OPIS PREDAVATELJEV in PREDAVANJ

Trenutni izzivi kibernetske varnosti v EU

Luigi REBUFFI, Generalni sekretar, European Cyber Security Organisation – ECSO

Opis predavatelja: Luigi Rebuffi je generalni sekretar in ustanovitelj ECSO (Evropske organizacije za kibernetsko varnost) ter ustanovitelj in generalni sekretar Fundacije Women4Cyber.

Diplomiral je na področju jedrskega inženiringa na Politecnico di Milano. Sprva je delal v Nemčiji z mikrovalovnimi sistemi visoke moči za termonuklearski fuzijski reaktor ITER. Nato je v Thalesu prevzel odgovornosti glede evropskih raziskav in razvoja v različnih sektorjih: telekomunikacijskih, industrijskih, medicinskih in znanstvenih. Leta 2003je tako postal direktor za evropske zadeve. Ustanovil je EOS (Evropska organizacija za varnost) leta 2007 in je že 10 let njen CEO. Med 2012 in 2016 je bil svetovalec Evropske komisije za program EU za varnostne raziskave in predsednik usmerjevalnega odbora francoske ANR za varnostne raziskave. Leta 2016 je ustanovil ECSO in podpisal z Evropsko komisijo PPP o kibernetski varnosti. Leta 2019 je ustvaril Women4Cyber za spodbujanje sodelovanja žensk v kibernetski varnosti. Leta 2020 je bil nominiran na seznamu "IFSEC Global Influencers in security - Executives".

Opis predavanja: Sedanji izzivi kibernetske varnosti v EU so različne vrste:

- Kibernetske grožnje (DDoS, izsiljevalsko programiranje, goljufije, ...)
- Razumevanje potreb (povezava s CISO ...)
- Suverenost (uporaba zaupanja vrednih dobavnih verig)
- Lažne novice (vpliv na prebivalstvo in sprejemanje odločitev)
- Tehnologija (razvoj je nujen, vendar tudi ustrezna uporaba novih tehnologij)
- Cyber Threat Intelligence po vsej Evropi
- Zakonodaja (izvajanje in uporaba direktiv in predpisov, zlasti za kritično infrastrukturo)
- Ozaveščanje prebivalstva in odločevalcev
- Razpoložljivost strokovnjakov (izobraževanje, usposabljanje, vključevanje)
- Podpora MSP (uporabnikom in dobaviteljem)
- Lokalni / regionalni / nacionalni / evropski pristopi

Te številne izzive bomo na predavanju pregledali in združili v vizijo razvoja skupne evropske kibernetske varnosti.

Ključni trendi na področju kibernetske varnosti

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

Opis predavatelja: 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.

Opis predavanja: Tehnološke inovacije, kot so umetna inteligenca (AI), 5G, industrija 4.0, pametna mesta in povezana vozila (IoT) ter masovni podatki (big data), prinašajo številne koristi, hkrati pa tudi nove grožnje kibernetskega prostora. V zadnjem času so kar nekaj pozornosti pritegnili tudi vdori v informacijske sisteme, ki so bili posledica ranljivosti pri dobaviteljih IKT opreme oz. vzdrževalcih le-te (ranljivosti dobavne verige). Ne nazadnje, trenutne geopolitične spremembe povečujejo tveganja pri zagotavljanju visoke ravni varnosti omrežij in informacijskih sistemov v Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Na predavanju bomo izpostavili ključne trende krepitve kibernetske obrambe, kot od nas to zahtevajo standardi in zakonodaja.

Kibernetske grožnje – aktualno dogajanje

Dalibor Vuković, Specialist kibernetske varnosti, Telekom Slovenije d.d.

Opis predavatelja: Dalibor Vukovič – Produktni vodja pri Telekomu Slovenije je specialist za kibernetsko varnost z več mednarodno priznanimi certifikati. Ima več kot 20 let delovnih izkušenj v IKT sektorju. Ukvarja se z razvojem in implementacijo novih varnostnih produktov tako v zasebnem kot javnem sektorju vključujoč največje delovne organizacije, kritično infrastrukturo in državne institucije. Je avtor več člankov in prispevkov na strokovnih konferencah in predavatelj s področja kibernetske varnosti. Raziskovalno se ukvarja z OSINT metodologijo in predikcijo kibernetskih napadov.

Opis predavanja: Eno največjih bolnišničnih verig v ZDA je pred kratkim prizadel kibernetski napad z izsiljevalsko programsko opremo kar je povzročilo odložene operacije, zastoje pri oskrbi pacientov in prestavljene preglede pri zdravnikih po vsej državi.

Od februarja do danes je bila napadena kritična infrastruktura praktično vseh evropskih držav. Samo v zadnjih dveh mesecih je bila dvakrat žrtev kibernetskega napada slovenska kritična infrastruktura.

Na predavanju bomo govorili o aktualnih tipih kibernetskih napadov in njihovih posledicah.

Trend ali nujnost? Krepitev varnosti kritične informacijske infrastrukture je skupna odgovornost.

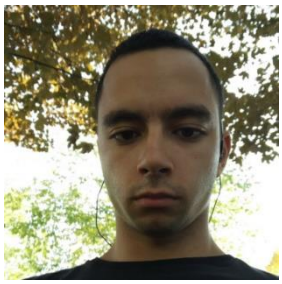
Vencel Cserhati, Uradnik za kibernetsko varnost in zasebnost, Hungary and Adriatic region, Huawei Technologies

Opis predavatelja: Vencel je višji strokovnjak na področju informacijske tehnologije/kibernetske varnosti/zasebnosti podatkov s CIPP/E, CIPM, CIPT in Green Belt certifikati ter več kot 25 let izkušenj na področju kibernetske varnosti in informacijske tehnologije. Pred kratkim se je pridružil Huaweiju kot uradnik za kibernetsko varnost in zasebnost v regiji Madžarske & Adriatika. Odgovoren je za upravljanje in načrtovanje kibernetskih zahtev glede varnosti in zasebnosti, zunanje komuniciranje, skladnost in obvladovanje tveganj ter krepitev ozaveščenosti.

Opis predavanja: Krepitev kibernetske varnosti kritičnih infrastruktur je skupna odgovornost. Ampak kako? Kakšna orodja, standardi in smernice lahko pomagajo?

"TA ŠKATLA"

Peter Kavčič, Svetovalec za kibernetsko varnost/Etični heker, Pro.Astec d.o.o.



in **Elijah Benjamin Hlastan,** Svetovalec za kibernetsko varnost/Etični heker Pro.Astec d.o.o.

Opis predavatelja: Peter Kavčič je svojo kariero v IT svetu začel že kot dijak, ko je reševal probleme sodelavcev in svetoval o novostih. V času študija je izpopolnjeval svoje znanje na področju kibernetske varnosti in se udeleževal konferenc kibernetske varnosti, kjer je tudi večkrat predaval. Po končanem magistrskem študiju organizacije in managementa informacijskih sistemov se je redno zaposlil v podjetju PRO.Astec, kjer je aktivno nadaljeval svojo karierno pot v kibernetski varnosti. Nedavno je potrdil svoje znanje z uspešnim opravljanjem certifikata etičnega hekerja, ki je mednarodno priznan certifikat v kibernetski varnosti. Kljub temu, že načrtuje nadaljevanje izobraževanja s praktičnim delom CEH practical. Poleg redne službe, je Peter tudi član v slovenski fundaciji etičnih hekerjev, kjer aktivno sodeluje praktično od samega začetka fundacije.

Opis predavatelja: Elijah Benjamin Hlastan je svojo pot na področju kibernetske varnosti začel že v srednji šoli, kjer je pod mentorstvom IT podpore dokazoval ranljivosti šole in razkrival varnostne luknje v internetnih sistemih šole. Iz tega se je razvila njegova ljubezen in naklonjenost do testiranja kibernetske varnosti. Tekom študija se je pridružil ekipi ISF Teama, kjer je opravljal razne projekte s področja kibernetske varnosti, najraje pa se je ukvarjal s socialnim inženiringom ter red team testi/napadi. V zadnjem letu je aktiven na področju raziskav zlonamernih programov ter zlonamernih akterjev z namenom identificiranja ter zbiranja podatkov za mednarodno skupino neodvisnih raziskovalcev z imenom »The Vaccinators«. Ta skupina deluje kot podpora različnim proizvajalcem protivirusne in varnostne opreme, kot tudi Interpolu in drugim službam s področja kibernetske varnosti.

Trenutno aktivno razvija odprto-kodno ogrodje za prepoznavanje, zbiranje in poročanje o aktivnih napadih socialnega inženiringa.

Opis predavanja: S »to škatlo« kot smo jo poimenovali, želimo strankam ponuditi znanje naših strokovnjakov iz različnih področij kibernetske varnosti. Gre za popolnoma prilagodljivo obliko rešitve, ki jo stranka izbere sama. Delujemo tako na področju zunanjih in notranjih varnostnih pregledov, kot tudi z izvajanjem socialnega inženiringa. Po drugi strani, pa ponujamo tudi Red teaming storitve, pri čemer se napada na organizacijo lotimo kot dejanski zlonamerni heker in pri tem

uporabimo vsa sredstva, ki so na voljo. Podjetja tako z našo pomočjo pridobijo vpogled v stanje lastne kibernetske varnosti in priporočila ter nasvete za izboljšave na tem področju.

Vloga standardov pri načrtovanju kibernetske varnosti v okoljih kritične infrastrukture Predavatelj

Peter Ceferin, Tehnični direktor, Smart Com d.o.o

Opis predavatelja: Peter Ceferin, tehnični direktor, Smart Com je specialist za arhitekture in omrežne tehnologije na osnovi IP tehnologij. Strokovno se že preko 25 let ukvarja z načrtovanjem in implementacijo omrežnih in varnostnih rešitev v okolja kritične infrastrukture, predvsem v okolja elektroenergetskih sistemov. Posveča se tudi razvoju in uvajanju naprednih komunikacijskih rešitev ter specializiranih varnostnih rešitev v okolja, kjer sta zanesljiva in učinkovita omrežna povezljivost ter kibernetska odpornost ključni za neprekinjeno delovanje organizacije.

Opis predavanja: Peter bo v predavanju izpostavil tveganja, ki jih predstavljajo hekerske dejavnosti na operativne sisteme v okoljih kritične infrastrukture. Ti sistemi pridobivajo osrednjo vlogo pri pospešeni digitalizaciji in tako postajajo ranljivi in privlačni za kiberkriminalce, saj je kibernetska obramba operativnih sistemov pomanjkljiva. Ranljivost operativnih sistemov bo prikazal s primeri javnih znanih varnostnih incidentov. Podal bo rešitev za okrepitev obrambe pred kibernetskimi napadi v elektroenergetiki in sicer uporabo referenčnih arhitektur in sektorskih standardov.

Razvoj specialističnega kadra na vajah in tekmovanjih

Gregor Spagnolo, Direktor, SSRD d.o.o.

Opis predavatelja: Gregor Spagnolo je član izvršnega odbora SeKV in soustanovitelj Društvo OWASP Maribor, ki si prizadeva za izboljšanje varnosti programske opreme. Prizadeva si zapolniti vrzel v znanju mladih – srednješolcev, predvsem pa študentov računalništva – na področju kibernetske varnosti.

Opis predavanja: Razvoj kadra na področju informacjiske varnosti predstavlja velik izziv. Vsi si želimo večji bazen kadra vendar se vsak srečuje z drugačnimi izzivi. Kako privabiti mlade jim predati znanje in izkušnje, ter jih srečati z realnimi porblemi. O tem in še več bomo govorili na predavanju.

Povečajte stopnjo kibernetske varnosti z varnostnim pregledom

Boštjan Špehonja, CEO, GO-LIX d.o.o

Opis predavanja: Na predavanju bomo predstavili delo etičnih hekerjev ter razložili kaj so varnostni pregledi oziroma penetracijski testi. Na konkretnih primerih bomo predstavili, kako lahko varnostni pregledi pomagajo pri dvigu stopnje kibernetske varnosti ter kako se jih izvaja. Če se želite resnično prepričati, ali ste varni pred hekerskimi napadi, morate najeti etične hekerje.

Uveljavljanje kibernetske varnosti v malih in srednje velikih podjetjih na podlagi standardov

Marko Ličina, Inžinir varnostnih rešitev, CREAplus d.o.o.

Opis predavatelja: Marko Ličina ima večletne izkušanje v panogi IT, kjer je bil aktiven v različnih podjetjih na različnih pozicijah in področjih. Zadnjih nekaj let je aktiven predvsem na področju zagotavljanja informacijske varnosti. Vloge vključujejo analizo, načrtovanje in uvedbo rešitev, predprodaje aktivnosti, svetovanje in izpopolnjevanje strank kot tudi samo preverjanje Informacijske varnosti naročnikov z izvedbo sistemskih varnostnih pregledov. Marko je tudi nosilec certifikatov: Microsoft Certified Systems Engineer, Microsoft Certified Solutions Associate, Comptia PenTest+, Comptia Security in ITIL V3 foundational.

in Miha Lavrič, CTO, CREAplus d.o.o

Opis predavanja: Predavanje »Uveljavljanje kibernetske varnosti v malih in srednje velikih podjetjih na podlagi standardov« prikaže koristnost uporabe informacijskih standardov kot naprimer ISO/IEC 27001 pri izgradnji zanesljivega in varnega informacijsko komunikacijskega sistema podjetja. Dotaknili se bomo tudi tehničnih kontrol, ki so definirane v aneksih ISO/IEC 27001 in njihovo pomembnost orisali na realnih primerih.