# Razlika između podatka i informacije

1

00:00:00,000 --> 00:00:09,533

Dobrodošli. U ovom videu saznat ćete što je to podatak, a što informacija i po čemu se razlikuju.

2

00:00:09,533 --> 00:00:19,399

Za podatak kažemo da je jednostavna neobrađena i izolirana misaona činjenica koja ima neko značenje. Podatak je nematerijalne prirode.

3

00:00:19,400 --> 00:00:28,600

Objašnjenje poveznice između podatka i informacije te znanja i mudrosti dugo je predmet istraživanja. Jedan od modela je i DIKW piramida

4

00:00:28,600 --> 00:00:37,366

koju bismo, vrlo općenito, mogli objasniti kao činjenicu da iz podataka dobivamo informacije na osnovi kojih gradimo znanje i u konačnici

5

00:00:37,366 --> 00:00:48,366

postajemo mudriji. Za lakše shvaćanje rečenog, primjeri podataka su: Crveno. A1. Split. Zadar. Dobivene informacije iz

6

00:00:48,366 --> 00:00:59,599

navedenog jesu: Crveno svjetlo na semaforu, na ulazu u tunel na autocesti A1. Znanje odnosno kontekst napisanog jest: Upalilo se crveno svjetlo

7

00:00:59,600 --> 00:01:09,200

na prometnici na kojoj se nalazim. A mudrost koju bismo primijenili bila bi: Moram zaustaviti vozilo.Usredotočit ćemo se još na razliku između

8

00:01:09,200 --> 00:01:15,900

podatka i informacije.Dok je podatak jednostavna neobrađena i izolirana misaona činjenica

9

00:01:15,900 --> 00:01:25,233

Informacija je rezultat analize i organizacije podataka u smislu da daje novo znanje primatelju.Konstatacija da iz podataka dobivamo informaciju

10

00:01:25,233 --> 00:01:36,566

na temelju kojih se gradi znanje, dovoljan je pokazatelj zašto je danas namjera velikog broja ljudi upravo te podatke otuđiti.

11

00:01:36,566 --> 00:01:40,299

Lekcija je završena.

# Što je to kibernetički kriminal?

1

00:00:00,000 --> 00:00:10,266

Dobrodošli. U ovom videu saznat ćemo što je to kibernetički kriminal.Pri korištenju računalom vrlo je važno shvatiti ovu

2

00:00:10,266 --> 00:00:17,399

činjenicu: kako je naše računalo povezano s Internetom, jednako je tako i Internet „povezan“ s našim računalom.

3

00:00:17,400 --> 00:00:25,466

Odnosno, kako mi možemo do različitih sadržaja na Internetu, tako maliciozna osoba može do sadržaja na našem računalu.

4

00:00:25,466 --> 00:00:34,499

Danas smo svi svjesni i mogućnosti i prednosti Interneta. No osim svih prednosti koje nam pruža, omogućio je i nastanak nove vrste kriminala koji

5

00:00:34,500 --> 00:00:42,000

danas nazivamo kibernetičkim kriminalom.S obzirom na to da je „nastanak“ Interneta relativno nov događaj, još uvijek nedostaje

6

00:00:42,000 --> 00:00:51,633

dovoljno pravne regulative i učinkovitih zakona.Svaka kompanija ili pojedinac koji sudjeluje u radu na Internetu svakodnevno je izložen riziku od raznih

7

00:00:51,633 --> 00:01:01,399

vrsta napada i inficiranja koji mogu dovesti do krađe i/ili zloupotrebe podataka koji se nalaze na računalu, činjenja štete drugim korisnicima

8

00:01:01,400 --> 00:01:10,100

odnosno krađe identiteta. Sve navedeno predstavlja kriminalne radnje odnosno kibernetički kriminal.

9

00:01:10,100 --> 00:01:17,366

Lekcija je završena.

# Hakiranje, krekiranje i etičko hakiranje

1

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

Dobrodošli. U ovom videu naučit ćemo razlikovati hakere i krekere.Kada je riječ o računalnoj sigurnosti, stručnjaci će

2

00:00:09,000 --> 00:00:16,766

se složiti da pri korištenju informacijskim tehnologijama postoje tri vrste ljudi.Prvi od njih su stručnjaci koji se bave

3

00:00:16,766 --> 00:00:25,799

proučavanjem nepoželjnih i opasnih aktivnosti na Internetu te na osnovi svojih saznanja i rezultata istraživanja preporučuju preventivne mjere i

4

00:00:25,800 --> 00:00:36,900

rješenja (etički hakeri) kako bi se šira javnost, kao druga skupina koja osjeća posljedice sigurnosnih provala i krađe identiteta, obranila od treće

5

00:00:36,900 --> 00:00:47,200

skupine ljudi (hakeri odnosno krekeri). Kada govorimo o trećoj skupini ljudi, uglavnom je riječ o anonimnim počiniteljima raznih napada i

6

00:00:47,200 --> 00:00:56,000

nedjela. Treća se skupina u svakodnevnom govoru i dnevnom tisku naziva hakerima. Nekada je biti prozvan hakerom značilo čast i

7

00:00:56,000 --> 00:01:06,466

odnosilo se na nešto pozitivno te je označivalo da je osoba vješta u računalnom programiranju.Etički su hakeri obično programeri, no ne nužno

8

00:01:06,466 --> 00:01:15,432

jer mogu biti i sistemski administratori. Posjeduju napredno znanje o operacijskim sustavima i programskim jezicima. To im omogućuje da

9

00:01:15,433 --> 00:01:26,099

otkrivaju rupe i propuste u sustavima te uzroke tih propusta. Spadaju u, na početku lekcije spomenutu, prvu skupinu ljudi.

10

00:01:26,100 --> 00:01:33,133

Osoba koja „provaljuje“ u tuđa računala jest kreker (Cracker, crack – razbiti).

11

00:01:33,133 --> 00:01:39,699

Lekcija je završena.

# Nisu svi hakeri stručnjaci, niti su svi zlonamjerni…

1

00:00:00,000 --> 00:00:09,733

Dobrodošli. U ovom videu upoznat ćemo se sa različitim namjerama koje se skrivaju iza malicioznih napada na Internetu.

2

00:00:09,733 --> 00:00:18,966

Maliciozne radnje na Internetu mogu biti potaknute cijelim spektrom različitih razloga, od obične znatiželje pa do kriminalnih namjera. U moru

3

00:00:18,966 --> 00:00:28,532

različitih asocijacija uz izraz haker ističe se nekoliko skupina ljudi. Tu spadaju, primjerice, programerski geniji koji izmišljaju inovativne

4

00:00:28,533 --> 00:00:41,166

načine kodiranja nekih rješenja, zatim socijalni aktivisti koji poduzimaju određene radnje kao oblik protesta na npr. neka politička zbivanja. I naravno,

5

00:00:41,166 --> 00:00:51,499

treba još navesti kriminalce koji kradu, kontaminiraju ili uništavaju podatke zbog zarade, dokazivanja moći ili čiste pakosti. Jednako tako,

6

00:00:51,500 --> 00:01:01,666

postoji još jedna podjela vezana za motivaciju – podjela na tri skupine koje se označuju po bojama šešira (aluzija na stare kaubojske filmove u kojima

7

00:01:01,666 --> 00:01:12,199

su dobri dečki obično nosili bijele šešire, a loši crne). Tako imamo hakere crnih šešira (black-hat hacker) – hakere sa zlom namjerom da pronađu ili

8

00:01:12,200 --> 00:01:21,800

oštete povjerljive i važne podatke. Druga su krajnost hakeri bijelih šešira (white-hat hacker) – legitimni sigurnosni eksperti sa znanjem i

9

00:01:21,800 --> 00:01:32,133

iskustvom zlonamjernih hakera, no njime se koriste u svrhe zaštite. Treća su skupina hakeri sivih šešira (grey-hat hacker). Oni, kako se

10

00:01:32,133 --> 00:01:41,899

i može iz imena zaključiti, po aktivnostima i motivaciji ne spadaju ni u dobre ni loše, već negdje između. Za njih se smatra da ih više

11

00:01:41,900 --> 00:01:50,400

motivira znatiželja nego zlonamjernost. Redovima hakera sivih šešira često pripadaju ljudi koji su u svojoj prošlosti (adolescentskoj dobi)

12

00:01:50,400 --> 00:02:00,600

pripadali skupini hakera crnih šešira te su, nakon što su ih institucije otkrile u zlonamjernim napadima, zaposlili kao informatički stručnjaci

13

00:02:00,600 --> 00:02:04,766

zaduženi za sigurnost, često i u kompanijama kojima su željeli nanijeti (ili su nanijeli) štetu.

14

00:02:04,766 --> 00:02:06,399

Lekcija je završena.

# Prepoznavanje prijetnji podacima

1

00:00:00,000 --> 00:00:10,233

Dobrodošli.U ovom videu upoznat ćemo se s različitim vidovima opasnosti za naše podatke.

2

00:00:10,233 --> 00:00:20,599

Za računala neki često znaju reći da su u njima

pohranili cijeli život, razne radove, obiteljske

fotografije, različitu korespondenciju, poslovne

3

00:00:20,600 --> 00:00:28,166

podatke… Računalni su sustavi danas osnova poslovanja bilo

koje kompanije i sadržavaju vrlo važne informacije

4

00:00:28,166 --> 00:00:36,899

o poslovanju, zaposlenicima, kupcima, partnerima

i sl.Ugrožavanje njihove sigurnosti, postojanosti i

5

00:00:36,900 --> 00:00:49,800

nepromjenjivosti može dovesti do materijalnih

gubitaka i otkrivanja vrlo osjetljivih podataka o

korisnicima ili poslovanju kompanije.

6

00:00:49,800 --> 00:00:58,733

Nameće se zaključak da je takve podatke potrebno zaštititi. Zbog toga su razvijene različite metode zaštite.

7

00:00:58,733 --> 00:01:07,699

Pod zaštitom podataka najčešće

podrazumijevamo:definiranje i provođenje politike

lozinki (odnosno njihovu kompleksnost),

8

00:01:07,700 --> 00:01:18,066

ovlašćivanje samo određenih osoba koje će imati

pristup povjerljivim podacima, čuvanje integriteta

podataka, tj. da nitko ne može mijenjati podatke

9

00:01:18,066 --> 00:01:30,032

bez dozvole vlasnika podataka, dostupnost i

raspoloživost podataka ovlaštenim osobama kada

im je potrebno te sigurnosnu pohranu podataka.

10

00:01:30,033 --> 00:01:39,399

Računalni je sustav siguran onoliko koliko je

sigurna njegova najslabija karika. U tom se smislu

ne smije zanemariti fizička sigurnost jer nikakav

11

00:01:39,400 --> 00:01:49,766

sustav logičkih kontrola, procedura i pravilnika

neće spasiti sistemsku sobu od poplave ili požara,

neće spriječiti lopova da ukrade nezaštićeno

12

00:01:49,766 --> 00:01:59,132

prijenosno računalo ili računala iz nezaštićenog

ureda ili sistemske sobe.Jedan od aspekata sigurnosti računalnih sustava

13

00:01:59,133 --> 00:02:10,366

danas je i fizička zaštita odnosno fizička sigurnost.

Pod njome se razumijevaju skup mjera, pravila i

procedura koje sprečavaju nedopušteni fizički

14

00:02:10,366 --> 00:02:20,199

pristup informacijama.Prijetnje fizičkoj sigurnosti dolaze od prirodnih

nepogoda kao što su poplave, potres, požar, pa i

15

00:02:20,200 --> 00:02:26,933

rat.Kako bi se smanjila šteta nakon pojavljivanja neke

od spomenutih prijetnji, potrebno je uvesti

16

00:02:26,933 --> 00:02:38,766

odgovarajuće mjere zaštite. Pod mjerama kojima

je cilj smanjenje rizika podrazumijevaju se

osiguranje objekta i okoline te provođenje kontrole

17

00:02:38,766 --> 00:02:49,066

pristupa. Potrebno je također implementirati

zaštitnu opremu i uređaje kao što su alarmni

sustavi, sustavi za video nadzor i kontrolu pristupa,

18

00:02:49,066 --> 00:02:59,832

protupožarnu opremu i sl. Općenito gledajući,

prijetnje za fizičku sigurnost informacijskog

sustava mogu se podijeliti u sljedeće kategorije:

19

00:02:59,833 --> 00:03:16,099

Prirodne prijetnje (poplave, potresi, oluje, šumski požari, ekstremni temperaturni uvjeti i sl.). Infrastrukturne prijetnje/prijetnje iz okoline (prekidi

20

00:03:16,100 --> 00:03:25,433

ili problemi u napajanju električnom energijom,

kvarovi/curenje klimatizacijskih uređaja ili prijetnje

uzrokovane vodovodnim, plinskim i drugim

21

00:03:25,433 --> 00:03:34,966

instalacijama).Ljudske prijetnje koje čine neovlašteni pristup

zaposlenika ili drugih osoba, štete uzrokovane

22

00:03:34,966 --> 00:03:44,499

nepažnjom poput prolijevanje tekućine po

elektroničkoj opremi, unos zabranjenih tvari u

sistemske sobe, te namjerno uništavanje

23

00:03:44,500 --> 00:03:57,133

informacijskih resursa.Društveno uzrokovane prijetnje (ratovi, teroristički napadi, štrajkovi i sl.)

24

00:03:57,133 --> 00:04:06,699

Pri izgradnji novih zgrada ili procjeni rizika na

postojećima treba uzeti u obzir priličan broj

faktora. Prije svega, tu je riječ o konstrukciji

25

00:04:06,700 --> 00:04:16,200

zgrade. Ako je riječ o starijim zgradama, u obzir

treba uzeti činjenicu da su u konstrukcijama

podova i stropova često drvene grede, što

26

00:04:16,200 --> 00:04:25,500

svakako ima utjecaja na nosivost podova, ali i na

otpornost na požare. S obzirom na to da se

Hrvatska, odnosno neki njezini dijelovi mogu

27

00:04:25,500 --> 00:04:36,266

smatrati trusnim područjima, potrebno je uzeti u obzir i seizmičku otpornost zgrada.Jedan od primjer povećanja sigurnosti su

28

00:04:36,266 --> 00:04:48,332

sigurnosna vrata (trap door). To je sustav vrata koji se sastoji od dvaju vrata i jedne među prostorije, gdje oba vrata ne mogu istodobno biti otvorena,

29

00:04:48,333 --> 00:04:58,633

odnosno čovjek ne može proći druga vrata prije

nego što je zatvorio ona prva, a na takve primjere

danas nailazimo u većini financijskih institucija

30

00:04:58,633 --> 00:05:08,066

odnosno banaka.Uz navedene prijetnje, trebali bismo biti svjesni i

prijetnji koje mogu uzrokovati davatelji raznih vrsta

31

00:05:08,066 --> 00:05:16,799

vanjskih usluga te pojedinci koji nisu djelatnici

kompanije.Zajedničko im je da ne pripadaju kompaniji kao

32

00:05:16,800 --> 00:05:26,800

zaposlenici i da potencijalno raspolažu podacima

koji imaju neku vrijednost, a ne pripadaju njima

samima. Kao osnovna, preventivna mjera trebala

33

00:05:26,800 --> 00:05:37,233

bi se isticati zabrana pristupa računalnim

sustavima ili pristup uz jasno definirana

ograničenja te pristup pod nadzorom. Sve ovo

34

00:05:37,233 --> 00:05:45,966

radimo u svrhu sprečavanja gubitka ili uništenja

informacija. I za kraj. Sigurnosni sustav svake kompanije

35

00:05:45,966 --> 00:05:59,366

složen je sustav i čini ga šest slojeva: sigurnosna

politika i procedure, fizička zaštita računalnih

resursa, identifikacija i autentikacija korisnika,

36

00:05:59,366 --> 00:06:09,699

autorizacija korisnika, mjere osiguranja integriteta

podataka, revizija informacijskog sustava.

37

00:06:09,700 --> 00:06:13,066

Lekcija je završena.

# Korisnički računi i lozinke

1

00:00:00,000 --> 00:00:11,500

Dobro došli. U ovoj lekciji upoznat ćemo se sa

korisničkim računima i lozinkama.

2

00:00:11,500 --> 00:00:20,200

U računalnom svijetu, korisnički računi (User

Account) primarno su sredstvo kontroliranja

pristupa podacima i resursima računala. Upravo

3

00:00:20,200 --> 00:00:27,800

zbog toga napadači dobro poznaju osnovne

postavke operacijskog sustava u vezi s

korisničkim računima.

4

00:00:27,800 --> 00:00:37,666

Korisnički račun koji ima potpuni pristup računalu

jest administratorski račun. Za njega kažemo da

ima administratorske ovlasti. Pri instalaciji

5

00:00:37,666 --> 00:00:47,399

operacijskog sustava Windows 8 obvezno je

stvoriti najmanje jedan korisnički račun te svi

računi stvoreni u tom trenutku automatski su

6

00:00:47,400 --> 00:00:57,533

pridruženi grupi koja ima potpuni pristup računalnom sustavu, administratorskoj grupi. Sljedeći, potencijalno opasni detalj je i mogućnost

7

00:00:57,533 --> 00:01:11,399

ne postavljanja lozinke za takve račune. Ako

korisnik ostavi takve postavke „vrata“ računala

širom su otvorena za sve napadače.

8

00:01:11,400 --> 00:01:20,366

Kako bi se korisnik jednoznačno identificirao na

računalu, mora upotrebljavati korisnički račun. Korisnički je račun jedinstveni identitet svakog

9

00:01:20,366 --> 00:01:30,266

korisnika računalnog sustava. On omogućuje

dodjelu određenih prava i privilegija korištenja

dijelovima računalnog sustava. Važno je

10

00:01:30,266 --> 00:01:39,332

napomenuti da bi svaki korisnik trebao imati svoj

korisnički račun, odnosno da ne postoje zajednički

korisnički računi namijenjeni svakodnevnoj

11

00:01:39,333 --> 00:01:43,699

upotrebi.

12

00:01:43,700 --> 00:01:54,133

Korisnički račun, korisniku koji se njime služi

omogućuje identifikaciju odnosno utvrđivanje

identiteta te dozvolu pristupa resursima na

13

00:01:54,133 --> 00:02:03,299

računalu ili računalnoj mreži. Procesi koji omogućuju te dvije radnje nazivaju se

autentikacija i autorizacija.

14

00:02:03,300 --> 00:02:12,500

Autentikacija (Authentication) je proces kojim se

na temelju danih podataka korisnik identificira,

odnosno potvrđuje se njegov identitet. Danas

15

00:02:12,500 --> 00:02:21,700

najrasprostranjeniji način identifikacije uključuje

korisničko ime i lozinku koji su sastavni dio

korisničkog računa.

16

00:02:21,700 --> 00:02:30,500

Autorizacija (Authorization) je proces kojim se

pojedinom korisničkom računu dopuštaju ili

zabranjuju pristup i manipulacija određenim

17

00:02:30,500 --> 00:02:40,400

računalnim resursom.Kada govorimo o računalima s Windows operacijskim sustavima, susrećemo se s dvije

18

00:02:40,400 --> 00:02:49,400

vrste korisničkih računa.Prve nazivamo lokalnim korisničkim računima i

koriste se samo i isključivo za prijavu na računalo

19

00:02:49,400 --> 00:02:57,266

na kojem je i kreiran. Sve informacije o računu

uključujući i lozinku spremaju se u lokalnu

sigurnosnu bazu (Security Accounts Management)

20

00:02:57,266 --> 00:03:07,432

koja se nalazi na tom računalu. Ovakav način

kreiranja računa te prijave na računalo koristimo

uglavnom pri korištenju naših računala u kućnom

21

00:03:07,433 --> 00:03:15,433

okruženju.Drugu vrstu korisničkih računa nazivamo

domenskim korisničkim računima. Svojevrsna su

22

00:03:15,433 --> 00:03:25,666

suprotnost lokalnim korisničkim računima. U tom

slučaju i računala na koja se prijavljujemo, ne

učestvuju u radu na mreži na način kako to imamo

23

00:03:25,666 --> 00:03:38,366

u našim domovima nego su takva računala članovi

domene. Kratko ćemo samo spomenuti da je

domena hijerarhijski način organiziranja, serverski

24

00:03:38,366 --> 00:03:48,666

baziranih, mreža. U tzv. domenskom načinu rada,

postoji centralno poslužiteljsko računalo koje

nazivamo domenskim kontrolorom i tamo su

25

00:03:48,666 --> 00:03:59,332

pohranjeni svi korisnički računi. Ovakav način rada

karakterističan je za većinu kompanija.

26

00:03:59,333 --> 00:04:04,933

Rad u domeni garantira nam veću sigurnost.

27

00:04:04,933 --> 00:04:15,233

Svaki korisnički račun, neovisno o tome radi li se

o lokalnom ili domenskom računu mora obvezno

sadržavati ime kojim se može korisnik

28

00:04:15,233 --> 00:04:25,366

identificirati. Pri imenovanju potrebno se

pridržavati sljedećih naputaka.Ime korisničkog računa (Username) mora biti

29

00:04:25,366 --> 00:04:40,199

jedinstveno. Može ukupno sadržavati 20 velikih ili malih slova, ali ne i specijalne karaktere, i mogu se kombinirati posebni i alfanumerički znakovi.

30

00:04:40,200 --> 00:04:46,900

Znak razmaka je dopušten, no nije preporučljiv.

31

00:04:46,900 --> 00:04:56,666

Svaki korisnički račun bi trebao imati pridruženu lozinku. Ne bismo se smjeli koristiti korisničkim računima koji nemaju postavljenu lozinku. Lozinke

32

00:04:56,666 --> 00:05:07,199

su primarna metoda dobivanja pristupa računalu

(operacijskom sustavu) ili aplikaciji. No važno je

napomenuti da lozinke također mogu dati lažni

33

00:05:07,200 --> 00:05:18,033

osjećaj sigurnosti. Dobra je lozinka jedan od

ključnih elemenata sigurnosti koji smo skloni

previdjeti pa ćemo spomenuti i kompleksnost

34

00:05:18,033 --> 00:05:26,933

lozinki. Za dobru lozinku kažemo da ima najmanje osam

znakova, da sadržava najmanje jedno veliko slovo,

35

00:05:26,933 --> 00:05:40,599

najmanje jedno malo slovo, najmanje jednu brojku

te najmanje jedan posebni znak. Primjer dobro

kreirane lozinke dan je na ekranu.

36

00:05:40,600 --> 00:05:53,966

Navedene lozinke, osim što su kompleksne pa

samim time i teže za razbijanje, zadovoljavaju i

izbjegavanje efekta socijalnog inženjeringa.

37

00:05:53,966 --> 00:06:05,466

Razbijanje (cracking) lozinki jedna je od najlakših i

najčešće korištenih metoda kojima se napadači

koriste da bi zadobili neovlašteni pristup računalu

38

00:06:05,466 --> 00:06:12,799

ili mreži. S obzirom da se lozinke oslanjaju na tajnost,

nakon što je lozinka kompromitirana, početni

39

00:06:12,800 --> 00:06:23,400

vlasnik lozinke više nije jedina osoba koja može

dobiti pristup računalu. I tu počinju problemi.

Ljudski faktor i tehničke ranjivosti glavni su razlozi

40

00:06:23,400 --> 00:06:34,666

zbog kojih su lozinke jedna od najslabijih karika u

lancu informacijske sigurnosti. Korisnici odabiru

lozinke koje su kratke, jednostavne i predvidljive.

41

00:06:34,666 --> 00:06:45,166

Ne mijenjaju ih, rabe iste lozinke na više mjesta i

zapisuju ih na nesigurnim mjestima. Drugi dio

problema uključuju loši mehanizmi za šifriranje,

42

00:06:45,166 --> 00:06:59,799

nesigurna pohrana lozinki na računalnim

sustavima i aplikacije koje ne skrivaju lozinku na

ekranu pri upisivanju (prikazuju je dok se upisuje).

43

00:06:59,800 --> 00:07:10,866

Napadači se koriste raznim metodama razbijanja i

pribavljanja lozinki. Ciljaju bilo kakve lozinke, no

najzanimljivije su im administratorske lozinke s

44

00:07:10,866 --> 00:07:21,366

pomoću kojih mogu dobiti najvišu razinu pristupa

računalu i mogu izvršiti gotovo bilo koju radnju na

sustavu. Napadač može dobiti lozinku tako da

45

00:07:21,366 --> 00:07:29,266

korisnika jednostavno zatraži da mu je da

(socijalni inženjering) predstavljajući se kao

administrator ili neka stručna osoba, s nekim

46

00:07:29,266 --> 00:07:38,499

uvjerljivim razlogom. Jednako tako, lozinke se

mogu doznati „gledanjem preko ramena“

(Shoulder surfing) – promatranjem dok korisnik

47

00:07:38,500 --> 00:07:53,000

upisuje lozinku. Takve se metode često primjenjuju

i u svakodnevnom životu, npr. u trgovini dok kupac

upisuje PIN za autorizaciju kupnje preko kartice.

48

00:07:53,000 --> 00:08:02,233

Preporučuje se rabiti i kompleksnije lozinke koje

nije lako pogoditi. U nastavku je dan kratki pregled

sigurnosnih pravila kojih bi se trebalo pridržavati

49

00:08:02,233 --> 00:08:11,866

kada je riječ o lozinkama: Ugrađenom korisničkom računu "Administrator"

uvijek treba postaviti što sigurniju lozinku.

50

00:08:11,866 --> 00:08:19,332

Na operacijskom sustavu Windows 8

administratorski račun nije u uporabi i standardno

je onemogućen.

51

00:08:19,333 --> 00:08:29,999

Moguće je odrediti tko će upravljati lozinkama:

hoće li to raditi sami korisnici ili oni neće imati

mogućnost promjene svojih lozinki, već će to za

52

00:08:30,000 --> 00:08:37,366

njih raditi administrator.Korisnike treba educirati o opasnostima za

računalni sustav koje vrebaju ako lozinke nisu

53

00:08:37,366 --> 00:08:47,566

postavljene ili ih je moguće lako pogoditi:uzaludno je rabiti lozinke s očitim asocijacijama kao što su prezime ili datum rođenja;

54

00:08:47,566 --> 00:08:57,899

lozinke veće dužine teže je pogoditi. Kako je ranije navedeno, preporučljivo je koristiti se kombinacijama velikih i malih slova, numeričkih i

55

00:08:57,900 --> 00:09:02,466

posebnih znakova.

56

00:09:02,466 --> 00:09:08,899

Lekcija je završena

# Metode autentikacije

1

00:00:00,000 --> 00:00:13,100

Dobrodošli. U ovoj lekciji ćemo naučiti kojim još

metodama osim lozinke možemo potvrditi naš

identitet.

2

00:00:13,100 --> 00:00:23,433

Klasične metode identifikacije temelje se na metodama fizičke i logičke identifikacije pri čemu se pojedinac identificira s onim što posjeduje

3

00:00:23,433 --> 00:00:38,033

(ključ, značka, identifikacijska kartica pa i osobna iskaznica ili putovnica) ili onime što zna (lozinka, pin, korisničko ime), međutim, danas te metode

4

00:00:38,033 --> 00:00:44,766

identifikacije postaju sve manje pouzdane.

5

00:00:44,766 --> 00:00:56,232

Sve se to, naime, može izgubiti, zaboraviti,

prepustiti nekom drugom ili odati. Nasuprot tomu,

kod biometričkih metoda identifikacije pojedinac

6

00:00:56,233 --> 00:01:07,133

se identificira s onim što posjeduje odnosno s

onime što jest (otiskom prsta, otiskom i

geometrijom šake, obilježjima lica, obilježjima

7

00:01:07,133 --> 00:01:20,599

šarenice ili mrežnice oka i dr.) ili onime što ga ili

kako ga čini različitim od sviju ostalih (obilježjima

vlastoručnog potpisa, glasom, načinom hoda,

8

00:01:20,600 --> 00:01:28,033

načinom pisanja po tipkovnici i dr.).

9

00:01:28,033 --> 00:01:41,333

Biometrijska su obilježja jedinstvena, pojedinac ih

"nosi sa sobom", samo ih on posjeduje, njima

raspolaže i ne može ih prenijeti na drugu osobu.

10

00:01:41,333 --> 00:01:52,866

Dakle, uz metodu autentikacije lozinkom (ono što

znaš), postoji i metoda autentikacije pametnom

karticom ili generatorom jednokratnih lozinki, gdje

11

00:01:52,866 --> 00:02:04,032

se za generator često rabi riječ token, a za

jednokratnu se lozinku susrećemo s kraticom OTP.

Kombinacijom ovakvog načina autentikacije

12

00:02:04,033 --> 00:02:15,366

koristimo se onim „što imamo i onim što znamo“,

gdje je ono što znamo uglavnom PIN za karticu ili

za pokretanje generatora koda.

13

00:02:15,366 --> 00:02:25,099

Generator jednokratnih lozinki (token) je

elektronički uređaj s kojim dokazujemo svoj

identitet, ali ovaj put elektroničkim načinom.

14

00:02:25,100 --> 00:02:34,900

Jednako tako, kako mi sami stvaramo lozinku, isto

tako ju za nas stvara generator jednokratnih

lozinki. S obzirom da su jednokratne, mijenjaju se

15

00:02:34,900 --> 00:02:42,566

dogovorenim algoritmom u nekom vremenu i

vrijede samo određeno vrijeme.

16

00:02:42,566 --> 00:02:52,499

Kod metoda autentikacije biometrijom (ono što

jesi), kao i kombinacijom navedenih metoda,

dolazimo do najpouzdanijeg načina autentikacije

17

00:02:52,500 --> 00:03:05,733

kojeg čini: ono što znaš (lozinka), ono što imaš

(PIN za generator ili pametnu karticu) i ono što jesi

(biometrija).

18

00:03:05,733 --> 00:03:12,999

Lekcija je završena.

# Datotečni sustav i zaštita podataka na njemu

1

00:00:00,000 --> 00:00:10,633

Dobro došli. U ovoj lekciji ćemo naučiti kako je jošmoguće zaštiti podatke od ne autoriziranihkorisnika.

2

00:00:10,633 --> 00:00:21,633

Uz upotrebu korisničkih računa te različitih vrstalozinki, dodatnu sigurnost datoteka te pravapristupa nad njima može se definirati na još

3

00:00:21,633 --> 00:00:31,433

nekoliko načina.To su redom: Kontrola prava pristupa uz korištenjeNTFS datotečnog sustava, Šifriranje i Bitlocker.

4

00:00:31,433 --> 00:00:44,133

Datotečni sustav NTFS omogućuje veću sigurnostpodataka na tvrdom disku (odnosno particijama ilijedinicama) od datotečnog sustava FAT koji se

5

00:00:44,133 --> 00:00:47,566

koristio u ranijim verzijama Windows operacijskihsustava.

6

00:00:47,566 --> 00:00:57,866

Pri formatiranju tvrdog diska može se odabratiFAT32 ili NTFS datotečni sustav (File system).Oba imaju svoje prednosti i nedostatke, ali sa

7

00:00:57,866 --> 00:01:10,432

sigurnosnoga gledišta NTFS nudi više.FAT32 ne omogućuje nikakvu sigurnost mapa idatoteka, što ostavlja sustav otvorenim za napade.

8

00:01:10,433 --> 00:01:19,799

NTFS zato omogućuje osiguravanje datoteka naindividualnoj razini i ograničavanje pristupadatotekama. Na operacijskom sustavu Windows

9

00:01:19,800 --> 00:01:26,133

8, FAT32 standardno se više ne koristi.

10

00:01:26,133 --> 00:01:36,233

Još jedan od načina zaštite podataka kojegmožemo koristiti na računalima sa NTFSdatotečnim sustavom je i šifriranje podataka ili

11

00:01:36,233 --> 00:01:46,533

informacija. Šifrirani datotečni sustav (Encrypting File System,EFS) obilježje je Windows operacijskih sustava

12

00:01:46,533 --> 00:01:56,899

koji vam omogućuje pohranu mapa i datoteka natvrdi disk u šifriranom obliku. Šifriranje podatakanajveća je zaštita podataka koju nam pruža

13

00:01:56,900 --> 00:02:04,633

Windows operacijski sustav.Odlikuje ga jednostavnost korištenja gdje samiodređujemo tko može pročitati naše šifrirane

14

00:02:04,633 --> 00:02:08,099

datoteke.

15

00:02:08,100 --> 00:02:19,366

Šifriranje odnosno enkripcija jedna je od prednostiNTFS datotečnog sustava, a u nastavku će bitidetaljnije opisana.

16

00:02:19,366 --> 00:02:28,799

Povjerljivost (confidentiality) je najočitiji aspektinformacijske sigurnosti. Povjerljivostpodrazumijeva osiguravanje tajnosti informacija:

17

00:02:28,800 --> 00:02:37,533

informacije (podaci) moraju biti dostupne isključivoosobama kojima su te informacije (podaci)namijenjene. Jedan od načina postizanja

18

00:02:37,533 --> 00:02:47,499

povjerljivosti je upotreba šifriranja datoteka.Koncept povjerljivosti rabi se već tisućljećima –vojske i generali oduvijek su rukovali tajnim

19

00:02:47,500 --> 00:02:58,533

informacijama. Još se 50 godina prije Krista, JulijeCezar koristio tehnikom koja se danas nazivaCezarovim enkripcijskim algoritmom i to kako bi

20

00:02:58,533 --> 00:03:08,333

osigurao povjerljivost svojih poruka. Cezar sekoristio jednostavnim supstitucijskim algoritmom ukojem je sva slova abecede pomaknuo za

21

00:03:08,333 --> 00:03:21,099

određeni broj pozicija, npr. u tekstu koji šaljepromijenio je sva slova A u D, sva slova B u E itd.

22

00:03:21,100 --> 00:03:32,400

Uz korištenje EFS sistema, moguće je i šifriranjediska uz pomoć BitLocker-a. BitLocker jesttehnologija dostupna u Microsoft Windows 8

23

00:03:32,400 --> 00:03:36,466

operacijskim sustavima. Za rad može upotrebljavati

24

00:03:36,466 --> 00:03:47,766

integriranu funkcionalnost u većini današnjihprijenosnih i stolnih računala – TPM (TrustedPlatform Module) čip. Trusted Platform Module(

25

00:03:47,766 --> 00:03:57,932

TPM) jest mikročip koji omogućuje korištenjenaprednih sigurnosnih značajki na računalu, kaošto je npr. BitLocker šifriranje pogona. TPM je

26

00:03:57,933 --> 00:04:07,133

ugrađen u neka novija računala, a kako biste bilisigurni da li ga vaše računalo ima, pročitajtedokumentaciju proizvođača računala.

27

00:04:07,133 --> 00:04:17,633

BitLocker također štiti podatke u slučaju krađeračunala i jezgru operacijskog sustava pripokretanju i to od zlonamjernih programa.

28

00:04:17,633 --> 00:04:29,466

Općenito gledajući, postoje dvije metode zaštitepovjerljivosti informacija: primjena kontrolepristupa (fizička i logička) i šifriranje. Kontrola

29

00:04:29,466 --> 00:04:39,966

pristupa omogućuje pristup informacijama samoonim korisnicima koji su za taj pristup i ovlašteni, asvim se ostalim korisnicima pristup onemogućuje.

30

00:04:39,966 --> 00:04:49,499

Najjednostavniji primjer logičke kontrole pristupajesu pristupne liste na datotekama koje omogućujupristup datoteci samo određenim korisnicima ili

31

00:04:49,500 --> 00:04:59,633

grupama. Kod primjene šifriranja, bez obzira nakontrolu pristupa, samo korisnici koji posjedujuodgovarajući ključ za dešifriranje mogu informaciju

32

00:04:59,633 --> 00:05:08,999

i vidjeti, time se osigurava njezina tajnost jer drugikorisnici mogu vidjeti samo podatke koji nemajunikakvog smisla.

33

00:05:09,000 --> 00:05:15,900

U praksi se kontrola pristupa i enkripcija čestorabe istodobno.

34

00:05:15,900 --> 00:05:24,766

U slučajevima kada nismo u mogućnosti koristitiprednosti šifriranja ili korištenja BitLockera,moguće je dodatnu sigurnost nad datotekama

35

00:05:24,766 --> 00:05:35,999

postići postavljanjem lozinke koju će biti potrebnounijeti pri otvaranju datoteke. Isto pravilo vrijedi i zakomprimirane („zipane“) datoteke. No bitno je

36

00:05:36,000 --> 00:05:44,300

napomenuti da ovo, zbog lakoće probijanjamehanizama zaštite, ne bi trebalo biti preferiraninačin zaštite.

37

00:05:44,300 --> 00:05:51,433

Navedeno možemo učiniti za Word, Excel,PowerPoint dokumente.Napravit ćemo to tako da kliknemo na gumb

38

00:05:51,433 --> 00:06:02,233

Microsoft Office , odaberemo "Spremi kao (Save As)" te potom Alati --> Općenite postavke. Gdje u dijelu "Lozinka za otvaranje" unesemo željenu

39

00:06:02,233 --> 00:06:12,333

lozinku. Moguće je unijeti do 255 znakova, a lozinka treba biti kompleksna.

40

00:06:12,333 --> 00:06:52,699

Lekcija je završena.

# Makronaredbe

1

00:00:00,000 --> 00:00:12,666

Dobrodošli. U narednom videu, a u sklopu poglavlja Mjera zaštite, naučit ćemo što su to makronaredbe i zašto predstavljaju rizik za naše

2

00:00:12,666 --> 00:00:15,666

računalo i podatke.

3

00:00:15,666 --> 00:00:26,232

Korištenje makronaredbi vrlo je popularno u sklopu Microsoft uredskog paketa, međutim sa sigurnosnog stanovišta predstavljaju veliki rizik.

4

00:00:26,233 --> 00:00:35,866

Makronaredbu čini zbirka naredbi koje se na dokument mogu primijeniti jednim klikom čime je omogućena automatizacija bilo koje radnje koju

5

00:00:35,866 --> 00:00:44,799

radimo nad dokumentom. S obzirom na to da su makronaredbe jedan od oblika programiranja, iako za njih nije potrebno nikakvo specifično

6

00:00:44,800 --> 00:00:52,433

znanje programiranja, logično je da su zbog toga svojevrsni sigurnosni rizik.

7

00:00:52,433 --> 00:01:03,999

Većina se naredbi može otvoriti u programima Microsoftovog uredskog paketa, a napisane su u programskom jeziku Visual Basic for Application.

8

00:01:04,000 --> 00:01:13,833

Kada su makronaredbe stvorene sa zlom namjerom, mogu sadržavati zlonamjerne kodove koji mogu oštetiti ili dokumente ili operacijski

9

00:01:13,833 --> 00:01:17,399

sustav.

10

00:01:17,400 --> 00:01:28,466

Kako bismo zaštitili datoteke i naš operacijski sustav, poželjno je ne omogućavati makronaredbe od neznanih nam pošiljatelja. Preporuka je

11

00:01:28,466 --> 00:01:41,032

postaviti sigurnost makronaredbi na „Srednje“. U tom ćemo slučaju svaki put moći odabrati što želimo s naredbom, izvesti je ili ne.

12

00:01:41,033 --> 00:01:48,599

Lekcija je završena.

# Digitalni certifikati

1

00:00:00,000 --> 00:00:08,600

Dobrodošli. U ovom videu naučit ćemo što su to digitalni certifikati.

2

00:00:08,600 --> 00:00:18,566

Kao pouzdani način identifikacije odnosno predstavljanja kada je to potrebno, u „stvarnom svijetu“ koristimo osobne iskaznice. U digitalnom

3

00:00:18,566 --> 00:00:29,266

svijetu odnosno u radu na Internetu, najpouzdaniji način predstavljanja čine digitalni certifikati. Digitalni certifikat je naša „osobna iskaznica“ ,

4

00:00:29,266 --> 00:00:35,232

sredstvo kojim dokazujemo identitet na Internetu.

5

00:00:35,233 --> 00:00:45,399

Budući da na Internetu, nema „službenih osoba“ koje bi provjeravale naš identitet ta je uloga dana tzv. certifikacijskim tijelima odnosno sustavima

6

00:00:45,400 --> 00:00:54,933

(CA - Certificate Authority) čija je uloga da provjere i utvrde nečiji identitet i nakon toga mu izdaju digitalni certifikat.

7

00:00:54,933 --> 00:01:05,566

Nakon što se izda nečiji digitalni certifikat, certifikacijsko ga tijelo digitalno potpiše svojim tajnim ključem.

8

00:01:05,566 --> 00:01:17,266

Područje informacijske sigurnosti koje je znatno pridonijelo migraciji tradicionalnih poslovnih procesa (npr. trgovina) na Internet svakako je

9

00:01:17,266 --> 00:01:25,432

infrastruktura javnog ključa, odnosno PKI (public key infrastructure). Ona adresira neka od ključnih pitanja kada je riječ o sigurnosti internetskog

10

00:01:25,433 --> 00:01:36,433

poslovanja, kao što su neporecivost, autentičnost, integritet i povjerljivost informacija. Jednako tako, omogućuje definiranje temeljnog okvira za

11

00:01:36,433 --> 00:01:47,566

uspostavu povjerenja između pojedinih sudionika na Internetu koji sudjeluju u razmjeni informacija.Za uspostavu sustava povjerenja ključno je da u

12

00:01:47,566 --> 00:01:54,132

sustavu postoji barem jedan entitet kojem vjeruju svi korisnici sustava.

13

00:01:54,133 --> 00:02:07,966

I za kraj, CA je odgovoran za izdavanje digitalnih certifikata koji će omogućiti povezivanje digitalnih identiteta korisnika s njihovim stvarnim

14

00:02:07,966 --> 00:02:10,566

identitetom.

15

00:02:10,566 --> 00:02:17,999

Lekcija je završena.

# Izbjegavanje krađe osobnih podataka

1

00:00:00,000 --> 00:00:10,800

Dobrodošli. U ovom videu ćemo naučiti na štotrebamo obratiti pažnju kako bi izbjegli krađuosobnih podataka.

2

00:00:10,800 --> 00:00:20,866

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

3

00:00:20,866 --> 00:00:31,399

drugima. Kako pojedinci žele otuđiti nekuinformaciju kompanijama i ilegalno izvućimaterijalnu ili neku drugu korist, jednako će tako to

4

00:00:31,400 --> 00:00:33,500

poželjeti napraviti i nama.

5

00:00:33,500 --> 00:00:42,300

Ono što nikako ne bismo željeli jest da netkoukrade naše osobne podatke jer smo bilinesmotreni pri internetskoj kupnji te da nam nakon

6

00:00:42,300 --> 00:00:43,933

toga nanese financijsku štetu.

7

00:00:43,933 --> 00:00:55,933

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

8

00:00:55,933 --> 00:01:07,266

osobnih podataka zaštita privatnog života i ostalihljudskih prava i temeljnih sloboda u prikupljanju,obradi i korištenju osobnih podataka. Dalje se

9

00:01:07,266 --> 00:01:18,899

kaže da je zaštita osobnih podataka u RepubliciHrvatskoj osigurana svakoj fizičkoj osobi bezobzira na državljanstvo i prebivalište te neovisno o

10

00:01:18,900 --> 00:01:28,700

rasi, boji kože, spolu, jeziku, vjeri, političkom ilidrugom uvjerenju, nacionalnom ili socijalnompodrijetlu.

11

00:01:28,700 --> 00:01:40,233

I Europska unija je kroz Direktivu o zaštiti osobnihpodataka koja je usvojena 1995.godine donijelazakonske akte u pogledu obrade i korištenja

12

00:01:40,233 --> 00:01:50,799

osobnih podataka. Radi se o važnom člankueuropskog zakona koji štiti privatnost i ljudskaprava te ukazuje na važnost zaštite i izbjegavanja

13

00:01:50,800 --> 00:01:55,766

krađe osobnih podataka zbog osobne koristi.

14

00:01:55,766 --> 00:02:08,332

Često nas s novinskih stranica zasipaju naslovipoput: „Ukradena dva milijuna lozinki“,„Facebookom se služi 93% djece i mladih između

15

00:02:08,333 --> 00:02:20,999

11 i 18 godina“, „Društvene mreže postalesastavni dio života 54% Hrvata“. Na osnovi svega nije teško zaključiti da, ako i nije

16

00:02:21,000 --> 00:02:31,900

ugrožena naša osobna sigurnost, trebamo poraditina osiguranju nepovredljivosti naših osobnihpodataka.

17

00:02:31,900 --> 00:02:41,066

Krađa osobnih podataka, često je usko povezanas fenomenom koji nazivamo socijalniminženjeringom. Socijalni smo inženjering,

18

00:02:41,066 --> 00:02:50,499

prikladno, spomenuli u poglavlju koji se odnosi nalozinke. Jedan od glavnih ciljeva socijalnoginženjeringa jest upravo saznavanje informacija o

19

00:02:50,500 --> 00:02:57,300

korisniku, a najčešće su na meti korisničkelozinke.U ovim modulima, o socijalnom inženjeringu, govorimo u kontekstu informacijske

20

00:02:57,300 --> 00:03:06,900

 sigurnosti, a odnosi se na psihološku manipulaciju ljudima s namjerom saznavanja povjerljivih informacija bilo kojeg oblika.

21

00:03:06,900 --> 00:03:17,433

Namjera manipulacije ljudima jest uzpomoć raznih trikova doći do povjerljivihinformacija s ciljem postizanja aktivnosti

22

00:03:17,433 --> 00:03:24,599

usmjerenih na prevaru i pristup informacijskomsustavu, a često se sastoji od nekoliko koraka.

23

00:03:24,600 --> 00:03:35,600

Prvi od koraka jest uspostavljanje odnosapovjerenja s osobom koju se želi prevariti ili od njedobiti povjerljive informacije. U načelu je takva

24

00:03:35,600 --> 00:03:44,700

osoba ljubazna prema nama, suosjećajna i uvećini slučajeva djeluje naivno i dobroćudno.Prije nego što nam je pristupila, o nama je saznala

25

00:03:44,700 --> 00:03:53,400

određene informacije, i to uglavnom prikupivši ihna društvenim mrežama poput Facebooka,Twittera i sl. Obično o nama zna dovoljno

26

00:03:53,400 --> 00:04:02,300

informacija kako bi nam nesmetano moglapristupiti hineći poznanstvo ili poznavanje našesituacije.

27

00:04:02,300 --> 00:04:12,466

Da bi smo spriječili krađu identiteta, u nastavku ćebiti dano nekoliko korisnih savjeta.U ljetnim mjesecima, često u novinama i na

28

00:04:12,466 --> 00:04:22,399

televiziji možemo naići na naputke o tome kakospriječiti da naši stanovi ne budu opljačkanitijekom godišnjih odmora. Jedan od savjeta je da

29

00:04:22,400 --> 00:04:32,866

na Facebook-u ne ostavljamo poruke o tome kadai kamo odlazimo na godišnji odmor. Bitno jeshvatiti da isto tako kako „klasični“ lopovi imaju

30

00:04:32,866 --> 00:04:42,332

različite metode da dođu do naše materijalneimovine, pa iz tog razloga ne ostavljamo „ključispod otirača“, isto tako i kibernetički kriminalci

31

00:04:42,333 --> 00:04:45,533

imaju svoje, prokušane metode.

32

00:04:45,533 --> 00:04:55,199

Dakle, kako nećemo ostaviti „ključ ispod otirača“isto tako ne bi trebali ostavljati nepoznatimosobama svoje korisničke podatke poput

33

00:04:55,200 --> 00:04:58,833

korisničkog imena, lozinki i sl.

34

00:04:58,833 --> 00:05:09,066

Danas, vrlo često, imamo primjere kada nas se urazličitim elektroničkim porukama koje su kreiranena način da mislimo da su poslane iz naše banke

35

00:05:09,066 --> 00:05:17,899

ili kartičarske kuće, traže informacije o osobnimidentifikacijskim brojevima, brojevima tekućihračuna i sl.

36

00:05:17,900 --> 00:05:28,066

Nikada, kada se u takvim porukama ili narazličitim web lokacijama od nas traže osobnipodaci ne smiju se dati odnosno ostaviti sljedeći

37

00:05:28,066 --> 00:05:39,866

podatci: Korisničko ime i pripadajuća mu lozinka;Brojevi bankovnih računa ili kreditnih kartica; Datumi rođenja, Djevojačko prezime naše majke,

38

00:05:39,866 --> 00:05:51,532

Osobni identifikacijski brojevi (PIN).Za kraj, ono čega moramo biti svjesni je činjenica da sve ove radnje koje smo poduzeli ili ćemo

39

00:05:51,533 --> 00:06:04,233

poduzimati su iz razloga zaštite osobnih podatakaodnosno informacija, kako bi smo izbjegli, prije svega, krađu našeg osobnog identiteta.

40

00:06:04,233 --> 00:06:24,266

Lekcija je završena.