# Vrste računalnih mreža

1

00:00:00,000 --> 00:00:09,900

Dobrodošli. U ovom videu naučit ćemo koje vrste računalnih mreža postoje.

2

00:00:09,900 --> 00:00:20,100

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

3

00:00:20,100 --> 00:00:29,533

informacijama ima i moć. Danas pristup informacijama smatramo jednim od osnovnih prava čovjeka, a upravo je računalo ono koje nam

4

00:00:29,533 --> 00:00:31,966

to omogućava.

5

00:00:31,966 --> 00:00:39,432

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

6

00:00:39,433 --> 00:00:47,833

Prednosti umrežavanja računala su slijedeće: Razmjena podataka – korisnici čija su računala povezana u mrežu mogu razmjenjivati podatke

7

00:00:47,833 --> 00:00:57,033

odnosno datoteke; Dijeljenje datoteka – Ukoliko smo povezani u računalnu mrežu, osim datoteka koje se nalaze na našem računalu, možemo se

8

00:00:57,033 --> 00:01:00,299

koristiti i datotekama koje se nalaze na drugim računalima; Dijeljenje resursa – umrežavanje računala nam omogućuje korištenje printera koji

9

00:01:00,300 --> 00:01:03,966

nisu direktno spojeni na naše računalo; Racionalizacija troškova – u našim kompanijama odnosno uredima više nije potrebno da svaki

10

00:01:03,966 --> 00:01:06,966

korisnik ima svoj printer već se sa jednim printerom spojenim u mrežu rješava ispis više korisnika; Pristup Internetu odnosno elektroničkoj

11

00:01:06,966 --> 00:01:09,166

pošti – pristup informacijama koje se nalaze na drugim poslužiteljima te brža i lakša komunikacija unutar neke kompanije uz pomoć elektroničke

12

00:01:09,166 --> 00:01:11,099

pošte.

13

00:01:11,100 --> 00:01:15,666

Računalna mreža nastaje povezivanjem dvaju i više mrežnih uređaja (računalo, mrežni pisač i sl.) pa možemo reći da je to skupina međusobno

14

00:01:15,666 --> 00:01:23,532

povezanih uređaja s ciljem omogućivanja međusobne komunikacije odnosno dijeljenja podataka i uređaja kojima se može pristupiti

15

00:01:23,533 --> 00:01:28,133

preko mreže. Jednako tako, danas se računalnom mrežom koristi za stvaranje distribuirane obrade podataka. Razvojem i širokom primjenom osobnih

16

00:01:28,133 --> 00:01:39,233

računala pojavila se mogućnost kreiranja velike količine programa i multimedijalnog sadržaja koje je potrebno dijeliti s drugim korisnicima na mreži.

17

00:01:39,233 --> 00:01:53,999

Prije izgradnje računalnih mreža sadržaj se razmjenjivao uz pomoć prijenosnih medija (magnetske vrpce, diskete, CD ROM i sl.) No s

18

00:01:54,000 --> 00:02:04,533

obzirom na ograničenja medija povezana s veličinom prostora za pohranu podataka, uskoro je takav način postao nedostatan.

19

00:02:04,533 --> 00:02:13,166

Umrežena računala mogu pristupati podacima (datotekama) na drugim računalima, koristiti se perifernim uređajima (npr. mrežni pisač), koristiti

20

00:02:13,166 --> 00:02:19,599

se programima na drugim računalima (npr. zajednički servisi) i pristupati bazama podataka na drugim računalima.

21

00:02:19,600 --> 00:02:30,366

Upravo zbog navedenog, kada se na mreži nalazi puno drugih računala, a dijeljenje resursa (dokumenti, slike, muzika, filmovi i sl.) nikada nije

22

00:02:30,366 --> 00:02:41,932

bilo lakše, prilikom svakog povezivanja na mrežu, a pogotovo na javne mreže (Internet kafići, aerodromi i sl.) postoji mogućnost da naše

23

00:02:41,933 --> 00:02:52,666

računalo bude inficirano malicioznim softverom. Korisnici koji su izolirani i rabe svoja računala bez povezanosti s drugima nemaju mogućnost, prije

24

00:02:52,666 --> 00:03:01,366

svega, dijeliti zajedničke hardverske resurse. Primjenom mrežne tehnologije korisnici imaju potrebnu radnu infrastrukturu, ali bez

25

00:03:01,366 --> 00:03:11,899

nepotrebnoga dodatnog investiranja kompanije u opremu za svakoga pojedinog korisnika (npr. svako računalo ne mora imati svoj pisač, nego

26

00:03:11,900 --> 00:03:18,266

može dijeliti jedan zajednički, mrežni i sl.).

27

00:03:18,266 --> 00:03:29,366

Mreže je moguće podijeliti na nekoliko načina, a nama je zanimljiva podjela prema njihovoj veličini. Računalne mreže možemo podijeliti prema veličini

28

00:03:29,366 --> 00:03:38,532

odnosno fizičkoj rasprostranjenosti korisnika i uređaja u dvije osnovne grupe prikazane na slici u nastavku: LAN (Local Area Network) – lokalna

29

00:03:38,533 --> 00:04:00,299

mreža (Local Area Network) jest mreža uređaja pod kontrolom zajedničke administracije koja uređuje politiku sigurnosti i pristupa. Lokalnu

30

00:04:00,300 --> 00:04:11,000

mrežu čine uređaji povezani na maloj fizičkoj udaljenosti i obično obuhvaća jedno zemljopisno područje, pruža servise za korisnike u zajedničkoj

31

00:04:11,000 --> 00:04:22,833

organizacijskoj strukturi, kao što su tvrtka, kampus ili regija.Lokalna mreža može biti reda veličine od dva do više stotina međusobno povezanih uređaja

32

00:04:22,833 --> 00:04:32,566

koji se nalaze na manjoj ili većoj udaljenosti jedno od drugoga. Primjer lokane mreže je i naša „kućna mreža“ gdje imamo spojeno nekoliko računala s

33

00:04:32,566 --> 00:04:41,599

našim ADSL usmjernikom (router).

34

00:04:41,600 --> 00:04:47,800

WAN (Wide Area Network) – mreža širokog područja (Wide Area Network) jest mreža koja spaja lokalne mreže koje su fizički na različitim

35

00:04:47,800 --> 00:04:56,600

geografskim područjima. U pitanju je mreža uređaja (host) povezanih brzim i sporim vezama.

36

00:04:56,600 --> 00:05:07,400

Dvije podskupine mreža koje na neki način možemo smatrati „hibridnima“ i koje je zapravo teško pravilno svrstati u neku od kategorija jesu:

37

00:05:07,400 --> 00:05:16,666

intranet (često se naziva „lokalni Internet“) – međusobno primjenjuje iste tehnologije kao i Internet, ali pristup imaju samo zaposlenici tvrtke.

38

00:05:16,666 --> 00:05:28,366

On po svojoj veličini spada u LAN mreže, no rabi vrlo sličnu infrastrukturu kao Internet; ekstranet (Extranet) – tip mreže koji biranim vanjskim

39

00:05:28,366 --> 00:05:42,232

korisnicima (partnerima, klijentima itd.) daje pristup ograničenim informacijama tvrtke, npr. sustavu za centralno naručivanje i sl. Ova vrsta

40

00:05:42,233 --> 00:05:54,566

mreže također po svojoj veličini spada u LAN mreže, no s obzirom na to da obično rabi resurse Interneta, također je na granici LAN-a i Interneta.

41

00:05:54,566 --> 00:06:10,499

Uz lokalnu mrežu (LAN), mrežu širokog područja (WAN), razaznajemo i treću vrstu mreža: VPN. Virtualna privatna mreža (VPN, Virtual Private

42

00:06:10,500 --> 00:06:22,633

Network) jest tehnologija koja omogućuje sigurno povezivanje privatnih mreža u zajedničku virtualnu privatnu mrežu preko javne mrežne infrastrukture,

43

00:06:22,633 --> 00:06:33,266

što je danas najčešće Internet. Ostvaruje se siguran „tunel“ između dvije krajnje točke. Kod tuneliranja se provode kompresija i šifriranje

44

00:06:33,266 --> 00:06:35,966

podataka.

45

00:06:35,966 --> 00:06:44,399

Lekcija je završena.

# Važnost zahtjeva za lozinkom pri pristupu bežičnoj mreži

1

00:00:00,000 --> 00:00:11,600

Dobrodošli. U slijedećem videu ćemo naučiti zašto je bežične računalne potrebno mreže štiti lozinkom.

2

00:00:11,600 --> 00:00:20,700

Bežične računalne mreže pojavile su se

devedesetih godina prošlog stoljeća kada su

proizvođači počeli nuditi proizvode koji su radili na

3

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

frekvenciji od 900 MHz. Brojne prednosti ovih

proizvoda postale su odmah vidljive: mobilnost

korisnika i zaposlenika koji su u stanju obavljati

4

00:00:29,800 --> 00:00:39,500

svoje aktivnosti s bilo kojeg mjesta; smanjenje

troškova jer više nije potrebno ulagati u fizičku

povezanost radnih mjesta zaposlenika s internom

5

00:00:39,500 --> 00:00:45,733

računalnom mrežom korporacije; fleksibilnost i

jednostavnost,

6

00:00:45,733 --> 00:00:59,199

Mrežne sastavnice bežičnih računalnih mreža

jesu:radna stanica – uređaj na bežičnoj računalnoj

mreži. Tipični primjeri takvog uređaja jesu

7

00:00:59,200 --> 00:01:07,966

prijenosna računala odnosno drugi mobilni uređaji

poput npr. mobilnih telefona, PDA uređaja ili drugih

elektroničkih uređaja;pristupni uređaj (Access

8

00:01:07,966 --> 00:01:16,499

Point) – logički povezuje jednu ili više radnih

stanica.

9

00:01:16,500 --> 00:01:29,100

Navedene mrežne sastavnice mogu biti spojene s

pomoću dvije osnovne mrežne topologije pa tako

postoje ad hoc i infrastrukturna topologija. Ad hoc

10

00:01:29,100 --> 00:01:40,866

topologija – u ovom se slučaju bežična mreža

uspostavlja isključivo između različitih radnih

stanica (prijenosno računalo, mobitel ili drugo

11

00:01:40,866 --> 00:01:51,299

prijenosno računalo), bez upotrebe pristupnih

uređaja. Ovaj način rada koji se još često naziva i

engl. peer-to-peer i omogućuje izravnu

12

00:01:51,300 --> 00:02:04,166

komunikaciju između dva bežična uređaja.Infrastrukturna topologija – u slučaju infrastrukturne

arhitekture bežične mreže sastoji se od jednog ili

13

00:02:04,166 --> 00:02:13,966

više pristupnih uređaja (Access point) te jedne ili

više radnih stanica.

14

00:02:13,966 --> 00:02:23,832

Uz klasične zahtjeve za sigurnost koji se

postavljaju i pred žične, fizičke računalne mreže,

zbog prirode djelovanja bežične su računalne

15

00:02:23,833 --> 00:02:34,599

mreže podložne čitavom nizu prijetnji koje se ne

mogu ostvariti nad fizičkim računalnim mrežama.

U nastavku ovog modula dani su primjeri prijetnji

16

00:02:34,600 --> 00:02:44,100

za bežične računalne mreže te zahtjevi za

sigurnost koji se postavljaju pred njih.Klasični zahtjevi za sigurnost koji se postavljaju

17

00:02:44,100 --> 00:02:52,633

pred bežične mreže, a zahtijevaju određene radnje

od administratora sustava, uključuju:povjerljivost

(Confidentiality), koja osigurava da mrežnu

18

00:02:52,633 --> 00:03:03,599

komunikacija ne mogu nadgledati neautorizirani

korisnici; integritet (Integrity), čiji je cilj otkriti bilo

kakve namjerne ili nenamjerne promjene podataka

19

00:03:03,600 --> 00:03:14,700

koji se prenose. Integritet je posebno bitan kod

bežičnih računalnih mreža jer tehnologija prijenosa

podataka sama po sebi može unijeti smetnje u

20

00:03:14,700 --> 00:03:25,933

prenošene podatke što narušava njihov

integritet;dostupnost (Availability), čime se postiže

da svi uređaji i korisnici koji pristupaju bežičnoj

21

00:03:25,933 --> 00:03:32,066

računalnoj mreži mogu to ostvariti kada im je god

potrebno.

22

00:03:32,066 --> 00:03:42,632

Uz ove zahtjeve postoji cijeli niz prijetnji za bežične

računalne mreže od kojih su neke prijetnje

svojstvene i prisutne bez obzira na prijenosni

23

00:03:42,633 --> 00:03:55,466

medij (bežično, žičano), a druge su specifične

zbog bežičnog rada ovakvih mreža: napadi

uskraćivanja resursa (Denial of Service) –

24

00:03:55,466 --> 00:04:02,532

napadač onemogućuje ili ograničava pristup

bežičnoj mreži što utječe na sve radne stanice

koje se koriste navedenim pristupnim

25

00:04:02,533 --> 00:04:09,766

uređajem;prisluškivanje mrežnog prometa

(Eavesdropping) – zbog prirode medija koji se

rabi za prijenos podataka napadač može pasivno

26

00:04:09,766 --> 00:04:22,099

nadgledati sav mrežni promet razmijenjen između

pristupnog uređaja i radne stanice i time „vidjeti“

svu našu aktivnost na Internetu;

27

00:04:22,100 --> 00:04:33,733

 Man-in-the-Middle napadi – napadač

se aktivno predstavlja kao jedan ili više uređaja

prisutnih na bežičnoj računalnoj mreži. Klasičan

28

00:04:33,733 --> 00:04:45,166

slučaj napada jest lažiranje pristupne točke, kada

se napadač svim korisnicima bežične računalne

mreže predstavlja kao njihova pristupna točka. Na

29

00:04:45,166 --> 00:04:58,399

ovaj način napadač postiže da sav mrežni promet

prolazi kroz njega te ga može pregledavati i po

želji modificirati;prikrivanje (Masquerading) –

30

00:04:58,400 --> 00:05:07,533

slučaj u kojemu se napadač predstavlja kao

autorizirani korisnik bežične računalne mreže ne bi

li ostvario pristup podacima ili servisima na

31

00:05:07,533 --> 00:05:16,833

mreži;promjena podataka (Message Modification)

– Napadač mijenja legitimnu poruku (mrežni

paket) u smislu brisanja, dodavanja, mijenjanja ili

32

00:05:16,833 --> 00:05:27,999

promjene redoslijeda podataka u poruci. Ova

prijetnja općenito označuje bilo koju prijetnju

integritetu podataka koji se prenose bežičnom

33

00:05:28,000 --> 00:05:32,066

računalnom mrežom; analiza mrežnog prometa

(Traffic Analysis) – zbog prirode medija koji se

rabi kod bežičnih računalnih mreža, bilo koji

34

00:05:32,066 --> 00:05:41,099

napadač koji je u dometu jednog od dvaju uređaja

koji komuniciraju preko bežične računalne mreže

(bez obzira na to je li riječ o ad hoc ili

35

00:05:41,100 --> 00:05:44,700

infrastrukturnom načinu rada) može pasivno

prikupljati mrežni promet te provoditi njegovu

analizu.

36

00:05:44,700 --> 00:05:56,533

Kao što se može vidjeti iz rečenog, većina prijetnji

dolazi zbog toga što napadač ima pristup mediju

kojem se prenose podaci. Ovo je i ključna razlika

37

00:05:56,533 --> 00:06:08,333

između zaštite bežičnih i fizičkih, žičnih računalnih

mreža, a to je mogućnost korisnika u presretanju,

nadgledanju i slanju mrežnog prometa u bežičnu

38

00:06:08,333 --> 00:06:18,866

računalnu mrežu bez ikakvih ograničenja.Da bi neovlašteni napadač ostvario pristup žičnoj,

fizičkoj računalnoj mreži, obično mora ostvariti

39

00:06:18,866 --> 00:06:28,832

fizički pristup prostorijama kompanije. S bežičnim

računalnim mrežama stvar je drukčija jer se

napadač mora nalaziti samo u dometu bežične

40

00:06:28,833 --> 00:06:34,333

mreže. Ovo znači da vrlo često napadač može

pristupiti bežičnoj računalnoj mreži kompanije i

izvan fizičkih prostorija kompanije odnosno našeg

41

00:06:34,333 --> 00:06:37,733

doma, s obzirom na to da je bežične mreže teško

fizički ograničiti.Upravo zbog svega navedenog,

kako bi se bežične mreže osigurale od

42

00:06:37,733 --> 00:06:45,799

neovlaštenog pristupa, uvode se autentikacija i

kontrola pristupa koje su opisane u nastavku.

Dakle, bitno je napomenuti da su ovo sve više

43

00:06:45,800 --> 00:06:55,966

nego dobri razlozi zbog kojih pristup bežičnim

mrežama moramo štititi lozinkom, kako bi smo

prije svega spriječili nedozvoljeni odnosno

44

00:06:55,966 --> 00:07:00,799

neautorizirani pristup našim podacima.

45

00:07:00,800 --> 00:07:08,266

Lekcija je završena.

# WEP, WPA, MAC

1

00:00:00,000 --> 00:00:11,600

Dobrodošli. U ovom videu ćemo vidjeti koje načine autentikacije možemo korisiti kod spajanja na bežične mreže.

2

00:00:11,600 --> 00:00:22,966

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

3

00:00:22,966 --> 00:00:31,832

ključem. Ovdje je potrebno odmah napomenuti da se nijedan od navedenih načina autentikacije danas ne smatra dovoljno sigurnim.

4

00:00:31,833 --> 00:00:43,133

Otvorena autentikacija jest praktički autentikacija bez ikakvog autentikacijskog mehanizma i smatra se dopuštenim pristupom za sve radne stanice.

5

00:00:43,133 --> 00:00:53,233

Pri ovakvoj se autentikaciji ne provodi prava identifikacija radne stanice, nego se prikupljaju samo sljedeće informacije, koje napadači vrlo

6

00:00:53,233 --> 00:01:05,799

jednostavno mogu krivotvoriti. Prva od njih he Service Set Identifier (SSID). SSID jest ime dodijeljeno bežičnoj računalnoj mreži, odnosno

7

00:01:05,800 --> 00:01:18,233

pristupnoj točki. SSID radnoj stanici omogućuje definiranje bežične računalne mreže kojoj želi pristupiti. Odašilje se u čistom tekstualnom obliku

8

00:01:18,233 --> 00:01:29,499

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

9

00:01:29,500 --> 00:01:40,400

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

10

00:01:40,400 --> 00:02:01,300

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

11

00:02:01,300 --> 00:02:13,000

svakom uređaju dodjeljuje proizvođač. Gotovo svi proizvođači pristupnih točaka administratorima omogućuju definiranje pristupnih listi preko kojih

12

00:02:13,000 --> 00:02:22,600

se pristup bežičnoj računalnoj mreži dopušta samo određenim MAC adresama. No promjena MAC adresa radnih stanica jednostavna je i dostupna

13

00:02:22,600 --> 00:02:33,100

su programska rješenja koja omogućuju jednostavnu promjenu MAC adrese. Zbog navedenog se nedostatka filtriranje prema MAC

14

00:02:33,100 --> 00:02:37,800

adresama smatra nedovoljno dobrim.

15

00:02:37,800 --> 00:02:55,366

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

16

00:02:55,366 --> 00:03:07,466

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

17

00:03:07,466 --> 00:03:10,866

vidjeti) ovaj se način autentikacije ne smatra nimalo sigurnijim od otvorene autentikacije. Detalji autentikacije dijeljenim ključem navedeni su u

18

00:03:10,866 --> 00:03:12,432

nastavku poglavlja.

19

00:03:12,433 --> 00:03:20,699

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

20

00:03:20,700 --> 00:03:25,700

od načina postizanja veće sigurnosti bežičnih mreža.

21

00:03:25,700 --> 00:03:35,433

Provođenje napada na ovakav način autentikacije izrazito je jednostavno. Naime, pasivni napadač može samo prikupljati sav mrežni promet koji vidi

22

00:03:35,433 --> 00:03:55,533

te može, ako prikupi sve pakete vezane za autentikaciju, jednostavno doći do tajnoga, dijeljenog ključa.

23

00:03:55,533 --> 00:04:05,599

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

24

00:04:05,600 --> 00:04:20,400

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

25

00:04:20,400 --> 00:04:23,600

starijim mrežnim uređajima.

26

00:04:23,600 --> 00:04:31,666

Lekcija je završena.

# Povezivanje na mrežu

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 ili WPA2).

20

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

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.