CYBER SECURITY ACADEMY

5—9/10/2020 / AMERICKÉ CENTRUM V PRAZE
TRŽIŠTĚ 13, PRAHA 1

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Prague Security Studies Institute

Prague Security Studies Institute

ve spolupráci:

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

hlavní partneři

US embassy

British Embassy Prague

CYBEXER TECHNOLOGIES

partneři

Norwegian Embassy

Check Point SOFTWARE TECHNOLOGIES LTD

OBECNÉ INFORMACE

Dress code: Business Casual

Lokace: Americké centrum v Praze (Tržiště 13, Praha 1) – jedná se o budovu hned pod Americkou ambasádou v Praze. Vstupte a projděte skleněnými dveřmi a po schodech vystoupejte do prvního patra, kde zazvoníte na zvonek.

Formát CSA 2020: Všechny naše přednášky se řídí pravidly **Chatham House**, což znamená: „Pokud se setkání řídí pravidly Chatham House, tak účastníci mohou využít získané informace, ale neprozradí, od koho tyto informace získali."

PONDĚLÍ, 5. ŘÍJNA, 2020

08:30–9:00 **Registrace**

09:00–09:15 **Přivítání a Úvodní slovo**
Zástupci PSSI, americké a britské ambasády

09:15–10:30 **Ruská federace a její působení v kyberprostoru**
Michal Myklín, NÚKIB

Shrnutí ofenzivního i defenzivního působení Ruské federace v kyberprostoru od aktérů a jejich silných a slabých stránek, přes konkrétní operace, legislativu, až po bezpečnostní dopady na národní bezpečnost České republiky.

Michael Myklín na NÚKIB působí jako analytik se zaměřením na postsovětský prostor. Je absolventem bezpečnostních a strategických studiích na Fakultě sociálních studií Masarykovy univerzity.

10:45–12:15 **Budoucí výzvy kybernetické bezpečnosti**
Luboš Přikryl, NÚKIB

Přednáška se zaměří na nové technologie, které mají potenciál výrazně proměnit charakter kybernetické bezpečnosti, jako například sítě 5G, internet věcí (IoT) nebo umělá inteligence (AI).

Luboš Přikryl je analytikem NÚKIB se zaměřením na nejnovější technologie. Vystudoval Bezpečnostní a Strategická studia na Fakultě sociálních studií Masarykovy univerzity.

12:30–13:30 **Obědová pauza**

13:45–15:15 **Kybernetická bezpečnost a mezinárodní právo**
Tomáš Minárik, NÚKIB

Přednáška se zaměří na principy, normy a pravidla kybernetické bezpečnosti z pohledu mezinárodního práva. Východiskem přitom bude Tallinnský manual 2.0 k interpretaci a uplatňování mezinárodního práva v kyberprostoru. Součástí bude také vysvětlení „International Cyber Law: Interactive Toolkit“

Tomáš Minárik je vedoucí Oddělení mezinárodních organizací a práva NÚKIB. Více než pět let působil jako výzkumný pracovník v NATO CCD COE v estonském Tallinnu. Je absolventem Právnické fakulty univerzity Karlovy v Praze. V minulosti působil jako právní poradce na Ministerstvu obrany.

15:30–17:00 **Kybernetická bezpečnost z pohledu Evropské unie**
Adam Botek, NÚKIB

Přednáška představí kompetence unijních institucí a hlavním strategickým i legislativním nástrojům EU v oblasti kybernetické bezpečnosti. Zvláštní pozornost bude věnována směrnici NIS (Network Information Security); EU 5G Toolbox nebo EU Cyber Diplomacy Toolbox.

Adam Botek působí v Oddělení mezinárodních organizací a práva NÚKIB se zaměřením na právo a politiky EU. Je absolventem Právnické fakulty univerzity Karlovy.

ÚTERÝ, 6. ŘÍJNA, 2020

09:00–10:30 **Kybernetická válka českou optikou**
pplk. Ing. Tomáš Novák, Ph.D
pplk. Ing. Lubomír Chylík, Velitelství Kybernetických sil a Informačních operací

Podplukovník Tomáš Novák stál u zrodu Střediska psychologických operací u pozemního vojska a později vybudoval Středisko psychologických a informačních operací Speciálních sil AČR. V současné době působí na Velitelství Kybernetických a informačních sil v Brně. V roce 2017 získal v rámci postgraduálního studia a práce na téma „Psychologické operace k podpoře brigádního úkolového uskupení AČR“ doktorandský titul na Univerzitě obrany. Během své kariéry získal mnoho taktických a operačních zkušeností v rámci nasazení do úkolových uskupení AČR v Kosovu, Afghánistánu a Litvě. Aktuálně řeší problematiku budování a rozvoje schopností AČR potřebných pro působení v informačním prostředí.

Podplukovník Lubomír Chylík vystudoval vojenskou robotiku a kybernetiku na Vojenské akademii v Brně. Následně v rámci Armády České republiky působil v oblasti IT zabezpečení u rezortních vzdělávacích středisek ve Vyškově a později se podílel na plánování výstavby, implementaci a využívání schopností nástrojů pro modelování a simulace u mezinárodní vojenské organizace Joint Chemical, Biological, Radiological and Nuclear Defence Centre of Excellence. Ve Spolkové republice Německo působil na operačním velitelství EU Multinational Headquarters Ulm, kde zastával funkci Cyber Information Security Officer. Aktuálně řeší problematiku budování a rozvoje schopností působení v kybernetickém prostoru na Velitelství kybernetických sil a informačních operací.

10:45–12:15 **Bezpečnost v moderním světě**
Miloslav Lujka, Check Point Software Technologies

Miloslav Lujka pracuje dvanáctým rokem pro Check Point Software Technologies, světového lídra v oblasti kybernetické bezpečnosti. Má za sebou přes 20 let zkušeností v mezinárodních firmách, klíčové projekty vedl například pro Cisco Systems a Vodafone. Strategické řízení si osvojil během studia MSc. a MBA na The Nottingham Trent University.

Je zakladatelem neziskového vzdělávacího projektu www.digitalnipevnost.cz kde se věnuje mj. bezpečnosti běžných lidí. Můžete ho pravidelně vidět v televizi, kde komentuje aktuální bezpečnostní dění. V roce 2019 se zařadil mezi TEDx speakery s přednáškou: „Vaše soukromí neexistuje…"

12:30–13:30 **Obědová pauza**

13:45–15:15 **NATO a kybernetická bezpečnost**
Laura Brent, NATO

Spojenci uznali nejen existenci kybernetických hrozeb, ale také to, že jsou stále častější, komplexnější, ničivější se stále větším nátlakovým aspektem. Kybernetická bezpečnost respektive kybernetická obrana se tímto stala pro aliančí spojence zásadním tématem, které se z čistě technického problému transformovalo do problému politického a operačního s nejvyšší prioritou. S ohledem na výše zmíněné bude přednáška pokrývat adaptaci kybernetických složek NATO, priority v této oblasti a roli, kterou v oblasti kybernetické obrany hraje NATO a jeho spojenci.

Laura Brent v současnosti pracuje v NATO v sekci kybernetické obrany, kde má na starosti implementaci kybernetické obrany do struktur NATO. V minulosti pracovala jako konzultantka v Ernst & Young se zaměřením na kybernetickou kriminalistu a vyšetřování. Má za sebou i pozici v americké vládě jako seniorní poradce na Ministerstvu vnitřní bezpečnosti (U.S. Department of Homeland Security). Laura Brent získala bakalářský titul na Harvardu a magisterský na Johns Hopkins School of Advanced International Studies.

Doporučené čtení:
NATO's role in cyberspace

15:30–17:00 **Role 5G sítí v geoekonomickém soupeření**
Dr. Richard B. Andres, National War College

Jedním z nejdůležitějších aspektů je čínské, a z části jistě úspěšné, tažení ve snaze ovládnout infrastrukturu a standardy vztahující se k technologii 5G. Tato konfrontace mezi dvěma světovými hegemony je velmi důležitá, protože tato technologie má nakročeno k tomu být hnacím motorem přicházející nové průmyslové revoluce, která by mohla zásadně změnit mocenské postavení států. V době soupeření nejsilnějších států světa bude hrát honba za nadvládou nad 5G technologií zásadní roli a vítězi umožní lépe provádět špionážní a vojenské operace.

Richard B. Andres je profesorem v oboru národní bezpečnostní strategie na prestižní National War College, kde se zaměřuje na vývoj strategických doktrín a kybernetickou bezpečnost. Dále uči kurzy zaměřující se kybernetické strategie na Georgetown University a Johns Hopkins University. Během své kariéry působil na několika vysokých pozicích ve státní správě (konzultant pro US Cyber Command, US Air Force, team leader během Bushova i Obamova prezidentství atd.).

STŘEDA, 7. ŘÍJNA, 2020

09:00–10:30 **Hacking jako řemeslo**
Martin Leskovjan, Citadelo

V přednášce budou představeny základní fakta o tématu penetračního testování neboli etického hackingu. Posluchači s seznámí s etickými a právními principy, metodologiemi, které se v této oblasti používají, dále s nejčastějšími typy testů, testovacími nástroji a postupy a také s nečekanými úskalími, které může tato činnost přinést. Samostatnou kapitolu budeme věnovat nejúčinnějšímu typu kybernetického útoku, a tím je útok na wetware. V rámci něj si představíme základní postupy a principy testování metodami sociálního inženýrství.

Martin Leskovjan je certifikovaný auditor managementu informační bezpečnosti a člen boardu společnosti Citadelo zaměřené na penetrační testování a audity, která působí v ČR, na Slovensku a ve Švýcarsku. Vystudoval Právnickou fakultu UK a následně se zaměřil na oblasti práva související s bezpečností informací a autorskými právy na internetu ve spojení s praxi etických hackerů, které nejprve obchodně zastupoval a následně v roce 2017 založil český team. Profesní deformace ho vede k hledání slabin ve všech systémech, proto se začal zabývat také kryptoměnami, ochranou soukromí na internetu a antifragilními strukturami jako jsou např. anonymní kryptomarkety.

10:45–12:15 **Technologie klamu**
Lukáš Březina, Taktik s.r.o.

Technologie klamu je známá již po staletí. Vídáme ji v politice, sportu, ale i v osobním životě. Jak nám technologie klamu pomůže v rámci kyberbezpečnosti? Jak funguje, jakým způsobem a proč je nutné útočníka uvnitř organizace detekovat okamžitě? Technologie klamu se postupně stává nedílnou součástí dobře zabezpečené sítě a ve spojení s dalšími moderními Next-Gen technologiemi patří k maximálně možnému zabezpečení organizace.

Lukáš Březina vystudoval informační management na Fakultě Informatiky a Managementu v Hradci Králové. Pracoval jako administrátor v hkfree.org (jedna z největších free-netových sítí v ČR), kde se postupně propracoval do vedení celé organizace. Později působil jako IT/IS admin a auditor pro střední a jihovýchodní Evropu pro švédskou firmu Alfa Laval. Od listopadu 2019 působí na pozici Presales a Security Engineer v Taktik s.r.o.

12:30–13:30 **obědová pauza**

13:45–15:15 **Digitální identita**
Jiří Bulan, Společník & CEO RaulWalter CZ

Jiří Bulan je společníkem a ředitelem v RaulWalter CZ, která se specializují na „identity solutions" pro veřejný a soukromý sektor. Jiří se zejména zaměřuje na oblast digitální identity, kryptografie a chytrých karet. Spolupracoval na technologických řešení pro biometrické pasy a další formy e-ID ve Velké Británii, Irsku, Švédsku, Libanonu a Jordánsku. Před příchodem do privátní sféry Jiří pracoval pro různé státní a vládní úřady.

Doporučené čtení:
EU Regulation eIDAS
EU Regulation for biometric eID
Jiří Bulan's commentary

15:30–17:00 **Aspekty norské kybernetické bezpečnosti**
Håkon Bergsjø, Norský národní bezpečnostní úřad

Přednáška se bude věnovat norskému pohledu na kybernetickou bezpečnost, způsobu jak je v Norsku kybernetická bezpečnost organizována a jaké jsou „best practices", které by si Česká republika mohla odnést.

Håkon Bergsjø v současnosti pracuje jako vedoucí společného koordinačního kybernetického centra spadající pod Norský národní bezpečnostní úřad (NSM). Posledních 20 let se věnuje různým aspektům bezpečnosti a zastával různé pozice v norské armádě, v národním bezpečnostním úřadu a také vedl norský CERT tým. Napsal několik knih o digitální bezpečnosti a digitální etice.

ČTVRTEK, 8. ŘÍJNA, 2020

09:00–10:30 **Kybernetické útoky v bankovním sektoru**
Milan Zrcek, ČSOB

Milan Zrcek je zkušeným expertem v oblasti informační bezpečnosti, kde se zaměřuje na vymýšlení bezpečnostní IT strategie, koordinaci kybernetické bezpečnosti a kontrolních programů, hodnocení rizik a implementaci Data Loss Prevention řešení. V minulosti pracoval jako konzultant a auditor informačních systému v PwC. Vystudoval informační management na VŠE v Praze.

10:45–12:15 **Diplomacie a kybernetická bezpečnost**
Richard Kadlčák, Ministerstvo zahraničních věcí

Richard Kadlčák v současnosti působí na Ministerstvu zahraničních věcí ČR jako ředitel odboru kybernetické bezpečnosti a zároveň jako zvláštní zmocněnec pro kybernetický prostor. Zabývá se koordinací mezinárodní spolupráce v oblasti kybernetické bezpečnosti. Na ministerstvu zahraničních věcí pracoval uplynulých 20 let a vykonával mimo jiné funkci mimořádného a zplnomocněného velvyslance ČR v Estonsku.

12:30–13:30 **obědová pauza**

13:45–15:15 **Vojenské implikace kyber prostoru**
Mgr. et Mgr. Jakub Fučík, Ph.D, Univerzita Obrany

Rozvoj komunikačních a informačních technologií vede nejen k novým možnostem a příležitostem, jak zlepšit blahobyt společnosti, ale také k závislosti na těchto technologiích. Ze strategického hlediska představuje kyberprostor novou dimenzi, kde státní a nestátní aktéři navzájem soutěží v prosazování svých vlastních zájmů – často

na úkor jiných. Škodlivé kybernetické aktivity z tohoto pohledu představují nový druh hrozeb (a nástrojů), které mají negativní dopad nejen v této doméně, ale též v ostatních (fyzických) dimenzích. Kybernetická obrana a kybernetická bezpečnost se tak stávají nedílnou součástí veřejných a soukromých zájmů. Přednáška se zaměří na vojenské implikace kyberprostoru a jejich vlivu na charakter současných ozbrojených konfliktů.

Jakub Fučík v letech 2010–2012 absolvoval magisterský obor Mezinárodní vztahy na Fakultě sociálních studií Masarykovy univerzity v Brně. Současně vystudoval Právo na Právnické fakultě Masarykovy univerzity v Brně. V roce 2018 na katedře Mezinárodních vztahů a Evropských studií, FSS MU obhájil disertační práci a byl mu udělen akademický titul Ph.D. Od února 2016 působí jako akademický pracovník Centra bezpečnostních a vojenskostrategických studií Univerzity obrany v Brně a jako tajemník odborného časopisu Obrana a strategie.

Doporučené čtení:
Technologický vývoj: implikace pro schopnosti ozbrojených sil ČR 2019

15:30–17:00 **Útočné operace v kyberprostoru**
Dr. Tim Stevens, King's College London

Přednáška se zaměří na to, jak útočné kybernetické operace mohou být integrovány do národní bezpečnostní strategie. Na příkladu Velké Británie se podíváme na několik zásadních otázek, které musí řešit všechny země, které by chtěly využít kyberprostor jako vojenskou operační doménu. Mezi tyto otázky patří smysl ofenzivních kybernetických operací, právní rámec, institucionální adaptace a mezinárodní partnerství. Útočné kybernetické operace se zdají být jako atraktivní možnost pro vhodně vybavené státy, ale rozhodně se nedá říct, že by to bylo jednoduché řešení s nulovým riskem

Tim Stevens je docentem na londýnské King's College London kde učí Global Security a je vedoucím výzkumné skupiny KCL Cyber Security Research Group. Ve svém výzkumu se zaměřuje se na průsečík technologie, politiky a světové bezpečnosti – zejména se zajímá o informační technologie a jejich roli ve formování celosvětových bezpečnostních postupů. V současné době zkoumá roli ofenzivních kybernetických operací v rámci britské bezpečnostní strategie. Stevens získal magisterský titul i doktorát na King's College London a působí v několika světových výzkumných institucích.

Doporučené čtení:
The strategic promise of offensive cyber operations

PÁTEK, 9. ŘÍJNA, 2020

09:00–13:30 **Table Top cvičení: Simulace kybernetického útoku od Cybexer Technologies**
Lucie Kadlecová a Lauri Almann, Cybexer Technologies

Table Top cvičení je verbálně prezentovaný scénář, který může mít velmi vážné dopady, pokud by se stal v reálném životě. Během cvičení si účastníci vyzkouší, jak by reagovali během takového útoku v realitě. Budou rozděleni do několika týmů, kde budou muset vyhodnocovat situaci a na základě vstupních informací adekvátně reagovat. Po cvičení s lektory proberou svá rozhodnutí a možnosti (případně) lepšího postupu.

Lucie Kadlecová je Senior Associate v Cybexer Technologies. Během své kariéry pracovala v Národním centru kybernetické bezpečnosti a byla trainee v sekci kybernetické bezpečnosti v sídle NATO a také působila v kabinetu komisaře pro rozšíření a evropskou sousedskou politiku v Evropské komisi. Vystudovala londýnskou King's College, pracovala jako výzkumník na MIT přes Fulbrightovo stipendium a v současnosti pracuje na svém doktorátu na Univerzitě Karlově.

13:30–14:00 **Závěrečné vyhodnocení**