NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Role SOC při ochraně KII

17.9.2019 Praha

Petr Slavík

Ochrana kritické infrastruktury v České republice

- Historické reminiscence
- Role státu a soukromého sektoru
- Role Security Operations Centra
- Zákon č. 181/2014 Sb. v současném znění v praxi
- Usnesení vlády ze dne 18. dubna 2018 č. 241

NAKIT

Role SOC ve státní správě

- Koncepce pracoviště, rozvoj a provoz Security Operation Centra
- SOC a provozní monitoring
- Faktory ovlivňující úspěch
- Zkušenosti z vlastního provozu a používaných nástrojů
- Budování kapacit a personální práce, role pracovníků SOC, správa bezpečnostních nástrojů
- Služby SOC

NAKIT

Zkušenosti s budováním SOC

Účel budování SOC

- Monitoring a detekce
- incident response
- analytická práce, poradenská činnost apod.

Funkční bloky jednotky

- Tým operátorů a analytiků pro standardní provoz
- Správa/rozvoj nástrojů
- Incident response tým
- Propojení na ostatní funkce IT bezpečnosti v organizaci (vzdělávací a osvětové programy, architektura, risk assessment, service desk)

Režim

- Faktory určující režim – počet lidí a počet hodin zajištění SOC

NAKIT

DCeGOV a bezpečnost KII

Co je to DCeGOV

- Dohledové centrum eGovernmentu a jeho působnost v rámci rezortu Ministerstva vnitra ČR

SOC a provozní monitoring aneb provozní versus bezpečnostní monitoring

- Koncentrace na „čistou“ bezpečnost vs. pokrývání části provozních aktivit
- Co různá prostředí DEV/TEST/PROD
- Fungování SOC v cloudu

Incident management

- Role Manažera kybernetické bezpečnosti
- Role Architekta kybernetické bezpečnosti

NAKIT

Faktory ovlivňující úspěch SOC

Zdroje a podpora managementu

- Chránit a podporovat misi SOC
- Finance

Kultura organizace

- Jeden z klíčových faktorů
- Spolurozhoduje o rychlosti implementace a výsledcích práce

Umístění v rámci organizace

- V rámci IT bezpečnosti (pod CISO)
- Ve struktuře IT
- Mimo IT

Oprávnění/mandát v režimu řešení závažných incidentů

- Primárně pro incident response
- Začlenění do krizového řízení v společnosti

NAKIT

Personální zabezpečení SOC

Rozvoj personálních zdrojů SOCu

- Lze zajistit kvalitní personál (L1/L2/L3) ?
- Identifikace lidského potenciálu a práce s ním
- Najímání zkušených L2/L3 mimo společnost vs. povyšování v rámci týmu

Zapojení HR do osobnostního rozvoje

- „výzvy“ ($) v oblasti specifických technických školení
- Soft skills pro analytiky na vyšších úrovních
- Rotace v rámci funkcí SOC i lokací kde SOC operuje (v případě více regionů)

Komunikace a kooperace mimo SOC

- Zaměření na budování sítě kontaktů mimo SOC – kritické primárně pro incident response
- Budování reputace SOC v rámci (IT) organizace – od generátoru incidentů k „partnerství“
- Spolupráce s NUKIB a CSIRTs (Computer Security Incident Response Team)

NAKIT

Potenciál nástrojů pro SOC

V rámci monitoringu jsou primárně používány

- SIEM systémy
- Nástroje pro řízení bezpečnostních incidentů (v rámci ITSM, či samostatně)
- Specializované prostředky pro vyšetřování (EDR/MDR – antivirus, threat intel, machine learning, sand box)

Maximalizace potenciálu vs. rozšíření počtu nástrojů

- Ladění stávajícího řešení vs. implementace dalšího produktu
- Výzva pro vedení – nutná schopnost „prodat“ technickou analýzu
- Komu patří management FW, IDS, Vulnerability scany apod.?
- Je to skutečně jen o nástrojích ?
- Security by default, Security by design…

O jakých datech to je?

	• Měsíc 1	• Měsíc 2	• Měsíc 3
SIEM alerty (Triage)	5020	3 985	6 078
Bezpečnostní incident	1	2	1
Bezpečnostní událost	49	28	37
Analytická činnost	42	98	151
Optimalizace a správa bezpečnostních nástrojů	57	68	67

NAKIT

Služby SOC DCeGOV

Primární zákazník MV ČR

- SOC pro eGovernment
- Potenciál služeb pro státní a veřejnou správu

Možnosti spolupráce

- Vzdělávání, výměna zkušeností
- Komunikace v rámci CSIRT/CERT komunity
- Možnost nabízet služby SOC dalším subjektům

NAKIT

Děkuji

Q&A

Petr Slavík
Vedoucí odboru Informační bezpečnosti a BCM

E: petr.slavik@nakit.cz
M: +420 731 553 223
W: www.nakit.cz

NÁRODNÍ AGENTURA PRO KOMUNIKAČNÍ A INFORMAČNÍ TECHNOLOGIE, S. P.