

**Tema:**  
**IT bezbednost na drugačiji način**

Oblast: Security  
Predavač: doc dr Igor Franc

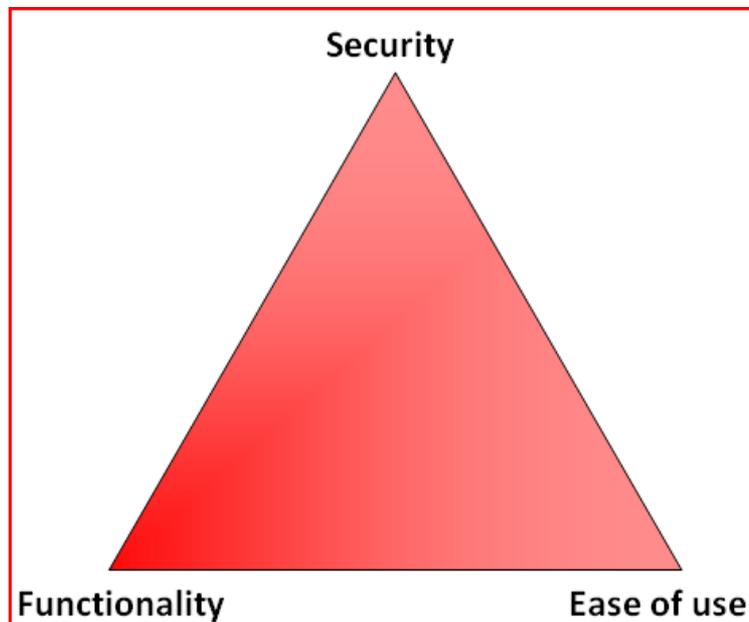
## Sadržaj:

- Odnos bezbednosti i funkcionalnosti
- Osnova IT bezbednosti CIA trojstvo
- Autentikacija i autorizacija
- Ko nas zapravo napada?
- Osnovne vrste pretnji
- Socijalni inženjering
- Kako se zaštititi?

## Sadržaj:

- Penetration testing
- Pravo i etika u IT bezbednosti
- Bezbednost dece na internetu
- Zaključak
- Korisni linkovi
- Pitanja i kontakt podaci

## Odnos bezbednosti i funkcionalnosti



# Osnova IT bezbednosti CIA trojstvo



# Autentikacija i autorizacija



AAA – Autentication, Autorization, Accounting



## Ko nas zapravo napada?



**WHITE HAT**



**GRAY HAT**



**BLACK HAT**



## Ko nas zapravo napada?



## Po lokaciji:

- Interni
- Externi

## Vrste napada



## Po cilju:

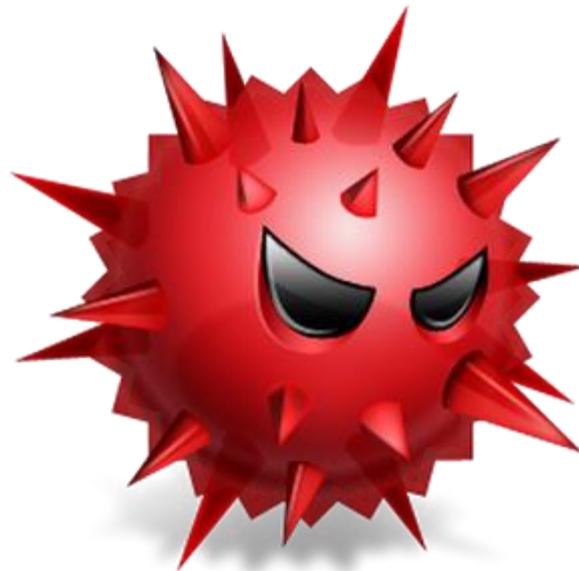
- Neovlašćen pristup
- Izmena podataka
- Onemogućavanje korišćenja resursa

## Po razlogu nastanka:

- Zabava
- Kriminal, krađa
- Politika, terorizam

## Osnovne vrste pretnji

- Virusi
- Crv
- Trojanci
- Logičke bombe
- Spyware
- Backdoor/rootkit
- DOS/DDOS napadi
- Zloupotreba emaila - HOAX
- Socijalni inženjering



# Virusi



## Crvi - worms



## Stuxnet – najsofisticiranija pretnja



# Trojanci



# Logičke bombe



## Spyware – špijunski programi



## Backdoor i rootkits



# DOS/DDOS napadi





## HOAX - prevare



## Socijalni inženjering – “wet-ware”

- War dialing
- War driving
- Phishing
- Dumpster diving
- Shoulder surfing
- Eavesdropping
- Tailgating
- Impersonation

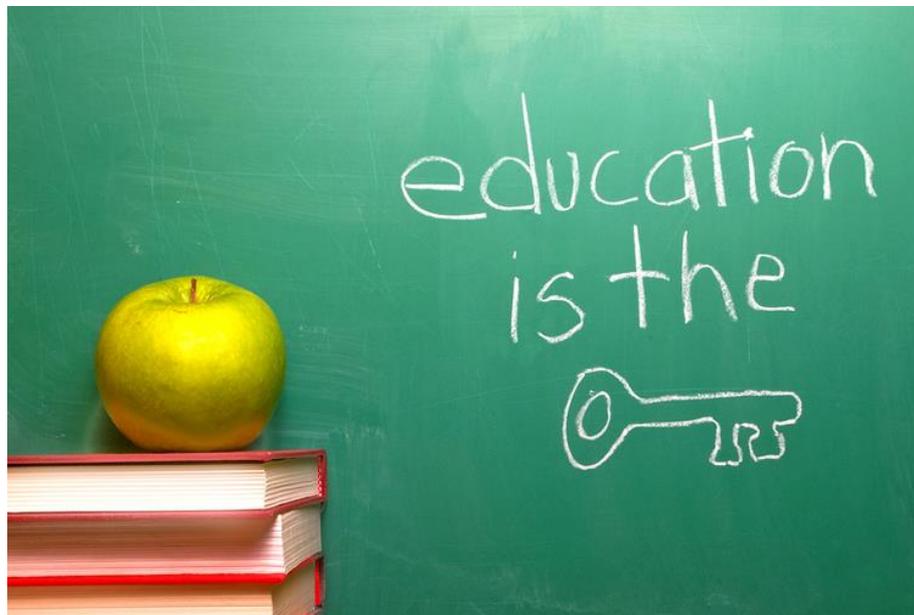


## Kako se zaštititi?

- Edukacija korisnika
- Korišćenje kompleksnih pasworda i nikako admin naloga
- Redovni backup podataka
- Pravilno uništavanje podataka
- Korišćenje kriptografije
- Korišćenje antivirus, antimalware i antispyware programa
- Pravilno konfigurisan firewall i operativni sistem
- Redovno ažuriran operativni sistem i ostali programi
- Pravilno konfigurisana mrežna infrastruktura žična i bežična
- Definisane politika, pravila i procedura za korisnike (BYOD)
- Fizička bezbednost – najmanje pažnje od strane IT osoblja



## Edukacija korisnika



## Kompleksni paswordi i admin nalozi

Windows: Administrator

Linux: root

Komleksni password:

Minimum 8 karaktera

2 mala slova, 2 velika slova

2 broja i 2 specijalna znaka

elementi	komb. (char)	vreme
mala slova	26	5 dana
velika slova	52	3 godine
brojevi	62	14 godina
spec. simboli	96	458 godina

## Backup podataka



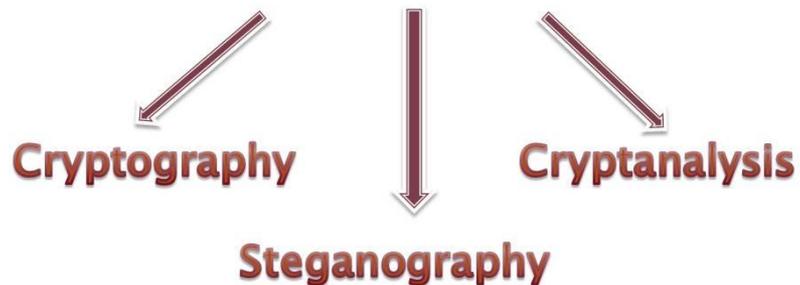
## Uništavanje podataka



# Kriptologija

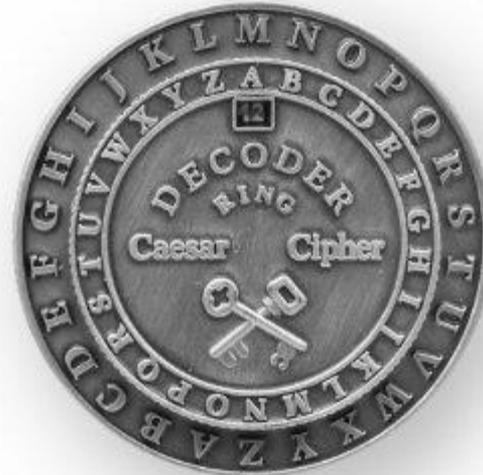


**CRYPTOLOGY**





## Kriptografija



# Steganografija



# Mail kriptografija – PGP/GPG



# Antivirus, antimalware i antispyware



## Windows 7 - demonstracija

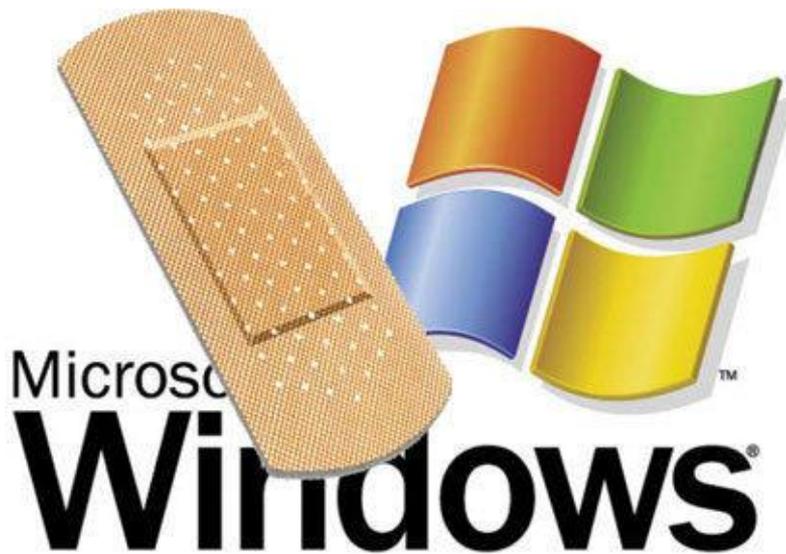
- Windows update
- Windows firewall
- Windows firewall with advanced security
- Windows defender
- Parental controls
- Event viewer
- User accounts
- Folder options
- Internet options
- System restore



# Firewall



# Windows security updates





**Center for Career Development**

by LINKgroup

**Zero-day**

**Zero-Day**



**Exploit**

# Wi-fi security



## Wi-fi security – demonstracija TP-link

- Default user names and passwords
- Default SSID
- No broadcast SSID
- Antena positions
- WEP-WPA/WPA2
- RADIUS
- Mac adress filtering



[TP-Link WA501G](#)



# BYOD – korišćenje u kompaniji



## Fizička bezbednost



## Penetration testing



# Pravo i etika u IT bezbednosti



## Bezbednost dece na internetu

KEEP YOUR **KIDS**  
**SAFE** Online



## Zaključak

- Edukacija ljudi je ključna u povećanju nivoa bezbednosti
- Potrebno je koristiti višestruke sisteme odbrane od pretnji
- Vrlo je bitno naći pravu meru između bezbednosti i funkcionalnosti
- Redovan update operativnog sistema i antivirus programa je odlična mera
- Redovno pravite rezerve kopije svojih podataka kao preventivu
- Dobro zaštitite svoju kućnu wi-fi mrežu
- Vodite računa da ne kršite zakone u oblasti IT
- Stare računare koji se ne koriste obavezno očistite od svojih ličnih podataka
- Neophodno je voditi računa o bezbednosti dece na internetu



## Korisni linkovi:

<http://www.informacija.rs>

<http://thehackernews.com>

<https://krebsonsecurity.com>

<http://www.net-security.org>

<http://www.wired.com/security>

<http://www.sans.org/reading-room>

<http://www.hackread.com/category/hacking-news>

<http://iase.disa.mil/stigs/Pages/index.aspx>

<http://csrc.nist.gov/publications/PubsSPs.html>

<http://ddosattackprotection.org/blog/cyber-security-blogs>

<http://karen-s-hasler.software.informer.com>

<https://veracrypt.codeplex.com/releases/view/565079>

# HVALA NA PAŽNJI!

**Kontakt podaci:**

Mail: [ifranc@secitsecurity.com](mailto:ifranc@secitsecurity.com)

Web: <http://secitsecurity.com>

Twitter: <https://twitter.com/francigorbg>

LinkedIn: <https://rs.linkedin.com/in/ifranc>

