Pracovní skupina kybernetické bezpečnosti české pobočky AFCEA
Policejní akademie ČR v Praze

Bezpečnostní dohledová centra (SOC)

- ***Význam dohledových center***
- ***Budování dohledových center***
- ***Technologie pro dohledová centra***
- ***Personál a vzdělávání personálu dohledových center***
- ***Budoucnost dohledových center***

3. listopadu 2022, 9:30 – 12:00

Policejní akademie ČR v Praze

09:30 **Přivítání**

Petr JIRÁSEK, Předseda Pracovní skupiny kybernetické bezpečnosti

Úvodní sekce

09:35 – 10:10 **Úvodní slovo – 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.

10:10 – 10:40 **Budování PKI infrastruktury a certifikačních autorit**

David ŘÍHOŠEK, vedoucí implementačního týmu, ProID/Monet+

PKI (Public Key Infrastructure) je základním pilířem digitální důvěry uvnitř organizace. V rámci PKI získá každý uživatel či zařízení elektronickou obdobu své identity, která umožňuje jednoznačnou autentizaci s ověřením jejich původu a integrity. V přednášce vám představíme naše zkušenosti z výstavba těchto PKI systémů a nejčastější chyby, na které uvnitř organizací narážíme.

10:40 – 11:10 **Bezpečnost aplikací jako klíčová prerekvizita úspěšného SOC**

Matěj SYCHRA, CORPUS Solutions, a.s.

Největší zranitelnosti pochází ze zakázkově budovaných aplikací; Mnoho skrytých zranitelností takovýchto aplikací nelze odhalit pouze penetračními testy; Zanedbání principů bezpečnosti ve vývoji aplikací má dopady do účinnosti jejich bezpečnostního dohledu; Jak tento stav systémově změnit?

11:10 – 11:25 *Přestávka*

11:25 – 11:55 **Prevence je ideální, ale detekce je nezbytná: modelování hrozeb pro oblast security operations**

Jan KOPŘIVA, Team Leader Incident Response, ALEF NULA

Cílem existence „modrých týmů" je poskytnout organizacím co možná nejvyšší míru ochrany před kybernetickými hrozbami a schopnost detekovat případné kybernetické útoky a další incidenty, kterým nedokáží bezpečnostní opatření zabránit. Často však security operations týmy při plnění tohoto úkolu vychází spíše z „out-of-the-box" technických schopností implementovaných bezpečnostních nástrojů, než z bezpečnostních potřeb a specifického profilu chráněné organizace. To může v některých případech vést ke vzniku „slepých míst", která není organizace schopná korektně monitorovat, přestože jsou pro ni vysoce relevantní, a tedy k neschopnosti detekovat vybrané typy škodlivých aktivit. Nejen na to, jak přenést organizační bezpečnostní požadavky do oblasti bezpečnostního monitoringu a zajistit tak, že všechny relevantní oblasti jsou jím pokryty, se podíváme v této prezentaci.

11:55 – 12:30 **Centrum kybernetických operací MF a státního cloudu - next gen SOC**

Ondřej NEKOVÁŘ, CISO, CDO & Jan POHL, Threat Hunter, SPCSS

Historický vývoj struktury SOC nám jasně ukazuje primární zaměření na reaktivní elementy. Tato doba je již dávno za námi. S rostoucí úrovní útoků a vyspělostí útočníků bylo nezbytné pro nás tento stav revidovat.

Next gen SOC SPCSS (Centrum kybernetických operací) je řízen na principu custom threat based loop SPCSS. Tradiční reaktivní přístup je posunut pro-aktivním směrem dle doporučení Active Cyber Defense Gray Zone by DCG420, kdy řízení činností je založeno na CTI (Cyber threat intel, passive, active), detection engineering, adversary emulation a threat hunting. Jako nasazení opatření k blindspot jsou mimo jiné využívány deception technologie. V rámci efektivního budování odolnosti (resiliency) prostředí jsou využívány orchestrační a automatizační nástroje (SOAR). Mezi další činnosti pak patří awareness a lessons learned.

Mezi dohledovaná prostředí patří privátní cloud MF (NDC), komerční cloudové služby MS Azure, Google Cloud a hybridní platforma MS AzureStack.

12:30 **Závěrečné slovo**

Petr JIRÁSEK, Předseda Pracovní skupiny kybernetické bezpečnosti

12:35 **Ukončení akce**

Hlavní partneři akce

ProID

ALEF

NAKIT

CORPUS SOLUTIONS CYBERSECURITY EXPERTS

SPCSS Státní pokladna Centrum sdílených služeb

FUTURE FORCES FORUM EVENT