Centar Informacijske Sigurnosti

Sigurno rukovanje dnevničkim podacima

kolovoz 2012.

CIS-DOC-2012-08-058

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

Dnevnički podaci su računalni zapisi u koje se standardiziranim načinima unose podaci koji opisuju zbivanja na računalnim sustavima i mrežama. Sastoje se od dnevničkih unosa (eng. *log entry*). Svaki zapis sadrži svoj identifikator te opis zbivanja koje je zabilježeno. Količina podataka koje se bilježe u zapise je golema te se shodno tome javlja potreba za sustavom koji bi upravljao ovakvim podacima odvajajući bitne podatke i odbacujući irelevantne. Prema definiciji iz [1] upravljanje dnevničkim zapisima je proces stvaranja, prenošenja, pohranjivanja i analiziranja podataka s računala u svrhu računalne sigurnosti. Izvori stvaranja sigurnosnih dnevničkih zapisa su sigurnosni programi kao što su antivirusni alati, vatrozidi, programi za otkrivanje i sprečavanje upada u sustave, operacijski sustavi za radne stanice i poslužitelje te mrežna oprema s pripadajućim primjenama. Za upravljanje dnevničkim podacima od ključne je važnosti spremanje dovoljne količine podataka kroz dovoljno dug vremenski period. Rutinska analiza dnevničkih zapisa pomaže pri identifikaciji i klasifikaciji sigurnosnih incidenata, zlonamjernih aktivnosti, kršenja sigurnosnih pravila (slika 1) te identifikaciji funkcionalnih problema. Pošto sadrže brojne povjerljive podatke, pristup dnevnicima mora biti ograničen i nadgledan jer zlonamjerni korisnici moraju izmijeniti ili obrisati dnevničke podatke kako bi prekrili ilegalne radnje.

Osnovni problem s upravljanjem dnevničkim podacima koji se javlja u većini organizacija je učinkovito balansiranje ograničenih resursa za tu aktivnost, iz razloga što se dnevnički podaci stalno stvaraju. Stvaranje i pohrana dnevničkih podataka može biti problematična zbog inkonzistencije sadržaja dnevničkih podataka, formata i vremenskih oznaka među različitim izvorima dnevničkih podataka.

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

Slika 1. Dnevnički zapis Intrusion Detection Sustava (IDS)
Izvor: Guide to Computer Security Log management

U prvom poglavlju govori se o doprinosu sigurnosti koje donosi upotreba dnevničkih podataka te o vrstama informacija koje se bilježe. Drugo poglavlje donosi pregled sklopovske i programske arhitekture potrebne za agregaciju i pohranjivanje dnevničkih podataka.

2. Dnevnički zapisi s aspekta sigurnosti

Unutar mrežnih i računalnih resursa tvrtki i organizacija svakodnevno se stvaraju velike količine (reda veličine nekoliko GB) dnevničkih podataka iz različitih izvora, dajući sliku o aktivnostima u IT (eng. *Information Technology)* sustavu. Svaka se aktivnost bilježi u digitalnom dnevničkom zapisu, primjerice pristup mrežnim resursima kao što su podatkovni poslužitelji, posrednički poslužitelji i sl. Ako nezadovoljni zaposlenik tvrtke pokuša ukrasti povjerljive podatke, vjerojatno o tome postoji dnevnički zapis koji sadrži korisničko ime zlonamjernog zaposlenika, IP (eng. *Internet Protocol*) adresu s koje je pristupio resursu kao i točno vrijeme pristupa.

Osim nezadovoljnih zaposlenika, dnevnički zapisi mogu spriječiti s aspekta sigurnosti štetne aktivnosti, tako da administratori na vrijeme identificiraju sigurnosne prijetnje, kršenje sigurnosnih politika tvrtke, izmjenu datoteka, zaobilaženje korisničkih ograničenja itd. S inherentnim prednostima dnevničkih zapisa u vidu, korištenje dnevničkih zapisa nameće se kao temelj računalne sigurnosti, a u nekim zemljama njihovo je korištenje zakonski regulirano. U SAD-u nekoliko je zakona kao što su savezni zakon o upravljanju informacijskom sigurnošću (eng. *Federal Information Security Management Act of 2002*, FISMA) ili zakon o prenosivosti zdravstvenog osiguranja (eng. *Healt Insurance Portability and Accountability Act of 1996,* HIPPA) koji obvezuju federalne i zdravstvene organizacije da koriste dnevničke zapise u svrhu računalne sigurnosti. Sigurnosni standard industrije platnih kartica (eng. *Payment Card Industry Data Security Standard,* PCI-DSS) obvezuje organizacije koje se bave financijskim transakcijama putem kreditnih kartica bilježenje svojstvenih detalja o transakcijama kako bi se spriječile prijevare, krađa osjetljivih informacija i hakiranje u sustave. PCI-DSS se također obvezuje najmanje jednom dnevno pregledavati dnevničke zapise za sve komponente sustava. Prikaz svih zahtjeva PCI-DSS dan je tablicom 1.

Tablica 1: zahtjevi PCI-DSS;
Izvor: Wikipedia

Kontrolni ciljevi	PCI-DSS zahtjevi
Izgradnja i održavanje sigurne mreže	Instalacija vatrozida kako bi se zaštitili podaci
	Izbjegavanje korištenja osnovnih vrijednosti programa za sigurnosne postavke i lozinke
Zaštita kartičnih podataka	Kriptiranje spremljenih kartičnih podataka
	Kriptiranje prijenosa kartičnih podataka kroz javne mreže
Održavanje programa za rukovanje ranjivostima	Korištenje nadograđenog antivirusnog alata na svim sustavima
	Razvoj sigurnih primjena
Primjena jakih mjera za provjeru pristupa	Ograničite pristup kartičnim podacima
	Dodjela jedinstvenog identifikatora osobama s pristupom unutarnjoj računalnoj mreži
Nadgledanje i ispitivanje mreža	Nadgledanje mrežnog pristupa
	Regulatorno ispitivanje sustava i procesa
Održavanje sigurnosne politike	Održavanje sigurnosne politike tvrtke na visokoj razini

Dnevnički zapisi izravno ili neizravno imaju veze s računalnom sigurnošću organizacija. Dnevničke zapise može se razvrstati u tri veće skupine:

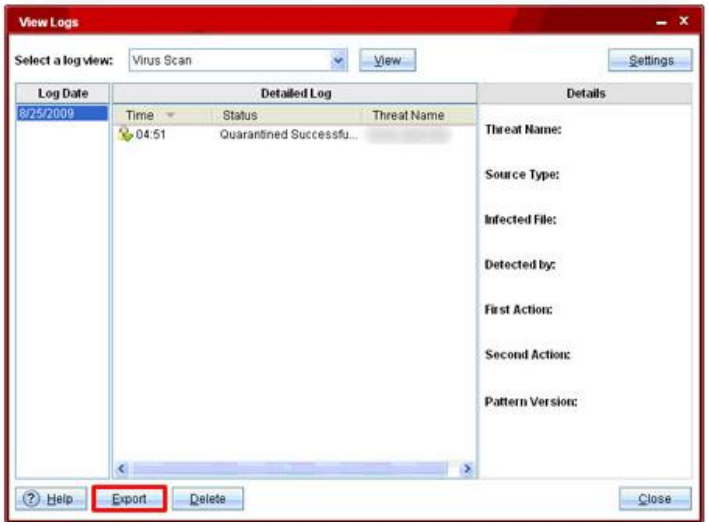
- dnevnički zapisi sigurnosnih programa,
- dnevnički zapisi operacijskog sustava i primjena,
- mrežni dnevnički zapisi.

Prvi sadržavaju samo zapise vezane uz sigurnost dok drugi mogu sadržavati i ostale informacije koje nisu bitne za sigurnost sustava odnosno mreže, ali administratorima pružaju uvid u opće stanje sustava.

2.1. Dnevnički zapisi sigurnosnih programa

Većina organizacija koristi nekoliko vrsta mrežnih i lokalnih sigurnosnih programa za otkrivanje zlonamjernih aktivnosti, zaštitu podataka i sanaciju štete uzrokovane zlonamjernim djelovanjem korisnika. Tipični primjeri ovakvih programa su:

- antivirusni alati - bilježe vrste otkrivenih zlonamjernih programa, pokušaje uklanjanja istih te koje su sve datoteke zaražene koje su u karanteni i sl. (slika 2),
- IDS (eng. *Intrusion Detection Systems*) i IPS (eng. *Intrusion Prevention Systems*) sustavi - detaljno bilježe sve informacije sumnjivog ponašanja korisnika te moguće pokušaje napada. Svoje rezultate uspoređuju s bazom poznatih napada te upozoravaju administratore. Razlika između IDS i IPS sustava je ta da IPS sustavi mogu aktivno blokirati sumnjive radnje, npr. blokiranje IP (eng. *Internet Protocol*) adrese za koju se sumnja da je izvor napada,
- programi za udaljeni pristup (eng. *Remote Access Software*) - udaljeni pristup obavlja se putem VPN (eng. *Virtual Private Network*) mreža. VPN sustavi bilježe uspješnost autorizacije, broj prenesenih podataka i druge.,
- *web* posrednički poslužitelji (eng. *proxy*) - služe za dohvaćanje web stranica umjesto korisnika, mogu blokirati određene stranice, a bilježe i spremaju sve stranice koje se preko njih dohvaćaju,
- programi za rukovanje ranjivostima - koriste se za nadogradnju i procjenu ranjivosti programskih rješenja, tipično bilježe instalacijsku povijest programa te trenutačnu ranjivost sustava,
- autentifikacijski poslužitelji - bilježe svaki pokušaj autentifikacije s porijeklom autentifikacije, korisničkim imenom, uspješnošću te vremenom pokušaja,
- usmjerivači (eng. *routers*) - programska rješenja i operacijski sustavi na usmjerivačima mogu se konfigurirati tako da blokiraju ili dopuštaju određeni oblik mrežnog prometa ovisno o svojim postavkama. Bilježe samo osnovna svojstva blokiranih aktivnosti,
- vatrozidi (eng. *firewalls*) - prate stanje mrežnog prometa i mogu pregledati sadržaj paketa podataka,
- poslužitelji za mrežnu karantenu - poslužitelji na koje se spajaju vanjski klijenti čija se sigurnost treba provjeriti prije nego što se mogu priključiti na mrežu.



Slika 2. Prikaz dnevničkog zapisa antivirusnog programa, Izvor: Trendmicro

2.2. Dnevnički zapisi operacijskih sustava

U ovom poglavlju razmatraju se dnevnički zapisi operacijskih sustava za poslužitelje, radne stanice i mrežne uređaje koji obično bilježe velike količine informacija vezanih za sigurnost. Tipični primjeri takvih zapisa su:

- zapisi sustavnih događanja (eng. *system events*) – bilježe se operacije koje izvode komponente operacijskog sustava, koje su skrivene očima korisnika, kao što su gašenja i uključenja ključnih servisa sustava. Administratori sustava obično određuju koji će se podsustavi i događaji nadgledati,
- dnevnički zapisi nadgledanja sustava (eng. *audit records*) – sadrže informacije kao što su uspješni i neuspješni pokušaji prijave na sustav, pristup datotekama, izmjene na zapisima i druge.

Dnevnički zapisi su dobri za identifikaciju ili istraživanje sumnjivih aktivnosti *host* računala. Na primjer mrežni uređaj može otkriti napad na pojedino *host* računalo, a operacijski sustav bilježi korisnika koji je tad bio prijavljen na računalo pa indicira potencijalnog krivca za napad. Velik broj operacijskih sustava bilježi dnevničke zapise u *syslog* formatu, za razliku od operacijskog sustava Windows na kojima se zapisi spremaju u formatu zatvorenog koda (Slika 3).

```
Event Type:   Success Audit
Event Source: Security
Event Category:      (1)
Event ID:     517
Date:         3/6/2006
Time:         2:56:40 PM
User:         NT AUTHORITY\SYSTEM
Computer:     KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM       Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)   Client User Name: userk
Client Domain: KENT             Client Logon ID: (0x0,0x28BFD)
```

Slika 3. Dnevnički zapis Windows operacijskog sustava: Izvor: NIST

2.3. Dnevnički zapisi programa

Zapisi aplikacija variraju od svojih izvedaba. Neke aplikacije koriste sustave zapisa koji su ugrađeni u operacijski sustav, dok druge koriste vlastite. Obično se bilježe sljedeće vrste informacija:

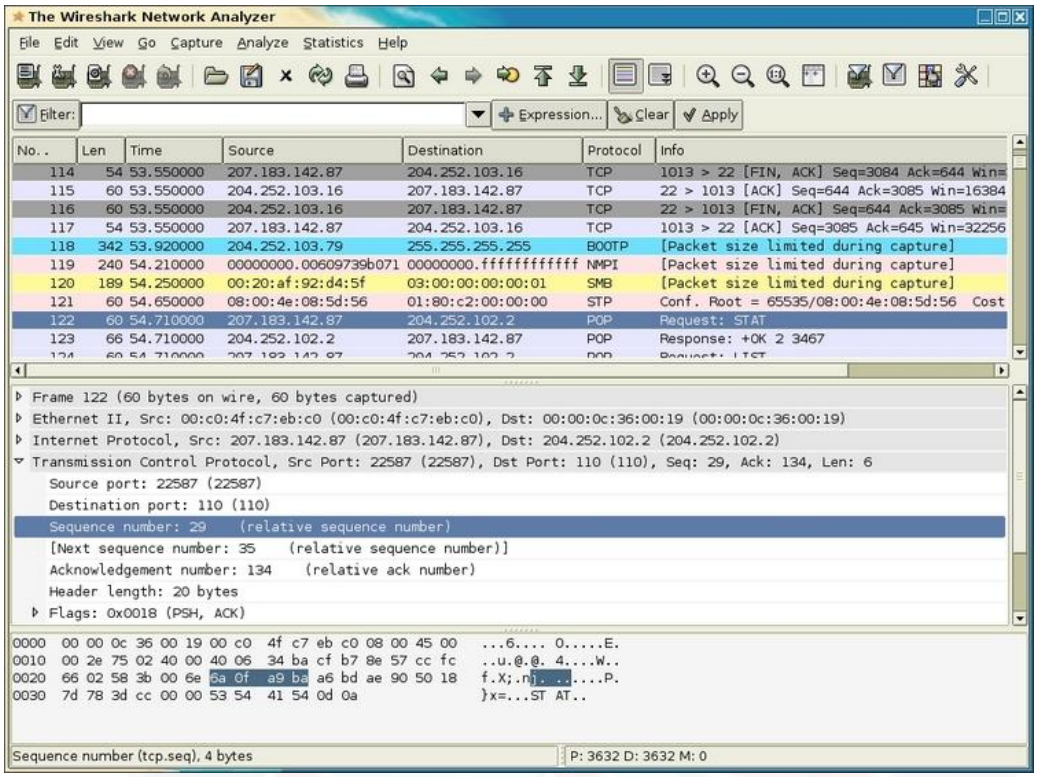
- informacije o instalaciji,
- zahtjevi i odgovori arhitekture klijent - poslužitelj,
- informacije o korisničkim računima,
- informacije o korištenju,
- akcije koje program ima u registru operacijskog sustava.

2.4. Mrežni dnevnički zapisi

Mrežni dnevnički zapisi opisuju podatke koji se šalju i primaju preko mreže te se mogu koristiti za praćenje cjelokupne mrežne infrastrukture organizacije. Za razliku od dnevničkih zapisa prethodne dvije skupine, mrežni dnevnički zapisi nisu ograničeni isključivo na jedno računalo nego izvještavaju administratore o aktivnostima na čitavoj mreži. Aktivnosti koje prate su veze među računalima, izvori i destinacije poruka, vrste poruka, vrijeme kada su poruke poslane, protokole koji su korišteni za prijenos, duljinu poruke i prvih nekoliko okteta poruke. Ovakvi zapisi ne daju informaciju o korisniku koji je koristio određenu mrežnu vezu nego isključivo podatke o vezama. Primjer alata za generiranje mrežnih dnevničkih zapisa je Wireshark čiji je ispis prikazan na slici 4.

Na sredini slike mogu se vidjeti ključni dijelovi dnevničkog zapisa:

- vrsta protokola,
- izvorišni priključak (eng. *source port*),
- odredišni priključak (eng. *destination port).*



Slika 4: Prikaz rada alata Wireshark
Izvor: Canadian content

3. Infrastruktura za rukovanje dnevničkim zapisima

Infrastruktura za rukovanje dnevničkim zapisima sastoji se od sklopovlja, programa mreža i medija za stvaranje, prijenos, pohranu, analizu i arhiviranje podataka. Infrastruktura za sigurno upravljanje dnevničkim zapisima sastoji se od tri kategorije:

- stvaranja zapisa,
- analize i pohrane,
- nadgledanje (eng. *monitoring*) zapisa.

U prvoj kategoriji nalaze se svi računalni resursi koji stvaraju dnevničke zapise te ih prenose lokalnom mrežom do ostalih računala radi sinkronizacije ili Internetom do dnevničkih poslužitelja. Druga kategorija sastoji se od jednog ili više dnevničkog poslužitelja koji prihvaćaju dnevničke zapise iz prve kategorije. Podaci se između prve dvije kategorije prenose u stvarnom vremenu kako bi se osiguralo pravodobno reagiranje na posebne događaje kao što su upad u mrežu i sl.. Dnevnički poslužitelji koji prikupljaju dnevničke zapise s više izvora nazivaju se kolektori (eng. *Collectors*). Infrastruktura druge kategorije može varirati u svojoj složenosti i strukturi. Najjednostavnija struktura je jedan dnevnički poslužitelj. Drugi složeniji primjeri sastoje se od višestrukih poslužitelja koji obavljaju specijaliziranu funkciju, analize ili kratkotrajne, odnosno, dugotrajne pohrane podataka.

Treća kategorija sadržava konzole koje se koriste za pregled dnevničkih podataka i rezultata automatizirane analize. Konzolama iz treće kategorije može se upravljati uređajima iz prve dvije kategorije, dnevničkim poslužiteljima i računalnom opremom.

Infrastruktura za rukovanje dnevničkim podacima obično obavlja funkcije koje ne izmjenjuju izvorne dnevnike, a mogu se svrstati u tri osnovne funkcijske kategorije:

- obrada dnevničkih podataka - izvlačenje podataka iz dnevničkih zapisa kako bi se mogli koristiti kao ulaz za drugi dnevnički proces,
- filtriranje događaja - uklanjanje zapisa iz procesa analize, prijavljivanja ili dugotrajne pohrane jer njihove svojstva indiciraju da je malo vjerojatno da sadržavaju relevantne informacije. Primjeri su duplicirani dnevnički podaci i sl.,
- agregiranje događaja - slični događaji se spajaju u jedinstven zapis koji sadrži broj ponavljanja događaja. Agregacija događaja provodi se simultano sa stvaranjem dnevničkih podataka.

3.1. Pohrana podataka

Rotacija dnevnika je zatvaranje jedne datoteke u koju se pohranjuju dnevnički podaci i otvaranje nove kada se prva smatra dovršenom. Rotacije se obično pravilno ponavljaju ili prema nekom rasporedu (svaki sat, dan ili tjedan) ili kad se dosegne određena veličina datoteke. Korist rotacije dnevnika je održavanje veličine dnevnika dovoljno malom za pregledavanje, a moguće je i komprimirati prethodne podatke kako bi se smanjio prostor potreban za pohranu.

Arhiviranje dnevnika je spremanje dnevnika kroz dulji vremenski period, na pokretne medije (CD, USB medij) ili mrežu za pohranu (eng. *storage area network*, SAN). Postoje dva načina arhiviranja:

- retencija - standardni način pohrane,
- prezervacija - čuvanje dnevničkih zapisa koji bi se inače odbacili.

Kompresija dnevničkih podataka je pohrana dnevničkog zapisa koja smanjuje prostor potreban za pohranu bez izmjene sadržaja dnevnika. Redukcija dnevnika je uklanjanje nepotrebnih zapisa iz dnevnika kako bi se dnevnik učinio manjim. Pretvorba dnevnika je obrada dnevničkog zapisa u jednom formatu i pohrana u drugom, primjerice iz XML formata u tekstualni format.

Normalizacija dnevničkog zapisa svako polje zapisa pretvara se u zaseban podatkovni prikaz i tako se kategorizira. Najčešća uporaba normalizacije je pohrana datuma i vremena u jedinstveni format. Primjerice, jedan generator podataka mogao bi pohraniti zapis vremena u 12 satnom obliku dok bi drugi to mogao napraviti u 24 satnom obliku. U ovom slučaju postoji mogućnost ne prepoznavanja o kakvom se podatku radi ako naiđe na broj veći od 12, ali pošto se normalizacijom dobiva jedinstvena kategorija vremena analizator prepoznaje o čemu se radi.

Provjera integriteta podataka sastoji se od izračunavanja sažetka poruke za svaku datoteku i spremanje sažetka datoteke na sigurnu adresu. Sažetak datoteke je digitalni uzorak koji jedinstveno opisuje podatke te promjena u jednom bitu podatkovne datoteke uzrokuje stvaranje drukčijeg sažetka. Korelacija događaja je pronalaženje logičkih povezanosti između dva ili više dnevnička zapisa. Najčešći oblik korelacije događaja je korelacija zasnovana na nizu pravila. Ona uspoređuje višestruke zapise s istog ili više izvora kako bi se pronašla povezanost među različitim zapisima.

Pregled dnevničkih zapisa (eng. *Log viewing)* je komponenta koja prikazuje dnevničke zapise u zapise pogodne za pregled čovjeku. Većina generatora pruža takve mogućnosti, a ako ne, koriste se zasebni alati.

3.2. Syslog specifikacija

Syslog je jednostavna radna okolina (eng. framework) za stvaranje, pohranu i prijenos dnevničkih zapisa koju mogu koristiti brojni programski alati i operacijski sustavi umjesto svojih nativnih formata dnevničkih zapisa.

Syslog pridružuje prioritete svakoj poruci na osnovu važnosti dva atributa:

- tip poruke poznat kao *facitlity* - primjeri ovakvih poruka su poruke jezgre operacijskog sustava, sustavne poruke elektroničke pošte, autorizacijske poruke te poruke programa za nadgledanje,
- težina - svaki zapis ima nekoliko vrijednosti od 0 (hitan slučaj) do 7 (kasnije debugiranje).

Atributi se koriste kako bi se odredio prioritet poruka te se zbog toga poruke višeg prioriteta šalju brže nego one nižeg prioriteta. Prioritet poruke ne određuje vrstu akcije koja se provodi nad porukom. *Syslog* se može konfigurirati tako da omogućuje poduzimanje različitih akcija u ovisnosti o tipu i težini poruke.

Svaka *Syslog* poruka sadrži tri dijela. Prvi dio specificira tip poruke i težinu reprezentiranu numeričkom vrijednosti. Drugi dio sadrži vremensku oznaku, ime računala ili IP adresu izvora dnevničkog zapisa. Treći dio je tijelo zapisa koje u sebi nosi sadržaj poruke. Tijelo poruke problematičan je za automatiziranu analizu iz razloga što nema standardiziran format i većina generatora koristi zaseban format.

Syslog je razvijen u doba kad sigurnost nije bila u prvom planu pri korištenju dnevničkih zapisa te stoga nisu odmah implementirane sigurnosne provjere koje čuvaju povjerljivost, integritet i dostupnost dnevničkih zapisa, a koje imamo danas. Na primjer većina *Syslog* zapisa koristi nepouzdan UDP (eng. *User Datagram Protocol*) protokol. UDP ne osigurava da zapisi stignu točnim redoslijedom ili da stignu uopće. Većina *Syslog* alata ne koristi nikakvu provjeru pristupa i na taj način izlaže sustave organizacija koje ih koriste velikom riziku.

Standard RDC 3195 donesen je kako bi ispravio sigurnosne propuste iz ranijih razdoblja i sadrži sljedeće osobine:

- RLD (eng. *reliable log delivery)* - pouzdan prijenos zapisa, koristi se TCP kao dodatak UDP protokolu. TCP je spojno orijentiran protokol i osigurava pouzdano prenošenje informacija kroz mrežu. Negativna strana RLD-a je korištenje više mrežnih resursa te povećano vrijeme stizanja dnevničkih zapisa na odredište,
- TCP (eng. *Transmission Confidentiality Protection*) - koristi se TLS (eng. *Transport Layer Security*) protokol kako bi se zaštitila povjerljivost pri prijenosu dnevničkih zapisa mrežom. TLS ne može zaštititi IP zaglavlja paketa pa je moguće otkriti izvornu i odredišnu IP adresu, pa se ponekad, u svrhu zaštite, koriste SSH (eng. *Secure Shell*) tuneli za mrežni promet,
- TIPA (eng. *Transmission Integrity Protection and Authentication)* za zaštitu integriteta i autentifikaciju, a koriste se i algoritmi za stvaranje sažetaka poruka kao što su SHA-1,
- robusno filtriranje - izvorna primjena *Sysolog* protokola nije omogućavala složenija filtriranja jer su se poruke obrađivale na temelju prioritetnih i težinskih zaglavlja. Novije primjene *syslog* protokola omogućuju filtriranje po izvoru ili po elementima tijela *syslog* poruke, a moguća je i višestruka kombinacija filtara te se dobiva filtriranje visoke konfigurabilnosti,
- analiza podataka - izvorno *syslog* poslužitelji nisu izvodili nikakvu analizu podataka jer su izvodili samo snimanje i prijenos,
- odgovor na događaje - neke primjene *syslog* protokola mogu inicijalizirati akcije kad se otkrivaju određeni događaji. Na primjer ukoliko se pošalje elektronička pošta s neke adrese koju administrator nadgleda, moguće je aktivirati skriptu koja će obavijestiti administratora,
- alternativni oblici poruke - određene *syslog* primjene mogu primati podatke u drugom formatu kao što je SNMP (eng. *Simple Network Management Protocol*),
- kriptiranje dnevničkih zapisa - *syslog* protokol može se konfigurirati tako da kriptira rotirane podatke automatski,
- ograničenje broja poruka - neke primjene mogu ograničiti broj *syslog* poruka ili TCP veza od nekog izvora kroz proizvoljan vremenski period.

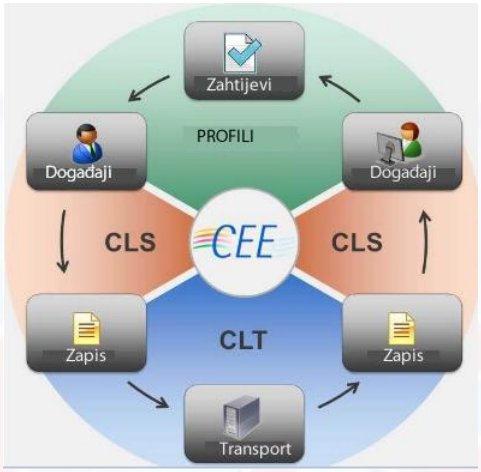
3.3. CEE specifikacija

CEE (eng. *Common Event Expression*) je otvorena, praktična i nadogradiva specifikacija zapisivanja događaja, s ciljem reprezentacije i klasifikacije unificiranih događaja. Razvijana je u tvrtci MITRE Corporation u koordinaciji s informatičkom industrijom i skupinama krajnjih korisnika, razvojnim inženjerima SIEM (eng. *Security Information and Event Management Software*) proizvoda te organizacija vlade SAD-a. Specifikacija se temelji na bilježenju događaja (eng. *event data*), a izrađena je zbog nekonzistentnosti formata dnevničkih zapisa, koje otežavaju IT analizu. CEE odgovara na nedostatke donoseći sintaksu i vokabular koji se koristi za zapisivanje,

dijeljenje spremanje i interpretaciju dnevničkih podataka. Za krajnje korisnike to smanjuje troškove i ubrzava analizu.

Proces skupljanja, diseminacije i analize dnevničkih zapisa može se opisati ciklusom u šest koraka, koji CEE naziva *životni ciklus upravljanja događajima* (Slika 5):

1. OPIS (eng. *describe*) - događaji su opisani na temelju zahtjeva industrijskih praksi i sigurnosnih politika,
2. KODIRANJE (eng. *encode*) - događaj i relevantni podaci se kodiraju u zapis,
3. SLANJE (eng. *send*) - zapisi se šalju na analizu i spremanje,
4. PRIHVAT(eng. *recieve*) - zapisi se zaprimaju na uređaje potrošača (obično poslužitelja) koji rade analizu podataka,
5. DEKODIRANJE(eng. *decode*) - zapisi se dekodiraju kako bi se dobila izvorna informacija o događaju
6. ANALIZA (eng. analysis) - događaj se analizira kako bi se ustvrdilo da li je konzistentan sa zahtjevima ili sadržava probleme koji zahtijevaju dublju analizu i istraživanje.



Slika 5. CEE životni ciklus
Izvor: MITRE

Pošto je nemoguće izraziti potpunu taksonomiju svih postojećih dnevničkih podataka, odnosno njihove elemente, CEE definira CEE profil, model za opisivanje događaja. CEE profil sastoji se od dvije osnovne komponente:

- rječnik polja - lista polja koja predstavlja podatke o događaju, odnosno skupu dnevničkih zapisa koji su iste kategorije primjerice: „ip“, „ip_adress“, „ip adress“ mogu biti polja dnevničkih zapisa, a odnose se na isti pojam različitog nazivlja,
- taksonomija događaja - provjereni vokabular događaja kako bi se omogućila klasifikacija tipova događaja iz različitih formata dnevničkih zapisa.

Struktura profila omogućuje proizvođačima programskih rješenja za upravljanje dnevničkim podacima te regulatornim tijelima opisivanje kako bi se događaji određenog tipa trebali prijavljivati. Profili su nasljedni što bi značilo da se specifični profil (npr. HIPAA praćenje za web poslužitelje) može proširiti na općenitiju namjenu (praćenje *web* poslužitelja). Ipak dva su osnovna slučaja korištenja profila:

- funkcijski profili - definiraju zajednički mehanizam prijave događaja,
- profil proizvoda - definicija mehanizma za korištenje jednog proizvoda.

Specifikacija još sadrži i sintaksu za dnevničke podatke (CLS- CEE *log syntax*). CLS definira zahtjeve za kodiranje i dekodiranje CEE događaja u zapis događaja u povezani CEE profil. CLS su dizajnirani kako bi osigurali najvišu funkcionalnost s postojećim standardima za zapisivanje dnevničkih zapisa. Kodiranje se obavlja u XML (eng. *extensible markup language*) i JSON[1] (eng. *JavaScript Object Notation*) formatu.

[1] JSON je jednostavni format za razmjenu podataka. Bazira se na podskupu naredbi programskog jezika JavaScript, no radi se o tekstualnom formatu koji je neovisan o bilo kojem programskom jeziku.

4. Alati za rukovanje dnevničkim zapisima

Security Information and Event Management Software, SIEM je skup programskih rješenja za rukovanje u stvarnom vremenu dnevničkim zapisima o sustavnim događajima i sigurnosnim informacijama. Kombinacija je dvije donedavno odvojene kategorije proizvoda, upravljanje sustavskim informacijama (eng. *system information management)* i upravljanje događajima u sigurnosti (eng. *security event manager,* SEM *). SIEM* proizvodi imaju jedan ili više dnevničkih poslužitelja koji obavljaju analizu podataka i jedan ili više poslužitelja baza podataka koji pohranjuju dnevničke podatke. Većina SIEM proizvoda podržava dva načina skupljanja dnevničkih zapisa iz generatora zapisa:

- bezagentski - SIEM poslužitelj prima podatke s individualnih generatora zapisa bez potrebe za odvojenim programskim paketom instaliranim na računalima na kojima se odvija proces stvaranja zapisa,
- agentski - SIEM poslužitelj prima podatke generirane s računala domaćina, na koje je instaliran agentski program. Agentski program osim komunikacije s poslužiteljem može obavljati filtraciju, agregaciju i normalizaciju dnevničkih zapisa. Prijenos dnevničkih zapisa prema poslužitelju obavlja se u stvarnom vremenu ili vremenu blizu stvarnog vremena (eng. *near real time*). Neki SIEM proizvodi pružaju agentsku podršku koja podržava protokole *syslog* i SNMP, dok neki pružaju podršku za promijenjene agente koji prihvaćaju proizvoljan oblik dnevničkih zapisa.

Prednost bezagentskog pristupa je izbjegavanje instalacije, konfiguracije i održavanja agentskog programa na svakom računalu domaćinu, dok su nedostaci nepostojeće mogućnosti agregacije i filtriranja na računalu domaćinu.

SIEM proizvodi obično uključuju potporu za nekoliko desetaka tipova izvora dnevničkih zapisa (kao što su operacijski sustavi, sigurnosni alati, aplikacijski poslužitelji) i uređaja za provjeru fizičkog pristupa (kao što su biometrijski i kartični identifikatori osoba). Za svaki podržani izvor dnevničkih podataka, osim generičkih (npr. *Syslog*), SIEM proizvodi organiziraju i kategoriziraju najvažnija polja u zapisima, što uvelike olakšava i ubrzava normalizaciju, analizu i korelaciju podataka.

SIEM proizvodi obično uključuju nekoliko komponenata kako bi olakšali poslove administratorima:

- grafičko sučelje - posebno dizajnirano kako bi olakšalo analizu pri identifikaciji potencijalnih problema,
- baza podataka s informacijama o svim poznatim ranjivostima, značenjima određenih poruka iz dnevničkih zapisa i drugim tehničkim podacima,
- sustav za praćenje i prijavljivanje incidenata,
- informacije o pohrani i korelaciji.

Drugi tipovi programa za upravljanje dnevničkim zapisima su:

- HIDS (eng. *Host based intrusion detection system*) - nadgleda svojstva jednog računala domaćina i otkriva sumnjive aktivnosti. Uglavnom se nadgledaju pozivi jezgre operacijskog sustava, izvještaji sigurnosnih alata te aplikacijski dnevnički zapisi. Neki HIDS proizvodi koriste dnevničke zapise kao jedan od nekoliko izvora podataka pri otkrivanju sumnjivih aktivnosti, dok su nekima jedini izvor. HIDS sadrže bazu potpisa poznatih napada te uspoređuju trenutne dnevničke podatke s njima kako bi se identificirali događaji.
- alati za vizualizaciju - vizualizacijski alati predstavljaju podatke o događajima sigurnosne vrste u grafičkom obliku, slagajući podatke na način da neke povezanosti među određenim događajima postanu očigledne te je lako otkriti sumnjive aktivnosti. Sigurnosno osoblje tada lako može prepoznati uzorke koji indiciraju napad te lakše otkriti počinitelja i načine izvođenja napada. Brojni SIEM proizvodi imaju ovu mogućnost, dok je kod drugih moguće korištenje alata treće strane (eng. *third party tools)*.
- alati za rotaciju dnevničkih podataka - ukoliko nisu ugrađeni u SIEM proizvod koji se koristi ili je iskoristivost ugrađenog rješenja slaba, administratori mogu koristiti alate treće strane kako bi poboljšali upravljanje dnevničkim zapisima.
- alati za pretvorbu dnevničkih podataka - na Internetu postoji puno ovakvih rješenja koji pretvaraju jedan format dnevničkih podataka u drugi. Ovi alati korisni su za inkorporiranje dnevničkih zapisa koji su stvoreni nepopularnim generatorima zapisa ili kad se dnevnički zapisi stvaraju iz različitih izvora.

5. Rukovanje dnevničkim zapisima

U ovom poglavlju opisane su upute za pravilno rukovanje dnevničkim zapisima, preuzete iz upute za upravljanje dnevničkim zapisima u svrhu sigurnosti i suglasnosti s propisima u Europskoj uniji. Zakoni koji se odnose na rukovanje dnevničkim zapisima su Sarbanes-Oxley, Basel II te MiFD (eng. *Markets in Financial Instruments Directive*) i njihovo nepoštivanje može imati visoke financijske kazne. Zakoni se uglavnom koriste za reguliranje zapisa financijskih transakcija no preporuke iz ovih zakona mogu se općenito primjenjivati.

1. Definiranje kategorija politike nadgledanja (eng. *Audit Policy*) - termin se koristi za referiranje na tipove sigurnosnih događaja koji se bilježe na poslužiteljima i radnim stanicama.
2. Automatsko središnje konsolidiranje zapisa - pri odabiru ELM rješenja potrebno je odabrati što automatiziranije rješenje za pohranu i kompresiju podataka kako bi se ubrzao proces centraliziranog prikupljanja dnevničkih podataka. Rješenje bi trebalo samo jednom podesiti i pustiti u pogon. Kod pristupa arhiviranim dnevničkim podacima potrebno je imati točne podatke, a automatizacijom uklanja se ljudski faktor pogreške i kompromitiranja integriteta podataka. Automatizacija se također koristi za bolje korištenje mreže pri transferu dnevničkih podataka. *Syslog* i Windows *event* zapisi (najčešće korišteni) su po osnovnim postavkama decentralizirani te je potrebna automatizacija prikupljanja i spajanja zapisa u središnju bazu podataka za potpuno nadgledanje događaja i analiziranje podataka.
3. Nadgledanje događaja salarmima u stvarnom vremenu - većina organizacija ima heterogen IT okoliš s različitim operacijskim sustavima, uređajima i sustavima. Potrebno je stoga koristiti opće prihvaćene standarde u dnevničkim zapisima kao što je *Syslog* koji podržava zapise sa usmjeritelja, prekidača, IDS sustava, vatrozida te sustava Linux i Unix. Po mogućnosti potrebno je primijeniti bezagentski sustav nadgledanja prometa, što će smanjiti poslove ukoliko će se računalna mreža organizacije proširivati.
4. Stvaranje izvještaja za sigurnosni tim organizacije – izvještaji bi trebali pokrivati široko područje sigurnosti, od ponašanja korisnika na sustavu do otkrivanja problema na mreži. Postoji nekoliko ključnih točaka koje bi trebale biti u izvještaju o dnevničkim zapisima:
    - identifikacija - trebali bi se zabilježiti u dnevničke zapise i staviti u izvještaj svi identiteti i privilegije korisnika kroz organizaciju,
    - autentikacija - trebali bi se zabilježiti u dnevničke zapise i staviti u izvještaj sve transakcije sustava koji pružaju autentifikacijske mehanizme,
    - kontrola pristupa zasnovana na politici - zabilježiti u dnevničke zapise i staviti u izvještaj popis autoriziranih poslovnih korisnika koji imaju pristup sustavima, podacima i mrežnim resursima,
    - zaštita podataka i integriteta - zabilježiti u dnevničke zapise i staviti u izvještaj pristup podacima (tko je pristupio, koliko dugo je pregledavao podatke, je li promijenio ili kopirao podatke),
    - pregled identiteta - zabilježiti u dnevničke zapise i staviti u izvještaj pristupe svih korisnika uključujući vremenska ograničenja ili ograničenja prava pristupa na temelju adrese s koje se pristupalo resursu.
5. Pregled dnevničkih podataka - jedan od najproblematičnijih dijelova upravljanja dnevničkim podacima jer je potrebno većinom ručno proći kroz dnevne količine dnevničkih zapisa te otkriti relevantne informacije iz već arhiviranih podataka. Pri korištenju automatiziranog alata potrebno je naći programsko rješenje koje omogućuje predefinirane i konfigurabilne načine pretraživanja i filtriranja. Sposobnost da se definira prilagodljiva pretraga i filtriranje su od ključne važnosti. Dnevnički podaci bi se trebali automatski grupirati u korelirane odsječke s identifikacijskim kodovima pretvorenim u ljudski čitljive podatke.

Pri odabiru programskog rješenja za rukovanje dnevničkim podacima potrebno je uzeti u obzir faktore koji uključuju skalabilnost, multiplatformsku podršku, modularnost, visoku iskoristivost, tehničku podršku, malu cijenu održavanja te dobru korisničku dokumentaciju.

6. Zaključak

Broj događaja koji se svakodnevno bilježi na sustavima tvrtki, bilo da su izvori mrežni resursi, poslužitelji ili mobilni uređaji zaposlenika, predstavljaju administratorima velik izazov. Problemi se javljaju prvo sa skladištenjem velike količine podataka, reda veličine nekoliko GB. Također tu je problem i sigurnosti pohrane dnevničkih zapisa koji, ukoliko se neovlašteno zlonamjerno izmijene mogu administratore uvjeriti u lažnu neispravnost sustava ili prikriti tragove provale u sustav. Potrebni su veliki resursi za pohranu, transport i zaštitu dnevničkih zapisa, a još veći za njihovu analizu i istraživanje. Pronalaženje dobrog, automatiziranog alata za analizu je od ključne važnosti za administratore sustava zbog smanjenja opsega posla i uklanjanja mogućnosti eventualnih pogrešaka u analizi. Također se nameće pitanje koliko dugo zadržavati dnevničke zapise na sustavu te kako ih frekventno rotirati i arhivirati. Danas postoji sve više standarda koji propisuju kako upravljati dnevničkim zapisima, dok je u Europskoj uniji i Sjedinjenim Američkim Državama to zakonski regulirano za velike tvrtke (>75 milijuna dolara profita) i državne službe. Zakoni koji propisuju upravljanje dnevničkim zapisima u EU su Sarbanes-Oxley, Basel II te MiFD, a u SAD-u FISMA, HIPPA te PCI-DSS dok u Hrvatskoj za to još nema zakonske regulative.

7. Reference

[1] Log management Basics, http://www.csoonline.com/article/626296/log-management-basics, listopad, 2010.

[2] Log, management in the age og Compliance, http://www.computerworld.com/s/article/9027080/Log_management_in_the_age_of_compliance, srpanj, 2007.

[3] Using computer log data to support a forensic investigation, http://www.networkworld.com/newsletters/2009/051809bestpractices.html, svibanj, 2009.

[4] Log Management – Lifeblood of Information Security, http://www.net-security.org/article.php?id=975, veljača, 2007.

[5] Guide to Computer Security Log Management, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf, rujan, 2009.

8. Leksikon pojmova

NIST

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

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

Ostale poveznice: http://www.nist.gov/index.html

RSA - Rivest, Shamir, Adelman algoritam

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

Ostale poveznice: http://library.thinkquest.org/27158/concept2_4.html

http://searchsecurity.techtarget.com/definition/RSA

DES - DES algoritam šifriranja

Vrlo popularan kriptografski standard, danas zamijenjen standardom AES. Tajni ključ za šifriranje podataka sastoji se od 56 bita, što znači 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 znači da obadvije strane moraju imati tajni ključ kako bi mogli komunicirati.

Reference: http://nvl.nist.gov/pub/nistpubs/sp958-lide/250-253.pdf

Ostale poveznice: http://en.wikipedia.org/wiki/Data_Encryption_Standard

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

Ostale poveznice: http://www.webopedia.com/TERM/D/DoS_attack.html

http://en.wikipedia.org/wiki/Denial-of-service_attack

Priključnica

Krajnje točke u komunikaciji transportnih protokola - brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju.

Reference: http://searchnetworking.techtarget.com/definition/port-number

Ostale poveznice: http://www.iana.org/assignments/port-numbers

TCP - Transmission Control Protocol

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

Ostale poveznice: http://www.networksorcery.com/enp/protocol/tcp.htm

http://searchnetworking.techtarget.com/definition/TCP

RIB - Routing Information Base

RIB je baza koju svaki BGP usmjeritelj održava, a koja sadrži informacije u putovima. Na temelju podataka u toj bazi, usmjeritelj određuje kojim putem će slati pakete.

Reference: http://www.inetdaemon.com/tutorials/internet/ip/routing/routing_information_base.shtml

Ostale poveznice: http://www.birds-eye.net/definition/acronym/?id=1165714009

http://www.networkers-online.com/blog/2010/03/bgp-routing-information-base-rib/

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

Ostale poveznice: http://searchnetworking.techtarget.com/definition/router

IP - IP protokol - Internet Protocol

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

Ostale poveznice: http://en.wikipedia.org/wiki/Internet_Protocol http://www.ietf.org/rfc/rfc791.txt

JavaScript - Programski jezik JavaScript

JavaScript je skriptni programski jezik, koji se izvodi u web pregledniku na strani korisnika. Napravljen je da bude sličan Javi, zbog lakšega korištenja, ali nije objektno orijentiran kao Java, već se temelji na prototipu i tu prestaje svaka povezanost s programskim jezikom Java. Izvorno ga je razvila tvrtka Netscape (www.netscape.com). JavaScript je izrađen primjenom ECMAScript standarda.

Reference: http://javascript.about.com/od/reference/p/javascript.htm

Ostale poveznice: http://www.w3schools.com/js/default.asp

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

Ostale poveznice: http://www.dce.fe.untz.ba/MAC%20LAYER.pdf

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

Ostale poveznice: http://en.wikipedia.org/wiki/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

Ostale poveznice: http://labs.apache.org/webarch/uri/rfc/rfc3986.html

IV - Inicijalizacijski vektor

Broj koji se koristi zajedno sa tajnim ključem prilikom šifriranja podataka. Stalno se mijenja kako bi osigurao nasumičnost što je vrlo važno svojstvo u svim kriptografskim algoritmima. Reference: http://whatis.techtarget.com/definition/initialization-vector.html

Ostale poveznice:

http://www.pcmag.com/encyclopedia_term/0,2542,t=initialization+vector&i=44997,00.asp

http://www.javvin.com/networksecurity/IV.html

TLS - Transport Layer Security

TLS je kriptografski protokol koji pruža sigurnu komunikaciju Internetom. TLS šifrira dijelove iznad transportnog sloja koristeći simetrične kriptografske ključeve i autentikacijski kod poruka. TLS je nasljednik SSL protokola.

Reference: http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS

Ostale poveznice: http://www.techsoup.org/learningcenter/networks/page11959.cfm

http://datatracker.ietf.org/wg/tls/charter/

Virus - Računalni virus

Virusi su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

Reference: http://www.ust.hk/itsc/antivirus/general/whatis.html

Ostale poveznice: http://os2.zemris.fer.hr/ns/2008_Mackovic/virusi.htm

Sigurnosna stijena - Firewall

Sigurnosna stijena (engl. Firewall) je skup komunikacijskih nakupina koji služe kako bi odvojili privatnu mrežu od javne. Sastoje se od programa koji služe kako bi pratili i upravljali promet između računala i mreža. Sigurnosne stijene mogu propuštati, blokirati, šifrirati promet na temelju pravila koja korisnik postavlja.

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

Ostale poveznice: http://kb.iu.edu/data/aoru.html

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

Ostale poveznice: http://www.w3schools.com/xml/default.asp

http://www.w3.org/XML/

Napad rječnikom - Metoda pogađanja lozinke

U kriptografiji napad rječnikom predstavlja metodu pogađanja lozinke (ili tajnog ključa) isprobavanjem svih mogućih riječi iz određenog popisa koji se zove rječnik. Za razliku od napada grubom silom gdje se isprobavaju sve moguće kombinacije znakova, kod napada rječnikom isprobavaju se samo one kombinacije koje su statistički vjerojatnije.

Reference: http://www.webopedia.com/TERM/D/dictionary_attack.html

Ostale poveznice: http://www.tech-faq.com/dictionary-attack.html

http://www.pinkas.net/PAPERS/pwdweb.pdf

Brute-force napad - 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

Ostale poveznice: http://www.imperva.com/resources/glossary/brute_force.html

https://www.owasp.org/index.php/Brute_force_attack

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

Ostale poveznice: http://communication.howstuffworks.com/how-to-leverage-an-api-for-conferencing1.htm

OSI model - Open Systems Interconnection model

OSI model se koristi za standardizaciju mrežnih protokola. Definira sedam logičkih razina ili slojeva: aplikacijski, prezentacijski, sjednički, transportni, mrežni, sloj podatkovne poveznice i fizički sloj. Kontrola se prenosi iz jednog sloja u drugi, počevši od aplikacijskog sloja.

Reference: http://www.webopedia.com/quick_ref/OSI_Layers.asp

Ostale poveznice: http://www.roseindia.net/technology/networking/osi.shtml