Pracovní skupina kybernetické bezpečnosti české pobočky AFCEA
Policejní akademie ČR v Praze
ve spolupráci s
Národním úřadem pro kybernetickou a informační bezpečnost ČR

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Kybernetická bezpečnost VIII

- ***Stav kybernetické bezpečnosti ČR a aktuální strategické plány***
- ***Aktuální bezpečnostní hrozby a zranitelnosti***
- ***Zkušenosti z krizového stavu***
- ***Moderní nástroje a řešení v oblasti kybernetické bezpečnosti a obrany***

23. září 2020, od 9:00
ONLINE

9:00 ***Přivítání & Úvodní slovo***
Tomáš MÜLLER, Prezident, České pobočky AFCEA

Úvodní sekce

9:10 – 9:40 **Bezpečnostní standard pro videokonference**
Vladimír JEŘÁBEK, NAKIT s.p.
Bezpečnostní doporučení pro videokonference zpracované NÚKIB a NAKIT ve spolupráci s odbornou komunitou.

9:40 – 10:30 **Aktuální stav kybernetické bezpečnosti v České republice**
Adam KUČINSKÝ, NÚKIB ČR
Cloudová vyhláška, Minimální bezpečnostní standard a další novinky z oblasti kybernetické bezpečnosti.

10:30 – 11:00 **Překvapující zranitelnosti odhalené při penetračních testech**
Jan KOPŘIVA, Senior Lead, CSIRT, ALEF NULA, a.s.
Při penetračních testech často přicházíme do styku s dlouhodobě nezáplatovanými systémy nebo zastaralými webovými aplikacemi, které obsahují velké množství závažných zranitelností. Přestože jsme na takové případy po mnoha letech práce v oboru zvyklí, některé zranitelností nás stále dokáží svým potenciálním dopadem velmi nepříjemně překvapit. Právě jim bude věnována tato prezentace.

11:00 – 11:30 Přestávka

Sekce praktických příkladů a řešení v oblasti kybernetické bezpečnosti

11:30 – 12:00 **Moderní kybernetická bezpečnost potřebuje data a signály**

Dalibor KAČMÁŘ, National Technology Officer, Microsoft CZ&SK

V globálním světě internetu a cloud technologií útočníci působí bez hranic, prostřednictvím libovolné technologie a s využitím všech datových zdrojů. Je tedy možné realizovat efektivní a bezpečnou teritorialitu bez globálního přístupu? Prezentace představí, jak se na tuto otázku v Microsoftu prakticky díváme a jaký přístup volíme.

12:00 – 12:20 **Anatomie ransomware útoku a jeho včasná detekce**

Pavel MINAŘÍK, Chief Technology Officer, Flowmon Networks

Jaké projevy předchází zašifrování dat? Jaké indikátory kompromitace je možné identifikovat a zabránit tak ochromení infrastruktury? Jaké cíle sledují útočníci? V prezentaci rozebereme vzorovou anatomii útoku a ukážeme možnosti detekce. To vše na živo v izolovaném laboratorním prostředí.

12:20 – 12:30 **Vesmírná mise – ECSC 2021**

Jaroslav BURČÍK, Předseda Výkonného výboru ECSC 2021, ČVUT / FEL

Informace o přípravě a konceptu evropského finále European Cyber Security Challenge.

12:30 – 13:30 Přestávka

Sekce zkušenosti z krizového stavu

13:30 – 14:00 **Praktické zkušenosti s provedením bezpečnostního auditu v nemocnicích**

Pavel Klimeš, Ředitel rozvoje bezpečnostních produktů, Corpus Solutions a.s.

Nemocnice jsou stále vděčným terčem potencionálních hackerů, kteří využívají dlouhodobě nahromaděných nedostatků v kybernetické ochraně v rámci tohoto celého segmentu. Jaké jsou naše praktické zkušenosti v této oblasti a jakým směrem vedeme tato zařízení tak, aby významným způsobem zajistily schopnost detekovat, analyzovat a reagovat na moderní hrozby je hlavní náplní naší prezentace.

14:00 – 14:20 **Kybernetický útok na významného zákazníka a jeho řešení**

Eliška BARTŮŠKOVÁ a Kamil VIRÁG, GORDIC

Prezentace se zabývá kybernetickým útokem na významného zákazníka společnosti Gordic a jeho řešením. Díky prezentaci se dozvíte, na co všechno byste se měli připravit a promyslet v rámci vašeho systému zajištění kybernetické bezpečnosti, abyste případnou bezpečnostní událost či incident vyřešili, co nejrychleji a co možná nejlépe. Zároveň se dozvíte, jak se řeší konkrétní typ útoku ve středně velké organizaci, koho je nutné kontaktovat, kdo vám může pomoci a jaká krátkodobá a dlouhodobá opatření přijmout.

14:20 – 14:40 **Bezpečnostní deštník zajišťující orchestraci, automatizaci a reakci na krizové události**

Adam MUŠKA, Software Architect, IBM

V otázce nastavení plánů krizového řízení nestačí prosté nastavení metodických postupů, je třeba zajistit i funkční nástroje, které jsou bezpečnostním týmům ve vypjatých situacích aktivní podporou. Mimo jiné se může jednat o centrální správu a vyhodnocování incidentů různého původu, automatizace určitých akcí, eskalace atp.

14:40 – 14:55 **Vyhledávání v rozsáhlé kolekci videa pomoci nového systému SOMHunter**

Jakub LOKOČ, MFF UK

Vyhledávání libovolné scény v rozsáhlých kolekcích videa je stále považováno ze nesmírně složitou úlohu zahrnující techniky automatické anotace, podobnostního modelování, využívání zpětné vazby od uživatelů a efektivní vizualizace výsledků. Díky nejnovějším poznatkům z oblasti hlubokého učení je dnes možné vytvářet vyhledávače, které vykazují daleko větší efektivitu, než na jakou jsme se museli spoléhat ještě před pár lety. V této přednášce představím nový systém SOMHunter, vyvíjený na MFF UK,

který letos zvítězil v mezinárodní soutěži VideoBrowserShowdown. První polovina přednášky shrnuje moderní technologie použité k tvorbě takového vyhledávače, zatímco druhá polovina se zaměří na demonstraci aktuální verze vyhledávače pro několik zvolených typů úloh.

14:55 – 15:20 **Každý má svá tajemství**

Miroslav NEČAS, TOVEK

Eliminace rizik spojených s dodavatelským řetězcem a privilegovanými uživateli prověřováním klíčových osob a dodavatelů z otevřených zdrojů.

15:25 ***Závěr***

Vyplňte nám prosím krátký dotazník. Děkujeme!

https://forms.office.com/Pages/ResponsePage.aspx?id=ZalWmLDxu0yewO20Se2aQRCrLlbgLxVNjxbSLB_hY05UN1RGUjk5NFI2WUdVRTFDMFhGOTVFRlNSWS4u

Partneři akce

ALEFNULA

GORDIC

Microsoft

CORPUS SOLUTIONS CYBERSECURITY EXPERTS

TOVEK

Flowmon Driving Network Visibility