porasla je za 50%. Prema trenutnim podacima oko 20% tvrtki uspjelo je kombinirati svoje programske proizvode s bazama podataka otvorenog koda, a kroz nekoliko se godina očekuje udvostručenje tog broja.

Sa strane sigurnosti koda, nakon brojnih istraživanja u računalnoj industriji, pokazalo se da su baze otvorenog koda obično bolje od komercijalnih zbog velike podrške zajednice. Nažalost, to se odnosi samo na neke od SUBP-a, dok primjerice jedan od većih predstavnika baza podataka otvorenog koda, MySQL nema implementirane sigurnosne mogućnosti, vanjsku autentifikaciju, sigurnost na razini redaka i sl. Unatoč tim problemima, razvojni timovi sve više se oslanjaju na baze podataka otvorenog koda jer im se sigurnost kontinuirano poboljšava u korak sa komercijalnim bazama podataka.

6. Zaključak

Baze podataka s gledišta sigurnosti neiscrpna je i uvijek aktualna tema. Svaki veći posao, kao na primjer zdravstvena skrb ili državne ustanove oslanjaju se na baze podataka u kojima spremaju ključne podatke. Upravo zbog toga vrlo je važno baze podataka zaštiti i njima upravljati na pravi način. Kao glavne preporuke za čuvanje sigurnosti baze podataka su stalna nadogradnja programskih paketa, odvajanje baze na sigurne segmente mreže, korištenje enkripcije pri transferu i skladištenju osjetljivih podataka, korištenje autorizacije autentifikacije i uloga. Postoje različiti načini napada na baze podataka, koji su već dobro poznati, ali zbog nedostataka u drugim sustavima mogu pogoditi i SUBP i bazu podataka kojom se upravlja. Takvi napadi su izazivanje DoS i/ili SQL umetanje. No, osim nedostataka drugih sustava, postoje ranjivosti koje uključuju ljudske faktore kao što su dodjeljivanje akreditacije zlonamjernim korisnicima, nemarnost administratora pri nadgledanju baza podataka i sl.

Provale u baze podataka sve su češće, a sanacija štete sve je skuplja. U 2011. godini procjena štete nastale u većim korporacijama iznosila je oko 200 milijuna dolara po provali. Prema istraživanjima tvrtke Appsec pet najvećih uzročnika provala u 2012. godini su redom :

- nezakrpane ranjivosti,
- napredne perzistentne prijetnje,
- loša konfiguracija SUBP-a,
- napadi unutar tvrtke te
- pogreške unutar tvrtke.

Iako su baze podataka ranjive na navedene vanjske i unutarnje prijetnje, moguće je smanjiti broj ranjivosti na prihvatljivu razinu rizika. To se postiže tako da se koriste napredni sigurnosni mehanizmi opisani u prethodnim poglavljima, konstantno nadograđuju programski paketi vezani uz operacijskih sustav i SUBP, koriste sigurni mrežni resursi te sigurnosni proizvodi kao što su vatrozidi i antivirusni alati.

7. Leksikon pojmova

NIST

Institucija oja se bavi standardizacijom tahnologije - Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardim i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života. - Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardizacijom tehnologija u cilju poboljšanja ekonomske sigurnosti i kvalitete života.

Reference: http://www.nist.gov/public_affairs/overview_video/overview_video.html

RSA - Rivest, Shamir, Adelman algoritam

Popularan algoritam kriptografije javnih ključeva baziran na faktorizaciji velikih brojeva. - Popularan algoritam kriptografije javnih ključeva baziran na faktorizaciji velikih brojeva. Predstavlja prvi algoritam koji je bio pogodan za šifriranje i potpisivanje poruka, te se smatra jednim od prvih postignuća u kriptografiji javnog ključa. RSA se koristi u mnogim protokolima za sigurnu komunikaciju i smatra se da je dovoljno siguran za sve današnje potrebe.

Reference: http://web.math.hr/~duje/kript/rsa.html

AES - Advanced Encryption Standard

Kriptografski standard zasnovan na algoritmima sa simetričnim ključem, što znači da svaka strana u komunikaciji mora imati tajni ključ kako bi pročitala i poslala poruku. Standardom se opisuju tri blokovske šifre AES-128, AES-192 i AES-256. Svaki koriste blokove veličine 128 bitna, te ključeve veličine 128, 192 i 256 bita ovisno o algoritmu. Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael. - Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael - Ponajbolji kriptografski standard, prihvaćen od vlade SAD-a i široko korišten. Poznat i pod nazivom Rijndael.

Reference: http://www.quadibloc.com/crypto/co040401.htm

DES algoritam šifriranja

Vrlo popularan kriptografski standard, danas zamjenjen standardom AES. - Vrlo popularan kriptografski standard, danas zamjenjen standardom AES. Tajni ključ za šifriranje podataka sastoji se od 56 bita, što znaći da postoji ukupno 2^56 (više od 72,000,000,000,000,000) mogućih kombinacija. Za šifriranje poruke se koristi jedan od ključeva iz velikog broja kandidata. Algoritam je simetričan, što znaći da obadvije strane moraju imati tajni ključ kako bi mogli komunicirati.
Reference: http://nvl.nist.gov/pub/nistpubs/sp958-lide/250-253.pdf

DoS napad (napad uskraćivanjem usluge)

Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

Reference: http://searchsoftwarequality.techtarget.com/definition/denial-of-service

MITM napad

Napad na sigurnost pri kojem se zlonamjerni napadač umiješa u komunikaciju na način da se postavi između sugovornika te čita i izmjenjuje poruke.
Reference: https://www.owasp.org/index.php/Man-in-the-middle_attack

SQL injection napad

Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika. - Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web programa bazi podataka. Na taj način moguće je ugroziti sigurnost web programa koji konstruira SQL upite iz podataka koje su unijeli korisnici.

Reference: https://www.owasp.org/index.php/SQL_Injection

TCP protokol

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

Reference: http://www.webopedia.com/TERM/T/TCP.html

Usmjeritelj

Uređaj koji usmjerava pakete između računalnih mreža - Usmjeritelji su uređaji koji imaju barem dva sučelja na različitim mrežama, a usmjeravaju pakete do njihovog odredišta. Na svom putu, paketi prolaze kroz nekoliko usmjeritelja, a svaki zasebno određuje put kojim će ga dalje slati.
Reference: http://www.webopedia.com/TERM/R/router.html

IP protokol

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

Reference: http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

URL (Uniform Resource Locator)

URL predstavlja adresu određenog resursa na Internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument, slika, datoteka ili bilo koja datoteka koja se nalazi na određenom web poslužitelju.

Reference: http://searchnetworking.techtarget.com/definition/URL

HTTP protokol

Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priljučak 80), čekajući da klijent inicira komunikaciju. - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.

Reference: http://hr.wikipedia.org/wiki/HTTP

MAC protokol

Komunikacijski protokol za pristup mediju - Media Access Control (MAC) je protokol za komunikaciju podacima, također poznat kao Medium Access Control protokol (protokol upravljanja pristupom mediju). On omogućuje mehanizme adresiranja i kontrole pristupa kanalima koji služe za komunikaciju terminala, odnosno čvorišta, s mrežom koja ima više pristupnih točaka.

Reference: http://ahyco.ffri.hr/ritehmreze/teme/mac.htm

Autentikacija

Autentikacija je proces potvrđivanja identiteta podatka ili osobe. - Autentikacija je proces određivanja identiteta nekog subjekta, najčešće se odnosi na fizičku osobu. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi da je subjekt upravo taj kojim se predstavlja. Najčešći primjeri su: uz korištenje kartice na bankomatu i upisivanje PIN-a, ili upisivanje (korisničkog) imena i zaporke.

Reference: http://searchsecurity.techtarget.com/definition/authentication

URI (Uniform Resource Identifier)

URI je niz znakova koji se koristi za identifikaciju imena ili nekog drugog resursa na Internetu. URI sintaksa započinje URI shemom (npr. http, ftp, mailto, sip), nakon čega slijedi dvotočka i niz znakova koji ovisi o odabranoj shemi.

Reference: http://searchsoa.techtarget.com/definition/URI

XML (EXtensible Markup Language)

XML je kratica za EXtensible Markup Language, odnosno jezik za označavanje podataka. Ideja je bila stvoriti jedan jezik koji će biti jednostavno čitljiv i ljudima i računalnim programima. U XML-u se sadržaj uokviruje odgovarajućim oznakama koje ga opisuju i imaju poznato, ili lako shvatljivo značenje.

Reference: http://webdesign.about.com/od/xml/a/aa091500a.htm

SPIT (Spam over Internet Telephony)

SPIT ili VoIP spam su neželjeni, automatski i unaprijed snimljeni pozivi koji koriste IP mrežu za prijenos govora (VoIP). SPIT je sličan e-mail spamu.

Reference: http://searchunifiedcommunications.techtarget.com/definition/SPIT

Šifriranje

U kriptografiji označava proces obrade podataka (izvorni tekst) koristeći kriptografski algoritam kako bi podatci bili nečitljivi svima osim onome tko posjeduje tajni ključ za dešifriranje podataka.

Reference: http://www.webopedia.com/TERM/E/encryption.html

Trojanski konj

Zloćudni program koji se pretvara kao legitimna aplikacija - Trojanski konj je oblik zloćudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zloćudnih programa se ne širi samostalno.

Reference: http://www.webopedia.com/TERM/T/Trojan_horse.html

Napad grubom silom

U kriptografiji napad grubom silom podrazumijeva strategiju pronalaska tajnog ključa ili lozinke koja se, u teoriji, može iskoristiti protiv svakog kriptografskog algoritma. Podrazumijeva sistematično isprobavanje svih mogućih ključeva ili lozinki dok se ne otkrije ispravan. U najgorem slučaju mora se proći kroz cijeli prostor ključeva.

Reference: http://www.computerhope.com/jargon/b/brutforc.htm

API (Application Programming Interface)

API predstavlja skup dobro definiranih pravila i koraka koji omogućuju interakciju dvaju ili više sustava. Služi kao sučelje između različitih programskih proizvoda i omogućuje njihovu interakciju.

Reference: http://www.webopedia.com/TERM/A/API.html

WWW (World Wide Web)

WWW (eng. World Wide Web) je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. hiperlink).

Reference: http://www.webopedia.com/TERM/W/World_Wide_Web.html

8. Reference

[1] Wikipedia: Database
http://en.wikipedia.org/wiki/Database, 7.2012.

[2] What is database,
http://searchsqlserver.techtarget.com/definition/database, 7.2012.

[3] Database Security: What Students Need to Know Meg Coffin Murray

[4] http://www.csoonline.com/article/220665/19-ways-to-build-physical-security-into-a-data-center?page=2

[5] http://www.profsandhu.com/articles/auerbach/a94dac.pdf

[6] http://www.mediawiki.org/wiki/Manual:Securing_database_passwords