Lekcija\_6\_1\_1

1

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

Dobrodošli. U ovom videu pozabavit ćemo se izradom rezervne kopije podataka na našemračunalu.

2

00:00:09,800 --> 00:00:20,500

Iako u kompanijama postoji središnja pohranapodataka i korisnici se uglavnom koriste mrežnompohranom, katkad je potrebno napraviti i

3

00:00:20,500 --> 00:00:31,600

sigurnosnu pohranu podataka na računalima.Ova značajka omogućuje obnavljanje stanja,datoteka, mapa i podataka te aplikacija

4

00:00:31,600 --> 00:00:37,366

operacijskog sustava, periodički ih pohranjujući naneku drugu lokaciju.

5

00:00:37,366 --> 00:00:50,632

Sigurnosna kopija (backup) ili rezervna kopija je„slika“ svih ili djelomičnih podataka koji se nalazena našem računalu. Izrađuje se u svrhu osiguranja

6

00:00:50,633 --> 00:01:02,566

dostupnosti podataka u slučaju kada je originalnimedij, npr. tvrdi disk oštećen ili izgubljen ili jeračunalo zaraženo nekim zloćudnim programom.

7

00:01:02,566 --> 00:01:13,632

Podaci koji čine rezervnu kopiju mogu bitidatoteke i/ili programi. Sigurnosne kopijepodataka mogu sadržavati mediji kao što su

8

00:01:13,633 --> 00:01:20,766

optički disk (CD ili DVD) te vanjski USB disk,magnetna traka i sl.

9

00:01:20,766 --> 00:01:28,566

Sustav windows 8 podržava izradu tzv. "Prethodnedatoteke" koja se nalazi na

10

00:01:28,566 --> 00:01:31,932

Upravljačka ploča -->

11

00:01:31,933 --> 00:01:35,033

Sustav i sigurnost -->

12

00:01:35,033 --> 00:01:37,466

Prethodne datoteke.

13

00:01:37,466 --> 00:01:50,466

Lokacija sigurnosno pohranjenih podataka nikako ne bi smjela biti tvrdi disk u našem računalu nego npr. USB tvrdi disk ili neka druga mrežna lokacija.

14

00:01:50,466 --> 00:02:00,432

Nakon što smo odabrali neku vanjsku lokaciju, npr. USB tvrdi disk odaberemo "Uključi".

15

00:02:00,433 --> 00:02:07,466

Novost u načinu izrade sigurnosne kopije jestmogućnost "Prethodne datoteke" unutar sustavaWindows 8.

16

00:02:07,466 --> 00:02:16,732

Uz pomoć aplikacije imamo mogućnost spremanja kopija naših datoteka nadrugi čvrsti disk, USB disk ili na mrežnu lokaciju.

17

00:02:16,733 --> 00:02:26,733

Nakon što se opcija Prethodne datoteke omogući,sustav automatski sprema datoteke svakih satvremena na definiranu lokaciju. Predefinirano se

18

00:02:26,733 --> 00:02:36,899

pohranjuju sljedeće mape: Kontakti, Radnapovršina, Favoriti.Dodatno se mogu uključiti i: Dokumenti, Glazba,

19

00:02:36,900 --> 00:02:51,733

Slike i Video. Kako ne bi ostali bez naših važnih privatnih dokumenata, fotografija i sl. bitno je u pohranjivanje uključiti i mapu Dokumenti, Slike

20

00:02:51,733 --> 00:02:57,733

odnosno Video te sve važne dokumente spremati u mapu Dokumenti.

21

00:02:57,733 --> 00:03:08,133

Za povrat datoteka potrebno je s lijeve straneodabrati: Vrati osobne podatke te odabrati mape idatoteke koje se želi vratiti.

22

00:03:08,133 --> 00:03:17,999

Dobro je ovu opciju koristiti u redovitim intervalima, iako dokumente i nismo izgubili, kako bi se uvjerili da izrada "Prethodne datoteke"

23

00:03:18,000 --> 00:03:23,933

uredno funkcionira.

24

00:03:23,933 --> 00:03:32,433

Dodatno, možemo odabrati vremenski interval nakon kojeg će se vršiti pregled novih ili mijenjanih datoteka te njihovo pohranjivanje.

25

00:03:32,433 --> 00:03:40,533

To mijenjamo odabirom opcije, s lijeve strane, "Dodatne postavke".

26

00:03:40,533 --> 00:03:44,066

Lekcija je završena.

Lekcija\_6\_1\_2

1

00:00:00,000 --> 00:00:07,866

Dobrodošli. U ovom videu, učit ćemo o sigurnom uništavanju podataka.

2

00:00:07,866 --> 00:00:18,166

Bilo koji podatak obrisan s tvrdog diska s velikomse vjerojatnošću može vratiti. Naravno, tu se neubraja slanje dokumenata u koš za smeće

3

00:00:18,166 --> 00:00:27,366

gdje je povratak podataka siguran i trenutačan.Najsigurnije uništavanje podataka s pogona iliuređaja jest fizičko uništavanje.

4

00:00:27,366 --> 00:00:40,266

S obzirom na to da se podaci ipak mogu povratiti,pogone odnosno tvrde diskove kojima se višenećemo koristiti, a sadržavaju povjerljive podatke,

5

00:00:40,266 --> 00:00:42,399

treba trajno uništiti.

6

00:00:42,400 --> 00:00:51,566

U nastavku će biti opisaninačini kako podatke trajno uništiti kako bi smo seosigurali od toga da ih zlonamjerna osoba pokuša

7

00:00:51,566 --> 00:01:02,566

oporaviti odnosno povratiti.Mogućnost povratka obrisanih podataka iznimnoje korisna u slučajevima kada ne postoji njihova

8

00:01:02,566 --> 00:01:12,566

sigurnosna kopija, no katkad želimo biti sigurni dapovrat obrisanih podataka neće biti moguć,odnosno da su podaci trajno i sigurno obrisani, a u

9

00:01:12,566 --> 00:01:17,066

takvim se situacijama najčešće nalazimo kodotpisa informatičke opreme.

10

00:01:17,066 --> 00:01:28,266

Upravo uz (neovlašteni) povrat podataka, uglavnom s otpisane opreme, vežemo i pojam iskopavanja informacija (Information diving).

11

00:01:28,266 --> 00:01:40,866

Iskopavanje informacija je način oporavka informacija s različitih medija za pohranupodataka, poput diskova, memorijskih kartica i sl.

12

00:01:40,866 --> 00:01:52,332

Uglavnom se pokušavaju „iskopati“ povjerljiveinformacije koje imaju nekakvu vrijednost i to uslučajevima kada su takvi uređaji odneseni na

13

00:01:52,333 --> 00:02:02,799

različita reciklažna dvorišta. Na taj se načinpokušava doći do različitih podataka u programima za obradu teksta i sl., a često se

14

00:02:02,800 --> 00:02:09,233

pokušavaju iskopati i informacije poput informacijao kreditnim karticama te različiti osobni podaci.

15

00:02:09,233 --> 00:02:19,233

Ako govorimo o opremi koja je poslana nauništenje iz neke od kompanija, u takvimslučajevima zlonamjerne osobe pokušavaju

16

00:02:19,233 --> 00:02:27,699

„iskopavanjem“ doći do korisničkih podataka te ihna taj način ukrasti. Drugim riječima,iskopavanjem informacija smatramo pretraživanje

17

00:02:27,700 --> 00:02:37,300

odbačenih odnosno otpisanih računala i ostaleinformatičke opreme u potrazi za informacijama.Upravo iz tih razloga, vrlo je bitno da otpisane

18

00:02:37,300 --> 00:02:46,833

elektroničke medije (diskove, memorijske kartice,optičke i magnetske medije) sigurno obrišemo.Kada se govori o sigurnom brisanju, susrećemo

19

00:02:46,833 --> 00:02:55,533

se sa sljedećim pojmovima. Sigurno brisanje(Cleaning) – postupak nepovratnog brisanjapodataka s medija nakon kojeg je moguća

20

00:02:55,533 --> 00:03:04,433

ponovna upotreba tog medija za pohranupodataka. Sanitacija podataka (Sanitization) –postupak brisanja podataka s medija ili fizičko

21

00:03:04,433 --> 00:03:14,433

uništavanje medija na kojem su pohranjeni podacitako da više nije moguć povrat podataka.Pri odabiru rješenja sistemski administratori

22

00:03:14,433 --> 00:03:24,799

moraju pozorno provjeriti njegove specifikacije, nonakon operacije brisanja obvezno treba provjeritijesu li podaci doista obrisani, i to upotrebom

23

00:03:24,800 --> 00:03:35,666

nekog od alata za povratak obrisanih podataka.

24

00:03:35,666 --> 00:03:44,232

Jedna od najbržih i najpouzdanijih metoda brisanja tvrdih diskova jest demagnetizacija pri čemu se medij briše izlaganjem jakom

25

00:03:44,233 --> 00:03:49,833

istosmjernom polju jakosti i do nekoliko tisuća Oersteda (Oe).

26

00:03:49,833 --> 00:04:00,599

CD/DVD medije trajno uništavamo s pomoću tzv.rezačica koje ih sijeku na tanke, neupotrebljivelistiće.

27

00:04:00,600 --> 00:04:10,333

Za razliku od ovih profesionalnih alata, poput uređaja za demagnetizaciju ili rezačica, na raspolaganju imamo i softverske alate.

28

00:04:10,333 --> 00:04:18,566

Premda su alati specijalizirani za nepovratno brisanje podataka s magnetskih medija potrebni tek u specifičnim okolnostima, jedan od primjera

29

00:04:18,566 --> 00:04:30,366

kada nam je potreban je prilikom prodaje diska.Klasičnim načinom brisanja datoteka ona zapravo fizički nije obrisana. Naime, prostor na disku na

30

00:04:30,366 --> 00:04:39,066

na kojem se nalazila netom obrisana datoteka, sa gledišta datotečnog sustava, biti će samo označen slobodnim za ponovno zapisivanje.

31

00:04:39,066 --> 00:04:48,366

Naime, brisanjem podatka samo se uklanjaju putanje do podataka. U međuvremenu, podaci koji su sačinjavali datoteku koja je prethodno

32

00:04:48,366 --> 00:04:52,566

zauzimala taj prostor i dalje će biti pohranjeni na disku.

33

00:04:52,566 --> 00:05:04,266

Formatiranje kao ni brisanje i rekreiranje particija ne pomaže jer uvijek postoje načini kako povratiti datoteka čak i unatoč tim naizgled destruktivnim

34

00:05:04,266 --> 00:05:05,532

operacijama.

35

00:05:05,533 --> 00:05:19,866

Primjeri programa s kojim trajno i nepovratno možemo uništiti podatke je Hardwipe. (http://www.hardwipe.com/) ili Eraser (

36

00:05:19,866 --> 00:05:27,432

http://sourceforge.net/projects/eraser/).

37

00:05:27,433 --> 00:05:35,699

Nakon što smo naše magnetske medije, tretirali sa jednim od takvih programa, sigurno ćemo ga moći proslijediti odnosno prodati nekome

38

00:05:35,700 --> 00:05:37,700

drugome.

39

00:05:37,700 --> 00:05:41,566

Lekcija je završena.