ZBORNIK

Leto 2025 je prineslo pravo prelomnico na področju kibernetske varnosti – leto, ko se teorija sooča z resničnostjo. Novi Zakon o informacijski varnosti (ZInfV-1) je stopil v veljavo, evropski krizni načrt Cyber Blueprint je dobil konkretno obliko, in organizacije se vse bolj zavedajo, da je odpornost več kot le tehnični pojem – je strateška nuja. Podjetja, javne institucije in posamezniki stojijo pred izzivom: kako prenesti zakonodajne zahteve v vsakodnevno prakso, kako prepoznati šibke točke in kako se pripraviti na neizogibne pretrese, ki jih prinaša digitalni svet. Konferenca Kibernetski cunami 2025 nas vabi, da skupaj pogledamo resnici v oči – da ocenimo, kako pripravljeni smo na val novih groženj in priložnosti. Program sledi celotnemu kibernetskemu življenjskemu ciklu – od prepoznavanja tveganj, zaščite in zaznave do odziva in okrevanja. Ponuja vpogled v ključne zakonodajne novosti, praktične prikaze rešitev in vpliv umetne inteligence na zaznavo groženj. Poseben poudarek bo namenjen iskrenemu dialogu z gospodarstvom: kako se odzivajo, kako krepijo odpornost in kaj so se naučili iz napadov, ki so že postali del naše vsakodnevne realnosti.

INTERAKTIVNO UVODNO PREDAVANJE – Milan Gabor, direktor, VIRIS d.o.o.

Milan Gabor je certificiran etični heker z več kot dvajsetletnimi izkušnjami in strokovnim znanjem na področju načrtovanja implementacije in testiranja s področja informacijske ter aplikacijske varnosti. Deluje na področju varnosti, ki vključuje varnostne preglede, penetracijska testiranja, preglede izvorne kode in svetovanja s področja varnosti najrazličnejšim podjetjem ter organizacijam. Visoko ocenjen in priljubljen govorec informacijske varnosti na konferencah širom sveta. Uživa v lovljenju računalniških hroščev in v raziskovanju informacijske varnosti. Aktivno sodeluje na nacionalnih in mednarodnih dogodkih, kjer je dokazal svojo strokovno usposobljenost, zato je cenjen in zaželen v informacijski sferi.

POZDRAVNI NAGOVOR – dr. Uroš Svete, direktor, Urad Republike Slovenije za Informacijsko Varnost

Dr. Uroš Svete, direktor Urada Vlade Republike Slovenije za informacijsko varnost, je strokovnjak za obrambo, varnostne študije, analizo konfliktov ter informacijsko in kibernetsko varnost. Med letoma 2011 in 2015 je vodil Oddelek za obrambne študije. Konec leta 2018 je postal generalni direktor Direktorata za informacijsko družbo na Ministrstvu za javno upravo, kjer je vodil ustanovitev Uprave za informacijsko varnost. Po ustanovitvi vladnega urada za informacijsko varnost leta 2021 je bil imenovan za njegovega direktorja.

POZDRAVNI NAGOVOR – Igor Zorko, podpredsednik GZS, pristojen za malo gospodarstvo in predsednik Združenja za informatiko in telekomunikacije

Igor Zorko je aktiven član Gospodarske zbornice Slovenije, kot podpredsednik GZS, pristojen za malo gospodarstvo in podjetništvo, in predsednik Združenja za informatiko in telekomunikacije aktivno zastopa slovenski IKT-sektor in predseduje Slovenski digitalni koaliciji. S svojim delovanjem si prizadeva za povezovanje vseh deležnikov za družbi in gospodarstvu prijazno digitalizacijo Slovenije. Je priznan poslovni strokovnjak in govornik na različnih prireditvah v zvezi z digitalno transformacijo, industrijo 4.0 in tudi digitalizacijo kot podpornim delom zdravstvenega sistema. Je aktiven član v združenjih, kot je Slovenski nacionalni forum za eRačun, in pobudnik Slovenske digitalne koalicije. V dolgoletni karieri je kot direktor podjetja ZZI pridobil veliko izkušenj na področju razvoja poslovnih rešitev, interoperabilnosti, e-poslovanja, digitalizacije, kibernetske varnosti in standardizacije e-poslovanja.

PREDAVANJE 1: Značilnosti kibernetskih incidentov v 2025, zaznava, odzivanje in kaj lahko izboljšamo

Gorazd Božič, vodja nacionalnega odzivnega centra za kibernetsko varnost SI-CERT

Gorazd Božič je vodja nacionalnega odzivnega centra za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team). Odzivni center SI-CERT od leta 1995 dalje preiskuje vdore v računalnike, okužbe z računalniškimi virusi in pomaga uporabnikom pri raznovrstnih drugih zlorabah na internetu, tudi skozi program ozaveščanja varninainternetu.si. Po Zakonu o informacijski varnosti je SI-CERT pristojen za obravnavo incidentov pri vseh zavezancih, razen za organe državne uprave, sprejema pa prostovoljne prijave tudi od vseh drugih subjektov v državi. Med letoma 2000 in 2008 je Gorazd Božič predsedoval evropski skupini odzivnih centrov TF-CSIRT, med leti 2004 in 2018 pa je bil predstavnik Slovenije v upravnem odboru Evropske agencije za kibernetsko varnost ENISA, med julijem 2020 in decembrom 2021 pa je predsedoval Mreži CSIRT, ki združuje vse nacionalne in vladne CSIRT skupine v EU. Gorazd je aktiven tudi pri podpori in mentorstvu novo formiranih odzivnih skupin v regiji jugovzhodne Evrope.

SI-CERT ustvarja pregled stanja na področju kibernetske varnosti v državi tako z dobro prepoznavnostjo (letno se bližamo 5.000 obravnavanih incidentov), kot tudi z obsežno vpetostjo v mednarodno CSIRT skupnost, ki je rezultat 30-letnega dela centra. Predavanje bo prikazalo delo centra v letu 2025, obravnavane incidente, obveščanje o ranljivostih in postreglo tudi z identifikacijo izzivov, ki še vedno niso popolnoma razrešeni. Novi zakonodajni okvir, ki prihaja iz EU naslavlja več tem, pomembno pa je pogledati, kako lahko ta okvir udejanimo v operativni praksi.

PREDAVANJE 2: Osnove (ne)varnosti

Matjaž Breskvar, CEO, Beyondsemiconductors

Ob poplavi kvantno-inspiriranih, umentnointeligenčno-izboljšanih, penetracijsko-stestiranih, military-grade-zaščitenih super-najnovejše-revolucionarnih kibernetsko-varnostnih storitev in produktov, katerih ustvarjalci pogosto ne poznajo niti varnostnih modelov izumljenih v 70-ih letih prejšnjega stoletja, bo predavanje neglamurozno osredotočeno zgolj na osnove in koncepte (ne)varnosti.

PREDAVANJE 2: Nove obvezne zahteve kibernetske varnosti za povezljive proizvode

Davorin Kacian, Pomočnik direktorja, SIQ Ljubljana

Proizvajalci fizičnih povezljivih naprav morajo s 1.8.2025 izpolnjevati tudi bistvene elemente kibernetske varnosti. Udeleženci bodo dobili vpogled v zahteve glede skladnosti iz Direktive o radijski opremi (RED 2014/53/EU), zlasti člena 3.3, in raziskali temeljne standarde kibernetske varnosti (ETSI EN 303 645 in EN 18031), ki oblikujejo obvezno zaščito za pametne naprave. Ta seja poudarja, kako bodo ti predpisi vplivali na uvajanje, trajnost in varnost naprav ter ustvarili priložnosti za podjetja, da prevzamejo vodilno vlogo na področju inovativne in varne tehnologije. Udeleženci bodo odšli s strateškim razumevanjem, kako krmariti po teh regulativnih spremembah na evropskem trgu in jih izkoristiti.

PREDAVANJE 3: Raziskovanje kibernetskih groženj in deljenje informacij

Metod Platiše, Telekom Slovenije d.d.

Bolje ko poznamo napadalce, značilnosti in tehnike njihovih napadov, odkrijemo podatke, ki so jih morda že pridobili, bolje se lahko pripravimo na njihove grožnje in učinkoviteje se lahko odzivamo. Vse te izkušnje pa je bolje, da držimo zase, ali ne ? Pogled na to temo tudi skozi prizmo EU projekta ALiEnS-SO.

PREDAVANJE 4: »Higienski minimum« kibernetske varnosti v notranjem omrežju
Grega Prešeren, tehnični direktor, Carbonsec d.o.o.

Grega Prešeren od leta 2017 deluje kot tehnični direktor in vodilni etični heker v soustanovljenem podjetju Carbonsec d.o.o. Je eden od pionirjev varnostnega testiranja v Sloveniji in se s tem področjem ukvarja od vsega začetka svoje karierne poti. Kot pentester v različnih podjetjih je od leta 2010 vodil in izvajal varnostne preglede omrežij, IT storitev, spletnih, mobilnih in drugih aplikacij in industrijskih oz. SCADA sistemov v Sloveniji in tujini. Je nosilec več strokovnih certifikatov s področja informacijske in aplikacijske varnosti in informacijskih omrežij. Aktivno deluje tudi kot predavatelj in izvajalec izobraževanj s področja aplikacijske varnosti. Svoja tehnična znanja nadgrajuje s poznavanjem različnih regulativ in standardov, zato je zaželen svetovalec pri oblikovanju strategij na področju kibernetske varnosti.

Kljub tehnološkemu napredku, regulatornim zahtevam in ozaveščanju na področju kibernetske varnosti vdorni testi in kibernetske vaje še vedno razkrivajo ranljivosti, ki jih v današnjem času ne bi več pričakovali. Katere ranljivosti najpogosteje odkrijemo pri izvajanju varnostnih testov v notranjih omrežjih? S kakšnimi ukrepi se jih da učinkovito odpraviti in kako nam pri tem lahko pomaga ocena tveganja?

V predavanju se bomo osredotočili na najpogosteje zaznane ranljivosti v slovenskih poslovnih okoljih in temeljne zakonitosti pri upravljanju informacijskih sistemov, ki pripomorejo k varnejšim informacijskim sistemom.

OKROGLA MIZA: Ko se prah poleže: Kako naprej po kibernetskem napadu?

Renato Burazer, direktor, AREM d.o.o. – MODERATOR okrogle mize

Renato Burazer, CISA, CISM, CRISC, CGEIT, CISSP, je IT revizor in poslovodni svetovalec v družbi AREM. Njegovo delo je tesno povezano z upravljanjem tveganj, digitalizacijo poslovanja, razvojem in implementacijo strategij ter z razvojem, kontrolo in revizijo informacijskih sistemov. Sodeluje z družbami različnih velikosti in javno upravo, izvaja neodvisne revizije informacijskih sistemov ter deluje kot neodvisni partner upravam in vodjem pri dvigovanju uspešnosti poslovanja in obvladovanju tveganj. Izkušnje je nabiral v panogah, kot so bančništvo, proizvodnja, zavarovalništvo, razvoj informacijskih rešitev, trgovina, avtomobilska industrija, distribucija in prodaja energije, storitve, nepremičninske agencije, razvoj nepremičninskih projektov, marine, javni sektor, farmacija in zdravstvo, izdelava maloserijskih kovinskih izdelkov ter načrtovanje plovil. V svoji karieri je vodil več kot 500 svetovalnih in revizijskih projektov v Centralni Evropi in ZDA.

Okrogla miza bo spodbudila prenos dragocenih izkušenj organizacij, ki so se soočile s kibernetskim napadom in lahko pomagajo usmeriti napore ter vire v prave smeri z ustreznimi prioritetami. Sogovornike bomo vprašali, kaj jim je šlo dobro pri obvladovanju kibernetskega napada in čemu so na podlagi teh izkušenj namenili dodatno pozornost. Skupaj bomo odgovorili na vprašanje, kaj naj vsaka slovenska organizacija v naslednjih šestih mesecih stori za izboljšanje svoje digitalne odpornosti. Udeleženci dogodka bodo pridobili konkretne ideje, ki jih bodo lahko prenesli v svoja delovna okolja ali pa potrdili ustreznost že implementiranih pristopov, če jih že izvajajo.

Ksenija Montani, Pomočnica direktorja, Lekarna Ljubljana

»Vse se zmore, če se hoče ali parafrazirano: Vse je mogoče. Če smo poslali človeka na Luno, bomo tudi ta problem/izziv/težavo rešili/odpravili.«

Več kot 20 let je zaposlena v Lekarni Ljubljana, kjer je kot pomočnica direktorja odgovorna za področje informatike in sodobnih tehnologij in s tem tudi za področje informacijske varnosti. V času njenega vodenja področja informatike in sodobnih tehnologij je IS Lekarne Ljubljana zrasel v kompleksen, razvejan in sodoben sistem, ki sledi trendom in priporočilom za varno ter neprekinjeno delovanje. V tem času je tudi temeljito vplivala na spremenjen odnos zaposlenih do informacijskih tehnologij, njihove uporabe oz uporabnosti, varnosti in pasti, ki jih s sabo prinaša vedno hitrejši in nebrzdan razvoj informatike.

Kibernetski napad 5.8.2019, iz posledic katerega se je Lekarna Ljubljana uspešno izvila in ponovno vzpostavila delovanje IS ter s tem poslovanja - predvsem po zaslugi pravilno zastavljenega koncepta IS, je bil zanjo učna ura ter opomnik, da se nič, kar se lahko stori že danes, ne odlaša na jutri. Kako zmanjševati tveganja in verjetnost, da do varnostnega incidenta pride.

Opis ukrepov, načina dela in razmišljanja. Izpostaviti pomembnost permanentnega izobraževanja zaposlenih in zaposlenih v IT-ju, preverjanja in merjenja kazalnikov kakovosti informacijskega sistema (npr pen testi ipd). Pridobivati neodvisno mnenje o stanju varnosti IS (zunanja revizija).Ozavestiti, da je neprekinjeno delovanje IS bistveno za neprekinjeno poslovanje organizacije.

Pavel Škerlj, izvršni direktor IT, Holding Slovenske Elektrarne d.o.o.

Pavel Škerlj je izkušeni strokovnjak s področja digitalne preobrazbe in kibernetske varnosti z več kot 30-letnimi izkušnjami na področjih IT, projektnega vodenja, logistike in kadrov. Kot vodja se osredotoča na ljudi, sodelovanje in rezultate. Uspešno je vodil odziv in obnovo po nedavnem kibernetskem napadu, kjer je ekipo usmeril k hitremu zajezitvi incidenta, vzpostavitvi varnega delovanja in krepitvi odpornosti.

Verjame, da kibernetska varnost ni le tehnologija, ampak predvsem ljudje, sodelovanje in pripravljenost.

Dr. Izidor Golob, pomočnik glavnega tajnika, vodja Računalniškega centra Univerze v Mariboru (RCUM)

Dr. Izidor Golob od leta 2009 vodi Računalniški center Univerze v Mariboru, pred tem je bil direktor Sekretariata Sveta za visoko šolstvo (sedaj NAKVIS). Začetne zaposlitvene izkušnje je od leta 1997 pridobival kot asistent in raziskovalec na UM FERI. Dalj časa je bil tudi predsedujoči Strokovnemu svetu ARNES. Ima pridobljene certifikate za vodjo informacijske varnosti (CISM), za revizorja informacijskih sistemov (CISA) ter certifikat ITIL F.

PREDAVANJE 5: Od pregleda do skladnosti: praktične izkušnje z ZInfV-1

Suzana Kužnik, višja svetovalka in Tevž Delak, višji menedžer FORVIS MAZARS IT d.o.o.

Suzana Kužnik je višja svetovalka v družbi Forvis Mazars IT d.o.o. Na začetku svoje kariere se je osredotočala predvsem na presoje in priprave na certifikacije po standardu ISO/IEC 27001. Kasneje je v sklopu svojega dela v varnostno operativnem centru (SOC) pridobivala izkušnje iz upravljanja varnostnih izzivov in problemov ter izpopolnila svoje sposobnosti reševanja incidentov. V zadnjih letih je sodelovala pri revizijah in pregledih informacijske in kibernetske varnosti ter pregledih skladnosti z različnimi standardi in zakonodajo (NIS2, SWIFT, DORA, ISO/IEC 27001 itd.). Suzana je diplomantka Informacijske varnosti in nosilka nazivov ISO/IEC 27001:2022 Information Security Manager in ISO/IEC 27001:2022 Information Security Auditor.

Tevž Delak je višji menedžer v podjetju Forvis Mazars IT d.o.o. Ima več kot 17 let izkušenj na področju revizije informacijskih sistemov, informacijske varnosti, kibernetske varnosti, upravljanja varstva osebnih podatkov, upravljanja tveganj, upravljanja neprekinjenega poslovanja, upravljanja IT storitev in projektnega vodenja. V 17 letih delovanja na področju upravljanja in varovanja I&T je izvajal svetovalne in revizijske storitve v različnih industrijah, predvsem zafinančni in storitveni sektor. V karieri je pridobil certifikate Certified Information Systems Auditor (CISA), Certified Data Privacy Soulutions Engineer (CDPSE), PRINCE2 Foundation, ITIL4 Foundation Certificate in je notranji presojevalec sistema upravljanja neprekinjenega poslovanja.

ZInfV-1 določa, da bistveni in pomembni subjekti vzpostavijo vrsto tehničnih in organizacijskih ukrepov, ki temeljijo na celovitem in sistematičnem ocenjevanju tveganj. Pregledi skladnosti v praksi pogosto pokažejo vrzeli ali celo neobstoj dokumentacije, nepopolno ocenjevanje tveganj, pomanjkljivo povezavo med oceno tveganj in izbiro varnostnih ukrepov ter nejasno razdelitev odgovornosti.

Na predavanju bomo predstavili naš pristop k izvedbi pregledov skladnosti z ZInfV-1, tipične ugotovitve iz različnih sektorjev ter dobre prakse pri odpravljanju neskladnosti. Udeleženci bodo spoznali, kako rezultate pregleda preoblikovati v izvedljiv načrt ukrepov, ki ne le izpolnjuje zakonske zahteve, ampak tudi krepi kibernetsko odpornost organizacije.

PREDAVANJE 6: Umetna inteligenca: priložnost za podjetja, ne grožnja

Marko Zavadlav, Actual IT d.d.

Marko Zavadlav je svetovalec na področju revizij informacijskih sistemov, varovanja informacij, skladnosti s standardi na področju varovanja informacij varovanja osebnih podatkov in neprekinjenega poslovanja. Je član ekipe Actual IT. Na področju informatike deluje že več kot 30 let, pred več kot 20 leti se je specializiral za področje varovanja informacij. Sodeluje v različnih strokovnih skupinah.

Kako iz regulative in standardov narediti konkurenčno prednost? Umetna inteligenca prinaša nova pravila, a tudi številne priložnosti. EU Akt o umetni inteligenci ni ovira, temveč vodilo, standard ISO 42001 pa orodje, ki podjetjem pomaga pri varni, pregledni in uspešni uporabi umetne inteligence.

PREDAVANJE 7: Izzivi zagotavljanja skladnosti z ZinfV-1 v praksi

Dr. Andrej Rakar, Vodja informacijske varnosti, Petrol d.d.

Andrej Rakar, dr. elektrotehniških znanosti, je na Institutu Jožef Stefan deloval na področju nadzornih sistemov tehničnih procesov in uvajanju informacijskih tehnologij v proizvodnjo. Na področju informacijske varnosti deluje že od leta 2005, praktične izkušnje pa si je pridobil na najzahtevnejših projektih za finančne ustanove, zavarovalnice, telekomunikacijske operaterje, zdravstvo in podjetja iz gospodarstva doma in v tujini. Kot vodja informacijske varnosti (CISO) v podjetju Petrol d.d. je zadolžen za upravljanje z informacijsko varnostjo, uresničevanje strategije kibernetske varnosti ter nadzor izvajanja ukrepov varovanja informacij. Poleg tega predava na različnih konferencah in drugih prireditvah s tematiko informacijske varnosti.

Zakon o informacijski varnosti (ZInfV-1) predstavlja temeljni okvir za obvladovanje tveganj informacijskih in kibernetskih groženj, ki zahteva od bistvenih in pomembnih subjektov izvajanje tehničnih, organizacijskih in kadrovskih ukrepov. Ti ukrepi morajo biti učinkoviti, sorazmerni, preverljivi in prilagojeni dejanskim tveganjem ter vključujejo vse od podpore vodstva, varnosti kadrov, upravljanja dostopov, varnostnih kopij, kriptografije, do zaščite dobavne verige in fizične varnosti.

V praksi se organizacije soočajo z izzivi pri razumevanju obsega zakonskih obveznosti, usklajevanju z obstoječimi standardi, zagotavljanju dokazljivosti ukrepov ter sodelovanju z

zunanjimi ponudniki. Poleg tega zakon zahteva redno preverjanje učinkovitosti ukrepov, odzivanje na incidente in upoštevanje evropskih izvedbenih aktov, kar zahteva stalno prilagajanje in strateško upravljanje informacijske varnosti. Na predavanju bomo predstavili korake, ki smo jih prehodili na Petrolu za doseganje skladnosti, osvetlili primere dobrih praks ter opozorili na najpogostejše napake in pasti, ki se pojavljajo pri implementaciji zahtev.

PREDAVANJE 8: Phishing 2.0: Stara grožnja, nove metode – kako se branimo danes?
Lucija Starc, SOC analitičarka, Women4Cyber, T-2 d.o.o.

Lucija Starc že več kot 6 let deluje na področju telekomunikacij, zadnje leto pa se kot SOC analitičarka posveča kibernetski varnosti. Pri tem jo vodita radovednost in želja po razumevanju delovanja sistemov, kar ji pomaga pri hitrem prepoznavanju groženj, učinkovitih odzivih in grajenju varnejšega digitalnega okolja. Delo jo navdihuje, ker združuje analitično razmišljanje, reševanje izzivov in občutek odgovornosti do uporabnikov in podatkov.

Elektronska pošta ostaja ena najpogostejših in najuspešnejših vstopnih točk za kibernetske napade – od preprostih phishing poskusov do naprednih zlorab zaupanja in kompromitiranih poslovnih komunikacij. Kljub temu, da gre za dobro poznan vektor napada, je za podjetja še vedno ena najtežjih groženj. V predavanju predstavim, kako se s takšnimi incidenti soočamo v praksi, kakšno vlogo pri tem igrajo orodja, kot so SOAR in EPDR, ter predstavim učinkovite rešitve. Predavanje združuje tehnični vpogled in praktične izkušnje, zato je namenjeno tako strokovnjakom kot tudi odločevalcem v podjetjih.

PREDAVANJE 9: Kaj storiti v primeru kibernetskega napada

Uroš Lesjak, MBA, direktor, Inovis IT d.o.o.

Uroš Lesjak, MBA, je direktor podjetja Inovis IT, kjer že več kot desetletje svetuje podjetjem pri krepitvi njihove informacijske varnosti, digitalizaciji in skladnosti z zakonodajo. Združuje praktične izkušnje z vodenjem projektov in strateški pogled na kibernetsko varnost kot ključno področje odpornosti in zaupanja v sodobnem poslovanju. Kot predavatelj nastopa na gospodarski zbornici, strokovnih konferencah in v podjetjih, kjer z jasno razlago kompleksnih tematik povezuje poslovne odločevalce in IT strokovnjake.

Kibernetski napadi so realnost, s katero se danes soočajo podjetja vseh velikosti in sektorjev.

Povzročena škoda se meri v milijonih evrov, čas do odkritja incidenta pa je pogosto predolg, da bi lahko pravočasno preprečili posledice. Predavanje predstavi aktualne trende in številke s področja kibernetskih napadov, najpogostejše napadalne metode in ranljivosti ter konkretne ukrepe, ki jih lahko podjetja uvedejo za učinkovitejši odziv in hitrejše okrevanje. Poseben poudarek je namenjen zakonodajnemu okviru NIS2/ZInfV-1, ki prinaša nove obveznosti, a hkrati tudi koristi za boljšo pripravljenost organizacij.