

Kybernetická bezpečnosť na MPSVR SR



MINISTERSTVO

PRÁCE, SOCIÁLNYCH
VECÍ A RODINY
SLOVENSKEJ REPUBLIKY



Ked' sa hacker
zobudí skôr
ako admin

Predstavte si, že je pondelok ráno. Vy si dávate svoju prvú kávu... zatiaľ čo niekto iný si práve dáva vašu databázu.

Ciele projektu SOC na MPSVR SR

Zabezpečiť kybernetickú
bezpečnosť organizácií v
pôsobnosti MPSVR SR

Znížiť resp. predíť nákladom
na riešenie incidentov
prostredníctvom prevencie

Zaviest' procesy, ktoré doteraz
neexistovali alebo boli len
čiastočne implementované

Riadiaci rámec SOC

SOC ako súhra technológií, procesov
a ľudských zdrojov



Interakcia so zainteresovanými
stranami



Riadenie na základe aktuálnych
hrozieb a legislatívnych požiadaviek

SOC Governance Framework

SECURITY OPERATION CENTER GOVERNANCE FRAMEWORK

Stratégia & Riadenie

Organizácia

Hlavné procesy

Zber dát

Analýza a
triedenie

Riešenie
incidentov

Správa hrozieb

Podporné procesy

Správa bezpečnostných
nástrojov

Riadenie rizík

Forenzná analýza

Bezpečnostné
povedomie a školenia

Procesné interfejsy

Riadenie zmien

Prevádzka IT

Riadenie ľudských
zdrojov

Legislatíva a štandardy

Riadenie externej
komunikácie

Verejné obstarávanie

Riadenie tretích strán

Technológia

SIEM

SOAR (Automatizácia)

MISP

ZAINTERESOVANÉ OSOBY

Ministerstvo práce,
sociálnych vecí a rodiny
SR

Ústredie práce, sociálnych
vecí a rodiny

Inšpektoráty práce

Centrum pre
medzinárodnoprávnú
ochranu detí a mládeže

Inštitút pre výskum práce
a rodiny

CSIRT NBÚ- SK-CERT

CSIRT
(MIRRI)

Tretie strany (dodávateľia,
prevádzkovatelia IT
systémov)

Kľúčové funkcie SOC

Monitoring a detekcia: sledovanie prístupov, detekcia škodlivých aktivít

Incident management: riešenie bezpečnostných incidentov

Threat intelligence: analýza hrozieb a zdieľanie informácií

Riadenie rizík a zraniteľností: identifikácia slabín a ich mitigácia

Forenzná analýza a školenia: podpora vyšetrovania a zvyšovanie povedomia

Technologické a organizačné aspekty

Implementácia nástrojov ako SIEM, SOAR, EDR a MISP

SIEM – (Security Information and Event Management) centralizovaný nástroj na zber triedenie logov,

SOAR – (Security orchestration, automation and response) technológia, ktorá pomáha koordinovať, vykonávať a automatizovať úlohy medzi rôznymi ľuďmi a nástrojmi.

EDR – (Endpoint Detection and Response) technológia, ktorá nepretržite monitoruje koncové body a hľadá dôkazy o hrozbách a vykonáva automatické akcie na ich zmiernenie.

MISP – (Malware Information Sharing Platform) open-source platforma na ukladanie, správu a zdieľanie informácií o kybernetických hrozbách.

Organizačné začlenenie SOC v rámci rezortu

Zmluvné vzťahy s tretími stranami, CSIRT NBÚ a CSIRT MIRRI

Tím SOC – Ako budeme chrániť?

SOC operátori 24/7: zabezpečenie nepretržitej prevádzky

Špecialisti SOC nástrojov: zodpovední za konfiguráciu a správu SIEM, SOAR, EDR a ďalších technológií

Interné kapacity rozdelené podľa kompetencií v kombinácii s externými špecialistami

Záver a výzvy

SOC ako kľúčový prvok
kybernetickej odolnosti
MPSVR SR

Výzvy: personálne
kapacity, koordinácia,
kontinuálne
zlepšovanie