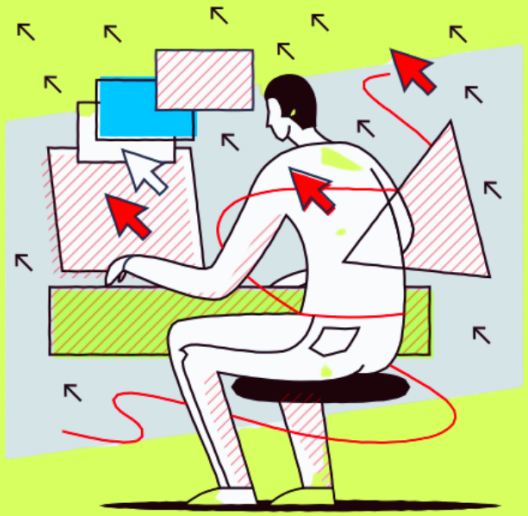
Posvet o izobraževanju zaposlenih o kibernetski varnosti

NACIONALNI ODZIVNI CENTER ZA KIBERNETSKO VARNOST SI-CERT

↘
NOVI PRISTOPI ZA NOVE GROŽNJE



Posvet o izobraževanju zaposlenih o kibernetski varnosti

PROSTOR EDVARD, IGRIŠKA 5, LJUBLJANA

4. junij 2025

si·cert

Program posveta

9.00 – 9.30	Registracija udeležencev in jutranja kava	
9.30 – 9.40	Uvodni nagovor organizatorja SI-CERT	
9.40 – 10.10	**Kibernetski napadi na vaše zaposlene – proti čemu se borimo?** Tadej Hren, SI-CERT, vodja ekipe za odzivanje na kibernetske incidente	Tehnologija postaja čedalje bolj kompleskna, obenem pa se trudi biti uporabniku prijazna. Slednje pomeni, da uporabniku oz. zaposlenim ni potrebno poznati ozadja delovanja sistemov, žal pa to neznanje s pridom izkoriščajo spletni napadalci. Velikokrat so najuspešnejši tisti napadi, ki so preprosti, ne vsebujejo kompleksnih in tehničnih elementov, ampak zgolj kakšen enostaven trik, ki pa ga uporabniki ne prepoznajo pravočasno. Tovrstni napadi tudi brez težav obidejo tehnologijo, ki ščiti pred omrežnimi napadi, saj delujejo na drugem nivoju. V predavanju bomo predstavili nekaj konkretnih primerov takih napadov, ki smo jih v zadnjem obdobju obravnavali na Nacionalnem odzivnem centru za kibernetsko varnost SI-CERT, in pogledali, zakaj postajajo nasveti za zaščito, ki smo jih lahko še pred kratkim dajali uporabnikom, čedalje bolj neuporabni.
10.10 – 10.40	**Največja varnostna luknja? Zaposleni brez znanja, podpore in jasnih usmeritev** doc. dr. Samo Tomažič, Uprava RS za jedrsko varnost, vodja Sektorja za upravljanje in kibernetsko varnost	Z različnimi pristopi zavedanja, kot so kratka predavanja, TTX in “hand-on” vaje, simulirani phishing napadi, informativni letaki, pa tudi bolj interaktivne metode, kot so križanke in enigme prek e-pošte, smo dosegli večjo prepoznavnost kibernetskih groženj med zaposlenimi. Sistematično izobraževanje in usposabljanje zaposlenih na različnih ravneh in vlogah v državni upravi omogoča boljše razumevanje tveganj ter krepitev veščin za varno uporabo informacijskih sistemov. Prilagojeni programi usposabljanja pripomorejo k boljši pripravljenosti na realne incidente. Sodelovanje z zunanjimi strokovnjaki pa prinaša dodatno strokovno znanje, sveže poglede in primere dobrih praks iz gospodarstva in mednarodnega okolja, kar dodatno prispeva k večji odpornosti državne uprave na kibernetske grožnje. Razvijanje varnostne kulture je dolgoročen proces, ki zahteva vključevanje vseh ravni organizacije. Le s skupnim razumevanjem pomena informacijske varnosti in redno komunikacijo o

		varnostnih temah lahko ustvarimo okolje, kjer je kibernetska varnost vsakodnevna praksa, ne zgolj tehnična odgovornost.
10.40 – 11.10	**Od pravil do navad: Kaj usmerja ravnanje zaposlenih v kibernetski varnosti?** dr. Špela Orehek, Fakulteta za družbene vede UL	V času “malih kibernetskih vojn” bi morala vsaka organizacija – ne glede na velikost ali dejavnost – zgraditi človeški požarni zid, ki skupaj s tehničnimi rešitvami predstavlja najmočnejši ščit pred napadalci. Morda se organizacije premalo zavedajo, da tvegano ali skrbno vedenje zaposlenih glede kibernetske varnosti usmerja vrsta različnih dejavnikov, od psiholoških na ravni posameznika, do tehnoloških in tudi organizacijskih. Ti dejavniki soustvarjajo šibko ali močno varnostno kulturo, ki je temelj organizacijske odpornosti proti kibernetskim grožnjam. Na predavanju bodo predstavljeni glavni gradniki varnostne kulture, s praktičnimi primeri in rezultati najnovejših raziskav pa bo prikazano, kako se ti dejavniki prepletajo in določajo vedenje zaposlenih.
11.10 – 11.45	odmor s pogostitvijo	
11.45 – 12.05	**Gremo s phishing simulacijami predaleč?** Jernej Porenta, 3fs, Staff Infrastructure Engineer	Simulacije phishing napadov so lahko že tako sofisticirane, da lahko pretentamo vsakega zaposlenega. Ampak ali s tem res dosežemo namen? Ali s tem samo pokažemo na zaposlenega, da je naredil nekaj narobe? Zato je potrebno pri simulaciji takih napadov vedno upoštevati tudi človeški dejavnik in pa tudi samo kulturo organizacije. V predavanju bomo tako spoznali dobre prakse pri postavljanju mej simulacij phishing napadov, da s tem dosežemo čimboljše rezultate na dolgi rok.
12.05 – 12.25	**Kako smo z »blagovno znamko« dvignili kibernetsko odpornost organizacije** Martin Vončina, GEN-I, Specialist za korporativno varnost in integriteto	Izobraževanje zaposlenih o kibernetski varnosti terja sodobne pristope, različna komunikacijska orodja in kanale, da bi to pomembno, a pogosto zapostavljeno področje, približali zaposlenim na zanimiv, razumljiv in predvsem dostopen način. Kako smo se tega lotili v GEN-I? Suhoparna, tehnično zahtevna in nezanimiva predavanja smo povsem transformirali v projektu GEN-I Shield. Nastala je celostna »blagovna znamka«, nova platforma, ki temelji na sodobnih pristopih in vključuje vse od kratkih video vsebin, interaktivnih izzivov, nagradnih iger, do rednih obvestil, praktičnih nasvetov ter vizualnih elementov, ki so postali prepoznavni del našega internega

		komuniciranja. Naš pristop je igriv, vključujoč in ciljno usmerjen – predvsem pa zasnovan z mislijo na uporabnika.
12.25 – 13.10	Okrogla miza **ČLOVEK – EDEN OD STEBROV KIBERNETSKE VARNOSTI**	Sodelujoči na okrogli mizi: Peter Krkoč, Zavarovalnica Triglav, Vodja informacijske varnosti – CISO doc. dr. Lili Nemec Zlatolas, Fakulteta za elektrotehniko, računalništvo in informatiko UM Ajda Marn, Svetovalka na področju upravljanja zaposlenih in kulture v podjetjih, 3fs
13.10 – 13.15	Zaključni pozdrav	