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

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Kybernetická bezpečnost X

- ***Stav kybernetické bezpečnosti v ČR***
- ***Trendy a moderní technologie v KB***
- ***Aktuální KB hrozby a jak se jim bránit***

27. září 2022, 9:30 – 16:00

Konferenční sál 201, budova C, Policejní akademie ČR v Praze

09:30 **Přivítání**
Petr JIRÁSEK, Předseda Pracovní skupiny kybernetické bezpečnosti
Luděk MICHÁLEK, Policejní akademie ČR v Praze

Úvodní sekce

09:35 – 09:50 **Úvodní slovo – aktuální stav kybernetické bezpečnosti v ČR**
Lukáš KINTR, ředitel, NÚKIB

09:50 – 10:20 **Závažné prohřešky v Active Directory**
David HORÁK, Security Systems Engineer, ALEF NULA, a.s.
V rámci přednášky se podíváme na nejčastěji chybějící bezpečnostní opatření v Active Directory. Tato bezpečnostní opatření si stručně vysvětlíme. Dále si z perspektivy útočníka ukážeme, jak lze jejich absence v rámci Windows infrastruktury zneužít.

10:20 – 10:40 **Hybridní infrastruktura a monitoring datového provozu v prostředí public cloud**
Pavel MINAŘÍK, Vice President of Technology, Progress Software
Monitorování a analýza síťového provozu je neoddělitelnou součástí kybernetické bezpečnosti bez ohledu na to, zda se vaše infrastruktura nachází v privátním datovém centru nebo prostředí veřejného cloudu. Současným

trendem je hybridní prostředí kombinující různé typy infrastruktur, často i kombinace více poskytovatelů veřejného cloudu (dual cloud strategy). Monitorování provozu v tradičních infrastrukturách je rutinní záležitostí. Prezentace představí současné technologické možnosti monitorování provozu v prostředí veřejného cloudu a možnosti konsolidace veškerých dat o provozu datové sítě v jednotném prostředí.

10:40 – 11:10 **Jak poznat, kdo je na internetu nebezpečný?**

Vojtěch BUMBA, Vedoucí vývoje, Trusted Network Solutions

Pustili byste si do bytu odsouzeného zločince, i kdyby chtěl jen kávu? Pravděpodobně asi ne. Proč si tedy pouštět do sítě IP adresy, o kterých se ví, že jsou nebezpečné? Přesně s touto myšlenkou operuje databáze aktivních hrozeb, která je jádrem bezpečnostních řešení KERNUN. Vyvinuli jsme inteligentní algoritmus na hodnocení reputace IP adres, pomocí kterého jsme schopni nepustit do interní sítě nikoho, o kom víme, že se v kyberprostoru chová podezřele. Řekneme si, jak se databáze aktivních hrozeb tvoří, jak se používá a proč je právě adaptivita řešením mnoha současných bezpečnostních problémů.

11:10 – 11:40 Přestávka

Sekce praktických příkladů a řešení v oblasti kybernetické bezpečnosti

11:40 – 12:00 **Using Microsoft® 365 & Teams in a secure and legally compliant manner - real data protection instead of standard contractual clauses**

Kurt KIRCHBERGER, Rohde&Schwarz Austria

Within this presentation you will get insight into current and future concerns when using public cloud services from US based cloud service providers. We will discuss different perspectives like the legal situation, law enforcement requests, hacking attacks and the post-quantum threat. We will also show you how the R&S® Cloud Data Protection Gateway mitigates these risks.

12:00 – 12:20 **Barracuda Networks – Zero Trust Network Access pro cloudové služby a hybridní prostředí**

Jakub JANČÍK, Sales Engineer, Barracuda Networks

Zero Trust Network Access (ZTNA) slouží k zajištění bezpečného přístupu do vzdálených prostředí, včetně cloudových služeb. Přiblížíme si implementaci ZTNA pomocí služby CloudGen Access od společnosti Barracuda Networks a porovnáme si rozdíly mezi VPN a ZTNA.

12:20 – 12:50 **Tbd**

Gigamon (Exclusive Networks)

12:50 – 13:30 Přestávka (oběd)

Sekce zkušeností a budoucích řešení

13:30 – 14:00 **NIS-2 / Nový zákon o KB**

Adam KUČÍNSKÝ, ředitel odboru, odbor regulace, NÚKIB ČR

14:00 – 14:20 **Alternativní způsob řešení problému nedostatku odborníků kybernetické bezpečnosti**

Václav PÁVEK, Director, Global Delivery Services, Novicom, s.r.o.

Nároky na komplexní zajištění kybernetické bezpečnosti se neustále zvyšují. Novicom CCM (Cybersecurity Compliance Management) je nástroj, ve kterém budou mít manažeři kybernetické bezpečnosti svou agendu jednoduše a přehledně pod kontrolou s plnou podporou odborníků pro případ potřeby.

14:20 – 14:50 **Nevyhnutelná automatizace a řízení certifikátů a důvěryhodných služeb**

Roman CINKAIS, 3Key Company

Digitální certifikáty jsou v současnosti nedílnou součástí skoro každého informačního systému nebo řešení. Jejich počet i variabilita rostou exponenciálně vzhůru s příchodem IoT, 5G sítí a nových technologií. Certifikáty zajišťují

nezbytnou důvěru a bezpečnost při komunikaci, reprezentují identitu ve virtuálním světě, ale taky vyžadují řádnou péči a řízení. Společnosti se často potýkají s vysokou pracnosti související se správou certifikátů a nedostatečným zabezpečením v souvislosti s chybně vydanými nebo nedůvěryhodnými certifikáty. To vše má dopad na naše soukromí a nejenom pro společnosti představuje vysoké finanční a reputační riziko.

PKI se stává nedílnou a kritickou součástí systémů a služeb a vzniká potřeba automatizovat procesy spojené s řízením životního cyklu certifikátů.

14:50 – 15:10 *Přestávka (oběd)*

15:10 – 15:30 **Vládní dohledové centrum**

Vladimír ROHEL, Bezpečnostní ředitel, NAKIT s.p.

Prezentace představí projekt „Vládní dohledové centrum" a jeho vznik z již plně fungujícího Dohledového centra eGovernmentu Ministerstva vnitra ČR. Prezentace dále ukáže jak stávající DCeGOV zapadá do komplexu bezpečnostních služeb zahrnutých v Kompetenčním centru bezpečnosti informací NAKIT, jak již poskytujeme a jak jsme v budoucnu připraveni poskytovat naše služby.

15:30 – 15:50 **Jak elegantně splnit náročné požadavky na šifrování dat a separaci šifrovacích klíčů**

Jan GÉRING, technický konzultant, ASKON INTERNATIONAL s.r.o.

Kde jsou uložené šifrovací klíče, kdo k nim má přístup a za jakých okolností? To jsou základní otázky, které musíme brát v potaz, pokud chceme důkladně zabezpečit nejen kritickou infrastrukturu, ale jakákoli citlivá data před jejich zneužitím. Kam tedy šifrovací klíče uložit? Na USB pod polštář, nebo …

15:50 – 16:20 **3xProč: Trendy v Evil Economy**

Robin BAY, TrendMicro

3xproč: Trendy v Evil Economy: Proč stále více nabývá na důležitosti výkup zranitelností. Proč je důležité míti EDR, NDR a Filipa! A konečně proč bývá SaaS řešením mnoha bezpečnostních neduhů ONPREMISE světa.

16:20 **Závěrečné slovo**

Petr JIRÁSEK, Předseda Pracovní skupiny kybernetické bezpečnosti

16:30 **Ukončení akce**

Připravované a podporované akce

- ***10. 10. 2022 – Festival bezpečnějšího internetu (FBI) – Online bezpečnost pohádkou, komiksem nebo s Instagramem***
- ***17. – 18. 10. 2022 – AFCEA TechNet Europe***
- ***19. – 21. 10. 2022 – Future Cyber Defense Conference & Live Hacking Zone (FFF)***
- ***26. 10. 2022 – Festival bezpečnějšího internetu (FBI) – Kybertalent ve třídě***
- ***3. 11. 2022 – Dohledová centra (SOC)***
- ***27. 4. 2023 – Národní finále Národní soutěže ČR v kybernetické bezpečnosti NSKB-7 ve Škoda Auto***

Hlavní partneři akce

ALEF

Kernun INTERNET SECURITY

Gigamon®

3KEYCOMPANY

EXCLUSIVE NETWORKS

Partneři akce

CORPUS SOLUTIONS CYBERSECURITY EXPERTS

novicom

FUTURE FORCES FORUM EVENT

Progress®

ROHDE&SCHWARZ

ASKON international s.r.o.

atlantis

MONET + Trust in digital