



CERT.hr



#SurfajSigurnije

Radionica za podizanje svijesti o kibernetičkoj sigurnosti

Autor: CERT.hr

Sadržaj

- Rekapitulacija znanja
 - Zaključci
 - Rasprava i pitanja
- Prikaz i promocija kampanje Hrvatski Naivci
- Evaluacija radionice

Zaključci

- [CERT.hr](#)
 - Computer Emergency Response Team
 - Proaktivne i reaktivne mjere
 - „čuvar nacionalnog online prostora“
 - [GrowCERT](#)
 - Sufinanciranje putem CEF programa (Connecting Europe Facility) – Instrument za povezivanje Europe
 - Dvogodišnji projekt: 01/07/2017 – 30/06/2019
-

- Misija Nacionalnog CERT-a:

- Jačanje nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o značajnim kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti
 - Podizanje svijesti opće populacije i ciljanih skupina o kibernetičkim prijetnjama i kibernetičkoj sigurnosti
 - Razvoj platforme za prikupljanje podataka o kibernetičko sigurnosnim incidentima na nacionalnoj i EU razini,
 - Podizanje ukupne razine kibernetičke sigurnosti (razvoj novih usluga)
 - Jačanje kapaciteta zaposlenika u području kibernetičke sigurnosti
-

- Izazovi:

- Internet je oblikovan tako da bude otvoren svima i omogući širok javni pristup te otežava regulaciju prometa državnim ili komercijalnim akterima
 - Kibernetička sigurnost više nije samo sigurnost informacijsko-komunikacijskih sustava, već predstavlja temeljnu sastavnicu sigurnosti cjelokupnog opsega ljudskih djelatnosti u informacijskom društvu
 - Prosječni korisnik u RH nije dovoljno upoznat s opasnostima kojima je izložen pri korištenju računala i interneta, ne prepoznaje potencijalne prijetnje
-

- Kako zaštititi prosječnog korisnika?
 - Edukacijom
 - Aktivan pristup edukaciji
 - Osvještavanjem
 - Internet je alat, ali ga neki korisnici koriste u zlonamjerne svrhe
 - Razgovorom
 - Dijeljenje informacija o incidentima i prijetnjama može pomoći nekoj potencijalnoj žrtvi
 - Pravilna prijava incidenta nadležnoj službi podiže opću razinu kibernetičke sigurnosti društva
 - Prilagodbom korisniku
 - Korisnik uvijek mora biti u središtu
 - Korisnikov propust je naš propust
 - Mentor i učitelj, a ne autoritativna figura
-

Zapamtiti i primijeniti

Sigurnost prijenosnih računala i stolnih računala

- Nikad ne ostavljajte post-it s lozinkom na svoje računalo
- Politika čistog radnog mjesta
- Pripazite na „shoulder surfing“ – gledanje preko ramena
- Postavite čuvare zaslona screen saver, sačuvane s lozinkom
- Ugasite WiFi ili Bluetooth ukoliko vam ne trebaju
- Ne instalirajte software koji ne poznajete ili nije iz provjerenih izvora

- Sigurnost mobilnih uređaja

- Pametni telefoni i tableti su kao prijenosna računala jer imaju veliki računalni i podatkovni kapacitet
- Koristite zaštitne kodove i lozinke
- Koristite enkripciju
- Instalirajte antivirusni i vatrozid na sve uređaje što blokira spam i phishing napade kad god je to moguće

- Sigurno korišćenje interneta i sigurno pretraživanje i pregledavanje
 - Biti pažljiv za svaku stranicu koju pregledavate
 - Koristite Tor, početnu stranicu ili duckduckgo za više sigurno pretraživanje
 - Pripazite na pop-up prozore

- Sigurnost e-pošte

- Nikad ne otvarajte poruke od pošiljatelja koje ne poznajete, sigurnije je izbrisati sumnjive mailove nego ih otvarati
- Ako poruke sadrže privitke prvo ih trebata skenirati – pdf, doc i sl.
- Pripazite kako je postavljen vaš outlook da ne otvara skriptu kod pretpregleda pošte

- Sigurnost podataka i enkripcija

- Podaci su prvi cilj kibernetičkog napada, kriminala, špijunaže i warfare-a
- Uvijek koristite enkripciju za vlastitu i poslovnu sigurnost [čak i na prijenosnim medijima]
- Budite oprezni u vezi USB stickova bilo koje vrste
- Svi podaci koji se šalju trebali bi biti šifrirani

- Fizička sigurnost (ured, zgrada, okruženje i podatkovni centar)
 - Brave, ulazni ključevi ili kartice i kamere
 - Zaštitari
 - Praćenje posjetitelja
 - Obratite pažnju na osoblje koje dolazi za održavanje i ne nalaze se na svom mjestu ili tvrde da su prijatelji od voditelja

Hrvatski Naivci

- **Kome komuniciramo?**
 - Široka ciljna skupina
 - Učenici, roditelji, mladi, stari, poslovni sektor...
 - **Kako razmišljaju?**
 - „Koristim isti password za sve račune, i to od osnovne!”
 - „Ma tko mi što može? Ionako su to stare slike!”
 - **Naš je zadatak bio osvijestiti problem i ukazati na rješenja**
 - Razmišljaj kako raspolažeš svojim podacima na internetu. Surfaj sigurnije!
-

Hrvatski Naivci

- Ciljna skupina nije svjesna opasnosti na internetu
 - **Neutemeljno su povjerljivi!**
 - Ne paze kako rukuju podacima, ulaze u komunikaciju bez da utvrde identitet, kupuju na nesigurnim stranicama, ne brinu o sigurnosti svojih uređaja...
 - Ali!
 - Svakodnevno se služe internetom, kupuju, komuniciraju i brinu o svemu osim o sigurnosti svojih uređaja...
 - Naivni su?
 - Oni su zapravo hrvatski naivci
-