HUP
Udruga informatičke i komunikacijske djelatnosti

HUP CYBER PRAKTIKUM: Iskustvom, vježbom i edukacijom do kibernetički otpornog poslovanja

Datum: 15. rujna 2026.

Vrijeme: 10:00 – 14:00 (registracija od 9:30)

Mjesto: HUP, Radnička cesta 37a, Zagreb

Prijave: putem poveznice **PRIJAVA**

Program:

09:30 – 10:00 **Registracija sudionika**

10:00 – 10:10 **Uvod i pozdrav**

10:10 – 10:30 **KAKO SE OBRANITI OD KIBERNETIČKIH NAPADA I ZAŠTITITI POSAO I UGLED?**

Tomislav Bronzin, Citus

Što vlasnici i direktori moraju odlučiti prije incidenta? Kako reagirati kada se napad dogodi, tko u organizaciji mora preuzeti odgovornost i od koga zatražiti pomoć?

Na konkretnim primjerima saznajte što organizacija može napraviti unaprijed kako bi smanjila posljedice napada.

Ne čekajte incident da biste počeli razmišljati o odgovoru – nije pitanje hoće li se dogoditi kibernetička ugroza, nego kada.

10:30 – 12:00 **TABLE TOP VJEŽBA: KAKO UPRAVLJATI KIBERNETIČKIM INCIDENTOM?**

Andro Galinović, Infobip

Jurica Čular, Infobip

Riko Luša, Končar

Središnji ured Zagreb: Radnička cesta 37a, 10000 Zagreb, tel: 01 4897 555, fax: 01 48 97 556, e-mail: hup@hup.hr, www.hup.hr
Privredna banka Zagreb d.d. IBAN: HR9223400091100151718, Erste&Steiermärkische Bank d.d. IBAN: HR0524020061101157712
matični broj: 00410128, OIB: 80978339255

Podružnica Osijek: Vukovarska ul. 31 (Eurodom, IV. kat), 31000 Osijek, tel: 031 370-074, e-mail: hup-osijek@hup.hr
Podružnica Rijeka: Dolac 8/II, 51000 Rijeka, tel: 051 321 494, e-mail: hup-rijeka@hup.hr
Podružnica Split: Dračevac 3D, 3 kat, 21000 Split, tel: 021 368 288, e-mail: hup-split@hup.hr
Podružnica Varaždin: Zagrebačka 89, 42000 Varaždin, tel: 042 352 034, e-mail: hup-varazdin@hup.hr

uz sudjelovanje predstavnika Nacionalnog centra za kibernetičku sigurnost (NCSC-HR)

Što biste napravili da se upravo sada dogodi ozbiljan kibernetički incident u vašoj organizaciji?

Koga biste prvo nazvali? Tko donosi odluke? Kada uključiti upravu? Kako procijeniti razmjere incidenta? Kako komunicirati sa zaposlenicima, korisnicima, partnerima i nadležnim institucijama – i što ako se situacija dodatno zakomplicira?

Kroz interaktivnu simulaciju kibernetičkog incidenta sudionici će pratiti razvoj stvarnog kriznog scenarija te proces donošenja odluka, koordinacije i upravljanja incidentom.

Bez teorije i unaprijed poznatih odgovora – cilj je iskusiti kako izgleda donošenje odluka kada je organizacija pod kibernetičkim napadom.

12:00 – 12:30 **PAUZA ZA KAVU**

12:30 – 12:50 **KIBERNETIČKA SIGURNOST U SME SEKTORU: KAKO NAPRAVITI VIŠE S OGRANIČENIM RESURSIMA?**

Luka Matić, NEP-054

Kako uskladiti sve veće sigurnosne zahtjeve s ograničenim financijskim i ljudskim resursima te svakodnevnim poslovnim prioritetima?

Koje su najčešće prepreke s kojima se susreću mali i srednji poduzetnici i što u praksi mogu napraviti kako bi postupno podizali razinu svoje kibernetičke otpornosti?

12:50 – 13:20 **REVIZIJE PREMA UREDBI O KIBERNETIČKOJ SIGURNOSTI – ŠTO OČEKIVATI U PRAKSI?**

Predstavnici ZSIS-a

Marko Žalac, Deloitte

Kako izgledaju nadzori i revizije u praksi? Što se provjerava, što organizacije mogu očekivati i kako se na vrijeme pripremiti?

Praktičan pogled na zahtjeve Uredbe o kibernetičkoj sigurnosti iz perspektive nadležnog tijela i revizora.

13:20 – 13:50 **ŠTO NOVO DONOSI NACIONALNI KOORDINACIJSKI CENTAR ZA KIBERNETIČKU SIGURNOST?**

Vlatka Marčan, Nacionalni koordinacijski centar za kibernetičku sigurnost (NKS)

U razgovoru 1 na 1 saznajte koje mogućnosti NKS otvara hrvatskim organizacijama – od edukacije i razvoja kompetencija do mogućnosti financiranja aktivnosti i projekata u području kibernetičke sigurnosti.

13:50 – 14:00 **ZATVARANJE HUP CYBER PRAKTIKUMA**