Ponedeljek, 04. 10. 2021	
14:00 -16:00	Okrogla miza: izboljšanje ekosistema za delovanje MSP v sektorju kibernetske varnosti

Na okrogli mizi bomo razpravljali o pogojih dela in ovirah ter potrebnih ukrepih na nacionalni ravni za nadaljnji razvoj podjetij v sektorju kibernetske varnosti, ki so pomemben del zagotavljanja kibernetske varnosti v državi.

Torek, 05. 10. 2021	
08:30-09:45	Okrogla miza: Razvoj kadra za kibernetsko varnost

Na okrogli mizi bomo razpravljali o kadrovski problematiki na področju kibernetske varnosti. Število tveganj se zelo hitro povečuje, število strokovnjakov za kibernetsko varnost pa ostaja isto oz. se zelo počasi spreminja. Zakaj ne uspevamo zagotoviti novih kadrov, zakaj ni dovolj interesa za to področje in kaj lahko storimo, da bi stanje izboljšali so ključna vprašanja na katera bomo skušali odgovoriti na okrogli mizi.

Torek, 05. 10. 2021		
10:00-11:30	Delavnica: Penetracijska testiranja	Matjaž Katarinčič in Boris Krajnc, Smart Com

Etična hekerja bosta predstavila najpogostejše tehnike napadov, ki jih uporabljajo kiberkriminalci za prodor v poslovno ali procesno okolje z namenom pridobitev finančne koristi, odtujitev intelektualne lastnine ali prekinitve poslovanja. Pri tem hekerji poleg socialnega inženiringa najpogosteje izrabijo varnostne ranljivosti oz. pomanjkljivosti informacijskega sistema organizacije. Predavatelja bosta predstavila, kako z neodvisnim varnostnim preverjanjem in penetracijskem testiranjem informacijskega sistema, ki ga izvajajo etični hekerji, identificirajo ranljivosti, varnostna tveganja ter z njihovo odpravo preprečijo, da do zlorab informacijskega sistema sploh pride.

Predavatelja:

Matjaž Katarinčič, etični heker in strokovnjak za kibernetsko varnost, Smart Com d.o.o.
www.linkedin.com/in/matjazkatarincic

Boris Krajnc, etični heker in strokovnjak za kibernetsko varnost, Smart Com d.o.o.
www.linkedin.com/in/boris-krajnc-41309829

Sreda, 06. 10. 2021

09:00-09:45	Odkrivanje in obravnave anomalij v omrežjih kot storitev	Janez Peršin, Smart Com

Podjetja se danes srečujejo s številnimi izzivi, ki jih prinaša sodobno poslovno omrežje, kot so veliko število naprav, počasno odkrivanje anomalij v poslovnih omrežjih ter napadalcev, ki so v omrežju lahko skriti tudi več mesecev. Zato potrebujejo IT ekipe širok nabor storitev in orodij za prepoznavanje, blokiranje, odkrivanje in odzivanje na napredne kibernetske grožnje za zagotavljanje ustreznega nivoja in celovitost kibernetske varnosti. Pri tem si IT ekipe lahko poslužijo najema naprednih storitev upravljanja na vseh nivojih, med katere spada storitev odkrivanja in obravnave anomalij v omrežjih. Govorec bo predstavil, kakšne prednosti s storitvami upravljanja pridobijo podjetja, kot so: hitrejše zaznavanje, analiziranje in odzivanje na incidente oz. dogodke v omrežju ter njihovo proaktivno spremljanje.

Predavatelj:

Janez Peršin, etični heker in strokovnjak za kibernetsko varnost, Smart Com d.o.o.
www.linkedin.com/in/janez-persin

10:00-10:45	Šifriranje in PKI – učinkovita zaščita pred kibernetskimi napadi	Dr. Nastja Cepak, CREAplus d.o.o.

Zaupnost, integriteta, nezatajljivost in avtentikacija so v digitalnem svetu osnovni varnostni aspekti, ki jih zagotavlja kriptografija. Različne aspekte implementiramo z različnimi tipi kriptografije, njihov namen pa je, da ob premišljeni uporabi ščitijo naše podatke, identitete in integriteto naših digitalnih sistemov.

Predavateljica:

Dr. Nastja Cepak, kriptografinja in strokovnjakinja za varnost IT, CREAplus d.o.o.
https://www.linkedin.com/in/nastja-cepak-78b753a5/

11:00-11:45	Post kvantna kriptografija (PQC) – nevarnost, ki se bliža hitreje, kot si mislimo	Dr. Nastja Cepak, CREAplus d.o.o.

Razvoj kvantnih računalnikov obeta postaviti razvoj tehnologije na glavo in omogočiti izračune, ki jim niso kos niti najmočnejši izmed današnjih super računalnikov. Po drugi strani pa predstavlja prekletstvo za varnost, saj bo kvantni računalnik lahko v minuti strl kriptografske algoritme, ki so bili poprej

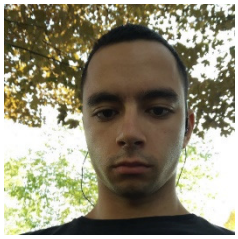
desetletja varni. Raziskovalci po vsem svetu zagrizeno razvijajo novo generacijo kriptografske infrastrukture in algoritmov, ki bodo sposobni prenesti nove kvantne modele napadov.

Predavateljica:
dr. Nastja Cepak
https://www.linkedin.com/in/nastja-cepak-78b753a5/

13:00-13:45	Socialni inženiring	Peter Kavčič, Unistar

Ker je v kibernetski varnosti najšibkejši člen ravno človek, napadi socialnega inženiringa rastejo, postajajo čedalje bolj prefinjeni in spadajo v kategorijo najuspešnejših napadov tako na podjetja kot uporabnike. Napadi socialnega inženiringa se na uporabnike in podjetja izvajajo z izrabljanjem kombinacije naprav in človeške psihologije. Na predavanju boste spoznali različne oblike tovrstnih napadov, nekaj realnih primerov in kako jih uspešno prepoznati ter se pred njimi tudi zavarovati.

Predavatelj:



Peter Kavčič, penetracijski tester
https://www.linkedin.com/in/peter-kav%C4%8Di%C4%8D-95a63b15b/

14:00-14:45	Na poti standardizacije kibernetske varnosti	Miha Ozimek in Branko Miličević, SIQ

15:00-15:45	Zasebno in anonimno brskanje	doc. dr. Marko Hölbl, UM FERI

Dandanes sta zasebnost in anonimnost na spletu aktualni temi tako na področju kibernetske varnosti kot širše pri uporabi spleta. Problem predstavlja nenehen nadzor in zbiranje podatkov s strani različnih deležnikov, posledica česar je vedno bolj nadzorovan splet z vedno manj zasebnosti. V okviru predstavitve bomo naslovili problem zasebnost in oblike sledenje uporabnikov na spletu. Protiukrep, ki vsaj zmanjša to »nevarnost« je brskanje s povečano zasebnostjo, ki vključuje različne tehnične in netehnične mehanizme ter pristope. Ena izmed bolj poznanih tehnologij, je tehnologija VPN, ki deloma rešuje problem anonimnosti na spletu in posledično povečanje zasebnost, a ne v celoti. Med naprednejše tehnologije pa sodijo namenska orodja za anonimnost brskanje, kot je tehnologije TOR. Globok in temni splet. Predstavitev bomo zaokrožili tudi z drugačnim pogledom in drugo platjo medalje anonimnosti na spletu – temni splet ter predstavili razlike med temnim in globokim spletom.

Predavatelj:
doc. dr. Marko Hölbl, Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
https://www.linkedin.com/in/markoholbl/

Četrtek, 07. 10. 2021

09:00-09:45	Automating cybersecurity	Gregor Berginc, XLAB

S predavanjem spoznamo osnove Ansible Security in predstavimo, kako se platforma Ansible koristi za to, da se poveže z raznimi varnostnimi platformami (npr. QRadar, Splunk) in primeri uporabe teh platform. Tu gre predvsem za naravno progresijo uvedbe varnosti, ko imamo avtomatizacijo delno že vpeljano v poslovne procese. Opaženo je tudi, da je prav želja po večji varnosti pogosto vzrok za vpeljevanje postopkov avtomatizacije tudi v drugih procesih organizacij. V okviru predavanja spoznamo rešitev, ki jo podjetje XLAB razvija, za povečanje varnosti pri ustvarjanju predlog IaC (angl. Infrastructure as Code), ki nam omogoča statično analizo ustvarjene kode. Z uporabo tega orodja tako lahko povečamo varnost in zaupanje v kodo oz. predloge postopkov kode IaC, in sproti odkrivamo ranljivosti te kode ter nanje opozarjamo avtorje. Znanje in orodje je plod razvoja in raziskav s področja varnosti v XLABu na področju raziskovalnih projektov, ki jih v predavanju tudi omenimo in predstavimo.

Predavatelj:

Gregor Berginc, CEO XLAB-a in vodja skupine XLAB Steampunk
https://www.linkedin.com/in/gberginc/

10:00-10:45	Combating cybersecurity using Artificial Intelligence	Uroš Majcen, S&T

Na področju kibernetske varnosti se zadnje čase dogajajo velike spremembe pri uporabi algoritmov ter napredne intelligence za potrebe analitike pri preiskovanju vzorcev in analize. Predvsem na področju obdelave velike količine podatkov. Na žalost se pa daje tudi prevelika pričakovanja pri uporabi umetne intelligence. Predavanje bo prikazalo trenutno stanje ter nekaj primerov uporabe z prikazom dodane vrednosti in omejitev.

Predavatelj:
Uroš Majcen, Direktor za kibernetsko odpornost, S&T Slovenija
https://www.linkedin.com/in/uros-majcen-3b9aa4/

11:00-11:45	The chepest way to save a quarter milion euros	Suzana Kužnik, NIL

When an incident (false or true) occurs, is it important that employee awareness and responses are at a high level. A lot of awareness is made through workshops or lectures, but employees usually forget the defined process. What can we do to make a difference in employee awareness? Different departments need different kinds of knowledge and most importantly, the IT department needs to know how to make the first response when an incident happened. Who to call, what to make, what to report, and most importantly, don't be ashamed to ask for help.

Predavateljica:

Suzana Kužnik, SOC Varnostni analitik
https:/www.linkedin.com/in/suzana-kuznik/

11:45-12:05	Managed security services in small and medium companies	Saša Jušič, INFIGO IS d.o.o.

Small and medium enterprises often lack dedicated resources to establish and maintain internal Security Operations Centers. In this presentation, we will discuss some common challenges and problems we see in practice and how to address them, from the perspective of a Managed Security Service provider for these profiles of enterprises.

Predavatelj:
Saša Jušić, Senior information security consultant, INFIGO IS d.o.o.
https://www.linkedin.com/in/saša-jušić-119078a

13:00-13:45	Practical and efficient implementation of standards lays the cornerstone of cyber security	Yoann Klein, HUAWEI

Cyber-attacks are increasing in their frequency and complexity, across all technologies and industries. That should trigger a change in our defense paradigm: further balance collective response and individual protection. In order to face global threats, strong cooperation are at paramount, and standards constitutes the necessary foundation. In his talk, Mr Klein will present how the successful example of the telco industry illustrates a pragmatic and efficient model of collaboration, leveraging powerful standards.

Predavatelj:

Yoann Klein, Višji svetovalec za kibernetsko varnost /Senior advisor Cyber Security Huawei

13:45-14:30	Operativni vidiki zagotavljanja celostne kibernetske zaščite	Sara Tomše, Telekom Slovenije

S porastom kibernetskih groženj in povečevanjem pomena zagotavljanja kibernetske zaščite, se pogosto pojavlja vprašanje, na kakšen način zaščititi informacijski sistem pred grožnjami. Pri delu nam lahko pomagajo različna orodja in viri podatkov, s katerimi lahko preprečimo ali ublažimo potencialne napade. Pri obravnavi varnostnih dogodkov in incidentov sta točnost podatkov in odzivnost pri ukrepanju ključnega pomena. Analitiki se pri delu pogosto srečujemo s pomanjkljivimi informacijami, kar pri raziskovanju nalaga dodatno breme naročniku. Poleg pomanjkljivih informacij pa predstavljajo

dodaten problem tudi lažno-pozitivni dogodki. Souporaba različnih orodij lahko zato olajša dodatno delo naročniku, analitiku pa pomaga ločiti lažno-pozitivne dogodke od varnostnih incidentov ter poiskati vstopne točke kibernetskih napadov. Na predavanju bomo s perspektive preiskovanja primerov predstavili souporabo različnih tipov orodij in s tem predstavili izzive in rešitve s katerimi se srečujemo pri analizi potencialnih napadov.

Predavateljica:

Sara Tomše, Analitik kibernetske varnosti – Operativni center za kibernetsko varnost, Telekom Slovenije, d. d.
https://www.linkedin.com/in/sara-tom%C5%A1e-30958b197/

Četrtek, 7. 10. 2021 Austria – European Pioneer in Cyber Security

14:30-15:00	Registracija in mreženje ob kavi	
15:00-15:45	Tracking Novel Cyber Threats for Critical Infrastructures	Dr. Stefan Schauer, AIT Austrian Institute of Technology GmbH

15:45-16:30	Cybersecurity in post-covid times	Miloš Krunić, A1 Slovenija
16:30 -	Mreženje, B2B in poslovne priložnosti	
	Prijave za obe predavanji se zbirajo preko povezave: https://www.izvoznookno.si/Prijavnica?id=195	

Predavatelja:

Dr. Stefan Schauer, AIT Austrian Institute of Technology GmbH: Tackling Novel Cyber Threats for Critical Infrastructures
https://www.linkedin.com/in/stefan-schauer-3aa14ab2/?originalSubdomain=at

Miloš Krunić, A1 Slovenija: Cybersecurity in post-covid times
https://www.linkedin.com/in/krunic-cybersec/?originalSubdomain=si

Več o dogodku: https://www.izvoznookno.si/aktualno/poslovni-forum-avstrija-%E2%80%93-evropski-pionir-v-kibern/

Prijave za obe predavanji se zbirajo preko povezave:
https://www.izvoznookno.si/Prijavnica?id=195

Petek, 8. 10. 2021 - Program konference:

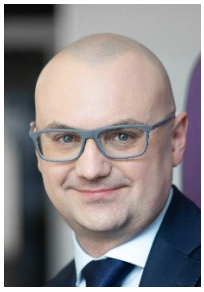
09:10-10:00	Modern cyber defense and the next wave of threats - are we ready?	Yoad Dvir, Microsoft, CEE Cybersecurity Lead

Let's take a moment to learn where we are as cyber defenders, and assess if are ready to play for the “big league” when it comes to modern threats and vulnerabilities.We will discuss trends, insights from the field, and wonder why do we still have ransomware around.

10:00- 10:40	Kako se lotevamo kibernetske varnosti znotraj Huawei	Rafał Jaczyński, Regional Cyber Security Officer CEE & Nordics Huawei Technologies

Vpogled v celostno strategijo in filozofijo kibernetske varnosti vodilnega IKT podjetja.

Predavatelj:



Rafal Jaczynski, direktor za kibernetsko varnost za Srednjo in vzhodno Evropo ter nordijsko regijo pri Huawei Technologies/ Rafał Jaczyński, Regional Cyber Security Officer CEE & Nordics Huawei Technologies

10:40 -11:10	Proaktivna kibernetska varnost	Dalibor Vukovič, Telekom

Dejavnost, ki naslavlja proaktivno kibernetsko varnost »Cyber Threat Intelligence« ali Obveščanje o grožnjah je ena najpomembnejših sestavin napredne kibernetske zaščite in orodje, ki nam omogoča izvajanje proaktivnih dejanj, ki lahko preprečijo ali ublažijo kibernetske napade. Obveščanje o grožnjah se nanaša na podatke: o potencialnih napadalcih, njihovih namenih, motivih in zmožnostih ter o možnih kazalnikih kompromisa (IoC). Te informacije nam pomagajo pri hitrih varnostnih odločitvah kar rezultira k boljši pripravljenosti na kibernetske grožnje. Na predavanju bomo v praktičnem prikazu spoznali delovanje sodobnega Threat Intelligence orodja , ki nam pomaga pri odkrivanju zlorabljenih podatkov kot so npr.: številke bančnih kartic, email naslovi, spletne domene, itd,…

Predavatelj:

Dalibor Vukovič, Produktni vodja – Specialist za kibernetsko varnost, Telekom Slovenije, d. d.
https://www.linkedin.com/in/dalibor-vukovic-60730775/

11:10-11:30	Dobre prakse upravljanja ukrepov kibernetske varnosti v podjetju	Dr. Andrej Rakar, Petrol d.d.

V današnjem času velikega porasta kibernetikih groženj, je uspešnost poslovanja podjetij močno odvisna od uspešne zaščite in hitrega odziva na kibernetske napade. Pri tem je potrebno zajeti vse nivoje ekosistema, od tehničnih, do organizacijskih ukrepov. Na predavanju bomo predstavili kako se upravljanja kibernetske varnosti lotevamo pri nas in kateri koraki so ključni za doseganje večje varnosti.

Predavatelj:

Dr. Andrej Rakar, Vodja informacijske varnosti (CISO), Petrol d.d.
www.linkedin.com/in/andrej-rakar-ph-d-ab0b0a1a9

12:30-12:50	Kako izboljšati varnostno zrelost podjetja?	Kristina Batistič, SmartCom

Kristina Batistič bo predstavila glavne motivacijske dejavnike za vlaganje v varnost in na kakšen način se lotiti strateškega vlaganja v varnost. Pri strateški odločitvi v vlaganje v varnost je zelo pomembno poznavanje zrelostnega modela kibernetske varnosti, ki jih bo govorka tudi predstavila. Osredotočila se bo na tudi na praktično izbiro modela ter na konkretne korake pri njegovi vpeljavi.

Predavateljica:

Kristina Batistič, inženirka informacijske varnosti, Smart Com
www.linkedin.com/in/kristinabatistic

12:50-13:10	Odkrivanje in preprečevanje prefinjenih in naprednih kibernetskih napadov	Miha Lavrič, CreaPlus

Predstavitev naprednih napadov s pomočjo legitiminih programov operacijskih sistemov. Osredotočili se bomo na Powershell, WMI ter kako z uporabo teh programov pridobiti dostop do končne točke. Predstavili bomo napade kot so “LOLbins”, ki so fukusirani na tem, da za zagon svoje zlonamerne kode, ne uporabljajo standardnih zagonskih datotek.

Predavatelj:

Miha Lavrič, CTO CREAplus d.o.o.
https://www.linkedin.com/in/miha-lavri%C4%8D-9b5a12145/

13:10-13:30	Modern approaches to incident response	Boštjan Žvanut, NIL d.o.o.

Recently, the number of attacks has been rising sharply. Attackers are becoming more and more advanced and sophisticated. Their malicious codes are made in a way that bypasses standard prevention controls. We can still see attackers present in the organization for a long time. What can we do to detect the incident and what can we do when the incident in organization is discovered? We know standard procedures of established good practices for responding to an incident, but many organizations still do not keep up with devastating progressive attacks. The key to successful incident response lies in proactivity of the organization, professionalism of the staff, advanced attacks knowledge and automation.

Predavatelj:

Boštjan Žvanut, GCIH, Incident Response Lead @ NIL part of Conscia

http://www.linkedin.com/in/bostjanzvanut

13:30-13:50	Threat intelligence: what can we learn by observing the attackers?	dr. Urban Sedlar, UL FE

We'll present the CyberLab environment, established at the Faculty of Electrical Engineering, University of Ljubljana, which we use to observe and study various kinds of cyberattacks. The environment comprises multiple honeypots/honeynets, data collectors and a /24 network telescope. All attacker and scanner metadata, as well as the collected session data and malware are enriched, analyzed and stored, and accessible through our APIs.

Predavatelj:
dr. Urban Sedlar, UL FE
http://www.linkedin.com/in/urbansedlar

13:50-14:10	Kako preživeti kibernetsko vojskovanje in nadgraditi svoj posel?	Mag. Matjaž Kosem in Grega Prešeren, CARBONSEC d.o.o.

Predavatelja:
mag. Matjaž Kosem, CEO, CARBONSEC d.o.o.
Grega Prešeren, CTO, CARBONSEC d.o.o.

14:10-14:30	Implement security governance to achieve cyber resilience	Uroš Majcen, S&T

Kibernetska odpornost združuje področja analize poslovnih učinkov, analize tveganj in neprekinjenega poslovanja ter zaznave in odziva na kibernetski incident. Predavanje bo prikazalo celovit pristop pristopitvi kibernetske odpornosti z opisom in prikazom posameznih področij.

Predavatelj:
Uroš Majcen, Direktor za kibernetsko odpornost, S&T Slovenija
https://www.linkedin.com/in/uros-majcen-3b9aa4/

17:00 -24:00	Cyber Night- CTF tekmovanje

CTF oziroma Capture the Flag (“Ujemite zastavo”) je posebna vrsta tekmovanja s področja informacijske varnosti, ki tekmovalce izziva v reševanju najrazličnejših nalog: od lova na zaklad do osnovnih programskih vaj, do hekanja v strežnik in kraje podatkov. Izziv poteka na pobudo Agencije Evropske unije za kibernetsko varnost (ENISA) in ga organizirajo Sekcija kibernetske varnosti pri GZS-ZIT, IKT-Horizontalna mreža in Projektna pisarna GZS.

https://cybernight.org/