Program seminara

”Zaštita ličnih podataka i IT bezbednost u školi”

1. Koncepti bezbednosti

1.1 Podaci

1.1.1 Razlika između podatka i informacije

1.1.2 Sajber kriminal, hakovanje, krekovanje i etičko hakovanje

1.1.3 Prepoznati pretnje podacima od strane zaposlenih, servis provajdera i pojedinaca iz spoljnog okruženja

1.1.4 Pretnje podacima kao što su: prirodne pretnje, infrastrukturne, društveno uzrokovane i ljudske pretnje

1.1.5 Pretnje podacima u oblaku (Cloud) poput: kontrole podataka, potencijalni gubitak privatnosti

1.2 Važnost informacija

1.2.1 Razlozi za zaštitu ličnih podataka: krađa identiteta i prevara

1.2.2 Razlozi za zaštitu osetljivih poslovnih informacija: krađa, prevara ili zloupotreba

1.2.3 Mere za sprečavanje neovlašćenog pristupa podacima, kao što su šifrovanje (enkripcija) i lozinke

1.2.4 Osnovne karakteristike bezbednosti informacija kao što su: poverljivost, integritet, dostupnost, autentičnost, neporecivost

1.2.5 Vrste zaštite podataka i privatnosti, kontrola pristupa podacima u našoj zemlji

1.2.6 GDPR - General Data Protection Regulation

2. Lična sigurnost

2.1 Socijalni inženjering i krađa identiteta

2.1.1 Socijalni inženjering i njegove implikacije, kao što su: prikupljanje informacija, pristup računarskoj mreži, prevare (fraud)

2.1.2 Metode socijalnog inženjeringa kao što su: telefonski pozivi, smishing, phishing, shoulder surfing

2.1.3 Značenje i implikacije termina krađa identiteta: ličnog, finansijskog, poslovnog i pravnog

2.1.4 Metode krađe identiteta kao što su: information diving, skimming, pretexting

2.2 Bezbednost fajlova

2.2.1 Efekti uključivanja/isključivanja makro naredbi

2.2.2 Prednosti i ograničenja šifrovanja (enkripcije). Važnost čuvanja ili gubitka lozinke, ključa, sertifikata

2.2.3 Šifrovati fajlove i foldere

2.2.4 Postaviti lozinke za fajlove kao što su: dokumenta, tabelarne kalkulacije, kompresovane fajlove

3. Zlonamerni programi

3.1 Vrste i metode

- 3.1.1 Zlonamerni programi (malware): trojanci, rootkits i back doors
- 3.1.2 Zlonamerni programi (malware): virusi i crvi
- 3.1.3 Pretnje definisane metodom ponašanja malvera: adware, spyware, botnets, ransomware, keystroke logging i diallers
- 3.1.4 Ransomware
- 3.1.5 Botnets i DDoS

3.2 Zaštita

- 3.2.1 Način rada i ograničenja antivirusnih programa
- 3.2.2 Razumeti da antivirusni softver treba instalirati na računare i druge uređaje
- 3.2.3 Skenirati specifične diskove (drives), foldere, fajlove koristeći antivirus program
- 3.2.4 Razumeti termin ''karantin'' i njegov uticaj na zaražene/sumnjive fajlove
- 3.2.5 Rizik korišćenja zastarelog softvera bez podrške i važnost redovnog ažuriranja antivirus programa

3.3 Rešavanje i uklanjanje

- 3.3.1 Efekat stavljanja zaraženih/sumnjivih fajlova u karantin i njihovo brisanje
- 3.3.2 Razumeti da se napad malvera može dijagnostikovati i spečiti pomoću mrežnih (online) resursa

4. Bezbednost mreže

4.1 Mreže i konekcije

- 4.1.1 Računarske mreže i vrste mreža: LAN, WLAN, WAN, VPN
- 4.1.2 Uticaj povezivanja na mrežu na bezbednost: zlonamerni programi, pristup podacima, zaštita privatnosti
- 4.1.3 Uloga administratora mreže
- 4.1.4 Funkcija i ograničenja zaštitnog zida (firewall) u ličnom radnom okruženju
- 4.1.5 Uključiti i isključiti lični zaštitni zid (firewall)

4.2 Sigurnost bežičnih mreža (Wireless Security)

- 4.2.1 Načini zaštite bežične mreže: WEP, WPA, WPA2, MAC filtering, SSID hiding
- 4.2.2 Biti svestan da korišćenje nezaštićene bežične mreže može dovesti do neovlašćenog pristupa vašim podacima, prisluškivanja, preuzimanja mreže ili postavljanja nekoga između
- 4.2.3 Pojam Personal hotspot
- 4.2.4 Uključiti i isključiti bezbedni personal hotspot, konektujte i diskonektujte uređaje