**Bezpečnostné, monitorovacie a certifikačné centrum**

**MODUL MDR**

**Služby riadenia kybernetických bezpečnostných incidentov**

Zákon o kybernetickej bezpečnosti riadi organizáciu a pôsobnosť jednotiek CSIRT. Akreditované jednotky CSIRT by mali na kybernetické bezpečnostné incidenty upozorňovať, detegovať ich, pomáhať pri ich riešení, riešiť ich, resp. ukladať povinnosť riešenia prevádzkovateľovi základnej služby.

Zákon o kybernetickej bezpečnosti zároveň ukladá prevádzkovateľovi základnej služby kybernetický bezpečnostný incident detegovať, riešiť, navrhovať opatrenia, hlásiť ho a zabezpečovať dôkazy alebo dôkazné prostriedky.

Detekcia (odhalenie) kybernetického bezpečnostného incidentu je spúšťacím a kľúčovým štartovacím bodom pri jeho riešení. Národný CSIRT momentálne nemá žiadne možnosti ani prostriedky na odhalenie negatívnych bezpečnostných udalostí v prostredí MV SR, ktoré by sa po prvotnom preskúmaní mohli kvalifikovať ako bezpečnostný incident.

Nasledujúce riešenie kybernetických incidentov v rámci procesu reakcie na incident (Incident Response Process) patrí medzi veľmi rýchle procesy (na rozdiel od iných procesov, ako napr. zmenový proces). Preto je prakticky nemožné, aby všetky fázy tohto procesu mohol riadiť alebo dokonca riešiť národný CSIRT. Národný CSIRT sa v súčasnej dobe sústreďuje skôr na prijímanie a zasielanie včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. V takom prípade sa jedná skôr o preventívnu bezpečnosť.

Aby MV SR mohlo účinne a v reálnom čase detegovať a riešiť kybernetické bezpečnostné incidenty, musí mať schopnosť svoje incidenty riešiť bez závislosti na okamžitých možnostiach a schopnostiach vládnej alebo národnej jednotky CSIRT.

***Pracovisko SOC (Security Operations Center)***

Detekčné a reakčné schopnosti v rámci procesu riadenia kybernetických bezpečnostných incidentov sú založené na troch pilieroch:

- Technológie (nástroje),

- Proces reakcie na incidenty (proces Incident Response),

- Ľudia v procese IR.

Detekčné a reakčné technológie sú základom činnosti SOC. Umožňujú získavať informácie o momentálnom dianí v rozsiahlom spektre prevádzkových a bezpečnostných technológií na základe princípu zberu udalostí (logov) a princípu monitorovania sieťovej komunikácie. Ďalšie vstupné informácie poskytuje analýza hrozieb a jej nástroje.

**SIEM**

Centrálnou časťou získavania a zberu udalostí je technológia SIEM (Security information and event management), ktorá centrálne zbiera bezpečnostne relevantné udalosti z najrôznejších zdrojov (agregácia), normalizuje dáta do jednotnej štruktúry (normalizácia), ukladá ich, hľadá spoločné bezpečnostné atribúty a spája udalosti do logických celkov (korelácia) a upozorňuje na také zoskupenia informácií v udalostiach, ktoré môžu znamenať negatívnu bezpečnostnú udalosť a z ktorých môže vzniknúť bezpečnostný incident. Pri vzniku incidentu je pomocou SIEM možné v rámci vyšetrovania incidentu získavať ďalšie informácie o udalostiach, ktoré predchádzali incidentu alebo ho sprevádzajú, pomocou vyhľadávania a logickej korelácie udalostí z relevantných zdrojov. Technológia SIEM je taktiež veľmi užitočná pri forenznej analýze.

V datacentre MV SR bol integrovaný systém SIEM od spoločnosti McAfee, ktorý monitoruje a vyhodnocuje bezpečnostné udalosti serverov, sieťovej infraštruktúry, aplikácií a databáz. Predstavuje hlavný komponent pri riešení celkovej bezpečnosti z pohľadu monitorovania a riešenia bezpečnostných incidentov. V prípade ak v budúcnosti bude integrované ďalšie riešenie SIEM od iného dodávateľa existujúci SIEM sa využije ako hlavný zdroj informácii a dát, ktorý bude bezpečnostné udalosti z infraštruktúry datacentra preposielať na nové riešenie. Nové riešenie SIEM systému od iného dodávateľa sa môže použiť na integráciu a monitorovanie koncových používateľských staníc.

*Nástroje SIEM*

Admin (Administration)

Nástroj, ktorý slúži na správu jednotlivých komponentov a súčastí riešenia (nielen SIEM). Je možné spravovať používateľov, konfiguráciu komponentov, licencie, pravidlá spracovania udalostí, aktív, používaných sietí a samozrejme aj spravovať ďalšie časti riešenia.

Dashboard

Tento nástroj slúži na poskytnutie prvého pohľadu pre analytika pri prihlásení do SIEM prostredia. Zobrazenia je možné upravovať podľa potrieb konkrétneho analytika. K dispozícii sú takisto preddefinované dashboard-y, z ktorých si môže analytik vybrať.

Offense

Tento nástroj poskytuje najdôležitejšie vstupy pre riešenie hrozieb a incidentov. Jeho súčasťou sú tzv. pravidlá (Rules), ktoré na základe kritérií identifikujú podozrivé udalosti. Nástroj zabezpečí generovanie alertov o incidentoch, zároveň poskytuje pohľad na konkrétne detaily identifikovaných hrozieb a incidentov. Súčasťou je aj možnosť použitia rôznych doplnkových nástrojov v procese analýzy.

Log Activity

Tento nástroj slúži na zobrazenie udalostí, ktoré SIEM systém prijal prostredníctvom komponentov Event Collector. Zobrazenie je možné obmedziť podľa definovaných podmienok tak, aby vo výstupe boli len požadované udalosti. Súčasťou nástroja sú aj možnosti zobrazenia v rôznej interpretácii (tabuľky, grafy a pod.). Zároveň slúži na vytvorenie „search“, ktoré sa využijú pri iných nástrojoch (napr. Report). Požiadavky na konkrétne udalosti a aj formát výstupu je možné definovať veľmi detailne prostredníctvom jazyka ADL. Súčasťou vybraného formátu môže byť aj tvorenie kumulovaných dát, pre konkrétne kritériá.

Report

Tento nástroj slúži na generovanie výstupov (reportov) na účely prezentácie a ich poskytovania mimo prostredia SIEM. Report môže obsahovať niekoľko rôznorodých typov informácií (napr. rôzne vyhľadávanie z udalostí a/alebo tokov v požadovanom formáte, použitie kumulovaných dát).

**Nástroje pre analýzu sieťovej komunikácie**

Ako nástroj pre sledovanie sieťových dátových tokov a ich anomálií by mal byť používaný nástroj so základnými komponentami:

- Sonda, určená na generovanie informácii o sieťovej prevádzke.

- Kolektor, určený na spracovanie a ukladanie prijatých informácii.

- Anomaly Detection System (ADS, určený na automatizovanú analýzu sieťovej prevádzky, analýzu bezpečnostných hrozieb a identifikáciu problémov.

sonda

Sonda obsahuje softvér, ktorého úlohou je spracúvanie sieťových informácií a tvorba záznamov. Prijaté informácie sú následne zasielané pomocou protokolov TCP alebo UDP smerom na kolektor. Vzájomná komunikácia prebieha medzi sondou a kolektorom, ktorých môže byť v rámci infraštruktúry zapojených niekoľko. Z dôvodu ochrany voči  prípadnému zahlteniu sondy sú vytvorené záznamy, ktoré sú na sonde uchovávané len do doby ukončenia spojenia.

kolektor

Zariadenie určené pre zobrazovanie, dlhodobé ukladanie a analýzu sieťovej prevádzky s podporou rôznych formátov (napr. zasielané zariadeniami ako prepínače, smerovače a taktiež sieťové sondy). Kolektor je možné implementovať ako samostatné fyzické zariadenie, alebo v rámci virtuálneho prostredia.

ADS (Anomaly Detection System)

ADS je rozširujúci nástroj kolektora a sondy. Pomocou technológie detekcie anomálií a analýzy správania v sieti poskytuje funkcionalitu pre odhaľovanie prevádzkových problémov a taktiež ako obrana pred kybernetickými hrozbami. Uvedená funkcionalita umožňuje identifikovať hrozby, ktoré prekonali perimetrový firewall, boli zanesené do vnútra počítačovej siete respektíve vnikli iným spôsobom. Funkcionalita zároveň poskytuje možnosti identifikácie hrozieb, pre ktoré doposiaľ neexistuje signatúra.

Hlavné výhody ADS:

a) automatizované detegovanie bezpečnostných incidentov,

b) detegovanie anomálií v počítačovej sieti,

c) detegovanie konfiguračných problémov,

d) proaktívna identifikácia príčiny problémov.

Základom systému je databáza, voči ktorej sa vykonáva korelácia s behaviorálnou analýzou a to s použitím algoritmov pozostávajúcich z prvkov umelej inteligencie.

**Nástroj pre prevenciu úniku dát**

Data Loss Prevention (DLP) technológia deteguje a bráni náhodným, neúmyselným alebo cieleným únikom dát, ktoré sú firemne dôležité alebo spadajú pod reguláciu mnohých noriem a zákonov ohľadne bezpečnosti dát. DLP vykonáva kontrolu obsahu a analýzu kontextu, v ktorom sú chránené dáta práve použité (data in use), odosielané (data in motion), alebo uložené a archivované (data at rest). Jednotlivé komponenty systému DLP použité na chránených koncových staniciach (notebooky, servery), sieti zabezpečujú reakciu na detegovaný možný únik dát na základe definovaných politík a pravidiel s cieľom zabrániť a upozorniť na možný únik dát mimo povolené/autorizované kanály. DLP technológia po integrácii so SIEM poskytuje informácie o aktuálnom stave a potenciálnych udalostiach spojených s únikom dát priamo v prostredí SIEM.

**Nástroj pre riadenie prístupu privilegovaných účtov**

Privileged Access Management (PAM) Technológia bezpečne riadi účty s vyššími právami, ktoré sú schopné privilegovaného prístupu na kritické systémy. Tento prístup môže byť priradený administrátorom, zariadeniam, aplikáciám, rôznym typom servisných účtov, alebo účtom pre automatizované úlohy pre DevOps. Hlavným cieľom je uplatnenie „least privilege“ modelu, ktorý je definovaný ako obmedzenie prístupových práv na absolútne nevyhnutné minimum na vykonávanie bežných autorizovaných činností. PAM zabezpečuje podrobnú kontrolu, zabezpečenie, monitoring a auditovanie nad privilegovanými účtami a nad aktivitami vykonanými využitím týchto účtov. PAM poskytuje technológii SIEM dodatočné informácie, ktoré napomáhajú presnejšiemu vyhodnoteniu a identifikovaniu udalostí.

**Nástroje pre vyšetrovanie incidentu, riešenie a reakciu**

Toto riešenie umožňuje hlbokú viditeľnosť diania na sietiach i koncových bodoch, umožňuje podrobné vyšetrovanie a „hunting“ (sledovanie chovania útočníka) a zastavovanie postupu kybernetických incidentov. Integruje rôzne horizontálne, vertikálne, hĺbkové i historické pohľady v reálnom čase a zároveň navrhuje konkrétne závery a riešenia vrátame prioritizácie činností.

*Základné funkčné časti*

– detekcia a prevencia na sieti

– ochrana koncových bodov

– inteligentné pasce (honeypots) – proaktívna detekcia

***Vlastnosti procesu Incident Response***

Proces riadenia kybernetických bezpečnostných incidentov (ďalej len proces IR) je typický cyklický proces, ktorý má definované ciele, vstupy, fáze, činnosti, nástroje, eskalácie, role a výstupy.

Vrcholovým cieľom procesu IR je pokrytie bezpečnostných rizík, ktoré neboli pokryté preventívnymi činnosťami a opatreniami, vyplývajúcimi z procesu riadenia bezpečnosti (ISMS), akceptovanými a neznámymi rizikami (pozri časť „Služby preventívnej a forenznej bezpečnosti“). Celý proces IR bude podrobne vytvorený na základe predpisových základní, ktoré určia parametre celého procesu, a to hlavne:

- režim práce

- presné činnosti, postupy a núdzové postupy

- prístupové práva k jednotlivým prvkom a nástrojom

- povinnosti/zodpovednosti/SLA

- spôsob schvaľovania a koordinácie a hlásení

- zachádzanie s informáciami

- potrebné vzdelanie, profil, znalosti a spôsobilosti členov týmu

- taktika reakcie rozpracovaná v postupoch pre zvládanie incidentov

***IR tím a jeho práca***

V procese IR musia byť všetky role definované, musí byť popísaná ich náplň činnosti a zodpovednosť a tieto role musia byť obsadené ľuďmi v potrebnom počte tak, aby bolo možné pokryť nielen bežný režim, ale aj prípadný režim v kritickej situácii.

Pre prevádzku procesu IR sú potrebné všeobecné i špecializované technické bezpečnostné nástroje. Tieto prostriedky by mali byť do vysokej miery nezávislé až autonómne, aby bola zaručená možnosť riešiť incidenty aj v prípade výpadku bežnej výpočtovej, úložnej a komunikačnej infraštruktúry organizácie. To sa tiež týka systému záloh, ktorý by mal byť čo najmenej prepojený s ostatnou prevádzkovou infraštruktúrou.

IR tím sa špecializuje predovšetkým na:

- detekciu incidentov

- analýzu a vypracovanie návrhov na prvotné protiopatrenia (odozva/ohraničenie/zastavenie incidentu)

- implementáciu a overovanie účinnosti protiopatrení

Na takúto činnosť je potrebné mať nevyhnutné opatrenia pre prístupy (typu read/write) k väčšine bezpečnostných technológií. V procese IR sú v definovaných prípadoch tiež potrebné zvýšené rozhodovacie práva kvôli nemožnosti bežnej komunikácie/eskalácie z časových a iných dôvodov.

Pre takúto činnosť nie je možné využívať pracovníkov týmu preventívnej bezpečnosti, ktorí nepracujú v rýchlom "online" režime procesu IR. Táto činnosť sa preto koncentruje na pracovníkov tímu IR. Spolupráca s pracovníkmi preventívnej bezpečnosti je však naďalej nevyhnutná, pretože môžu pomáhať pri vyšetrovaní incidentov a vždy pomáhajú pri implementácii definitívnych opatrení.

***Nástroje procesu IR***

*Detekčné nástroje*

Hlavnými detekčnými nástrojmi je SIEM a monitorovanie sietí a infraštruktúry

*Komunikačné nástroje*

- nástroje pre vzdialené pripojenie (aj out-of-band)

- IP/mobilná telefónia

- mailová/chatová komunikácia

- iné nástroje strategickej a krízovej komunikácie

*Procesné nástroje*

- DMS pre dokumenty a dokumentáciu

- nástroj pre prevádzku knowledge base

- nástroj pre Incident Response Management

*Nástroje pre lokálnu obnovu BMCC*

- fungujúci systém záloh  
- nástroje pre automatizovanú inštaláciu/deployment

*Lokálne laboratórium*

- R&D, testovanie

- overovanie účinnosti protiopatrení

- nástroje pre analýzu malware

- nástroje pre kryptoanalýzu

- forenzné nástroje a úložisko pre dôkazný materiál, image diskov, dumpy pamäti

- nástroje pre packet capturing (kompletný záchyt sieťovej prevádzky)

*Podporné nástroje*

- kamerové systémy pre fyzický dohľad

- monitorovanie fyzickej bezpečnosti (prístupové systémy)

- fyzické úložisko dôležitých papierových dokumentov