Vabimo vas na strokovno izobraževanje:

KIBERNETSKA IN INFORMACIJSKA VARNOST KOT NOVA ODGOVORNOST SVETA DELAVCEV

Kako obvladovati kibernetska tveganja v praksi - s specialistom za kibernetsko varnost Daliborjem Vukovičem

ki bo v **ČETRTEK, 23. aprila 2026**, od 08.30 do 15.15 ure,
Dvorana Urban, **URBAN RING Hotel Ljubljana**, Dolenjska cesta 242c

Vsebina izobraževanja

»Vse je izgledalo popolnoma normalno – en klik, in v nekaj minutah nisem več imel dostopa ne do podatkov ne do denarja.«

Kolikokrat na dan vzamete telefon v roke in brez razmisleka kliknete na povezavo, odprete sporočilo ali potrdite dostop? Kolikokrat ste že prejeli SMS od "banke", e-pošto od "dostavne službe" ali obvestilo, ki je zahtevalo takojšnjo reakcijo – in ste se odzvali instinktivno, brez posebnega preverjanja? To danes počnemo vsi. Vsak dan. Doma in v službi.

In prav v teh na videz nedolžnih trenutkih se skriva **eno največjih, a hkrati še vedno močno podcenjenih tveganj sodobnega časa** – kibernetska ranljivost. Ne samo za podjetja. Tudi za vsakega posameznika. Posledice takšnih napak niso več majhne ali nepomembne. Govorimo o izgubi osebnih podatkov, finančnih sredstev, dostopa do ključnih informacij – in v primeru podjetij tudi o zaustavitvi poslovanja, resnih finančnih škodah in dolgoročnih posledicah za stabilnost organizacije.

Gre za tveganja, ki so lahko – brez pretiravanja – tudi katastrofalna! In kljub temu jih še vedno podcenjujemo. Deloma tudi zato, ker se sploh **ne zavedamo, na kakšne načine in od kod** vse danes prihajajo nevarnosti. Metode napadov se razvijajo izjemno hitro – postajajo vse bolj prepričljive, personalizirane in na prvi pogled popolnoma legitimne. Gre za pristope, na katere večina ljudi sploh ne bi pomislila, dokler se z njimi ne sooči.

»Napadalci uporabljajo tudi deepfake glasove prijateljev, sodelavcev, direktorjev … »
- Dalibor Vukovič

To izobraževanje ne bo tehnično, temveč **praktično razumevanje, kako kibernetske grožnje delujejo** v vsakdanjem življenju in v podjetju, kako jih prepoznati in kako se zaščititi – kot posameznik in kot del organizacije. Ker ista nepazljivost, ki ogrozi podjetje, lahko ogrozi tudi vas osebno. In prav zato to ni samo tema varnosti. To je tema odgovornosti, zavedanja in znanja, ki ga danes preprosto ne moremo več ignorirati.

Poudarki iz vsebine	
08.30 – 09.00	*Sprejem in registracija udeležencev, priprava na izobraževanje*
09.0 – 14.30	**Kibernetska tveganja kot nova življenjska realnost podjetij in posameznikov** • Kako lahko kibernetski napadi dejansko vplivajo na poslovanje podjetij (produkcija, finance, ugled) • Zakaj danes nobeno podjetje ni "premajhno", da ne bi bilo zanimivo za napadalce • Najpogostejši scenariji napadov v praksi (phishing, ransomware, socialni inženiring) • Zakaj so zaposleni najpogostejša vstopna točka v sistem **Človek kot največja ranljivost – in največja zaščita** • Kako napadalci izkoriščajo psihologijo posameznikov • Najpogostejše napake – konkretni primeri iz prakse • Kako prepoznati sumljive situacije pri vsakodnevnih opravilih • Zakaj klasična pravila pogosto odpovejo v realnem okolju **Osnovni ukrepi, ki dejansko delujejo (v podjetju in doma)** • Osnove varnega ravnanja: gesla, MFA, e-pošta, datoteke, dostopi • Delo od doma in uporaba zasebnih naprav – kje so največja tveganja • Kako se zaščititi pred najpogostejšimi prevarami (tudi v zasebnem življenju) • Kaj storiti ob sumu na napad – prvi koraki brez panike **Odpornost – kako zmanjšati tveganja** • Kaj pomeni "varnostna kultura" in zakaj je ključna • Minimalni standardi, ki jih mora poznati vsak • Zakaj samo tehnični ukrepi niso dovolj • Kako poteka odziv na incident – vloga posameznikov in organizacije **Vloga sveta delavcev v kibernetski varnosti** • Kje svet delavcev lahko zazna realna tveganja v praksi • Kako sodelovati z vodstvom in IT službo brez poseganja v strokovne pristojnosti • Vloga sveta delavcev pri ozaveščanju zaposlenih • Kako odpreti temo kibernetske varnosti na konstruktiven način **Praktična priporočila za takojšnjo uporabo** • Checklista: kaj lahko svet delavcev preveri v podjetju • 3–5 konkretnih ukrepov, ki jih lahko predlaga vodstvu • Najpogostejše napake pri uvajanju varnostnih praks
14.30 – 15.15	*Sklepne misli in zaključek izobraževanja*

Predavatelj

Dalibor Vukovič
Je specialist za kibernetsko varnost, ki je večji del svoje strokovne poti posvetil razumevanju in obvladovanju sodobnih digitalnih tveganj. S področja kibernetske varnosti ima več kot 20 let praktičnih izkušenj, pridobljenih z delom v različnih organizacijah in okoljih.

Je nosilec številnih mednarodnih certifikatov, med drugim tudi certificirani etični heker, kar mu omogoča neposreden vpogled v načine razmišljanja in delovanja napadalcev. Pri svojem delu poudarja, da je kibernetska varnost, kot jo poznamo danes, relativno novo področje, ki se izjemno hitro razvija – zato klasično znanje pogosto ne zadostuje.

Kot sam izpostavlja: »Prava šola kibernetske varnosti je praksa – vsakodnevna.«

Danes deluje kot produktni menedžer na področju kibernetske varnosti v družbi Telekom Slovenije, kjer se ukvarja z razvojem rešitev za zaščito organizacij pred sodobnimi digitalnimi grožnjami. Njegova predavanja temeljijo na realnih primerih iz prakse, zaradi česar udeleženci hitro prepoznajo lastna tveganja in pridobijo znanje, ki ga lahko takoj uporabijo.

Prijave in kotizacija

Udeležbo lahko prijavite do **TORKA, 21. aprila 2026** prek spletne prijavnice na naši spletni strani ali po e-pošti: **scid.izobrazevanja@zsds.si** Natančnejše informacije o izobraževanju lahko pridobite tudi na **GSM (041) 749 090** – Mitja Gostiša.

Kotizacija z gradivom, osvežilnimi napitki, prigrizki in kosilom **za člane Združenja svetov delavcev Slovenije** znaša **240,00 € + DDV**, za ostale udeležence pa 270,00 € + DDV.

Pri plačilu lahko uveljavljate 10% popust, če organizacija prijavi najmanj dva udeleženca.

Kotizacijo nakažete na podlagi prejetega računa (po zaključku izobraževanja) na transakcijski račun podjetja ŠCID IZOBRAŽEVANJA d.o.o., **št.: SI56 0400 0027 8569 294,** odprt pri OTP Banki (BIC: KBMASI2X).

Lep pozdrav in nasvidenje na izobraževanju!