Osnove sigurnosti u Cyber prostoru (webinar)

Objavljeno: 09.04.2025
Prijave moguće ostaviti u periodu: 09.04.2025 - 21.04.2025
Datum održavanja: 22.04.2025 - 25.04.2025
Organizator: Agencija za državnu službu BiH

Webinar će se realizovati putem **Adobe Connect** platforme. Prijave će biti otvorene do **21.4.2025.** godine. Nakon isteka roka za prijavu svi polaznici će emailom dobiti korisničke informacije i uputstva za pristup webinaru.
Webinar će se održati **22, 24. i 25. aprila 2025.** godine u terminu **09:00-10:30** sati.

PREDAVAČ: IVAN MARKIĆ

SADRŽAJ

I UVOD

Upoznavanje sa pojmom zlonamjerne aktivnosti na internetu. Upoznavanje sa osnovnim pojmovima i nazivima zlonamjernih aktivnosti. Motivi za izvođenje zlonamjernih aktivnosti.

II OPASNOSTI I PRIJETNJE U TEORIJI I PRAKSI

Opis različitih zlonamjernih aktivnosti na internetu o kojima svakodnevno možemo ćuti iz medija. Primjeri zlonamjernih aktivnosti iz prakse pojedninaca i organizacija u Bosni i Hercegovini. Implikacije uspješnih cyber napada na život i rad pojedinca i poslovne organizacije.

III ZAŠTITA - BESPLATNI ALATI I SERVISI

Korištenje besplatnih alata za provjeru URL adresa, IP adresa, datoteka kroz prikaz praktičnih primjera prilikom prijema poruke elektronske poruke koja sadrži link na neku adresu ili dokument u prilogu. Kroz ovo poglavlje biti će opisane osnovne rutine i postavke kojima svatko može učiniti svoj Windows računar mnogo sigurnijim i otpornijim na napade korištenjem već ugrađenih Windows alata i korištenjem drugih besplatnih alata. Obzirom na ogromnu važnost mobilnih uređaja na isti način će biti obrađena zaštita istih kroz korištenje ugrađenih postavni i besplatnih alata. Ovo poglavlje će obraditi i zaštitu podataka na prenosnim medijima (USB memorije) kao i zaštitu od špijunaže kroz IOT uređaje.

IV ZAŠTITA U ORGANIZACIJI – NAPREDNA RJEŠENJA IT SIGURNOSTI

Ponašanje u uređenom IT okruženju koje posjeduje napredna rješenje IT sigurnosti. Opis rada naprednih IT rješenja sigurnosti zbog boljeg razumijevanja i suradnje između osoblja koje obavlja temeljnu djelatnost organizacije i IT osoblja koje ima zadatak da osigura najbolji odnos između rizika i funkcionalnosti u IT okruženju. Isto tako kroz ovo poglavlje će biti opisan princip slojevite zaštite sa posebnim naglaskom na značaj edukacije korisnika, regulative i procedura za korištenje IT resursa.

V DISKUSIJA – STANJE U TEORIJI I PRAKSI

Diskusija o konkretnim primjerima, problemima i dilemama koje imaju polaznici ove obuke. Savjeti i pojašnjavanje situacija iz prakse.

CILJ

Upoznati se sa vrstama zlonamjernih aktinosti na internetu i njihovim posljedicama.
Naučiti koristiti ugrađene i besplatne alate za zaštitu računara i mobilnog uređaja kao i podataka na prenosnim USB memorijama. Naučiti kako funkcionira uređeni IT sustav organizacije/institucije sa svojim zaštitinim mehanizmima u vidu tehnoloških rješenja i procedura. Unaprijediti razumijevanje i suradnju sa IT osobljem organizacije.

OČEKIVANI ISHODI

Nakon uspješne obuke polaznici će naučiti:

- osnovne pojmove o zlonamjernih aktivnosti na internetu;
- šta motivira i pokreće zlonamjerene aktivnosti;
- da ne postoji nikto na internetu tko napadačima nije zanimljiv,
- kakve mogu biti posljedice napada;¸
- kako provjeriti sadržaj elektronske pošte (linkovi i prilozi);
- zaštiti svoj računar korištenjem ugrađenih i besplatnih alata;
- zaštiti svoj mobitel korištenjem ugrađenih i besplatnih alata ;
- zaštiti svoje podatke na prenosnom USB mediju;
- razumiju kako radi IT sustav u organizaciji/intituciji;
- razumiju mjere zaštite IT sustava organizacije/institucije;
- bolje surađuju sa IT osobljem organizacije/institucije;

CILJNA GRUPA

Svi državni službenici.

BROJ KREDITA: 3