ZBORNIK

V sklopu meseca kibernetske varnosti vas vabimo, da se pridružite naši konferenci in izboljšate varnost svojega podjetja ter zaščitite svojo prihodnost! Predstavili bomo nov Zakon o informacijski varnosti (ZInfV), ki prinaša pomembne spremembe in v slovensko zakonodajo vpeljuje direktivo NIS 2. Ta zakon bo razširil krog organizacij, ki bodo zavezane k strožjim varnostnim standardom, ter dodatno opredelil odgovornosti zavezancev in njihovih odgovornih oseb – vključno s podjetji v dobavni verigi. Predstavili bomo tudi na najnovejše grožnje, kibernetske napade in izzive, s katerimi se soočamo v digitalnem svetu. Strokovnjaki bodo predstavili nove tehnologije in inovativne rešitve za preprečevanje kraje podatkov, zaščito pred napadi ter vzpostavitev trajnih strategij odpornosti v podjetjih in organizacijah. Cilj konference je ozaveščanje podjetij in organizacij ter širše javnosti o pomembnosti kibernetske varnosti. S prenosom znanja med udeleženci pa želimo prispevati k višji ravni kibernetske zaščite v poslovnem okolju v Sloveniji.

POZDRAVNI NAGOVOR – Marjana Majerič, izvršna direktorica, GZS

Marjana Majerič, magistra ekonomije, izvršna direktorica za strateški razvoj in internacionalizacijo na GZS, prej direktorica Zbornice osrednjeslovenske regije znotraj GZS ima več kot 30 let delovnih izkušenj na področjih finančnega upravljanja, poslovne strategije in načrtovanja ter internacionalizacije podjetji. V okviru GZS je tudi izvršna direktorica Sekcije za startup in scaleup podjetja, Sekcije za fitnes, rekreacijo in regeneracijo ter Sekcije slovensko-kitajskega poslovnega sveta. Pred vstopov v GZS je bila v podjetju PWC zunanja svetovalka za področje javnega sektorja in razvojnih politik EU, še prej pa pomočnica direktorja Tehnološkega parka Ljubljana ter pobudnica in soustvarjalka Iniciative Startup Slovenija ter aktivna članica Združenja inkubatorjev in tehnoloških parkov Slovenije. Hkrati je bila pobudnica ustanovitve Sekcije ženskih managerk v Svetovnem združenju znanstvenih in tehnoloških parkov.

POZDRAVNI NAGOVOR 2 – 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.

UVODNO PREDAVANJE 1: Navigating the EU Cyber Security Landscape: Technologies, Roadmaps, and Challenges *(*english)*

Roberto Cascella, CTO, European Cyber Security Organisation (ECSO)

Roberto Cascella works as Chief Technology Officer at the European Cyber Security Organisation (ECSO). He also coordinates the two technical ECSO WGs with a high impact on the European cybersecurity strategy focused on the definition of the cybersecurity R&I roadmap for trusted and resilient technologies, and the establishment of trusted supply chains at EU level. He also represents ECSO in different committees, including the SCCG established under the Cybersecurity Act. Roberto serves as Project Coordinator of the European Cybersecurity Community Support project (ECCO) that received funding from DEP to support the activities necessary to develop, promote, coordinate and organise the work of the Cybersecurity Competence Community at European Level, within the scope and operations of the ECCC and National Coordination Centres Network. Roberto holds a Ph.D. (2007) in ICT from University of Trento, an M.Sc. in Telecommunication engineering from Politecnico di Torino and KTH Stockholm.

This lecture will provide some insights on the evolving European cybersecurity landscape, starting from a quick view of the evolving threats and regulatory framework to promote cyber resilience in Europe. Then, the focus will be on the challenges to sustain the digitalisation of the society and industrial sectors towards EU digital autonomy by developing and fostering trusted technologies.

PREDAVANJE 2: ZInfV-1: regulatorne zahteve in odgovornost podjetij za informacijsko varnost
Matjaž Mravljak, direktor Inšpekcije za informacijsko varnosti, URSIV

Matjaž Mravljak je direktor Inšpekcije za informacijsko varnost v Uradu Vlade Republike Slovenije za informacijsko varnost. S področjem informatike, telekomunikacij in informacijsko varnostjo se poklicno ukvarja več kot 15 let, z nadzorom pa zadnje tri leta. Matjaž Mravljak je magister prava, preizkušeni revizor informacijskih sistemov, vodilni presojevalec sistema upravljanja informacijske varnosti po ISO 27001, notranji presojevalec sistema upravljanja neprekinjenega poslovanja po ISO 22301 ter certificiran strokovnjak s področja informacijske in kibernetske varnosti.

Direktiva EU o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS 2) bo v slovenski pravni red prenesena z novim Zakonom o informacijski varnosti. Z novim zakonom se bo število zavezancev bistveno povečalo, spremenili se bodo pragovi in način določanja zavezancev, povečuje se tudi obseg varnostnih ukrepov, dodane so nekatere druge obveznosti. Pogledali bomo bistvene spremembe, ki jih prinaša implementacija NIS 2 direktive v naš pravni red, kako je z odgovornostjo odgovornih oseb in pravnih oseb za prekrške ter nekatera najpogostejša neskladja, ki jih na terenu zaznava inšpekcija za informacijsko varnost pri izvajanju nadzorov zavezancev iz Zakona o informacijski varnosti.

PREDAVANJE 3: Krepitev varnosti v industriji in kritični infrastrukturi z direktivo NIS 2
Boris Krajnc, certificiran etični heker in specialist za kibernetsko varnost, Telekom Slovenije d.d.

Boris Krajnc je certificiran etični heker in specialist za kibernetsko varnost. Ima 20 let izkušenj na področju informacijske tehnologije, s kibernetsko varnostjo pa se ukvarja že več kot 10 let. V zadnjih letih se je specializiral za področje kibernetske varnosti v industrijskih okoljih in okoljih kritične infrastrukture.

Prihaja iz podjetja Telekom Slovenije, kjer dela kot tehnični specialist za področje varnostnih pregledov, penetracijskih testiranj in digitalnih forenzičnih analiz omrežij v kritičnih, poslovnih, industrijskih in infrastrukturnih okoljih. Strokovno znanje nadgrajuje z mednarodnimi certifikati, kot so GICSP, GNFA,GRID, CEH, CCNP, CCNA-Sec in JNCIA.

Vsi se zavedamo pomembnosti kibernetske varnosti v okoljih IT in OT ter si prizadevamo doseči najvišje standarde. A vedno je prostor za izboljšave, kar poudarjajo tudi snovalci nove direktive NIS2. Ta direktiva postavlja enotna pravila za celotno Evropo, na predavanju pa bomo izpostavili ključne točke in prikazali, kako vam lahko pri implementaciji rešitev pomagamo.

PREDAVANJE 4: Nove tehnologije in trendi na področju kibernetske varnosti v svetu
Peter Novak, Vodja področja Cybersecurity rešitev, Microsoft

Peter Novak ima 30 let izkušenj na IT področju, tako na strani lokalnih ponudnikov rešitev kot v velikem globalnem podjetju. Zadnja leta je opravljal vodstvene naloge na različnih področij prodaje v EMEA regiji, zadnji dve leti pa vodi področje Kibernetske varnosti v podjetju Microsoft na trgih Vzhodne in južne Evrope, bližnjega vzhoda in Afrike za področje velikih podjetij.

Pri svojem delu se srečuje s srednjimi in velikimi podjetji, institucijami in specializiranimi IT partnerji s področja kibernetske varnosti in ima tako dober vpogled v izzive s katerimi se srečujejo strokovnjaki, ki delujejo na tem področju. Trenutni trendi so skrb vzbujajoči, a ostaja optimist, saj vedno več vodij in uprav spoznava strateški pomen kibernetske varnosti kot enega ključnih pogojev za inovativnost, ki v globalnem svetu (p)ostaja ključna prioriteta. Nove tehnologije prinašajo odgovore na ključne izzive sedanjosti, a odpirajo nova vprašanja v prihodnosti. Tehnologije so velik del rešitve, a brez pravih procesov in usposobljenih strokovnjakov zaželenih rezultatov ne bo moč doseči.

Kateri trendi krojijo področje kibernetske varnosti danes in kako to vpliva na trenutno stanje. Zakaj je Microsoft zaupanja vreden partner in v čem se razlikujemo od množice ponudnikov na tem področju. Kaj si želijo stranke in kako te izzive naslavljamo z našo celovito platformo? Kakšno vlogo pri tem igra umetna inteligenca?

PREDAVANJE 5: Sodobno digitalno okolje po uveljavitvi NIS 2 direktive – kako se pripraviti?
Uroš Majcen, direktor kibernetske odpornosti, Kontron SI d.o.o.

Uroš Majcen, direktor kibernetske odpornosti v podjetju Kontron SI d.o.o. je že vrsto let prisoten v slovenskem in mednarodnem prostoru na področjih zagotavljanja informacijske in kibernetske varnosti, tako za Kontron kot za stranke.

Sprejetje lokalne zakonodaje – ZinfV1, ki je zakon, ki prinaša NIS2 direktivo v slovenski pravni red je pred nami. Zakon širi obseg zavezancev, veča nabor nalog in daje določene specifične poudarke pri informacijski varnosti. Vse v luči izboljšanja stanja informacijske varnosti za potrebe zagotavljanja varnosti digitalnega okolja. Na predavanju se bomo na kratko ozrli na osnovne točke direktive in zakona, pokazali praktične korake pri vpeljevanju direktive in razbili nekaj mitov.

PREDAVANJE 6: Upravljanje privilegiranih dostopov (PAM): Ključ do varnosti v digitalni dobi
Borut Jenko, vodilni inženir za kibernetsko varnost, Smart Com d.o.o.

Borut Jenko je vodilni inženir za kibernetsko varnost in tehnološki navdušenec v podjetju Smart Com. Njegovo področje delovanja zajema predvsem upravljanje privilegiranih dostop (PAM) in sistemi za zaznavanje in odziv na incidente (SIEM). Borut je strasten zagovornik inovativnih rešitev in se posveča iskanju novih pristopov za preprečevanje kibernetskih napadov ter zaščito občutljivih podatkov.

PAM je ključnega pomena za zaščito kritičnih podatkov in sistemov z nadzorom dostopa privilegiranih uporabnikov. Zato bo Borut Jenko bo predstavil upravljanje privilegiranih dostopov kot ključ do varnosti v digitalni dobi.

PREDAVANJE 7: FutuReslience: Ali smo pripravljeni na prihodnje izzive kibernetske varnosti?
Luka Jelovčan, direktor Inštituta za Varnost in Strateške Raziskave (IVSR)

Luka Jelovčan je v upravljanje varnosti vpleten že od svojih študentskih let, ko je na Fakulteti za varnostne vede več let sodeloval na različnih raziskovalnih projektih. Je avtor in soavtor številnih znanstveno raziskovalnih objav, med drugim je tudi najmlajši prejemnik Študentske raziskovalne nagrade Fakultete za varnostne vede. Svojo pot je nadaljeval v podjetju SGB varnostno svetovanje d.o.o. kjer deluje kot operativni direktor in vodi projekte na področju korporativne varnosti, informacijske varnosti ter poslovne analitike. Je poslovni direktor Inštituta, poleg tega pa vodi tudi raziskovalno razvojne projekte in projekte varnosti na ključ.

Projekt Slovenian Cyber Resilience Lab (SCRL) je pilotni projekt evropskega konzorcija FutuResilience in deluje pod okriljem razvojne sheme Horizon Europe. Naloga konzorcija FutuResilience je odkriti sistemske rešitve za globalne krize, s katerimi se bo v prihodnosti soočala evropska družba. Posledično, se v okviru SCRL ukvarjamo z izzivi, ki jih kibernetske grožnje prinašajo razvojnim podjetjem danes in jih bodo prinašale v prihodnosti. S pilotnim projektom SCRL želimo prepoznati izzive s katerimi se na področju zagotavljanja kibernetske varnosti soočajo slovenska razvojna podjetja danes in izzive s katerimi se bodo na tem področju soočala v bližnji prihodnosti. Na podlagi naših ugotovitev bomo predlagali sistemske rešitve, ki bodo v naslednjih letih služile kot podlaga za sprejem politik in drugih ukrepov na lokalni, nacionalni in evropski ravni.

PREDAVANJE 8: Socialni inženiring? Kaj je to in kako vam lahko sodobne digitalne platforme za kibernetsko varnost pomagajo usposobit vaše sodelavce

Boštjan Špehonja, CEO, GO-LIX d.o.o.

Boštjan Špehonja je direktor podjetja GO-LIX d.o.o ter strokovnjak na področju kibernetske varnosti s kar nekaj mednarodno priznanimi certifikati (Certified Ethical Hacker – Master, Certified Network Defense Arcihtect, Security+, CEH Practical, CompTIA Advanced Security Practitioner ce, CompTIA CySA+). Ima širok nabor izkušenj, saj mu je pregled svojega IKT okolja zaupalo že več sto organizacij, kot so podjetja s kritično infrastrukturo, banke, zavarovalnice, ministrstva, ter številna druga. Izvaja tudi izobraževanja ter delavnice na temo varne uporabe interneta in etičnega hekanja, najbolj pa uživa ob odzivih na kibernetske incidente. Predaval je na vseh največjih konferencah informacijske varnosti v Sloveniji. Je soustanovitelj fundacije SICEH (Slovenian Certified Ethical Hackers) ter gostujoči strokovnjak Univerze v Mariboru in predavatelj na Gea Collegu.

PREDAVANJE 9: Upravljanje kibernetskih tveganj - pasti ali priložnosti?

dr. Saša Javorič, vodilna presojevalka sistemov vodenja ISO 9001 in 27001, SIQ

dr. Saša Javorič je vodilna presojevalka sistemov vodenja kakovosti (9001) in informacijske varnosti (27001), predavateljica in nosilka akreditiranega programa Skrbnik upravljanja tveganj informacijske varnosti / Information Security Risk Manager mednarodne mreže certifikacijskih organov IQNet. Že več kot dvajset let svetuje organizacijam na področju digitalizacije procesov, sistemov vodenja kakovosti, informacijske varnosti in neprekinjenega poslovanja v avtomobilski in letalski industriji, razvoju programskih rešitev, energetiki, šolstvu, zdravstvu, razvoju in proizvodnji medicinskih pripomočkih, ki so uspešno vpeljale in certificirale sisteme vodenja. Na podlagi izkušenj iz prakse bomo pregledali dejavnike učinkovitega upravljanja tveganj in se pogovorili, kakšne so pasti in kje so lahko priložnosti izboljšav pri obvladovanju tveganj informacijske / kibernetske varnosti.

PREDAVANJE 10: Avtomatizacija-Ključno orodje pri izvajanju MDR

Kristina Stojchevska, analitičarka za kibernetsko varnost, NIL d.o.o. in članica Women4Cyber SI

Kristina Stojchevska je magistrirala na Fakulteti za Varnostne vede, smer Informacijska Varnost. Trenutno dela kot analitičarka za kibernetsko varnost pri podjetju NIL d.o.o in je članica organizacije Women4Cyber.

V sodobnem svetu informacijske varnosti, kjer je količina podatkov in število varnostnih incidentov v stalnem porastu, avtomatizacija postaja ključno orodje - tudi za napadalce, ki svoje napade vse bolj avtomatizirajo. S pomočjo avtomatizacije lahko analitiki kibernetske varnosti, ki zaznajo alarme le-te hitreje in učinkoviteje preiskujejo ter se nanje tudi odzovejo. Prav avtomatizacija je ključnega pomena pri hitrem in učinkovitem odgovoru na grožnje, ki jih vsakodnevno predstavljajo novi kibernetski napadi. Avtomatizacija olajša delo analitikom in s tem pripomore k hitrejšemu triažiranju alarmov.

PREDAVANJE11: Novi pristopi k testiranju kibernetske varnosti in obvladovanju tveganj
Grega Prešern, CTO, Carbonsec d.o.o.

Izredno bogate izkušnje na področju etičnega hekanja in preverjanja učinkovitosti kibernetske varnosti omogočajo Gregu Prešernu širši pogled na to kompleksno področje in podpirajo njegove odločitve v skrbi za razvoj in kvaliteto naših storitev. Pri tem vedno večji poudarek namenja svetovanju na področju strateškega upravljanja kibernetske varnosti, saj vse bolj napredne oblike napadov od skrbnikov sistemov zahtevajo agilno in hkrati stroškovno učinkovito prilagajanje novim okoliščinam.

Nova zakonodaja na področju kibernetske in informacijske varnosti pričakuje od poslovodstva in od upravljavcev kibernetske varnosti drugačen, bolj celosten pogled na obvladovanje kibernetskih tveganj. Obseg predvidenih aktivnosti vključuje varnostne preglede, izobraževanje uporabnikov in obvladovanje celotne površine napada, vključno z dobavitelji, ki se povezujejo z našim omrežjem. Različne tehnike in oblike varnostnih testov prinašajo različne rezultate. Kako pristopiti k upravljanju kibernetske varnosti, da boste na podlagi rezultatov v največji možni meri izboljšali stanje kibernetske varnosti?

PREDAVANJE 12: Učinkovito prepoznavanje groženj in ocenjevanje tveganj v praksi
Erik Petelin, inženir varnostnih rešitev, CREAPLUS d.o.o.

Erik Petelin je inženir varnostnih rešitev s poglobljenim znanjem na področju kibernetske varnosti in obvladovanja informacijske tehnologije. Osredotoča se predvsem na analizo groženj, pri čemer je pridobil certifikat Foundation Level Threat Intelligence Analyst. Njegovo delo vključuje razvoj strategij za identifikacijo in odzivanje na varnostne grožnje, s čimer podjetjem omogoča zaščito njihovih informacijskih sistemov. Dodatno je certificiran tudi kot Microsoft Certified Azure Administrator Associate in Azure Solutions Architect Expert, kar mu omogoča oblikovanje, implementacijo in upravljanje rešitev v oblaku, ki so varne in optimizirane za različne poslovne zahteve.

Predstavitev se osredotoča na proaktivno obveščanje o kibernetskih grožnjah (CTI) kot ključni komponenti kibernetske varnosti. Poudarja pomen odkrivanja in blažitve groženj z nenehnim spremljanjem, analizo podatkov in razširjanjem. Z uporabo platform lahko organizacije sledijo grožnjam v različnih spletnih slojih. Predstavitev obravnava tudi glavne kibernetske grožnje, kot sta izsiljevalska programska oprema in lažno predstavljanje, podprta s študijami primerov iz resničnega sveta.

PREDAVANJE 13: Odgovor na izzive trga dela: Od Cyber kampa do študijskega programa
dr. Laura Fink, Gea College
GEA College - Fakulteta za podjetništvo je vodilna zasebna poslovna šola v Sloveniji, ki jo odlikuje 30-letna praksa odličnega poučevanja. Čeprav je GEA College začel s podjetništvom, nadaljuje v smeri izobraževanj, ki jih trg nujno potrebuje in za poklice prihodnosti, kot so: Digitalni marketing, Upravljanje s tveganji in korporativna varnost, Informacijska in kibernetska varnost, Cyber kamp za mlade.