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

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Kybernetická bezpečnost IX

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

7. října 2021, 9:00 – 16:00
Konferenční sál P1, Pavilón P, BVV, Brno

IDET 2021

9:00 **Přivítání**

Petr JIRÁSEK, Předseda pracovní skupiny kybernetické bezpečnosti

Úvodní sekce

9:10 – 9:40 **Úvodní slovo**

Lukáš KINTR, náměstek ředitele, NÚKIB ČR

9:40 – 10:10 **Zranitelný internet, aneb narůstající technologický dluh a s ním spojené hrozby**

Jan KOPŘIVA, ALEF NULA, a.s.

K internetu jsou v současnosti připojeny miliony zastaralých systémů, které jsou postiženy známými závažnými zranitelnostmi, a jejich počet kontinuálně narůstá. Tento stále se zvyšující „technologický dluh" nepředstavuje hrozbu pouze pro provozovatele a vlastníky samotných zranitelných systémů, ale i jakýkoli jiný subjekt, který internet využívá, neb zranitelné systémy může být pro útočníky relativně snadné kompromitovat a následně využít k útoku na jiné cíle. Jak závažná situace v oblasti zranitelných systémů dostupných z internetu v ČR a ve světě je, a jaké konkrétní hrozby pro státní i soukromé organizace jsou s nimi spojené, se zaměříme v této prezentaci.

10:10 – 10:40 **Role inteligentní pastí v systému integrované kybernetické ochrany organizace**

Pavel KLIMEŠ, Corpus Solutions, a.s.

V rámci prezentace bude vysvětlena role inteligentních pastí jako klíčové součásti celkového konceptu kybernetické ochrany. Bude vysvětlen přínos zejména v kontextu pokročilých útoků typu Ransomware, kdy nástroje preventivní ochrany mohou selhat a detekce aktivit útočníka nástroji SIEM, EDR není přímočará. Útočník tak nerušeně získává informace o napadené infrastruktuře tak, aby maximalizoval následný dopad útoku. Cílem pastí v těsné integraci s dalšími systémy je útočníka v reálném čase zastavit.

10:40 – 11:10 Přestávka

Sekce praktických příkladů a řešení v oblasti kybernetické bezpečnosti

11:10 – 11:40 **Bezpečnost tzv. legacy aplikací**

Pavel MINAŘÍK, Chief Technology Officer, Kemp Technologies (Flowmon Networks)

Řada organizací dosud provozuje tzv. legacy aplikace, na kterých často fungování a poskytované služby dané organizace závisí. Tyto aplikace je obtížné zabezpečit v souladu s aktuálně platnými standardy a jejich modernizace je zdlouhavý a nákladný proces. Mezi obvyklé problémy patří nevyhovující šifrování, zranitelnosti na úrovni webového/aplikačního serveru i aplikace samotné nebo způsob přihlašování bez možnosti ověření uživatele vůči systému správy identit. Přesto tyto aplikace je nutné udržet v chodu a zároveň minimalizovat rizika a eliminovat možné vektory útoku. Na modelové příkladu legacy aplikace, ukážeme prostřednictvím technologie Kemp LoadMaster, jak takovou aplikaci zpřístupnit uživatelům bezpečným způsobem (adekvátní úroveň šifrování), eliminovat dopad potenciálních zranitelností aplikace prostřednictvím webového aplikačního firewallu a zajistit další úroveň ochrany prostřednictvím autentizace uživatelů ještě před tím, než mohou s aplikací interagovat.

11:40 – 12:00 **Na cestě ke kvalifikovaným systémům**

Vít CVRČEK, GORDIC spol. s r.o.

Příspěvek shrnuje trendy v legislativní úpravě digitálního světa a zamýšlí se nad tím, zda jsou stávající možnosti digitalizace procesů dostatečné.

12:00 – 12:30 **PKI a multi-faktorová autentizace pro ochranu organizací**

Zástupce ProID/Monet+

Základním kamenem kyberbezpečnosti organizace je ochrana infrastruktury a identity jednotlivých prvků. Tyto problémy řeší technologie Public Key Infrastructure, založená na moderní kryptografii a doplněná o nástavbové moduly pro řízení digitálních certifikátů. Dalším bodem je zajištění digitální identity zaměstnanců. Tím se myslí

především bezpečné, multifaktorové přihlášení do počítačů, systémů a cloudů se silným šifrováním. Toto řešení bylo implementováno uvnitř největších českých úřadů či bank, kde jim pomáhá chránit jejich kyberprostor.

12:30 – 13:15 *Přestávka*

Sekce zkušenosti z krizového stavu

13:15 – 14:00 **Aktuální stav regulace kybernetické bezpečnosti v České republice**

Martin KLUMPAR, vedoucí oddělení regulace cloud computingu, NÚKIB ČR

Cloudová vyhláška, Minimální bezpečnostní standard a další novinky z oblasti kybernetické bezpečnosti.

14:00 – 14:20 **OSINT v analýze dezinformací**

Jindřich KARÁSEK, Trend Micro

Budou vysvětleny některé techniky OSINT, které využívají například investigativní novináři, hackeři a další analytici, kteří se snaží být informačně o krok napřed. Bude prezentováno, jak se tyto techniky dají využít při studiu aktivit dezinformátorů. To se týká zejména webových stránek, sociálních sítí a operativních aktivit. Bude představen projekt „EOLAS“, jakož i několik návrhů k zamyšlení a diskusi, například jak by mohla spolupracovat státní a soukromá sféra v bezpečnostní oblasti.

14:20 – 14:40 **Jak zvládat volumetrické útoky**

Petr KADLEC, ComSource

Strategie obrany před volumetrickými útoky a aktuální informace o jejich vývoji v ČR. Shrnutí vlastních poznatků a zkušeností z provozu antiDDoS služby FlowGuard.

14:40 – 15:00 **Analýza útoku na kritickou infrastrukturu**

Michal DROZD, Cyber Security Architect, spoluzakladatel GREYCORTEX

Jakým způsobem chráníte kritickou infrastrukturu ve vaší firmě?

V přednášce se budeme prakticky věnovat analýze reálného útoku na kritickou infrastrukturu. Cílem bude ukázat, jak lze jednoduše začít s bezpečnostním dohledem nejen v průmyslové řídicí síti, co může ohrozit vaši síť a proč byste měli uvažovat o bezpečnostním monitoringu, i když jste přesvědčeni, že se ve vaší síti nic neděje.

15:00 – 15:20 *Přestávka*

15:20 – 15:40 **DNS v rukou útočníka. Reálné příklady použití tohoto protokolu v útoku**

Jan RYNEŠ, Solutions Architect CEE, INFOBLOX

Drtivá většina destinací na internetu jsou definovaná jménem (FQDN). Pro počítačové systémy však potřebujeme IP adresu. Proto existuje služba DNS, na kterou spoléháme. Co to pro nás znamená? Jakýkoliv mail, jakákoliv webová stránka a obsah na ní. Drtivá většina moderních aplikací. Dříve než začne komunikace, musíme zjistit správnou adresu. Toto však platí i pro malware, ransomware, phishing útoky anebo sofistikovanější útoky, které známe pod zkratkou APT. Pojďme se podívat na způsob, jak útočníci zneužívají právě službu DNS. Jedině tak budeme vědět, jak tuto kritickou část moderních technologií bránit.

15:40 – 15:55 **Bezpečnostní doporučení pro e-identitu**

Petra ŠNOBLOVÁ, NAKIT s.p.

S rozvojem služeb eGovernmentu a narůstající potřebou využívání elektronických služeb v běžném životě je stále častěji využívána elektronická identita. Odborníci na systémy eGovernmentu z Ministerstva vnitra, kybernetickou a informační bezpečnost z NAKIT a odborníci z pracovní skupiny kybernetické bezpečnosti České pobočky AFCEA, proto společně vydali dokument s názvem Doporučení pro bezpečné nakládání s e-identitou, který má veřejnost informovat, pomoct zorientovat se v právním vymezení a zákonném ukotvení tohoto pojmu a upozornit na bezpečnostní rizika.

15:55 – 16:15 **Vyškolení zaměstnanci jako součást kybernetické ochrany organizace**

Božetěch BRABLC, DATASENSE

Při počtu útoku zaměřených na uživatele (hackeři takto cílí více než 90 % svých aktivit) jsou právě vyškolení zaměstnanci rozhodujícím ochranným faktorem vaší organizace. I když máte nasazené technologie, které detekují a blokují škodlivý obsah, snížit pravděpodobnost úspěšných útoku, jako je phishing nebo ohrožení obchodních e-mailu, můžete ještě o něco více prostřednictvím komplexního cíleného školicího programu zaměřeného na zvyšování povědomí o bezpečnosti. Díky Proofpoint Security Awareness Trainning posílíte u vašich zaměstnanců schopnost identifikace kybernetických útoku a ochráníte tak vaši organizaci.

16:15 – 16:35 **Budování dostupné kybernetické bezpečnosti**

Petr TODOROV, Novicom, s.r.o.

Představení cesty vedoucí k funkční a nákladově dostupné kybernetické bezpečnosti, která se opírá o sdílený bezpečnostní dohled postavený na principu aktivního SOCu. Dozvíte se, jak Novicom nástroje podporují koncept Aktivního SOCu a jaké jsou praktické zkušenosti s jejich nasazováním ve veřejném sektoru i v privátní sféře.

16:35 **Závěrečné slovo**

Tomáš MÜLLER, Prezident, České pobočky AFCEA

16:40 ***Neformální diskuse - číše vína***

17:30 **Ukončení akce**

Hlavní partneři akce

Partneři akce