ZBORNIK

Letna konferenca: Kako se spopasti z aktualnimi grožnjami v kibernetskem prostoru?

27. 10. 2023, 9:00-14:00, GZS, dvorana A

UVODNI 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 - Katja Kraškovic, direktorica in dekanja, Gea College - Fakulteta za podjetništvo, aktivna članica Sekcije za kibernetsko varnost

Mag. Katja Kraškovic je po zaključeni izobrazbi s področja financ zasedala različne položaje - od finančnega analitika do člana uprave v finančnih podjetjih, kot sta Poteza in KD Group. Predanost, delovna etika in strast do posla so ji prinesli številna napredovanja ter vodenje podjetij v regiji.

Po 10 letih dela v financah se je odločila za nove izzive. Na področju izobraževanja se je preizkusila že na IEDC Poslovni šoli Bled ter nadaljevala na GEA College. Čutila je, da z izobraževanjem perspektivnih bodočih kadrov lahko prispeva k izboljšanju učnih izkušenj.

Danes je direktorica in dekanja GEA College-a, Fakultete za podjetništvo - vodilne zasebne poslovne šole 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 (npr. Digitalni marketing, Upravljanje s tveganji in korporativna varnost, Informacijska in kibernetska varnost itd.) in so poklici prihodnosti.

Meni, da sta povezovanje in sodelovanje podjetij z izobraževalnimi sektorjem ključna. Prav zato sodeluje tudi v poslovni skupnosti in združenjih, ki počnejo prav to – povezujejo.

UVODNO PREDAVANJE 1: "Shielding Your Business: Essential Cybersecurity Strategies for SMEs in Europe" (English)

Vencel Cserháti, Cybersecurity and Privacy Officer, Huawei Technologies Hungary and Adriatik Region

Vencel Cserhati is a senior Information Technology / Cybersecurity / Data Privacy professional with CIPP/E, CIPM, CIPT, Green Belt certifications and possesses more than 25 years of experience in Cybersecurity and Information Technology. He has recently joined to Huawei as Cyber Security and Privacy Officer in the Hungary & Adriatic region Rep Office responsible for cybersecurity requirement management and planning, following security and privacy related regulatory developments, external communication, compliance and risk management, awareness building.

This presentation provides guidance and best practices for small and medium-sized enterprises (SMEs) in Europe to protect their businesses from cyber threats. It is going to discuss the importance of cybersecurity awareness and training for employees and provide practical tips and tools to help SMEs improve their cybersecurity posture.

Na dogodku bo predstavljena tudi slovenska izdaja vodnika: **Spodbujanje kibernetske varnosti za MSP v Evropi – Vodnik z vprašanji in odgovori.** V Evropi je 25 milijonov malih in srednje velikih podjetij (MSP), ki zaposlujejo 100 milijonov ljudi. MSP je kar 99,8 odstotkov vseh podjetij v Sloveniji. Pravimo, da so hrbtenica našega gospodarstva, saj zaposlujejo skoraj 70 odstotkov ljudi in ustvarijo 65 odstotkov prihodkov vseh podjetij. MSP so gonilna sila digitalnega preoblikovanja in gospodarske rasti. Spodbujanje kibernetske varnosti MSP je zato zelo pomembno. Vodnik jasno določa, kako lahko MSP izboljšajo svojo kibernetsko varnost, določa naravo različnih kibernetskih napadov in kako jih ublažiti. Vodnik ponuja tudi veliko koristnih informacij, kje lahko MSP poiščejo več informacij o tem, kako izboljšati kibernetsko odpornost. Povezava do angleške različice: HUA-2023-0048-PACD-SME-Cybersecurity-Brochure-20230213-V2.indd (huawei.com)

UVODNO PREDAVANJE 2: Kako se praktično odzvati na spremembe v okolju KV v podjetju?

Uroš Majcen, direktor kibernetske odpornosti, Kontron d.o.o.

Uroš Majcen vodi področje kibernetske odpornosti v podjetju Kontron Slovenija, kjer zagotavljajo rešitve in storitve kibernetske odpornosti zase, za skupino Kontron ter tudi na trgu.

Kibernetska varnost je postalo ključno polje zagotavljanja razpoložljivosti in varnosti storitev v digitalnem svetu. Zaradi tega je tudi družba kot takšna začela skozi regulativo dajati navodila in naloge uporabnikom in ponudnikom storitev. Predavanje bo poskušalo opisati novo realnosti in prevesti te zahteve v primere dobre prakse in osnovni nabor korakov za zagotavljanje kibernetske varnosti v sodobnem času.

PREDAVANJE 1: Varnostni pregledi v okoljih operativne tehnologije (OT)

Boris Krajnc, specialist za kibernetsko varnost, Telekom Slovenije d.d.

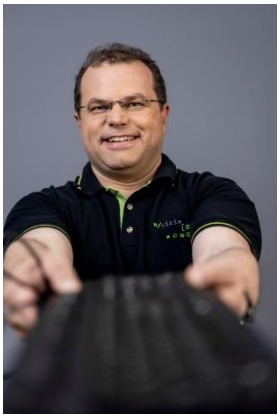
Boris Krajnc je certificiran etičnih heker in specialist za kibernetsko varnost. Ima 20 let izkušenj na področju informacijske tehnologije, s kibernetsko varnostjo pa se ukvarja že več kot 10 let. V zadnjih letih se je specializiral za področje kibernetske varnosti v industrijskih okoljih in okoljih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

Varnostni pregledi omrežja in opreme v okoljih informacijske tehnologije - IT predstavljajo za podjetje obliko "revizije". Na tak način ugotavljamo kje so pomanjkljivosti oziroma ranljivosti, glede na pridobljene rezultate pa je potrebno pristopiti k odpravi le teh. Vse to izvajamo z namenom, saj v okoljih informacijske tehnologije - IT varujemo **podatke**. Kaj pa okolja operativne tehnologije - OT, kjer varujemo **procese**. Žal se premalo zavedamo, da smo vsak trenutek odvisni od naprav, ki upravljajo procese. Dostava električne energije, komunalne storitve, promet, proizvodni procesi so odvisni od "zdravja" naprav in omrežja, ki so del operativne tehnologije. Torej je potrebno narediti varnostni pregled in ugotoviti, če so vključeni vsi varnostni mehanizmi in je oprema in omrežje ustrezno zaščitena. Žal v tem primeru klasični varnostni pregled NE pride v poštev, saj so okolja operativne tehnologije specifična in je zato potreben poseben pristop. Kako se lotimo pregledov in kako zagotovimo varnost v okolju operativne tehnologije pri Telekomu Slovenije pa v predavanju.

PREDAVANJE 2: Kaj deluje in kaj ne deluje pri preverjanju kibernetske varnosti v podjetjih?

Milan Gabor, ustanovitelj in direktor, Viris d.o.o.



Milan Gabor je certificiran etični heker, strokovnjak kibernetske varnosti, predavatelj na številnih konferencah s področja kibernetske varnosti tako doma kot v tujini, raziskovalec, svetovalec in TEDx govorec. Kot ustanovitelj in direktor podjetja Viris je le-tega zgradil in ga spremenil v pomembnega igralca V Sloveniji. Kot predavatelj je izvedel vrsto različnih tečajev in usposabljanj s področja informacijske vestnosti. V vlogi raziskovalca je vodil nekaj razvojnih projektov. Za njegovo strokovno mnenje ga pogosto zaprosijo vsi večji mediji, kot so RTV SLO, POP TV, Monitor, Večer in drugi.

Vavčerji s področja kibernetske varnosti so pokazali dobre in tudi nekatere slabe strani pri implementacijah, operativnem delovanju in tudi vzdrževanju na tem področju. Skozi predavanje bodo izpostavljene dobre prakse in tudi področja, ki bi jih bilo treba izboljšati. Rezultati bodo prikazani glede na naše lastne izkušnje z izvajanje pregledov na tem področju.

PREDAVANJE 3: NIS 2 in odpornost na kibernetske grožnje – smo pripravljeni na izzive?

Igor Mlakar, direktor operative, Smart Com d.o.o.

Igor Mlakar ima dolgoletne izkušnje z razvojem izdelkov in storitev v skladu s potrebami IKT trga ter izvajanjem storitev za podjetja, ki delujejo v dinamičnem agilnem poslovnem okolju. Specializiran je za vodenje poslovnih procesov, projektov, z odličnim poznavanjem poslovne analitike in strateškega načrtovanja. Je certificiran notranji revizor za standard ISO 27001.

Osnovni namen NIS2 je pospešiti prizadevanja pri vzpostavljanju višje ravni kibernetske varnosti in odpornosti v organizacijah Evropske unije. Organizacije bi se morale že sedaj pripravljati na svojo pot proti skladnosti. Pomembno je razumeti, da je uvedba ukrepov iz direktive proces, ki zahteva sodelovanje vseh deležnikov v podjetju. Prav tako je koristno pridobiti strokovno pomoč ali se posvetovati s kibernetskim varnostnim strokovnjakom, če podjetje nima dovolj internih virov za uresničitev teh ukrepov. S pravočasnim uveljavljanje ukrepov iz direktive bomo obenem odgovorili tudi na aktualne kibernetske grožnje.

PREDAVANJE 4: Kaj odkrivamo pri penetracijskih testih? – primeri iz prakse

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 5: Zakaj so pomembne raziskave in razvoj kibernetske varnosti v podjetjih? - primer iz prakse v elektro podjetju

Dr. Andrej Bregar, pomočnik direktorja poslovnega področja in Gorazd Rolih, direktor področja informacijsko-kibernetske varnosti, Informatika d.o.o.

Dr. Andrej Bregar obtained BSc, MSc, and PhD degrees in computer science from the University of Maribor, Slovenia. He is employed as Deputy CEO at Informatika d.o.o. SME company. He coordinates and cooperates in numerous projects in software development, R&D, cyber security, strategic planning and management, and digitalization of energy systems. This work includes EU-funded projects from the Horizon and Eureka programs and projects for Slovenian electricity energy DSOs. Dr. Andrej Bregar has 30 years of experience in IT, over 20 years of experience

in R&D, and over 10 years of experience in the electricity-energy sector. Since 2009 he has participated in the digitalization of Slovenian and European energy ecosystems. Since 2012 he has been a member of the ebIX Technical Committee (ETC). His work involves the standardization and application of business processes, harmonized structures for B2B/B2C/B2G data exchange, intelligent and data processing technologies, SOA integration technologies, and cyber security mechanisms for the energy supply and distribution ecosystems. Since 2000 he has been actively involved in research work. He regularly publishes scientific and professional papers in international journals, books, and other publications. He gave presentations from the fields of IT, energy, operations research, decision support systems, project management, and cyber security at approximately 100 scientific and professional conferences in Europe, Slovenia, and the USA. He is a reviewer for international scientific journals, and a member of several associations from the fields of IT, energy, and cyber security. He received several awards for outstanding research work. Since 2019 he has led the research and innovation group at Informatika d.o.o.

Gorazd Rolih je magistriral s področja modeliranja Varnostno-operativnega centra. Zaposlen je v Informatiki d.o.o. kjer je Direktor področja informacijsko-kibernetske varnosti in hkrati vodi VOC. Ukvarja se z vodenjem področja informacijsko-kibernetske varnosti, fokusno pa vodi in koordinira delo med naročniki storitev VOC, ekipo CSIRT, sistemsko podporo in drugimi partnerji znotraj energetike ter akterji kibernetske varnosti v državi in zunaj nje. Skrbi za skladnost z regulativo, dobrimi praksami in trendi ter posledično za izgradnjo procesov v VOC. Sodeluje na raziskovalnem projektu CyberSEAS kot vezni člen med potrebami VOC in implementacijo metod ter orodji, ki so predmet raziskovalnega dela projekta.

Preko 20 letne Izkušnje s področja informacijske in kibernetske varnosti je pričel nabirati v Slovenski vojski (SV), najprej kot sistemski administrator, nato kot analitik v Centru za Simulacije, vodja informacijske varnosti SV, nacionalni predstavnik na vajah kibernetske obrambe, nekaj let je delal v NATU v ekipi za razvoj kibernetskih zmogljivosti in regulative. Po zaključeni vojaški karieri je nadaljeval z delom na različnih projektih Kibernetske obrambe v ACT NATO in v ekipi za pripravo in izvedbo vaje Cyber Coalition. Zaposlen je bil tudi na Policiji v tamkajšnjem varnostno-operativnem centru.

Kibernetske grožnje postajajo vse bolj napredne, zaradi česar se je potrebno z njimi spopadati na proaktiven in sistematičen način. Ključni temelj za to predstavlja raziskovalna in razvojna dejavnost, ki omogoča podjetjem, zlasti tistim, ki so vpeta v kompleksnejše poslovne in tehnične sisteme ter kritično infrastrukturo, ohranjati stik z aktualnimi trendi, jih prehitevati in pridobiti strateško prednost na področju kibernetske varnosti. V predavanju osvetlimo razloge, prakse in pozitivne učinke, povezane z izvedbo razvojno-raziskovalnih projektov in procesov s področja kibernetske varnosti v podjetjih v slovenskem in širšem evropskem prostoru. Predstavimo praktično rešitev za proaktivno obvladovanje kibernetskih groženj in napadov, ki smo jo razvili v sklopu mednarodnega projekta Horizon 2020 CyberSEAS. Osredotočimo se zlasti na prikaz pozitivnih učinkov, ki smo jih dosegli z vpeljavo te rešitve v procese in nabor tehnologij varnostnega operativnega centra za elektroenergetsko domeno.

PREDAVANJE 6: Kako analizirati kibernetska tveganja ter ugotovitve praktično uporabiti?

Marko Zavadlav, višji svetovalec, Actual I.T./PRO.Astec d.o.o.

Marko Zavadlav je CISA – pooblaščeni revizor informacijskih sistemov, vodilni presojevalec ISO/IEC 27001, presojevalec ISO 22301, presojevalec TISAX, ITIL Foundation v2. Ima več kot 30 let izkušenj na različnih področjih informacijske tehnologije, od skrbnika operacijskih sistemov prek razvoja aplikacij, IT revizije, do vodenja projektov in vodenja velikih projektov, več kot 20 let pri implementaciji in delovanju IS ter pri vodenju Varnostno operativnega centra. Sodeloval pri pripravi zakonodaje s področja informacijske varnosti. Bil je glavni arhitekt in vodja projekta enega največjih varnostno operativnih centrov v Sloveniji. Njegovo strokovno znanje in podpora sta bila dobro sprejeta v vladi, pa tudi v bančništvu, zavarovalništvu in zdravstvu. Trenutno je vključen v 4 varnostno operativne centre kot vodja SOC ali član ekipe Tier3.

Kibernetske grožnje in z njimi povezana tveganja predstavljajo vedno večje izzive za organizacije, ki vsakodnevno uporabljajo elektronske storitve in komunikacijo. Grožnje so specifične, saj niso omejene ne časovno ne lokacijsko. Organizacije morajo prepoznati, kateri viri so zanje najbolj pomembni, kako jih varovati, kako prepoznati varnostne dogodke in kako se na njih učinkovito in uspešno odzvati. Ukrepi morajo biti celoviti, izvedljivi in merljivi. Hkrati morajo biti tudi sprejemljivi na način, da ne ovirajo delovnega procesa. Na predavanju bomo pogledali, kako se odločimo za metodologijo ocenjevanja tveganj kibernetske varnosti in kako si zgradimo register groženj in ranljivosti. Nadalje bomo preverili, kako iz groženj in ranljivosti ocenimo tveganja, kako se odločimo za ukrepe in zakaj uporabimo različne vrste kontrol za zmanjševanje tveganj.

PREDAVANJE 7: Kaj AI prinaša področju kibernetske varnosti? – Primer uporabe AI v obrambnih programih

dr. Blaž Ivanc, SVP Special Security Projects, CREAplus d.o.o.

Dr. Blaž Ivanc je mednarodno priznan strokovnjak s področja kibernetske obrambe. Sodeloval je pri različnih varnostnih projektih, namenjenih zagotavljanju interoperabilne infrastrukture za javno varnost v Evropi in obrambi sistemov kritične infrastrukture. Zadnja leta je bil vodja informacijske varnosti v večjih bančnih skupinah, kjer je nazadnje opravljal funkcijo Group CISO v NLB Skupini. Dr. Ivanc je v zadnjem desetletju izvedel predavanja v vodilnih tehnoloških centrih za kibernetsko obrambo po svetu.

Današnje rešitve za obvladovanje kibernetskih tveganj morajo nasloviti sodobne varnostno-operativne izzive v poslovnih sistemih in zagotavljati varovanje okolja z ene same platforme. Takšna platforma mora omogočati avtomatizirane delovne postopke, samodejno zaznavanje groženj z umetno inteligenco in integrirane zmogljivosti odzivanja. Poleg tega mora sodobna postavitev vključevati neprekinjeno, samodejno preverjanje varnostne situacije za učinkovito upravljanje kibernetske varnosti.

ZAKLJUČNO PREDAVANJE: Prihodnost izobraževanja iz kibernetske varnosti

izr. prof. dr. Marko Hölbl in vodjo projekta izr. prof. dr. Muhamed Turkanović, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko

Marko Hölbl je izredni profesor Fakulteti za elektrotehniko, računalništvo in informatiko, Univerze v Mariboru. Njegovo raziskovalno delo zajema kibernetsko varnost in zasebnost v najširšem smislu, od kriptografije do uporabniških vidikov informacijske varnosti in zasebnosti. Je nosilec predmetov na Fakulteti za elektrotehniko in računalništvo Univerze v Mariboru ter na Fakulteti za varnostne vede Univerze v Mariboru. Je aktiven član in glavni tajnik CEPIS LSI (Council of European Professional Informatics Societies - Legal and Security Issues special interest network), član European Cyber Security Organisation (ECSO), WG6: SRIA and Cyber Security Technologies, podpredsednik in član izvršnega odbora Slovenskega društva. Poleg tega je aktiven član in glavni tajnik združenja EAEEIE (Evropsko združenje za izobraževanje na področju elektrotehnike in informatike) ter ocenjevalec za EK v programu Obzorje Evropa. Je tudi član izvršnega odbora Sekcija za kibernetsko varnost pri Gospodarski zbornici Slovenije. Sodeloval je pri številnih projektih, seminarjih in delavnicah. Koordinira projekt EC H2020 CyberSec4Europe. Poleg tega sodeloval pri nacionalnem projektu, namenjenem izobraževanju o kibernetski varnosti RUKIV - Razvoj programov usposabljanja za kibernetsko varnost, ki ga financirata Javna agencija za raziskovalno dejavnost Republike Slovenije in Urad Vlade Republike Slovenije za informacijsko varnost.

Iskanje in usposabljanje kadrov na področju kibernetske varnosti je zahtevno. Globalno in tudi nacionalno pomanjkanje takšnega kadra je precejšnje in situacija se v kratkem času ne bo izboljšala. Tema predavanja bo naslavljala pomembnost posameznih kompetenc iz kibernetske varnosti. Predstavili bomo, kako na takšne kompetence gledajo v Evropskih visokošolskih študijskih programih oz. katerim znanjem se med študijem nameni največ pozornosti ter katere kompetence so med slovenskimi zaposlovalci najbolj iskane. Ob tem se bomo na kratko ustavili tudi pri trenutnem položaju slovenskih podjetij in njihovih željah za svoj kader na področju kibernetske varnosti. Zadnji del predavanja bo namenjen prihodnosti izobraževanja oz. izpopolnjevanja na tem področju. Predstavljen bo koncept mikrodokazil, v katerega se trenutno veliko vlaga v Evropski uniji in za katerega tudi v Sloveniji izvajamo obsežne projekte, ki bi lahko pripomogli pri izobraževanju iz kibernetske varnosti in premostitvi pomanjkanja takšnega kadra.

Pripravil: Tomaž Čebela, SeKV, ZIT
Ljubljana, 24. 10. 2023