AKADEMIJA KIBERNETIČKE SIGURNOSTI: Akt o kibernetičkoj otpornosti (CRA) i NIS2: sigurnost i otpornost kao poslovna odgovornost

15. listopada 2025. u 9:15, HGK- Rooseveltov trg 2, Zagreb

AGENDA

08:45 – 09:15 - Registracija

09:15 – 09:30 - Uvodni govori

09:30 – 10:10 - **Change management i organizacijski zahtjevi Zakona: od "IT problema" do poslovne odgovornosti**

Zašto Zakon i NIS2 izričito stavljaju odgovornost na Uprave (novčane kazne, osobna odgovornost)
Kako iz "sigurnost = trošak" prijeći u "sigurnost = poslovna investicija"
ROI u sigurnosti: konkretna formula i primjeri (trošak incidenata vs. ulaganja u prevenciju)
Primjeri kako cyber kultura smanjuje rizik i povećava otpornost tvrtke
Mindset shift: *"Cyber sigurnost nije IT linija budžeta to je dio korporativne kulture i odgovornosti Uprave."*

10:10 – 10:40 - **Akt o kibernetičkoj otpornosti (Cyber Resiliance Act) u praksi: što znači kad regulativa obvezuje proizvođače i dobavljače**

Akt o kibernetičkoj otpornosti (CRA) je već na snazi: rokovi i obveze koje kucaju na vrata
Kako CRA mijenja odgovornost dobavljača softvera i hardvera
Što to znači za korisnike kritične infrastrukture: izbor dobavljača, ugovorne obveze, audit trail
Mindset shift: *"Proizvod bez ugrađene sigurnosti postaje poslovni rizik a odgovornost prelazi i na korisnika."*

10:40 – 11:00 Pauza za kavu

11:00 – 11:30 - Akt o kibernetičkoj otpornosti (CRA) u praksi: uspavano tržište i koraci koje morate povući sada

Zašto tvrtke u regiji kasne i što to znači za konkurentnost
Tri najčešće zablude: "to se nas ne tiče", "imamo vremena", "to je IT-jev problem"
Akcijski plan: koje tri odluke Uprava mora donijeti do kraja 2025. da bi bila u skladu
Mindset shift: *"Čekanje je najskuplja opcija regulator neće čekati s kaznama."*

11:20 – 12:10 - Kako definirati značajne prijetnje i incidente: interna odluka kao temelj usklađenja

Uredba, o značajnosti incidenata: što točno traži i kako izgleda u praksi
Veza procjene rizika i kategorizacije incidenata: od teorije do Excel tablice
Kako izraditi internu odluku: kriteriji (tehnički, poslovni, reputacijski) i odgovornosti
Primjeri stvarnih incidenata i kako bi se klasificirali prema Zakonu
Mindset shift: *"Incident nije tehnički kvar incident je poslovni događaj koji može aktivirati regulatorne obveze."*

12:10 – 12:50 - SOC i Managed Security Services: kako Outsourcing postaje regulatorni alat

SOC u kontekstu NIS2: zašto više nije "luksuz" nego regulatorni zahtjev
Interni SOC vs. MSSP: trošak vs. brzina usklađenja
Kako ugovoriti MSSP da pokriva obveze iz Zakona (SLA, reporting, 24/7 response)
Primjeri modela: "shared SOC", "outsourced SOC", "hybrid model"
Mindset shift: *"Pitanje nije trebamo li SOC pitanje je kako ga implementirati bez blokiranja poslovanja."*

12:50 – 13:50 Ručak

13:50 – 14:30 - Sigurnost operativnih tehnologija (OT): kako obveznici moraju tretirati industrijske sustave

Zašto OT nije isto što i IT: primarno se štiti dostupnost i operativnost, a ne povjerljivost
Asset management u OT: kako popisati i klasificirati "nevidljivu" imovinu (PLC-ovi, SCADA, IoT)
Kako OT uključiti u procjenu rizika i poslovni kontinuitet
Koje kontrole traži Zakon i kako ih Uprava mora dokumentirati
Mindset shift: *"U OT-u ne štitimo podatke štitimo pogon, energiju, vodu i živote ljudi."*

14:30 – 15:10 - Kad Uprava igra defence team: table-top vježba

Kako izgleda simulacija napada u kojoj Uprava vodi obranu
Primjer scenarija: ransomware koji zaustavlja proizvodnju ili poslovne procese
Uloga svakog člana Uprave: tko donosi koje odluke pod pritiskom
Kako rezultate vježbe pretočiti u odluke i politike
Mindset shift: *"U trenutku napada Uprava ne može reći to je posao IT-a. Oni su ti koji odlučuju."*

14:40 – 15:00 ☕ Pauza za kavu

15:00 – 15:40 - Storytelling case study: što Uprave nauče kad prođu cyber krizu

Prezentacija stvarnog primjera (ili simulacije) incidenta i posljedica po poslovanje
Gdje su Uprave donijele krive odluke i koje su bile posljedice (kazne, reputacija, gubitak prihoda)
Kako bi pravilno vođena Uprava postupila u skladu sa Zakonom
Diskusija: što od ovoga vaša Uprava može odmah primijeniti
Mindset shift: *"Kibernetički napad je test vodstva a ne IT infrastrukture."*

15:40 – 16:00 - Završna diskusija i zaključci

Rekapitulacija: što zakon traži, što Uprava mora znati, što operativa mora provoditi
"Takeaway paket": tri zadatka koja sudionici nose kući
Mindset shift: *"Usklađenje nije administracija to je model poslovnog preživljavanja."*

HGK CROATIAN CHAMBER OF ECONOMY