# Sigurnost i rezervne kopije podataka

1

00:00:00,000 --> 00:00:08,800

Dobrodošli. U ovom videu pozabavit ćemo se

izradom rezervne kopije podataka na našem

računalu.

2

00:00:08,800 --> 00:00:18,333

Iako u kompanijama postoji središnja pohrana

podataka i korisnici se uglavnom koriste mrežnom

pohranom, katkad je potrebno napraviti i

3

00:00:18,333 --> 00:00:27,799

sigurnosnu pohranu podataka na računalima.Ova značajka omogućuje obnavljanje stanja,

datoteka, mapa i podataka te aplikacija

4

00:00:27,800 --> 00:00:34,366

operacijskog sustava, periodički ih pohranjujući na

neku drugu lokaciju.

5

00:00:34,366 --> 00:00:47,099

Sigurnosna kopija (backup) ili rezervna kopija je

„slika“ svih ili djelomičnih podataka koji se nalaze

na našem računalu. Izrađuje se u svrhu osiguranja

6

00:00:47,100 --> 00:00:57,600

dostupnosti podataka u slučaju kada je originalni

medij, npr. tvrdi disk oštećen ili izgubljen ili je

računalo zaraženo nekim zloćudnim programom.

7

00:00:57,600 --> 00:01:07,433

Podaci koji čine rezervnu kopiju mogu biti

datoteke i/ili programi. Sigurnosne kopije

podataka mogu sadržavati mediji kao što su

8

00:01:07,433 --> 00:01:14,299

optički disk (CD ili DVD) te vanjski USB disk,

magnetna traka i sl.

9

00:01:14,300 --> 00:01:22,066

Sustav windows 8 podržava izradu tzv. "Prethodne

datoteke" koja se nalazi na

10

00:01:22,066 --> 00:01:25,566

Upravljačka ploča -->

11

00:01:25,566 --> 00:01:28,799

Sustav i sigurnost -->

12

00:01:28,800 --> 00:01:41,300

Prethodne datoteke. Lokacija sigurnosno

pohranjenih podataka nikako ne bi smjela biti tvrdi

disk u našem računalu nego npr. USB tvrdi disk ili

13

00:01:41,300 --> 00:01:48,900

neka mrežna lokacija. Nakon što smo odabrali

neku vanjsku lokaciju, odaberemo "Uključi".

14

00:01:48,900 --> 00:01:57,533

Novost u načinu izrade sigurnosne kopije jest

mogućnost "Prethodne datoteke" unutar sustava

Windows 8. Uz pomoć aplikacije imamo

15

00:01:57,533 --> 00:02:08,299

mogućnost spremanja kopija naših datoteka na

drugi čvrsti disk, USB disk ili na mrežnu lokaciju.Nakon što se opcija Prethodne datoteke omogući,

16

00:02:08,300 --> 00:02:18,833

sustav automatski sprema datoteke svakih sat

vremena na definiranu lokaciju. Predefinirano se

pohranjuju sljedeće mape: Kontakti, Radna

17

00:02:18,833 --> 00:02:27,899

površina, Favoriti.Dodatno se mogu uključiti i: Dokumenti, Glazba,

Slike i Video.

18

00:02:27,900 --> 00:02:41,700

Za povrat datoteka potrebno je s lijeve strane

odabrati: Vrati osobne podatke te odabrati mape i

datoteke koje se želi vratiti.

19

00:02:41,700 --> 00:02:45,300

Lekcija je završena.

# Sigurno uništavanje

1

00:00:00,000 --> 00:00:07,800

Dobrodošli. U ovom videu, naučit ćemo o

sigurnom uništavanju podataka.

2

00:00:07,800 --> 00:00:18,533

Bilo koji podatak obrisan s tvrdog diska s velikom

se vjerojatnošću može vratiti. Naravno, tu se ne

ubraja slanje dokumenata u koš za smeće

3

00:00:18,533 --> 00:00:20,999

gdje je povratak podataka siguran i trenutačan.

4

00:00:21,000 --> 00:00:28,233

Najsigurnije uništavanje podataka s pogona ili

uređaja jest fizičko uništavanje.

5

00:00:28,233 --> 00:00:39,266

S obzirom na to da se podaci ipak mogu povratiti,

pogone odnosno tvrde diskove kojima se više

nećemo koristiti, a sadržavaju povjerljive podatke,

6

00:00:39,266 --> 00:00:49,299

treba trajno uništiti. U nastavku će biti opisani

načini kako podatke trajno uništiti kako bi smo se

osigurali od toga da ih zlonamjerna osoba pokuša

7

00:00:49,300 --> 00:00:52,833

oporaviti odnosno povratiti.

8

00:00:52,833 --> 00:01:03,533

Mogućnost povratka obrisanih podataka iznimno

je korisna u slučajevima kada ne postoji njihova

sigurnosna kopija, no katkad želimo biti sigurni da

9

00:01:03,533 --> 00:01:13,399

povrat obrisanih podataka neće biti moguć,

odnosno da su podaci trajno i sigurno obrisani, a u

takvim se situacijama najčešće nalazimo kod

10

00:01:13,400 --> 00:01:22,500

otpisa informatičke opreme.Upravo uz

(neovlašteni) povrat podataka, uglavnom sa

otpisane opreme, vežemo i pojam iskopavanja

11

00:01:22,500 --> 00:01:31,866

informacija (Information diving).Iskopavanje informacija je način oporavka

informacija sa različitih medija za pohranu

12

00:01:31,866 --> 00:01:41,666

podataka, poput diskova, memorijskih kartica i sl.

Uglavnom se pokušavaju „iskopati“ povjerljive

informacije koje imaju nekakvu vrijednost i to u

13

00:01:41,666 --> 00:01:53,499

slučajevima kada su takvi uređaji odneseni na

različita reciklažna dvorišta. Na taj se način

pokušava doći do različitih podataka

14

00:01:53,500 --> 00:02:00,700

u programima za obradu teksta i sl., a često se

pokušavaju iskopati i informacije poput informacija

o kreditnim karticama te različiti

15

00:02:00,700 --> 00:02:02,700

osobni podaci.

16

00:02:02,700 --> 00:02:11,500

Ako govorimo o opremi koja je poslana na

uništenje iz neke od kompanija, u takvim

slučajevima zlonamjerne osobe pokušavaju

17

00:02:11,500 --> 00:02:20,166

„iskopavanjem“ doći do korisničkih podataka te ih

na taj način ukrasti. Drugim riječima,

iskopavanjem informacija smatramo pretraživanje

18

00:02:20,166 --> 00:02:27,766

odbačenih odnosno otpisanih računala i ostale

informatičke opreme u potrazi za informacijama.

19

00:02:27,766 --> 00:02:38,532

Upravo iz tih razloga, vrlo je bitno da otpisane elektroničke medije (diskove, memorijske kartice,

optičke i magnetske medije) sigurno obrišemo.

20

00:02:38,533 --> 00:02:47,333

Kada se govori o sigurnom brisanju, susrećemo se sa sljedećim pojmovima. Sigurno brisanje

(Cleaning) – postupak nepovratnog brisanja

21

00:02:47,333 --> 00:02:56,433

podataka s medija nakon kojeg je moguća ponovna upotreba tog medija za pohranu

podataka. Sanitacija podataka (Sanitization) –

22

00:02:56,433 --> 00:03:06,133

postupak brisanja podataka s medija ili fizičko uništavanje medija na kojem su pohranjeni podaci

tako da više nije moguć povrat podataka.

23

00:03:06,133 --> 00:03:18,799

Pri odabiru rješenja sistemski administratori

moraju pozorno provjeriti njegove specifikacije, no

nakon operacije brisanja obvezno treba provjeriti

24

00:03:18,800 --> 00:03:30,966

jesu li podaci doista obrisani, i to upotrebom

nekog od alata za povratak obrisanih podataka.

25

00:03:30,966 --> 00:03:34,932

Jedna od najbržih i najpouzdanijih metoda brisanja

tvrdih diskova jest demagnetizacija pri čemu se medij briše

26

00:03:34,933 --> 00:03:41,233

izlaganjem jakom istosmjernom polju jakosti i do

nekoliko tisuća Oersteda (Oe).

27

00:03:41,233 --> 00:03:52,166

CD/DVD medije trajno uništavamo s pomoću tzv.

rezačica koje ih sijeku na tanke, neupotrebljive

listiće.

28

00:03:52,166 --> 00:03:55,766

Lekcija je završena.