OPISI PREDAVATELJEV IN PREDAVANJ

Prvi predavatelj: Aljaž Stare, Metronik d.o.o., predstavnik grozda Pametne tovarne v okviru SRIP TOP

Dr. Aljaž Stare je strokovnjak na področju avtomatizacije in digitalizacije procesov v industriji in infrastrukturi, z več kot 20 letnimi izkušnjami. Diplomiral je leta 2002 na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer je leta 2007 tudi doktoriral. V okviru raziskovalnega dela je leta 2009 prejel Zoisovo priznanje za pomembne dosežke na področju vodenja sistemov, ki ga podeljuje Ministrstvo za visoko šolstvo, znanost in inovacije. V podjetju Metronik je zaposlen od leta 2008 in pokriva portfelj programskih rešitev za avtomatizacijo in digitalizacijo. Je v stalnem stiku z uporabniki iz industrije in infrastrukture in jim z naprednimi tehnološkimi rešitvami za avtomatizacijo in digitalizacijo in sodobnimi pristopi pomaga povečati njihovo konkurenčno prednost. V zadnjih letih se v podjetju Metronik intenzivno ukvarja tudi s kibernetsko varnostjo v industriji in infrastrukturi.

Prvo predavanje: Kakšno je zavedanje o kibernetski varnosti v industrijskih podjetjih in kakšni izzivi nas čakajo?

S povečano digitalizacijo in globalno povezanostjo se v industrijskih podjetjih povečujejo tudi kibernetska varnostna tveganja. Predavanje se bo zato osredotočilo na splošno problematiko kibernetske varnosti v industriji. Pokazali vam bomo, zakaj je kibernetska varnost v OT okoljih pomemba, zakaj je ne smemo enačiti z varnostjo v IT okoljih, kakšne so razlike med temi okolji in kako ranljiva so OT okolja v industriji. Med drugim vam bomo predstavili tudi kakšne moderne rešitve za preprečevanje naprednih kibernetskih napadov v industrijskih okoljih poznamo ter praktični primer varnostnega orodja z vgrajenimi mehanizmi strojnega učenja in umetne inteligence.

Drugi predavatelj: Boris Krajnc, strokovnjak za kibernetsko varnost, Telekom Slovenije d.d.

Boris Krajnc ima več kot 18 let izkušenj na področju IT tehnologij in industrije. Kot strokovnjak za kibernetsko varnost se je specializiral za zunanje in notranje varnostne preglede v IT in OT okolju. Njegove veščine in strokovno znanje s področja IKT potrjujejo mednarodno priznani certifikati, kot so: GICSP, GRID, GNFA, CEH, CCNA – Security, CCNP JNCIA, ENA,

Drugo predavanje: Kibernetske grožnje v okoljih OT in kako se zaščitimo?

Primerjava IT(Informacijske tehnologije) in OT(Operativne Tehnologije) ter zavedanje pomembnosti kibernetske varnosti v OT okoljih. Obdelali bomo kako so organizacije z OT vidne skozi oči hekerjev in zakaj je vedno več kibernetskih napadov na tovrstna okolja. V predavanju si bomo ogledali kaj je potrebno upoštevati pri združevanju IT in OT omrežja, prav tako pa si bomo ogledali kako bi izgledal hekerski napad na okolje OT z uporabo socialnega inženiringa. Na koncu predavanja si bomo še ogledali na kak način izvajati zaščito v industrijskih okolji in okolji kritične infrastrukture.

Tretja predavateljica: Alenka Glas, PRO.astec d.o.o.

Alenka Glas je svojo kariero začela v finančnem sektorju sredi 80 ih let in se na začetku 90-ih priključila novi dejavnosti slovenskih bank – kartičnemu poslovanju. Pri razvoju kartičnega poslovanja v slovenskem prostoru je bil njen pomemben prispevek prav na zgodnjem odkrivanju in preprečevanju kartičnih zlorab. Temu je ob koncu 90-ih priključila odkrivanje in preprečevanje zlorab na informacijskem področju.

Sistematično se je z varovanjem informacij začela ukvarjati ob prelomu tisočletja, najprej skladno s smernicami in zahtevami kartičnih brandov, zelo hitro pa tudi z drugimi mednarodnimi dobrimi praksami. Vodila je enega prvih projektov vzpostavitve Sistema upravljanja varovanja informacij v Sloveniji po takrat veljavnem mednarodnem standard BS 7799. Veliko pozornosti je v tem obdobju posvetila področju neprekinjenega poslovanja, kar še vedno predstavlja njeno pomembno dejavnost.

V zadnjem času je njen interes usmerjen predvsem v ugotavljanje in zagotavljanje zasebnosti posameznika na delovnem mestu. Pri tem poskuša povezovati svoje izkušnje iz področja varovanja informacij in svoje poznavanje področja varstva osebnih podatkov.

Tretje predavanje: Implementacija standardov informacijske varnosti za industrijo 4.0

Standardi informacijske varnosti so na izkušnjah in dobrih praksah temelječi gradniki varnega delovanja vsake sodobne organizacije.

Kibernetska varnost je skrb sodobne družbe in se izraža skozi glavna zaznana tveganja organizacij, ki poslujejo v sodobnem svetu. Kibernetske varnosti temelji na vzpostavljenem in upravljanem sistemu upravljanja informacijske oziroma kibernetske varnosti. Vidiki kibernetske varnosti zajemajo najrazličnejša področja, od tehnologije, fizične varnosti, ljudi, procesov in organiziranosti. Če k temu dodamo še odpornost na krizne dogodke in pripravljenost na neprekinjeno poslovanje, hitro ugotovimo, da so dobre prakse, zapisane v standardih ISO/IEC 27001 in ISO 22301 učinkovite podlage delovanja vsake organizacije, ki se tveganj zaveda in jih želi upravljati.

Skozi predstavitev vas bomo seznanili z načinom vzpostavitve takih sistemov ter prednostmi in slabostmi, na katere naletijo organizacije. Predstavitev bo temeljila na praktičnih primerih iz Slovenskega okolja.

Četrto predavanje: Miha Ozimek, SIQ

mag. Miha Ozimek, spec. inf. var. je opravil podiplomski magistrski študij informatike ter specialistični študij informacijske varnosti s področja standardov informacijske varnosti in uvajanja politik varovanja informacij v organizacije. Od leta 2007 deluje kot svetovalec in presojevalec sistemov vodenja kakovosti, upravljanja z IT storitvami in varovanja informacij. Kot ISO presojevalec SIQ Ljubljana presoja v slovenskih organizacijah, EU in državah JV Evrope. Poleg tega sodeluje s APEK, Arhiv RS in IP-RS pri pripravi organizacij na izvajanje dela skladno z določili zakonodaje (ZVOP-2, ZEKOM-2, ZINFV, ZVDAGA-A, itd). Od leta 2008 sodeluje kot gostujoči predavatelj na Fakulteti za varnostne vede na področju sistemov varovanja informacij. Izobraževanja je izvajal že za več kot 5000 slušateljev iz različnih organizacij in izobraževalnih inštitucij.

Četrto predavanje: Standard IEC 62443 in kibernetska varnost v industriji

Standard IEC 62443 je mednarodni standard za varnost industrijskih nadzornih sistemov. Standard je oblikovalo Mednarodno združenje za avtomatiko (www.isa.org) in ponuja organizacijam za izboljšanje kibernetske varnosti IoT. Standard IEC 62443 je izpeljan iz standarda serije ISO / IEC 27000 in je prilagojen tako za okolje industrijskih nadzornih sistemov kot drugih, na primer zdravstveni sistem in kritična infrastruktura. Kaj pomeni skladnost s standardom in kako bo to pomagalo pri kibernetski odpornosti vašega podjetja boste izvedeli v tem predavanju.

Peti predavatelj: Andrej Rakar, CISO, 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.

Peto predavanje: Varnost v dobavnih verigah

V zadnjem času so kar nekaj medijske pozornosti pritegnili vdori v informacijske sisteme, ki so bili posledica ranljivosti pri dobaviteljih IKT opreme oz. vzdrževalcih le-te. Kakršen koli varnostni incident pri njih zaradi povezanih sistemov namreč lahko predstavlja resno varnostno grožnjo tudi za nas uporabnike. Obramba pred tovrstnimi grožnjami je še posebej težavna, saj njihov informacijski sistem ni pod našim nadzorom.

Na predavanju bomo predstavili potrebne korake, od tehničnih, pravnih, do organizacijskih ukrepov za zmanjšanje tveganja dobavne verige, s čimer si zagotovimo varno in učinkovito poslovanje.

Šesti predavatelj: Gregor Spagnolo, SSRD d.o.o

Gregor Spagnolo je član izvršnega odbora SeKV in soustanovitelj Društvo OWASP Maribor, ki si prizadeva za izboljšanje varnosti programske opreme. Je lastnik podjetja SSRD kjer se ukvarjajo z uvajanjem procesa varnega razvoja in razvojem varne programske opreme.

Šesto predavanje: Zagotavljanje kibernetske varnosti pri izvajanju projektov digitalizacije v industriji

Digitalizacija v industriji je postala pomembna gonilna sila za izboljšanje produktivnosti, povečanje učinkovitosti in zmanjševanje stroškov. Pogosto se osredotočamo na procese, kako digitalizirati naše poslovne operacije, vendar lahko v tej hitri poganjalni sili pogosto zanemarimo ključno komponento: informacijsko varnost. To lahko predstavlja veliko tveganje za celovitost in zanesljivost naših digitalnih sistemov, saj so ti pogosto tarča kibernetskih napadov in drugih varnostnih groženj.

V svetu digitalizacije je varnostna dobavna veriga enako pomembna kot sam poslovni proces. Varnostna dobavna veriga se nanaša na vse varnostne ukrepe, ki jih je treba sprejeti za zaščito digitalnih sistemov v celotni dobavni verigi, od začetne faze razvoja do končne uporabe. Ta veriga vključuje vse od dobaviteljev strojne in programske opreme do upravljanja podatkov in varovanja omrežja.

Sedmi predavatelj: Boštjan Špehonja, GO-LIX d.o.o

Boštjan Špehonja je višji svetovalec za informacijsko varnost, etični heker in direktor podjetja GO-LIX, d. o. o. z več mednarodno priznanimi certifikati na področju etičnega hekanja (Certified Ethical Hacker – Master, Certified Network Defense Arcihtect, Security+, CEH Practical, CASP+, CySA+). Ima bogate in raznolike izkušnje, saj mu je pregled svoje informacijsko-komunikacijske tehnologije zaupalo že več sto organizacij, med drugim podjetja s kritično infrastrukturo, banke, zavarovalnice, ministrstva. Izvaja tudi izobraževanja in delavnice o varni uporabi interneta in etičnem hekanju. Predaval je na vseh največjih domačih konferencah o informacijski varnosti. Je soustanovitelj fundacije SICEH (Slovenian Certified Ethical Hackers) ter gostujoči strokovnjak na Univerzi v Mariboru in predavatelj na Gea Collegeu. Leta 2018 je odkril ranljivost na uradni strani podjetja Microsoft in za to pridobil omembo na spletni strani Security Researcher Acknowledgments for Microsoft Online Services. Leta 2020 mu je mednarodno uveljavljena organizacija EC-Council kot prvemu v Sloveniji podelila certifikat CEH Master in ga uvrstila na svoji spletni strani v rubriko Global Ethical Hacking Leaderboard.

Sedmo predavanje: Sistemsko varnostno preverjanje v industrijskih sistemih

Na predavanju bomo predstavili kako etični hekerji izvajajo sistemske varnostne preglede in kako slednji pripomorejo k dvigu odpornosti na kibernetske grožnje. Prikazali bomo potek izvedbe sistemskega varnostnega pregleda, kaj zajema, kako naj se podjetje nanj pripravi ter kakšne prednosti prinaša.