Lekcija\_3\_1\_1

1

00:00:02,933 --> 00:00:08,133

Dobrodošli. U ovom videu naučit ćemo koje vrste

računalnih mreža postoje.

2

00:00:08,133 --> 00:00:19,766

U prethodnim poglavljima smo naučili da svaka

informacija ima vrijednost pa analogno tomu

možemo zaključiti da onaj tko ima pristup

3

00:00:19,766 --> 00:00:29,599

informacijama ima i moć. Danas pristup

informacijama smatramo jednim od osnovnih

prava čovjeka, a upravo je računalo ono koje nam

4

00:00:29,600 --> 00:00:40,633

to omogućava. Osim pristupa informacijama,

pobrojat ćemo i ostale prednosti umrežavanja

računala i korištenja računalnih mreža. To su:

5

00:00:40,633 --> 00:00:53,833

Razmjena podataka; Dijeljenje podataka;

Dijeljenje resursa, gdje nam umrežavanje računala

omogućuje korištenje printera koji nisu direktno

6

00:00:53,833 --> 00:01:02,133

spojeni na naše računalo; Racionalizaciju troškova

te; Pristup Internetu odnosno elektroničkoj pošti.

7

00:01:02,133 --> 00:01:14,699

Računalna mreža nastaje povezivanjem dvaju i

više mrežnih uređaja (računala, mrežnog pisač i

sl.) pa možemo reći da je to skupina međusobno

8

00:01:14,700 --> 00:01:24,733

povezanih uređaja s ciljem omogućivanja

međusobne komunikacije odnosno dijeljenja

podataka i uređaja kojima se može pristupiti

9

00:01:24,733 --> 00:01:34,199

preko mreže. Jednako tako, danas se računalnom

mrežom koristi za stvaranje distribuirane obrade

podataka. Razvojem i širokom primjenom osobnih

10

00:01:34,200 --> 00:01:44,366

računala pojavila se mogućnost kreiranja velike

količine programa i multimedijalnog sadržaja koje

je potrebno dijeliti s drugim korisnicima na mreži.

11

00:01:44,366 --> 00:01:54,599

Prije izgradnje računalnih mreža sadržaj se

razmjenjivao uz pomoć prijenosnih medija

(magnetske vrpce, diskete, CD ROM i sl.) No s

12

00:01:54,600 --> 00:02:05,700

obzirom na ograničenja medija povezana s

veličinom prostora za pohranu podataka, uskoro je

takav način postao nedostatan.

13

00:02:05,700 --> 00:02:12,966

Umrežena računala mogu pristupati podacima na

drugim računalima, koristiti se perifernim

uređajima, koristiti

14

00:02:12,966 --> 00:02:19,666

se programima na drugim računalima te pristupati

bazama podataka na drugim računalima.

15

00:02:19,666 --> 00:02:30,799

Upravo zbog navedenog, kada se na mreži nalazi

puno drugih računala, a dijeljenje resursa

(dokumenti, slike, muzika, filmovi i sl.) nikada nije

16

00:02:30,800 --> 00:02:42,400

bilo lakše, prilikom svakog povezivanja na mrežu,

a pogotovo na javne mreže (Internet kafići,

aerodromi i sl.) postoji mogućnost da naše

17

00:02:42,400 --> 00:02:53,000

računalo bude inficirano malicioznim softverom. Korisnici koji su izolirani i rabe svoja računala bez

povezanosti s drugima nemaju mogućnost, prije

18

00:02:53,000 --> 00:03:01,533

svega, dijeliti zajedničke hardverske resurse.

Primjenom mrežne tehnologije korisnici imaju

potrebnu radnu infrastrukturu, ali bez

19

00:03:01,533 --> 00:03:11,899

nepotrebnoga dodatnog investiranja kompanije u

opremu za svakoga pojedinog korisnika (npr.

svako računalo ne mora imati svoj pisač, nego

20

00:03:11,900 --> 00:03:17,500

može dijeliti jedan zajednički tzv. mrežni).

21

00:03:17,500 --> 00:03:29,466

Mreže je moguće podijeliti na nekoliko načina, a

nama je zanimljiva podjela prema njihovoj veličini.

Računalne mreže možemo podijeliti prema veličini

22

00:03:29,466 --> 00:03:44,932

odnosno fizičkoj rasprostranjenosti korisnika i

uređaja u dvije osnovne grupe: LAN, lokalne

mreže odnosno Local Area Network i WAN (Wide

23

00:03:44,933 --> 00:03:50,099

Area Network) odnosno Internet. LAN odnosno Local Area Network.

24

00:03:50,100 --> 00:03:59,133

Lokalna mreža jest mreža uređaja pod kontrolom

zajedničke administracije koja uređuju politiku

sigurnosti i pristupa.

25

00:03:59,133 --> 00:04:08,533

Lokalnu mrežu čine uređaji povezani na maloj

fizičkoj udaljenosti i obično obuhvaća jedno

zemljopisno područje.

26

00:04:08,533 --> 00:04:16,866

Pruža servise za korisnike u zajedničkoj

organizacijskoj strukturi kao što su tvrtka, kampus

ili regija.

27

00:04:16,866 --> 00:04:26,232

Lokalna mreža može biti reda veličine od dva do

više stotina međusobno povezanih uređaja koji se

nalaze na manjoj ili većoj udaljenosti jedno od

28

00:04:26,233 --> 00:04:27,599

drugog.

29

00:04:27,600 --> 00:04:35,800

Primjer lokalne mreže je i naša kućna mreža gdje

imamo spojeno nekoliko računala s našim ADSL

usmjernikom.

30

00:04:35,800 --> 00:04:48,266

Wide Area Netwwork (WAN) je mreža širokog

područja i to je mreža koja spaja lokalne mreže

koje su fizički na različitim geografskim

31

00:04:48,266 --> 00:04:55,966

područjima. U pitanju je mreža uređaja povezanih

brzim i sporim vezama.

32

00:04:55,966 --> 00:05:05,799

Sljedeće dvije podskupine mreža, koje na neki

način možemo smatrati hibridnima, i koje je

zapravo teško pravilno svrstati u neku od

33

00:05:05,800 --> 00:05:17,700

kategorija, jesu: Intranet, međusobno primjenjuje

iste tehnologije kao i Internet, ali pristup imaju

samo zaposlenici tvrtke. On po svojoj veličini

34

00:05:17,700 --> 00:05:25,100

spada u LAN mreže, no rabi vrlo sličnu

infrastrukturu kao Internet.

35

00:05:25,100 --> 00:05:34,700

Zatim imamo Ekstranet (Extranet) – tip mreže koji

biranim vanjskim korisnicima (partnerima,

klijentima itd.) daje pristup ograničenim

36

00:05:34,700 --> 00:05:47,900

informacijama tvrtke, npr. sustavu za centralno

naručivanje i sl. Ova vrsta mreže također po svojoj

veličini spada u LAN mreže, no s obzirom na to da

37

00:05:47,900 --> 00:05:55,000

obično rabi resurse Interneta, također je na granici

LAN-a i Interneta.

38

00:05:55,000 --> 00:06:10,333

Uz lokalnu mrežu (LAN), mrežu širokog područja

(WAN), razaznajemo i treću vrstu mreža: VPN.Virtualna privatna mreža – VPN (Virtual Private

39

00:06:10,333 --> 00:06:22,166

Network) jest tehnologija koja omogućuje sigurno

povezivanje privatnih mreža u zajedničku virtualnu

privatnu mrežu preko javne mrežne infrastrukture,

40

00:06:22,166 --> 00:06:33,432

što je danas najčešće Internet. Ostvaruje se

siguran „tunel“ između dvije krajnje točke. Kod

tuneliranja se provode kompresija i šifriranje

41

00:06:33,433 --> 00:06:36,933

podataka.

42

00:06:36,933 --> 00:06:44,399

Lekcija je završena.

Lekcija\_3\_1\_2

1

00:00:00,000 --> 00:00:09,833

Dobrodošli. U sljedećem videu ćemo naučiti zašto je bežične mreže potrebno štititi lozinkom.

2

00:00:09,833 --> 00:00:20,466

Bežične računalne mreže pojavile su se devedesetih godina prošlog stoljeća kada su proizvođači počeli nuditi proizvode koji su radili na

3

00:00:20,466 --> 00:00:29,966

frekvenciji od 900 MHz. Brojne prednosti ovih proizvoda postale su odmah vidljive: mobilnost korisnika i zaposlenika koji su u stanju obavljati

4

00:00:29,966 --> 00:00:39,199

svoje aktivnosti s bilo kojeg mjesta; smanjenje troškova jer više nije potrebno ulagati u fizičku povezanost radnih mjesta zaposlenika s internom

5

00:00:39,200 --> 00:00:45,500

računalnom mrežom korporacije te fleksibilnost i jednostavnost.

6

00:00:45,500 --> 00:00:58,233

Općenito, mrežne sastavnice bežičnih računalnih mreža jesu: radna stanica odnosno uređaj na bežičnoj računalnoj mreži. Tipični primjeri takvog

7

00:00:58,233 --> 00:01:06,699

uređaja jesu prijenosna računala odnosno drugi mobilni uređaji npr. poput poput mobilnih telefona.

8

00:01:06,700 --> 00:01:15,200

Zatim imamo pristupni uređaj (Access Point), on logički povezuje jednu ili više radnih stanica.

9

00:01:15,200 --> 00:01:28,000

Navedene mrežne sastavnice mogu biti spojene s pomoću dvije osnovne mrežne topologije pa tako postoje ad hoc i infrastrukturna topologija.

10

00:01:28,000 --> 00:01:39,100

Ad hoc topologija – u ovom je slučaju bežična mreža koja se uspostavlja isključivo između različitih radnih stanica (prijenosno računalo,

11

00:01:39,100 --> 00:01:51,766

mobitel ili drugo prijenosno računalo), bez upotrebe pristupnih uređaja. Ovaj način rada se još često naziva i engl. peer-to-peer i omogućuje

12

00:01:51,766 --> 00:01:55,899

izravnu komunikaciju između dva bežična uređaja.

13

00:01:55,900 --> 00:02:06,666

Slijedeća je Infrastrukturna topologija – u slučaju infrastrukturne arhitekture bežične mreže, ona se sastoji od jednog ili više pristupnih uređaja (

14

00:02:06,666 --> 00:02:14,499

Access point) te jedne ili više radnih stanica.

15

00:02:14,500 --> 00:02:23,600

Uz klasične zahtjeve za sigurnost koji se postavljaju i pred žične, fizičke računalne mreže, zbog prirode djelovanja bežične su računalne

16

00:02:23,600 --> 00:02:30,633

mreže podložne čitavom nizu prijetnji koje se ne mogu ostvariti nad fizičkim računalnim mrežama.

17

00:02:30,633 --> 00:02:40,066

U nastavku ovog modula dani su primjeri prijetnji za bežične računalne mreže te zahtjevi za sigurnost koji se postavljaju pred njih.

18

00:02:40,066 --> 00:02:50,932

Klasični zahtjevi za sigurnost koji se postavljaju pred bežične mreže, a zahtijevaju određene radnje od administratora sustava, uključuju: povjerljivost

19

00:02:50,933 --> 00:02:56,766

(Confidentiality), koja osigurava da mrežnu komunikaciju ne mogu nadgledati neautorizirani korisnici;

20

00:02:56,766 --> 00:03:04,566

integritet (Integrity), čiji je cilj otkriti bilo kakve namjerne ili nenamjerne promjene podataka koji se prenose.

21

00:03:04,566 --> 00:03:16,332

Integritet je posebno bitan kod bežičnih računalnih mreža jer tehnologija prijenosa podataka sama po sebi može unijeti smetnje u prenošene podatke

22

00:03:16,333 --> 00:03:26,933

što narušava njihov integritet i na kraju, dostupnost (Availability), čime se postiže da svi uređaji i korisnici koji pristupaju bežičnoj računalnoj mreži

23

00:03:26,933 --> 00:03:31,933

mogu to ostvariti kada god im je potrebno.

24

00:03:31,933 --> 00:03:42,499

Uz ove zahtjeve postoji cijeli niz prijetnji za bežične računalne mreže od kojih su neke prijetnje svojstvene i prisutne bez obzira na prijenosni

25

00:03:42,500 --> 00:03:50,066

medij (bežično, žičano), a druge su specifične zbog bežičnog rada ovakvih mreža.

26

00:03:50,066 --> 00:04:00,999

Tako imamo: Napadi uskraćivanja resursa (Denial of Service) – napadač onemogućuje ili ograničava pristup bežičnoj mreži.

27

00:04:01,000 --> 00:04:09,800

Zatim imamo prisluškivanje mrežnog prometa (Eavesdropping) – zbog prirode medija koji se rabi za prijenos podataka napadač može pasivno

28

00:04:09,800 --> 00:04:21,000

nadgledati sav mrežni promet razmijenjen između pristupnog uređaja i radne stanice i time „vidjeti“ svu našu aktivnost na mreži.

29

00:04:21,000 --> 00:04:33,033

Zatim imamo tzv. Man-in-the-Middle napade gdje se napadači aktivno predstavljaju kao jedan ili više uređaja prisutnih na bežičnoj računalnoj mreži.

30

00:04:33,033 --> 00:04:43,733

Klasičan slučaj napada jest lažiranje pristupne točke, kada se napadač svim korisnicima bežične računalne mreže predstavlja kao njihova pristupna

31

00:04:43,733 --> 00:04:54,433

točka. Na ovaj način napadač postiže da sav mrežni promet prolazi kroz njega te ga može pregledavati i po želji modificirati.

32

00:04:54,433 --> 00:05:02,666

Zatim kao slijedeću prijetnju imamo prikrivanje (Masquerading) – slučaj u kojemu se napadač predstavlja kao autorizirani korisnik bežične

33

00:05:02,666 --> 00:05:09,532

računalne mreže ne bi li ostvario pristup podacima ili servisima na mreži.

34

00:05:09,533 --> 00:05:18,366

Zatim, promjena podataka, gdje napadač mijenja legitimnu poruku (mrežni paket) u smislu brisanja, dodavanja, mijenjanja ili promjene redoslijeda

35

00:05:18,366 --> 00:05:21,366

podataka u poruci.

36

00:05:21,366 --> 00:05:30,332

I za kraj, kao prijetnju, imamo analizu mrežnog prometa (Traffic Analysis) – zbog prirode medija koji se rabi kod bežičnih računalnih mreža, bilo

37

00:05:30,333 --> 00:05:40,699

koji napadač koji je u dometu jednog od dvaju uređaja koji komuniciraju preko bežične računalne mreže, može pasivno prikupljati mrežni promet te

38

00:05:40,700 --> 00:05:44,000

provoditi njegovu analizu.

39

00:05:44,000 --> 00:05:55,033

Kao što se može vidjeti iz rečenog, većina prijetnji dolazi zbog toga što napadač ima pristup mediju kojem se prenose podaci.

40

00:05:55,033 --> 00:06:06,033

Ovo je i ključna razlika između zaštite bežičnih i fizičkih, žičnih računalnih mreža, a to je mogućnost korisnika u presretanju, nadgledanju i slanju

41

00:06:06,033 --> 00:06:12,633

mrežnog prometa u bežičnu računalnu mrežu bez ikakvih ograničenja.

42

00:06:12,633 --> 00:06:21,866

Da bi neovlašteni napadač ostvario pristup žičnoj, fizičkoj računalnoj mreži, obično mora ostvariti fizički pristup prostorijama kompanije.

43

00:06:21,866 --> 00:06:29,466

S bežičnim računalnim mrežama stvar je drukčija jer se napadač mora nalaziti samo u dometu bežične mreže.

44

00:06:29,466 --> 00:06:40,299

Upravo, zbog svega navedenog, kako bi se bežične mreže osigurale od neovlaštenog pristupa, uvode se autentikacija i kontrola

45

00:06:40,300 --> 00:06:41,866

pristupa.

46

00:06:41,866 --> 00:06:52,532

Dakle, bitno je napomenuti da su ovo sve više nego dobri razlozi zbog kojih pristup bežičnim mrežama moramo štititi lozinkom, kako bi smo

47

00:06:52,533 --> 00:07:00,433

prije svega spriječili nedozvoljeni odnosno neautorizirani pristup našim podacima.

48

00:07:00,433 --> 00:07:08,266

Lekcija je završena.

Lekcija\_3\_1\_3

1

00:00:00,000 --> 00:00:09,100

Dobrodošli. U ovom videu ćemo vidjeti kojenačine autentikacije možemo korisiti kod spajanjana bežične mreže.

2

00:00:09,100 --> 00:00:19,766

Postoje dva načina identifikacije bežičnih uređajakoji se žele spojiti na bežičnu računalnu mrežu:otvorena autentikacija i autentikacija dijeljenim

3

00:00:19,766 --> 00:00:21,266

ključem.

4

00:00:21,266 --> 00:00:28,099

Ovdje je potrebno odmah napomenuti dase ni jedan od navedenih načina autentikacijedanas ne smatra dovoljno sigurnim.

5

00:00:28,100 --> 00:00:38,233

Otvorena autentikacija jest praktički autentikacijabez ikakvog autentikacijskog mehanizma i smatrase dopuštenim pristupom za sve radne stanice.

6

00:00:38,233 --> 00:00:47,133

Pri ovakvoj se autentikaciji ne provodi pravaidentifikacija radne stanice, nego se prikupljajusamo sljedeće informacije, koje napadači vrlo

7

00:00:47,133 --> 00:00:50,666

jednostavno mogu krivotvoriti.

8

00:00:50,666 --> 00:01:03,599

Prva od njih je Service Set Identifier (SSID). Gdje je SSID ime dodijeljeno bežičnoj računalnoj mreži, odnosno pristupnoj točki.

9

00:01:03,600 --> 00:01:15,266

SSID, radnoj stanici omogućuje definiranje bežične računalne mreže kojoj želi pristupiti. Odašilje se u čistom tekstualnom obliku što znači

10

00:01:15,266 --> 00:01:25,966

da bilo koji pasivni napadač koji je u dometu bežične računalne mreže može vidjeti SSID. Kao što se može vidjeti, SSID ne označuje sigurnosnu

11

00:01:25,966 --> 00:01:34,966

kontrolu te kao takav nije niti bio dizajniran, već je osnovna funkcija SSID-a definicija bežične mreže.

12

00:01:34,966 --> 00:01:47,199

Sljedeća informacija koju imamo je Media Access Control (MAC) adresa radne stanice. MAC adresa uređaja treba označivati jedinstvenu 48-bitnu

13

00:01:47,200 --> 00:01:57,400

vrijednost koju svakom uređaju dodjeljuje proizvođač. Gotovo svi proizvođači pristupnih točaka administratorima omogućuju definiranje

14

00:01:57,400 --> 00:02:04,533

pristupnih listi preko kojih se pristup bežičnoj računalnoj mreži dopušta samo određenim MAC adresama.

15

00:02:04,533 --> 00:02:12,233

No promjena MAC adresa radnih stanica jednostavna je i dostupna su programska rješenja koja omogućuju jednostavnu promjenu MAC

16

00:02:12,233 --> 00:02:21,499

adrese. Zbog navedenog se nedostatka filtriranje prema MAC adresama smatra nedovoljno dobrim.

17

00:02:21,500 --> 00:02:30,133

Izvorna ideja autentikacije dijeljenim ključem bila je omogućiti sigurniji način autentikacije radnih stanica. Zbog nedostataka u implementaciji ovog

18

00:02:30,133 --> 00:02:41,133

načina autentikacije te sigurnosnih problema bežične tehnologije (prijenos podataka radijskim frekvencijama koje svaki pasivni napadač može

19

00:02:41,133 --> 00:02:47,199

vidjeti) ovaj se način autentikacije ne smatra nimalo sigurnijim od otvorene autentikacije.

20

00:02:47,200 --> 00:02:53,866

Detalji autentikacije dijeljenim ključem navedeni su u nastavku poglavlja.

21

00:02:53,866 --> 00:03:04,366

Autentikacija dijeljenim ključem utemeljena je na tajnom kriptografskom ključu koji se još naziva i Wired Equivalent Privacy (WEP) ključem.

22

00:03:04,366 --> 00:03:13,532

Jedan je od načina postizanja veće sigurnosti bežičnih mreža. Provođenje napada na ovakav način autentikacije izrazito je jednostavno.

23

00:03:13,533 --> 00:03:23,999

Naime, pasivni napadač može samo prikupljati sav mrežni promet koji vidi te može, ako prikupi sve podatke vezane za autentikaciju, jednostavno

24

00:03:24,000 --> 00:03:26,966

doći do tajnoga, dijeljenog ključa.

25

00:03:26,966 --> 00:03:38,932

WiFi Protected Access (WPA) stvoren je kako bise poboljšala sigurnost WEP-a. WPA, kao i WEP,šifrira informacije, ali i provjerava nije li mrežni

26

00:03:38,933 --> 00:03:51,866

sigurnosni ključ izmijenjen. Dvije su vrste WPAprovjere autentičnosti: WPA i WPA2. WPA2 jesigurniji od WPA-a, ali ne funkcionira sa svim

27

00:03:51,866 --> 00:03:54,832

starijim mrežnim uređajima.

28

00:03:54,833 --> 00:04:31,666

Lekcija je završena.

Lekcija\_3\_1\_4

1

00:00:00,000 --> 00:00:08,100

Dobrodošli. U ovom videu ćemo saznati kako se

možemo povezati na mrežu.

2

00:00:08,100 --> 00:00:18,000

Ako posjedujemo prijenosno računalo ili računalo

s ugrađenom karticom za bežično povezivanje,

treba kliknuti na odjeljak Povezivanje u dijelu

3

00:00:18,000 --> 00:00:36,600

područja obavijesti pri čemu je na popisu

dostupnih mreža potrebno odabrati onu na koju se

želimo spojiti, a zatim kliknuti na „Poveži“. Kao što

4

00:00:36,600 --> 00:00:45,333

smo vidjeli u prethodnom poglavlju, za neke je

mreže obvezan mrežni sigurnosni ključ ili pristupni

izraz.

5

00:00:45,333 --> 00:00:54,199

Kod povezivanja moramo znati spajamo li se na

mrežu koja ima aktiviranu zaštitu. Ako smo se

spojili na mrežu bez zaštite, također moramo imati

6

00:00:54,200 --> 00:01:03,533

na umu ono što smo do sada naučili, a to je da

naš promet na takvoj mreži može biti praćen

uključujući i web-mjesta koja smo posjetili,

7

00:01:03,533 --> 00:01:09,399

dokumente koje uređujemo te lozinke kojima se

koristimo.

8

00:01:09,400 --> 00:01:18,900

Kada se prvi put povežete s mrežom, morate

odabrati mrežno mjesto. Tako se automatski

postavljaju odgovarajuće postavke vatrozida i

9

00:01:18,900 --> 00:01:28,633

sigurnosne postavke za vrstu mreže s kojom se

povezujete. Ako se povezujete s mrežama na

različitim mjestima (primjerice, s mrežom kod

10

00:01:28,633 --> 00:01:38,666

kuće, u obližnjem kafiću ili na radnome mjestu),

zahvaljujući odabiru mrežnog mjesta računalo će

uvijek biti prikladno zaštićeno. Postoje četiri

11

00:01:38,666 --> 00:01:53,432

mrežna mjesta. Odaberite odjeljak Kućna mreža

za kućne mreže ili kada poznajete osobe i uređaje

povezane s mrežom i smatrate ih pouzdanima.

12

00:01:53,433 --> 00:02:03,733

Mreža na radnome mjestu označuje radnu mrežu ili

druge mreže na radnome mjestu. Značajka

Otkrivanje mreže, koja vam omogućuje da vidite

13

00:02:03,733 --> 00:02:12,333

druga računala i uređaje na mreži i omogućuje

drugim korisnicima na mreži da vide vaše

računalo, uključena je prema zadanim

14

00:02:12,333 --> 00:02:16,899

postavkama.

15

00:02:16,900 --> 00:02:26,233

Javna mreža definira postavke vatrozida i

dijeljenja datoteka te općenito pristupa računalu za

mreže na javnim mjestima (kao što su kafić ili

16

00:02:26,233 --> 00:02:36,299

zračne luke). Namjena je tog mjesta spriječiti da

vaše računalo bude vidljivo ostalim računalima

oko vas te zaštititi računalo od zlonamjernih

17

00:02:36,300 --> 00:02:41,200

programa s Interneta.

18

00:02:41,200 --> 00:02:51,400

Odabirom značajke Kućna mreža ili Mreža na

radnome mjestu mijenja se konfiguracija vatrozida

da bi se omogućila komunikacija. To može biti

19

00:02:51,400 --> 00:03:10,466

sigurnosni rizik.U bežičnim je mrežama bežična veza šifrirana tehnologijom Wi-Fi zaštićenog bežičnog pristupa (Wi-Fi Protected Access, WPA

20

00:03:10,466 --> 00:03:15,399

ili WPA2). Prednost ima WPA2 jer je sigurniji od WPA.

21

00:03:15,400 --> 00:03:25,133

Uz opisano spajanje na bežičnu mrežu, koju

možemo smatrati dijelom lokalne mreže (LAN),

spajanje na lokalnu mrežu moguće je i žičanim

22

00:03:25,133 --> 00:03:33,166

putem, rabeći tzv. UTP kabel koji na sebi ima tzv.

RJ-45 konektore.

23

00:03:33,166 --> 00:03:46,932

Na našem prijenosnom računalu odnosno stolnom

računalu potrebno je potražiti mrežni priključak koji

se obično nalazi na stražnjoj strani ili postrance.

24

00:03:46,933 --> 00:03:57,033

Ovakav način spajanja smatramo pouzdanijim jer

ne postoji opasnost da će neautorizirani korisnici

odnosno napadači presretati promet.

25

00:03:57,033 --> 00:04:04,499

Lekcija je završena.

Lekcija\_3\_1\_5

1

00:00:00,000 --> 00:00:14,700

Dobrodošli. U ovoj lekciji naučit ćemo o sigurnosnim politikama, zakonskoj regulativi te dodatnoj zaštiti podataka.

2

00:00:14,700 --> 00:00:20,433

Ranije smo spomenuli da informacija nastaje tumačenjem podataka te stavljanjem u kontekst značenja. Dakle, protumačeni podatak daje nam

3

00:00:20,433 --> 00:00:31,099

informaciju. Podatke je povremeno potrebno transformirati odnosno na neki način obraditi te protumačiti kako bismo dobili informaciju. Kao i

4

00:00:31,100 --> 00:00:39,800

kod bilo koje robe, a danas slobodno možemo tvrditi da je informacija „roba na tržištu“, pogotovo kada govorimo o poslovnim okruženjima,

5

00:00:39,800 --> 00:00:48,700

informacija ima svoju kvalitetu i, u konačnici, cijenu. S druge strane, s obzirom na to da je informacija rezultat neke „obrade podataka“, vrlo

6

00:00:48,700 --> 00:00:57,200

nam je važna i kvaliteta podataka. Kvaliteta podataka usmjerena je prije svega na točnost, ispravnost i urednost podataka.

7

00:00:57,200 --> 00:01:04,800

Danas se u modernom poslovanju bilo koje kompanije podaci pohranjuju u baze podataka kojima upravljaju sustavi za upravljanje bazama

8

00:01:04,800 --> 00:01:06,700

podataka (database management system, DBMS).

9

00:01:06,700 --> 00:01:14,800

Zbog svoje se važnosti u poslovanju podaci i informacije smatraju vrlo važnim resursom, odnosno „imovinom“ prijeko potrebnom u

10

00:01:14,800 --> 00:01:21,266

današnjem poslovanju. Negdje ćemo čuti da se govori i o informacijskoj imovini (information asset).

11

00:01:21,266 --> 00:01:30,032

Potrebno je spomenuti i kvalitetu informacije pa ćemo, ne ulazeći u dublju raspravu, samo reći i da je kvalitetna informacija točna, potpuna,

12

00:01:30,033 --> 00:01:35,399

primjerena odnosno relevantna i pravodobna, te samim time i vrijedna.

13

00:01:35,400 --> 00:01:38,700

Kvalitetna informacija ima sljedeća obilježja:

14

00:01:38,700 --> 00:01:43,400

Točnost – informacija je točna ako korektno opisuje stvarno stanje.

15

00:01:43,400 --> 00:01:50,933

Potpunost – informacija je potpuna ako potpuno opisuje stvarno stanje i ako se opisu nema što dodati.

16

00:01:50,933 --> 00:01:54,866

Potpuna informacija jest i objektivna informacija.

17

00:01:54,866 --> 00:02:00,866

Primjerenost (relevantnost) – informacija je primjerena (relevantna) ako odgovara kontekstu i osobi koja je prima.

18

00:02:00,866 --> 00:02:05,966

Pravodobnost – informacija je pravodobna ako je dobivena na vrijeme.

19

00:02:05,966 --> 00:02:15,199

U modernom poslovanju informacija daje podlogu za odlučivanje pa je realno za očekivati da će donositelj odluke na temelju kvalitetnije informacije

20

00:02:15,200 --> 00:02:24,833

donijeti bolju odluku, kao što ćemo mi kvalitetnije iskoristiti godišnji ako ćemo imati točnu, pravodobnu i primjerenu vremensku prognozu. I

21

00:02:24,833 --> 00:02:29,533

vremenska je prognoza „rezultat obrade“ podataka o meteorološkim zbivanjima.

22

00:02:29,533 --> 00:02:37,299

Iz svega se napisanog lako dade zaključiti da je svaka informacija vrijedna i da nikada nije besplatna.

23

00:02:37,300 --> 00:02:47,366

Jednako tako, ako govorimo o kontekstu prodaje informacija, određena kompanija može dio svojih podataka staviti na tržište pa se tako podaci o

24

00:02:47,366 --> 00:02:58,199

prodaji, u konačnici, mogu ponuditi novim kupcima, a obrađeni i depersonalizirani podaci mogu se npr. prodati marketinškoj agenciji.

25

00:02:58,200 --> 00:03:10,600

S obzirom na to da podatak odnosno informacija ima neku vrijednost, lako je zaključiti i da određeni krug ljudi ima želju podatke i informacije i otuđiti.

26

00:03:10,600 --> 00:03:16,800

Kada govorimo o informacijama odnosno korisničkim podacima, vrlo je bitna i njihova zaštita.

27

00:03:16,800 --> 00:03:26,000

Krađa korisničkih podataka ili bolje rečeno osobnih podataka, za početak kažnjivo je djelo i može izazvati nesagledive posljedice.

28

00:03:26,000 --> 00:03:37,666

Osobni podaci se kradu zbog puno razloga, a jedan od opasnijih je i tzv. fraud (prevara), termin koji se udomaćio i u našem jeziku a posebno ga

29

00:03:37,666 --> 00:03:41,899

se boje financijske institucije, telekomunikacijske kompanije i sl.

30

00:03:41,900 --> 00:03:54,566

Kada govorimo o kompanijama, otuđivanje njihovih podataka odnosno informacija noćna je mora svakog vlasnika, pogotovo ako je riječ o

31

00:03:54,566 --> 00:04:01,432

aspektu tzv. korisničkih podataka (matični podaci, podaci o kreditnim karticama i sl.).

32

00:04:01,433 --> 00:04:07,099

U brojnim kompanija danas sve više jača spoznaja o važnosti informacijske sigurnosti.

33

00:04:07,100 --> 00:04:17,300

U skladu s time razvija se i svijest o važnosti postojanja sigurnosne politike i svih ostalih dokumenata koji proizlaze iz sigurnosne politike.

34

00:04:17,300 --> 00:04:27,266

Ovisno o tipu kompanije (tj. veličini, broju zaposlenih, kompleksnosti informacijskog sustava, broju korisnika informacijskog sustava, tipovima i

35

00:04:27,266 --> 00:04:34,766

osjetljivosti informacija kojima organizacija raspolaže i sl.) razlikuju se i sigurnosne politike organizacije.

36

00:04:34,766 --> 00:04:44,399

No iskustvo je pokazalo da je efikasniji pristup u razvoju sigurnosne politike (za sve tipove kompanija) razviti niz dokumenata različitog

37

00:04:44,400 --> 00:04:52,533

područja pokrivanja nego imati jedan dokument koji će nazvati sigurnosnom politikom, koji će biti namijenjen svim korisnicima informacijskog

38

00:04:52,533 --> 00:04:57,233

sustava i koji će pokrivati sve aspekte informacijske sigurnosti organizacije.

39

00:04:57,233 --> 00:05:09,399

Zbog zaštite komercijalno osjetljivih informacija te sprečavanja krađe ili zloupotrebe detalja o klijentima te financijskih informacija razvijaju se

40

00:05:09,400 --> 00:05:10,700

sigurnosne politike koje služe za:

41

00:05:10,700 --> 00:05:13,066

1. zaštitu ljudi i informacija

42

00:05:13,066 --> 00:05:16,599

2. umanjivanje sigurnosnog rizika

43

00:05:16,600 --> 00:05:20,700

3. definiranje odnosa prema informacijskoj sigurnosti i očekivanja od informacijske sigurnosti

44

00:05:20,700 --> 00:05:29,800

4. definiranje pravila prihvatljivog ponašanja za korisnike informacijskog sustava, administratore, rukovoditelje itd.

45

00:05:29,800 --> 00:05:38,466

5. davanje ovlaštenja za nadzor, reviziju, ispitivanje, istraživanje i sl. osobama zaduženima za sigurnost u organizaciji

46

00:05:38,466 --> 00:05:43,699

6. usklađivanje sa zakonskim, regulatornim i ugovornim zahtjevima.

47

00:05:43,700 --> 00:05:51,966

Sigurnosne politike pružaju okvir za primjenu obveznih i dobrih praksi koje zaposlenici organizacije trebaju slijediti.

48

00:05:51,966 --> 00:06:01,566

Definiranjem sigurnosnih politika svi zaposlenici organizacije postaju čimbenici programa i sustava informacijske sigurnosti u organizaciji.

49

00:06:01,566 --> 00:06:11,999

Sigurnosne politike naglašavaju važnost informacija kao ključne imovine organizacije i propisuju pravila za zaštitu povjerljivosti, integriteta

50

00:06:12,000 --> 00:06:14,300

i raspoloživosti informacija.

51

00:06:14,300 --> 00:06:22,700

U današnje vrijeme brojne organizacije podliježu različitim zakonskim i regulatornim obvezama na području informacijske sigurnosti.

52

00:06:22,700 --> 00:06:34,666

U ovom su trenutku u Hrvatskoj u najvećoj primjeni sljedeći zakoni i industrijske regulative:

53

00:06:34,666 --> 00:06:47,032

Zakon o sigurnosno-obavještajnom sustavu RH – krovni zakon koji osniva sigurnosno-obavještajnu agenciju (SOA) te vojnu sigurnosno-obavještajnu

54

00:06:47,033 --> 00:06:48,766

agenciju (VSOA).

55

00:06:48,766 --> 00:06:57,899

Zakon također postavlja temelj za rad Vijeća za nacionalnu sigurnost, Savjeta za koordinaciju sigurnosno-obavještajnih agencija, ureda Vijeća

56

00:06:57,900 --> 00:07:07,033

za nacionalnu sigurnost, Zavoda za sigurnost informacijskih sustava te Operativno-tehničkog centra za nadzor telekomunikacija.

57

00:07:07,033 --> 00:07:17,133

Zakon o informacijskoj sigurnosti – primjenjuje se na „državna tijela“, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne

58

00:07:17,133 --> 00:07:27,533

osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke“ te na „pravne i fizičke osobe koje ostvaruju pristup ili

59

00:07:27,533 --> 00:07:31,866

postupaju s klasificiranim i neklasificiranim podacima“.

60

00:07:31,866 --> 00:07:42,866

Zakon o zaštiti osobnih podataka – bavi se zaštitom osobnih podataka o fizičkim osobama te nadzorom nad prikupljanjem, obradom i

61

00:07:42,866 --> 00:07:47,466

korištenjem osobnim podacima u Republici Hrvatskoj.

62

00:07:47,466 --> 00:07:59,299

Odluka Hrvatske narodne banke o primjerenom upravljanju informacijskim sustavom – industrijska regulativa koja se odnosi na banke i stambene

63

00:07:59,300 --> 00:08:02,600

štedionice.

64

00:08:02,600 --> 00:08:16,933

Payment Card Industry Data Security Standard (PCI DSS) – industrijska regulativa kojom kartične kuće (Mastercard, Visa, AMEX) obvezuju

65

00:08:16,933 --> 00:08:22,566

sve organizacije koje pohranjuju, prenose ili obrađuju kartične podatke.

66

00:08:22,566 --> 00:08:32,266

Navedeni zakoni i regulative (ali i brojne druge regulative) kao jedan od elemenata usklađivanja kompanijama propisuju i izradu te održavanje

67

00:08:32,266 --> 00:08:34,432

sigurnosnih politika.

68

00:08:34,433 --> 00:08:43,533

Sigurnosne politike služe kao alat za usklađivanje i temelj za dokazivanje da je kompanija implementirala sigurnosne kontrole i da provodi

69

00:08:43,533 --> 00:08:47,599

potrebne procese i prakse na području informacijske sigurnosti.

70

00:08:47,600 --> 00:08:54,400

Za kompaniju informacijska sigurnost označuje sastavni dio odgovornog upravljanja.

71

00:08:54,400 --> 00:09:05,066

U radu kompanija, postoje situacije kada ne možemo zabraniti fizički pristup računalnoj opremi te se često nalazimo u situacijama kada se u

72

00:09:05,066 --> 00:09:09,866

uredskim prostorijama mogu naći i neovlaštene osobe.

73

00:09:09,866 --> 00:09:19,099

Nerijetko se u takvim situacijama dešavaju krađe osobnih, a posebno prijenosnih računala. Sama prijenosna računala vrlo su pogodna za otuđivanje

74

00:09:19,100 --> 00:09:29,566

zbog svoje lakoće i malih dimenzija. U takvim situacijama dobro je koristiti tzv. kablovske brave kao jedan od faktora poboljšanja fizičke sigurnosti.

75

00:09:29,566 --> 00:09:39,599

U naravi se radi o čeličnim sajlama koje na sebi imaju posebno dizajnirane bravice prilagođene utorima na našim prijenosnim računalima.

76

00:09:39,600 --> 00:09:49,566

Koristeći takva pomagala, jednostavno jedan kraj kablovske brave stavimo za naše računalo dok drugi kraj, jednostavno zaključamo za npr. uredski

77

00:09:49,566 --> 00:09:56,399

stol.

78

00:09:56,400 --> 00:10:05,766

Slijedeća metoda koju koristimo radi sprječavanja neovlaštenog pristupa je i kontrola pristupa.Svrha kontrole pristupa je zaštititi od neovlaštenog

79

00:10:05,766 --> 00:10:18,666

ulaza u stambene i poslovne objekte ili njihove dijelove. Može biti mehanička (rampe), elektronička ili kombinirana a što će se koristiti

80

00:10:18,666 --> 00:10:24,866

ovisi o ugroženosti i o tome treba li kontrolirati pristup pješaka, vozila i / ili radnih strojeva.

81

00:10:24,866 --> 00:10:36,432

Primjena sustava je u velikom porastu jer sve veći broj tvrtki želi kontrolirati pristup i tako čuvati vrijednosti i informacija te nadzirati zaposlene.

82

00:10:36,433 --> 00:10:46,166

Rastu primjene doprinose pad cijena uređaja i dostupnost novih tehnologija identifikacije i komunikacije.

83

00:10:46,166 --> 00:10:55,599

Osim zaštitne funkcije u smislu prevencije kriminala, primjena kontrole pristupa značajno podiže razinu sigurnosti.

84

00:10:55,600 --> 00:11:01,433

Sve ovo radimo u svrhu sprečavanja gubitka ili uništenja informacija.

85

00:11:01,433 --> 00:11:15,066

Jedan od učinkovitih načina sprječavanja ili smanjenja šteta nastalih na informatičkoj opremi (neovisno o uzroku) je i popis lokacije opreme i

86

00:11:15,066 --> 00:11:17,199

njenih dijelova.

87

00:11:17,200 --> 00:11:25,433

Potrebno je imati popis svih prijenosnih računala, radnih stanica, poslužitelja te mrežne opreme. Također, bitno je imati i zabilješke o svim

88

00:11:25,433 --> 00:11:31,399

aplikacijama koje su ključne za poslovanje kompanije, a nalaze se na pojedinom uređaju.

89

00:11:31,400 --> 00:11:37,866

Najvažniju opremu je potrebno i kategorizirati, na primjer dodijeliti oznaku „kategorija 1“.

90

00:11:37,866 --> 00:11:46,632

Cilj ovakvog koraka je povećati svjesnost zaposlenika o svim računalima i aplikacijama o kojima ovisi normalno funkcioniranje kompanije.

91

00:11:46,633 --> 00:11:56,199

Također se, u slučaju bilo kakve prijetnje lako može definirati koju je opremu potrebno spašavati ili koji dio opreme mora imati spremnu zamjenu u

92

00:11:56,200 --> 00:12:03,900

slučaju prestanka funkcioniranja ili se čak mora nalaziti na drugoj (pričuvnoj) lokaciji.

93

00:12:03,900 --> 00:12:12,133

Skup propisanih pravila od strane kompanije, a čija je namjena zaštita fizičke imovine i informatičke opreme kompanije nazivamo

94

00:12:12,133 --> 00:12:23,166

sigurnosnom politikom (Security policy).Koliko je informacija odnosno podataka vidimo iz svega navedenog. Danas informacije možemo

95

00:12:23,166 --> 00:12:32,266

razmjenjivati na puno načina, kao npr. putem elektroničkih poruka, ali ono što se u kompanijama udomačilo kao brz i efikasan način

96

00:12:32,266 --> 00:12:39,499

razmjene poruka su i aplikacije za trenutnu razmjenu poruka (eng. Instant messaging).

97

00:12:39,500 --> 00:12:48,700

Ukoliko na našem računalu imamo neki od alata za trenutnu razmjenu poruka (Skype, Google talk i sl.), preporuka je da na računalima imamo

98

00:12:48,700 --> 00:12:59,400

uključeno šifriranje podataka, da ograničimo pristup našem računalu isključivanjem dijeljenja datoteka (eng. File sharing) te da nikako ne

99

00:12:59,400 --> 00:13:04,366

izlažemo osobne podatke i povjerljive informacije na taj način.

100

00:13:04,366 --> 00:13:11,366

Kada smo spomenuli šifriranje podataka, bitno je napomenuti da i ono ima svoje mane i prednosti.

101

00:13:11,366 --> 00:13:19,432

Kao što je rečeno, samo šifriranje se svodi na zamjenu određenih slova nečime drugim po nekom algoritmu.

102

00:13:19,433 --> 00:13:24,233

Gubitak tog algoritma odnosno njegovog „ključa“ znači i gubitak podataka.

103

00:13:24,233 --> 00:13:35,299

Prednost šifriranja je da čuva podatak npr. u trasportu, dakle dok ga šaljemo nekim elektroničkim putem ili smo šifrirani podatak

104

00:13:35,300 --> 00:13:38,533

spremili na USB ključić kojeg smo izgubili.

105

00:13:38,533 --> 00:13:48,199

Izvrsno rješenje za naše USB ključiće je npr. Windows Bitlocker.

106

00:13:48,200 --> 00:13:57,366

Sustav upravljanja sigurnošću uveden je radi efikasnog osiguranja povjerljivosti, integriteta i raspoloživosti informacija.

107

00:13:57,366 --> 00:14:07,266

Svrha takvog sustava jest osigurati poslovanje tvrtke i pružiti maksimalnu razinu zaštite te osigurati povjerenje svojih klijenata.

108

00:14:07,266 --> 00:14:17,532

Cilj politike informacijske sigurnosti jest definiranje načela informacijske sigurnosti i temeljnih uloga i odgovornosti kako bi se na prikladan način

109

00:14:17,533 --> 00:14:22,299

upravljalo uspostavljenim sustavom informacijske sigurnosti.

110

00:14:22,300 --> 00:14:31,933

Temelj sustava upravljanja informacijskom sigurnošću stalan je proces upravljanja rizikom čime se osigurava primjerena razina zaštite

111

00:14:31,933 --> 00:14:36,133

sustava uz poslovno opravdane investicije u mjere zaštite.

112

00:14:36,133 --> 00:14:45,433

U cilju zaštite svojih klijenata svi sigurnosni rizici koji se odnose na informacije klijenata ili informacije o klijentima svodit će se na minimalnu

113

00:14:45,433 --> 00:14:46,599

vrijednost.

114

00:14:46,600 --> 00:14:52,033

Ostali sigurnosni rizici bit će tretirani u skladu s poslovnim potrebama.

115

00:14:52,033 --> 00:15:01,433

Uprava se obvezuje da će poduzeti sve potrebne mjere kako bi sustav upravljanja informacijskom sigurnošću bio stalno usklađen sa svim važećim

116

00:15:01,433 --> 00:15:05,533

zakonskom propisima, kao i s ugovornim zahtjevima klijenata.

117

00:15:05,533 --> 00:15:13,033

U tom će smislu uprava prihvaćati politike, pravilnike, postupke i druge provedbene dokumente.

118

00:15:13,033 --> 00:15:24,599

Nadalje, kroz formalne programe, ali i prihvaćenu kulturu ponašanja u kompaniji, uprava će osigurati odgovarajuću edukaciju svojih zaposlenika i mjere

119

00:15:24,600 --> 00:15:27,200

za podizanje svijesti o informacijskoj sigurnosti.

120

00:15:27,200 --> 00:15:31,933

Uprava ovlašćuje rukovoditelja za informacijsku sigurnost za:

121

00:15:31,933 --> 00:15:35,133

•uspostavu i provođenje procesa upravljanja rizikom

122

00:15:35,133 --> 00:15:39,799

•nadzor uspostavljenog sustava za upravljanje informacijskom sigurnošću

123

00:15:39,800 --> 00:15:43,000

•praćenje ukupnog stanja informacijske sigurnosti

124

00:15:43,000 --> 00:15:47,166

•donošenje prijedloga o poboljšanju i provedbi sigurnosnih mjera.

125

00:15:47,166 --> 00:15:56,899

Od svih korisnika informacijskog sustava tvrtke, zaposlenika i vanjskih partnera očekuje se razumijevanje osobne odgovornosti za zaštitu

126

00:15:56,900 --> 00:16:08,266

informacijskih resursa tvrtke i njezinih klijenata preko primjene i poštovanja ove politike i drugih alata te aktivno sudjelovanje u poboljšanjima, i to

127

00:16:08,266 --> 00:16:13,766

uočavanjem i prijavom potencijalnih sigurnosnih problema i incidenata.

128

00:16:13,766 --> 00:16:29,832

Kako su kompanije svjesne vrijednosti svojih informacija, vrlo je važno da i mi shvatimo koliko su „naši podaci“ vrijedni, ne samo nama nego i

129

00:16:29,833 --> 00:16:31,299

drugima.

130

00:16:31,300 --> 00:16:42,066

Kako pojedinci žele otuđiti neku informaciju kompanijama i ilegalno izvući materijalnu ili neku drugu korist, jednako će tako to poželjeti napraviti i

131

00:16:42,066 --> 00:16:43,032

nama.

132

00:16:43,033 --> 00:16:52,166

Ono što nikako ne bismo željeli jest da netko ukrade naše osobne podatke jer smo bili nesmotreni pri internetskoj kupnji te nam nanese

133

00:16:52,166 --> 00:16:53,499

financijsku štetu.

134

00:16:53,500 --> 00:17:03,866

Koliko je zaštita osobnih podataka bitna, govori nam i članak 1. Temeljnih odredbi Zakona o zaštiti osobnih podataka koji kaže da je svrha zaštite

135

00:17:03,866 --> 00:17:13,332

osobnih podataka zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.

136

00:17:13,333 --> 00:17:23,999

Dalje se kaže da je zaštita osobnih podataka u Republici Hrvatskoj osigurana svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te

137

00:17:24,000 --> 00:17:35,033

neovisno o rasi, boje kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu.

138

00:17:35,033 --> 00:17:43,966

I Europska unija je kroz Direktivu o zaštiti osobnih podataka koja je usvojena 1995.godine donijela zakonske akte u pogledu obrade i korištenja

139

00:17:43,966 --> 00:17:45,366

osobnih podataka.

140

00:17:45,366 --> 00:17:58,666

Radi se o važnom članku europskog zakona koji štiti privatnost i ljudska prava te ukazuje na važnost zaštite i izbjegavanja krađe osobnih podataka

141

00:17:58,666 --> 00:18:01,266

zbog osobne koristi.

142

00:18:01,266 --> 00:18:09,566

Na osnovi svega nije teško zaključiti da, ako i nije ugrožena naša osobna sigurnost, trebamo poraditi na osiguranju nepovredljivosti naših osobnih

143

00:18:09,566 --> 00:18:10,899

podataka.

144

00:18:10,900 --> 00:18:18,033

Krađa osobnih podataka, često je usko povezana s fenomenom koji nazivamo socijalnim inženjeringom.

145

00:18:18,033 --> 00:18:26,699

Socijalni smo inženjering, prikladno, spomenuli u poglavlju koji se odnosi na lozinke. Jedan od glavnih ciljeva socijalnog inženjeringa jest upravo

146

00:18:26,700 --> 00:18:31,966

saznavanje informacija o korisniku, a najčešće su na meti korisničke lozinke.

147

00:18:31,966 --> 00:18:42,699

U ovome priručniku o socijalnom inženjeringu govorimo u kontekstu informacijske sigurnosti, a odnosi se na psihološku manipulaciju ljudima s

148

00:18:42,700 --> 00:18:48,766

namjerom saznavanja povjerljivih informacija bilo kojeg oblika.

149

00:18:48,766 --> 00:18:59,432

Namjera manipulacije ljudima jest uz pomoć raznih trikova doći do povjerljivih informacija s ciljem postizanja aktivnosti usmjerenih na prevaru i

150

00:18:59,433 --> 00:19:06,866

pristup informacijskom sustavu, a često se sastoji od nekoliko koraka.

151

00:19:06,866 --> 00:19:14,966

Prvi od koraka jest uspostavljanje odnosa povjerenja s osobom koju se želi prevariti ili od nje dobiti povjerljive informacije.

152

00:19:14,966 --> 00:19:22,032

U načelu je takva osoba ljubazna prema nama, suosjećajna i u većini slučajeva djeluje naivno i dobroćudno.

153

00:19:22,033 --> 00:19:30,099

Prije nego što nam je pristupila, o nama je saznala određene informacije, i to uglavnom prikupivši ih na društvenim mrežama poput Facebooka,

154

00:19:30,100 --> 00:19:31,433

Twittera i sl.

155

00:19:31,433 --> 00:19:40,399

Obično o nama zna dovoljno informacija kako bi nam nesmetano mogla pristupit hineći poznanstvo ili poznavanje naše situacije.

156

00:19:40,400 --> 00:19:50,433

Na sličan način provodi se i tzv. pretexting odnosno izgovaranje, i to s izmišljenim scenarijem tako da osoba napravi radnju koju u normalnim

157

00:19:50,433 --> 00:19:57,833

uvjetima ne bi nikada učinila, npr. dala lozinku, PIN i sl.

158

00:19:57,833 --> 00:20:19,299

NIkada ne ostavljajte nikome korisničko ime i pripadajuću mu lozinku, brojeve bankovnih računa ili kreditnih kartica te datum rođenja, djevojačko

159

00:20:19,300 --> 00:20:25,566

prezime majke, osobni identifikacijski broj.

160

00:20:25,566 --> 00:20:34,799

Za kraj, ono čega moramo biti svjesni je činjenica da sve ove radnje koje smo poduzeli ili ćemo poduzimati su iz razloga zaštite osobnih podataka

161

00:20:34,800 --> 00:20:40,000

odnosno informacija, kako bi smo izbjegli, prije svega, krađu našeg identiteta.

162

00:20:40,000 --> 00:20:50,866

Iako je krađa podataka kažnjiva u svim članicama EU, to nam može biti samo mala zadovoljština kada je šteta već učinjena, kako nama tako i

163

00:20:50,866 --> 00:20:51,366

kompanijama. Lekcija je završena.

164

00:20:51,366 --> 00:20:51,899

Lekcija\_3\_1\_6

1

00:00:00,000 --> 00:00:12,833

Dobrodošli. U ovoj lekciji govorit ćemo o

prijetnjama na društvenim mrežama te digitalnim

potpisima i certifikatima.

2

00:00:12,833 --> 00:00:22,199

O prijetnjama na Internetu smo već ranije govorili,

a sada ćemo spomenuti zastrašivanje odnosno

cyberbulling te lažne informacije i identitete te

3

00:00:22,200 --> 00:00:24,466

lažne linkove ili poruke.

4

00:00:24,466 --> 00:00:35,032

Kao što znamo, u stvarnom životu svoj identitet

dokazujemo pokazivanjem osobne iskaznice koje

je izdalo, u Internetskom svijetu znano kao CA,

5

00:00:35,033 --> 00:00:38,666

odnosno certifikacijski autoritet, odnosno MUP.

6

00:00:38,666 --> 00:00:48,832

No dokazati svoj identitet na Internetu i time

potvrditi vjerodostojnost svoje elektroničke poruke

te da smo ju mi i samo mi i nitko drugi poslali,

7

00:00:48,833 --> 00:00:53,266

možemo jedino uz posjedovanje digitalnog

potpisa.

8

00:00:53,266 --> 00:01:04,099

Kada spominjemo digitalni potpis, ovdje se ne

misli na mogućnost u Wordu kada možemo

priložiti svoj skenirani potpis nego pravom

9

00:01:04,100 --> 00:01:06,200

digitalnom certifikatu.

10

00:01:06,200 --> 00:01:15,300

Šifriranje e-poruke u programu Microsoft Outlook

štiti povjerljivost poruke tako da se pretvara iz

običnog teksta u šifrirani.

11

00:01:15,300 --> 00:01:25,766

Osnovni princip šifriranja je kroz Cezarov kod

objašnjen u poglavlju o Mjerama zaštite. Samo

primatelj poruke koji ima privatni ključ koji

12

00:01:25,766 --> 00:01:32,532

odgovara javnom ključu korištenom za šifriranje

može dešifrirati poruku te ju potom pročitati.

13

00:01:32,533 --> 00:01:36,999

Svi ostali primatelji koji nemaju odgovarajući

privatni ključ vide besmisleni tekst.

14

00:01:37,000 --> 00:01:49,400

Dakle, šifriranje jednoznačno možemo opisati kao

akciju čija je namjera osigurati da jedino osoba

kojoj je elektronička poruka namijenjena može tu

15

00:01:49,400 --> 00:01:51,000

poruku i pročitati.

16

00:01:51,000 --> 00:02:00,466

Preduvjet za slanje i prikazivanje šifriranih e-

poruka jest da pošiljatelj i primatelj razmijene svoje

digitalne identifikatore (ID) odnosno certifikate

17

00:02:00,466 --> 00:02:02,399

javnih ključeva.

18

00:02:02,400 --> 00:02:10,833

Digitalni potpis označuje matematičku shemu koja

omogućuje provjeru autentičnosti poruke ili

dokumenta.

19

00:02:10,833 --> 00:02:19,899

Na ovaj se način može sa sigurnošću provjeriti i

potvrditi autor poruke, i to s većom sigurnošću

nego što je to slučaj u normalnom svijetu, gdje se

20

00:02:19,900 --> 00:02:24,033

autentičnost poruke obično provjerava običnim

potpisom.

21

00:02:24,033 --> 00:02:32,699

Razlog ovome jesu obilježja digitalnog potpisa

koja osiguravaju nemogućnost krivotvorenja

digitalnog potpisa primjenom današnjih

22

00:02:32,700 --> 00:02:34,266

tehnologija.

23

00:02:34,266 --> 00:02:41,866

Da biste kreirali vlastiti digitalni potpis, morate

imati certifikat za potpisivanje koji dokazuje vaš

identitet.

24

00:02:41,866 --> 00:02:49,632

Prilikom slanja digitalno potpisane elektroničke

poruke ili dokumenta šaljete i svoj certifikat te javni

ključ.

25

00:02:49,633 --> 00:02:55,066

Certifikate izdaje ustanova za izdavanje

certifikata, a moguće ih je opozvati.

26

00:02:55,066 --> 00:03:09,266

Valjanost certifikata najčešće traje godinu dana te

ga nakon isteka valjanosti potpisnik mora obnoviti

ili pribaviti novi certifikat za potpisivanje da bi

27

00:03:09,266 --> 00:03:10,732

potvrdio svoj identitet.

28

00:03:10,733 --> 00:03:21,433

Da bi naručili svoj certifikat, morate se obratiti

ustanovi za izdavanje certifikata. Kod nas tu ulogu

izdavatelja certifikata ima Financijska agencija.

29

00:03:21,433 --> 00:03:31,866

Ona izdaje digitalne certifikate, potpisuje

certifikate da bi se potvrdila njihova valjanost te

bilježi opozvane certifikate i certifikate čija je

30

00:03:31,866 --> 00:03:33,699

valjanost istekla.

31

00:03:33,700 --> 00:03:42,600

Slijedeći problem nam predstavlja neovlašteno

traženje informacija (phishing i pharming) i mnoge

druge tehnike varanja korisnika temelje se na

32

00:03:42,600 --> 00:03:45,200

socijalnom inženjeringu.

33

00:03:45,200 --> 00:03:55,400

Prijevarom, manipulacijom se natjera korisnika da

samostalno izvrši neku radnju (instaliranje nekog

programa, otkrivanje osobnih podataka i sl.).

34

00:03:55,400 --> 00:04:04,566

Takva je radnja najčešće njemu samom na štetu,

ali je prijevara obično dovoljno dobro izvedena da

toga nije svjestan. Barem ne na vrijeme.

35

00:04:04,566 --> 00:04:15,832

Neovlašteno traženje informacija (phishing)

uključuje kontaktiranje žrtve preko elektroničke

pošte, soba za razgovor (chat rooms) ili usluga

36

00:04:15,833 --> 00:04:21,533

trenutačnih poruka (instant messaging) i jedan je

od oblika kibernetičkog kriminala.

37

00:04:21,533 --> 00:04:32,166

Najčešće se šalje neka vrsta obavijesti kako je

potrebno unijeti određene osobne podatke sa

svrhom potvrde ili ažuriranja korisničkog računa,

38

00:04:32,166 --> 00:04:40,799

pozivi za darivanje novca u lažne dobrotvorne

svrhe, obavijesti o nekom novčanom dobitku,

lažne obavijesti od administratora i slično.

39

00:04:40,800 --> 00:04:48,666

Mnogi korisnici nasjednu na takve prijevare,

pogotovo zato što je obično riječ o naizgled

legitimnim tvrtkama ili uslugama kao što su banke,

40

00:04:48,666 --> 00:04:57,566

pružatelji internetskih usluga (ISP), tvrtke za

internetsku trgovinu i slično. Prijevare često

uključuju poznata imena kao PayPal, eBay, Best

41

00:04:57,566 --> 00:04:59,366

Buy ili poznate banke.

42

00:04:59,366 --> 00:05:08,766

Unutar te obavijesti (najčešće e-poruke) nalazi se

poveznica (link) na neko web-odredište gdje je

potrebno unijeti podatke.

43

00:05:08,766 --> 00:05:17,499

Klikom na poveznicu, web-preglednik otvara

stranicu koja izgleda vrlo stvarno i uvjerljivo. To je

obično lažna stranica i sve unesene podatke

44

00:05:17,500 --> 00:05:27,366

preuzima autor prijevare. Podaci koji se traže jesu

osobni podaci, lozinke, brojevi kreditnih kartica,

brojevi bankovnih računa i slično, a cilj je vrlo očit –

45

00:05:27,366 --> 00:05:30,832

krađa identiteta i financijska prijevara.

46

00:05:30,833 --> 00:05:40,033

Klikom na takve poveznice, osim krađe osobnih

podataka, velika je vjerojatnost i da se inicira

instalacija i nekakvoga štetnog koda poput

47

00:05:40,033 --> 00:05:44,233

špijunskih programa (spyware), crva ili trojanskih

konja.

48

00:05:44,233 --> 00:05:53,533

Takva prijevara (phishing) uključuje integraciju više

elemenata, moguće špijunskog koda (spyware)

koji sakuplja informacije o korisniku koje poslije

49

00:05:53,533 --> 00:05:58,899

služe za slanje prave vrste obavijesti na koju će

konkretan korisnik nasjesti.

50

00:05:58,900 --> 00:06:08,200

Jednako tako, da bi se cijela zamka uspješno

izvršila, primjenjuju se tehnike zavaravanja

(spoofing) objašnjene ranije.

51

00:06:08,200 --> 00:06:19,366

Tehnike zavaravanja, lažnog predstavljanja

primjenjuju se da bi se lažirale adrese pošiljatelja

u e-porukama koje sadržavaju varku, za prikrivanje

52

00:06:19,366 --> 00:06:27,099

poveznica na koje korisnik treba kliknuti te da bi

se lažirala web-mjesta na kojima korisnik treba

unijeti potrebne podatke.

53

00:06:27,100 --> 00:06:37,666

Jedini način kako možemo provjeriti

vjerodostojnost takvog linka u lažnoj poruci je da

provjerimo, kada nam se stranica već otvorila, da

54

00:06:37,666 --> 00:06:39,432

li ima digitalni certifikat.

55

00:06:39,433 --> 00:06:49,033

Provjeru certifikata ćete napraviti tako da

pogledate da li u dijelu za unos linka postoji

oznaka lokotića.

56

00:06:49,033 --> 00:06:58,599

Dvostrukim klikom na taj lokotić te odabirom

opcije „View certificates“ dobit ćete podatke o

kojoj se zapravo stranici radi.

57

00:06:58,600 --> 00:07:12,666

Moja je namjera bila posjetiti stranicu

http://polaznici.algebra.hr i ovaj certifikat dokazuje

da se ja stvarno i nalazim na toj stranici.

58

00:07:12,666 --> 00:07:21,866

No, ono što moramo imati na umu kod

potencijalno lažnih linkova je činjenica je da

poznate tvrtke ili financijske organizacije od

59

00:07:21,866 --> 00:07:29,266

korisnika nikada ne traže osobne podatke na

takve načine, već obično šalju formalna pisma.

60

00:07:29,266 --> 00:07:36,999

Specifično je da su takvi tipovi elektroničkih

poruka često puni gramatičkih grešaka i pogrešno

napisanih riječi.

61

00:07:37,000 --> 00:07:45,900

Razlog takve „nečitljivosti“ jest korištenje

računalnim prevoditeljima, npr. Google Translate,

koji nisu dovoljno dobri kako bi stranicu preveli

62

00:07:45,900 --> 00:07:47,766

pravopisno i gramatički ispravno.

63

00:07:47,766 --> 00:07:58,866

Često se lažiraju i e-poruke Microsofta koje

navodno sadržavaju poveznice na najnovije zakrpe

ili se pak te zakrpe navodno nalaze u privitku te e-

64

00:07:58,866 --> 00:08:00,599

poruke.

65

00:08:00,600 --> 00:08:09,633

Opće je poznato da Microsoft nikada ne prakticira

takav pristup, već da je jedini siguran način ručno

preuzimanje zakrpa s Microsoftovih stranica ili

66

00:08:09,633 --> 00:08:13,566

korištenje uslugom automatskog ažuriranja

(AutomaticUpdates).

67

00:08:13,566 --> 00:08:21,166

Događa se da se takve poveznice šalju i preko

usluga trenutačnih poruka (instant messaging) i to

tako da se čini kao da pristižu od poznate osobe.

68

00:08:21,166 --> 00:08:29,132

Postoje mnogi oblici zavaravanja žrtve od kojih su

neki i na prvi pogled vrlo sumnjivi, no ipak dovoljno

uvjerljivi naivnom korisniku.

69

00:08:29,133 --> 00:08:38,966

Takve vrste prijevara obično se oslanjaju na

neznanje i naivnost korisnika koji im zapravo

svojevoljno predaju svoje osobne i povjerljive

70

00:08:38,966 --> 00:08:40,366

podatke.

71

00:08:40,366 --> 00:08:48,699

Osnovna premisa socijalnog inženjeringa na djelu

jest – bilo kakav podatak može se dobiti od

nekoga, samo treba pitati na pravi način.

72

00:08:48,700 --> 00:09:03,100

Sam izraz „phishing“ prilagođen je oblik engleske

riječi „fishing“ – pecanje, a aludira na lov i mamac

na koji se korisnici trebaju upecati.

73

00:09:03,100 --> 00:09:11,500

Neovlašteno traženje informacija prijevarom

(pharming) također je vrsta prijevare s istim ciljem

kao i prethodna, no s nešto opskurnijim

74

00:09:11,500 --> 00:09:18,266

metodama. Čak je i stručnjacima mnogo teže

otkriti takvu prijevaru jer je gotovo nevidljiva.

75

00:09:18,266 --> 00:09:26,199

Zastrašujuća je pomisao takve prijevare koja je

vrlo suptilna, dakle ne pokušava namamiti

korisnika i izmanipulirati ga na neke radnje, a

76

00:09:26,200 --> 00:09:35,200

opet, riječ je o ozbiljnom narušavanju sigurnosti.

Izraz „pharming“ prilagođeni je oblik engleske

riječi „farming“ – uzgoj na farmi.

77

00:09:35,200 --> 00:09:42,900

Riječ je o otmici prave adrese i postavljanju

imitacije tražene web-stranice. U osnovi,

„pharming“ se zasniva na preusmjeravanju

78

00:09:42,900 --> 00:09:50,900

korisnika na lažna web mjesta koja izgledom

podsjećaju ili su identična web mjestima koja smo

u stvari željeli posjetiti.

79

00:09:50,900 --> 00:09:58,500

Neovlašteno traženje informacija prijevarom

(pharming) zasniva se na tehnikama

kompromitiranja DNS (Domain Name Server)

80

00:09:58,500 --> 00:10:05,233

poslužitelja, i to mijenjanjem njihove priručne

memorije (cache) tako da pohranjuje pogrešne IP

adrese.

81

00:10:05,233 --> 00:10:14,399

Kada korisnik, primjerice, želi posjetiti web-mjesto

svoje banke, biva preusmjeren na lažnu stranicu

jer će DNS poslužitelj vratiti pogrešnu IP adresu.

82

00:10:14,400 --> 00:10:24,800

Stranica koja će se prikazati nalikovat će na pravu

stranicu banke, ali riječ je o imitaciji, lažnoj stranici

koja izgleda realno i uvjerljivo, ali kojom upravlja

83

00:10:24,800 --> 00:10:34,466

autor prijevare (pharmer). I naravno, nakon

unošenja osobnih podataka radi pristupa

korisničkom računu napadač dolazi u posjed

84

00:10:34,466 --> 00:10:40,266

povjerljivih osobnih podataka koje dalje

iskorištava u svrhe krađe identiteta i financijske

prijevare.

85

00:10:40,266 --> 00:10:48,932

Donekle je utješno to što se takva vrsta prijevare

događa rjeđe od ostalih (npr. phishing), međutim,

alarmantno je što je golem broj nevinih ljudi

86

00:10:48,933 --> 00:10:53,266

prevaren i opljačkan iako takvi napadi traju vrlo

kratko.

87

00:10:53,266 --> 00:11:02,666

Još je strašnija činjenica da tijekom tog procesa

web-preglednik uredno prikazuje da se nalazi na

ispravnom web-mjestu iako je ono lažno.

88

00:11:02,666 --> 00:11:12,332

Vrlo je malo toga što pojedinac može poduzeti u

obrani od takve prijevare osim provjere da li takva

stranica ima digitalni certifikat (dokaz da se

nalazimo na pravoj web stranici).

89

00:11:12,333 --> 00:11:20,733

To je problem koji rješavaju pružatelji internetskih

usluga (ISP) te telekomunikacijske tvrtke i

organizacije koje posjeduju DNS opremu na

90

00:11:20,733 --> 00:11:22,199

Internetu.

91

00:11:22,200 --> 00:11:37,733

Slijedeći problem koji imamo je cyberbullyng u

svijetu poznato kao cyberbullying, opći je pojam za

svaku komunikacijsku aktivnost na Internetu koja

92

00:11:37,733 --> 00:11:40,233

se može smatrati štetnom kako za pojedinca, tako

i za opće dobro.

93

00:11:40,233 --> 00:11:48,033

Tim oblikom nasilja djeca su izložena napadu

drugog djeteta, tinejdžera ili grupe djece, putem

interneta ili mobilnog telefona.

94

00:11:48,033 --> 00:11:56,766

Danas je takav način zastrašivanja poprilično

lagan s obzirom na sve sustave istovremenih

poruka, chatova, foruma i sl. i to uglavnom iz

95

00:11:56,766 --> 00:12:08,332

razloga jer se takva komunikacija odvija pod

"maskama" odnosno nadimcima, a bez

mogućnosti utvrđivanja pravoga

96

00:12:08,333 --> 00:12:14,566

identiteta.O dokazivanju identiteta smo govorili

koju minutu ranije, međutim takav način je malo

vjerojatan za forume, chatove i sl. pa nam i dalje

97

00:12:14,566 --> 00:12:20,666

kod korištenja tih alata odnosno web tehnologija

ne ostaje ništa drugo doli oprez.

98

00:12:20,666 --> 00:12:24,899

Lekcija je završena.

Lekcija\_3\_1\_7

1

00:00:00,000 --> 00:00:08,233

Dobro došli. U ovoj lekciji naučit ćemo što se krije iza skraćenice AAA te što su to botneti.

2

00:00:08,233 --> 00:00:19,199

U prethodnim poglavljima smo naučili da svaka informacija ima vrijednost pa analogno tomu možemo zaključiti da onaj tko ima pristup

3

00:00:19,200 --> 00:00:21,133

informacijama ima i moć.

4

00:00:21,133 --> 00:00:29,333

Danas pristup informacijama smatramo jednim od osnovnih prava čovjeka, a upravo je računalo ono koje nam to omogućava.

5

00:00:29,333 --> 00:00:37,133

Osim pristupa informacijama, pobrojat ćemo i ostale prednosti umrežavanja računala i korištenja računalnih mreža.

6

00:00:37,133 --> 00:00:40,133

Prednosti umrežavanja računala su slijedeće:

7

00:00:40,133 --> 00:00:47,199

Razmjena podataka – korisnici čija su računala povezana u mrežu mogu razmjenjivati podatke odnosno datoteke.

8

00:00:47,200 --> 00:00:57,700

Dijeljenje datoteka – Ukoliko smo povezani u računalnu mrežu, osim datoteka koje se nalaze na našem računalu, možemo se koristiti i datotekama

9

00:00:57,700 --> 00:01:00,366

koje se nalaze na drugim računalima.

10

00:01:00,366 --> 00:01:10,066

Dijeljenje resursa – umrežavanje računala nam omogućuje korištenje printera koji nisu direktno spojeni na naše računalo.

11

00:01:10,066 --> 00:01:19,132

Racionalizacija troškova – u našim kompanijama odnosno uredima više nije potrebno da svaki korisnik ima svoj printer već se sa jednim

12

00:01:19,133 --> 00:01:23,233

printerom spojenim u mrežu rješava ispis više korisnika.

13

00:01:23,233 --> 00:01:33,299

Pristup Internetu odnosno elektroničkoj pošti – pristup informacijama koje se nalaze na drugim poslužiteljima te brža i lakša komunikacija unutar

14

00:01:33,300 --> 00:01:36,666

neke kompanije uz pomoć elektroničke pošte.

15

00:01:36,666 --> 00:01:45,799

Zbog svega navedenog, kada se na mrežama nalaze podatci koje je potrebno zaštiti od zlonamjernih programa, vrlo je bitna i uloga

16

00:01:45,800 --> 00:01:47,833

mrežnih administratora.

17

00:01:47,833 --> 00:01:57,633

Oni se koriste tzv. mrežnim okvirom (eng. Framework) koji se skriva iza skraćenice AAA. Negdje ćemo se susresti i sa terminom „Triple A“.

18

00:01:57,633 --> 00:02:14,333

Skraćenica AAA dolazi od termina „Authentication“, Autorization“ i „Accounting“. Sve skupa čini okvir koji mrežni administratori koriste

19

00:02:14,333 --> 00:02:18,199

za inteligentno kontroliranje pristupa računala mrežnim resursima.

20

00:02:18,200 --> 00:02:25,400

Kroz ta pravila definiraju pravila „ponašanja na mreži“, pri čemu se ta pravila odnose i na računala i na ljude.

21

00:02:25,400 --> 00:02:35,333

Također kroz takav način rada omogućavaju nadzor mreže i skupljanje zapisnika događaja odnosno log datoteka te informacija za kreiranje

22

00:02:35,333 --> 00:02:41,566

računa korištenja mreže. Pri čemu se ovo zadnje uglavnom odnosi za pristup javnim mrežama.

23

00:02:41,566 --> 00:02:49,599

Sve spomenuto daje mogućnosti za efektivno upravljanje mrežom, a prvenstveno daje mogućnost za bolji nadzor sigurnosti mreže.

24

00:02:49,600 --> 00:03:00,833

Koliko je bitno voditi računa o sigurnosti i pravima pristupa mreži te dobrom upravljanju računalima koja istoj pristupaju vidi se iz opasnosti u obliku

25

00:03:00,833 --> 00:03:06,999

zlonamjernih programa koje zovemo „botnetima“ odnosno vojskom zombija.

26

00:03:07,000 --> 00:03:15,966

Vojskom zombija naziva se veći broj računala, koja uglavnom sudjeluju u radu na javnoj mreži odnosno Internetu, pri čemu ta računala mogu

27

00:03:15,966 --> 00:03:20,966

prosljeđivati veliku količinu ne željenih informacija odnosno spama ili virusa.

28

00:03:20,966 --> 00:03:32,266

Ovo se uglavnom dešava bez znanja vlasnika tih računala. Većina takvih računala koja su zaražena na taj način pripada tzv. kućnim računalima i to

29

00:03:32,266 --> 00:03:39,266

upravo iz razloga što u našim mrežama, uglavnom, ne primjenjujemo tzv. AAA koncept.

30

00:03:39,266 --> 00:03:47,466

Ovakvoj zarazni ovom vrstom zlonamjernog programa uglavnom pogoduje nedovoljno dobro konfiguriran vatrozid.

31

00:03:47,466 --> 00:03:51,266

Lekcija je završena.