Odporúčaný základný rámec architektúry navrhovaného riešenia - budúci stav

Za účelom zvýšenia úrovne zavedených postupov a opatrení týkajúcich sa kybernetickej a informačnej bezpečnosti (KIB) v subjektoch verejnej správy je potreba vybudovať novú, resp. konsolidovať existujúcu bezpečnostnú architektúru. Toto je možné dosiahnuť implementáciou nových, alebo inováciou existujúcich bezpečnostných nástrojov a procesov, a to najmä v nasledovných oblastiach:

- ochrana pred útokmi z externého prostredia,
- detekcia škodlivých aktivít a bezpečnostných incidentov,
- ochrana dát, dátových prenosov a komunikácie,
- budovanie bezpečnostného povedomia.

Biznis architektúra

Služby a funkcie uvedené v biznis architektúre budúceho stavu predstavujú základný rámec („baseline“), ktorý by mal byť implementovaný projektom. Aktuálny stav implementácie bezpečnostných služieb a funkcií na úrovni žiadateľov môže byť rôzny, preto každý žiadateľ môže žiadať o rôznu podporu v rámci tohto definovaného rámca.

Budúce riešenie základného rámca zabezpečenia informačnej a kybernetickej bezpečnosti žiadateľov na úrovni biznis architektúry by malo pozostávať najmä z nasledovných biznis funkcií:

- Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov:
    - Bezpečnostný monitoring, pozostávajúci z nasledovných procesov:
        - monitoring IS, platforiem, aplikácií a používateľských činností a aktivít,
        - monitoring sietí,
        - monitoring činností a aktivít privilegovaných používateľov,
    - Analýza založená na big-data a machine learning algoritmoch,
- Riadenie bezpečnostných incidentov, pozostávajúce z nasledovných procesov:
    - identifikácia a hlásenie bezpečnostných incidentov,
    - registrácia, kategorizácia a klasifikácia bezpečnostných incidentov,
    - akceptácia bezpečnostných incidentov a určenie riešiteľov,
    - analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov,
    - riešenie bezpečnostných incidentov a obnova prevádzky,
    - uzatvorenie bezpečnostných incidentov,
    - vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu.
- Ochrana dát, dátových prenosov a komunikácie:
    - bezpečnosť virtualizovaných prostredí,
    - ochrana dát na úrovni databáz a dátových úložísk (šifrovanie dát),

  - ochrana dát na úrovni koncových zariadení (EPP - šifrovanie dát pri každom ich prenose alebo uchovávaní v lokálnom alebo centrálnom úložisku, kontrola a šifrovanie externých médií a pod.),
  - riadenie prístupov (implementácia nástrojov IAM a remote access manažmentu),
  - proces bezpečnej výmeny informácií prostredníctvom EWS s vládnou jednotkou CSIRT, prípadne inými bezpečnostnými dohľadovými centrami zapojenými do EWS a integráciou na JISKB,
  - riadenie SW záplat (Patch management), manažment zraniteľností.
- Zvýšenie ochrany pred útokmi z externého prostredia:
  - ochrana pred malware a ransomware,
  - manažment bezpečnosti sietí (nasadenie nových moderných sieťových prvkov /AFW, NGFW, a pod./),
  - manažment bezpečnostných konfigurácií (implementácia systému pre jednotnú správu a deployment bezpečnostných politík a bezpečnostných konfigurácií),
- Budovanie bezpečnostného povedomia a bezpečnostnej kultúry:
  - výcvik a tréning zamestnancov v oblasti kybernetickej a informačnej bezpečnosti a sociálneho inžinierstva,
  - zabezpečenie školení a kurzov pre zamestnancov zabezpečujúcich prevádzku dohľadového centra,
  - informovanie o najnovších trendoch v oblasti KIB.

Z uvedeného dôvodu si každý žiadateľ musí zrealizovať analýzu aktuálneho stavu informačnej a kybernetickej bezpečnosti a prijatých bezpečnostných opatrení vo svojej pôsobnosti a na základe výsledkov tejto analýzy zadefinovať, o akú podporu v rámci vyhlásenej výzvy bude mať záujem.

Primárne by však malo platiť, že budú uprednostňované žiadosti, ktoré sa budú týkať implementácie nasledovných bezpečnostných funkcií:

- kybernetická ochrana a monitorovanie bezpečnostných incidentov:
  - bezpečnostný monitoring a identifikácia bezpečnostných incidentov,
  - riadenie bezpečnostných incidentov,
- ochrana proti externým hrozbám,
- ochrana dát, dátových prenosov a komunikácie,
- zvyšovanie bezpečnostného povedomia,
- implementácia bezpečnostných opatrení na zabezpečenie súladu so zákonom,
- prípadne iné aktivity zvýšenia úrovne správy a riadenia informačnej a kybernetickej bezpečnosti žiadateľa v súlade s bezpečnostnou architektúrou.

Architektúra informačných systémov

Budúci stav informačných systémov jednotlivých žiadateľov bude rôzny v závislosti od predkladaného projektu a jeho cieľov. Preto sú uvedené len príklady aplikačného rámca, resp. bezpečnostných nástrojov pre jednotlivé oblasti, v ktorých môžu žiadatelia zaviesť, resp. inovovať informačné systémy:

- Zvýšenie ochrany pred útokmi z externého prostredia:

- Web Application Firewall (WAF),
- Perimetrový firewall (NGF - Firewall novej generácie),
- Perimetrové IDS/IPS,
- Bezpečné demilitarizované zóny (DMZ),
- Perimetrové anti-malware riešenie,
- Ochrana pred DDoS útokmi,
- Filtrovanie webovej komunikácie,
- Ostatné nástroje určené na ochranu sieťového perimetra,

- Zvýšenie schopnosti detekcie škodlivých aktivít a bezpečnostných incidentov:
  - SIEM (Security Incident and Event Management) a ostatné nástroje určené zber a monitorovanie bezpečnostne relevantných udalostí,
  - Sieťový firewall (NGF -Firewall novej generácie),
  - Nástroje IDS/IPS sieťové a pre koncové zariadenia,
  - Nástroje pre jednotné riadenie hrozieb (UTM – Unified Threat Management),
  - Network Access Control (NAC),
  - Nástroje pre identifikáciu APT útokov,
  - Nástroje pre behaviorálnu analýzu dátových tokov,
  - Nástroje pre bezpečnosť bezdrôtových sietí (Wireless Security),
  - Network Forensic riešenia,
  - Deception technology (napr. Honeypot a ďalšie nástrahové technológie),
  - Nástroje na ochranu databáz,
  - Nástroje na testovanie kódu (code review),
  - Nástroje na automatizované zisťovanie zraniteľností,
  - Nástroje na zaistenie bezpečnosti koncových zariadení (anti-malware, mikro-virtualizácia, behaviorálna analýza aktivít používateľov),
  - Nástroje pre zaistenie integrity dátových súborov,
  - Nástroje pre manažment konfigurácií, aktualizácií a software,
  - Nástroje pre riadenie privilegovaných prístupov,
  - Nástroje pre riadenia bezpečnostných incidentov, vrátane asset managementu (CMBD),
  - Ostatné nástroje pre detekciu škodlivých aktivít a bezpečnostných incidentov,
- Ochrana dát, dátových prenosov a komunikácie:
  - Nástroje pre riadenie prístupu k dátam,
  - Nástroje pre audit a ochranu dát,
  - Riešenia PKI,
  - Riešenia IAM – Identity and Access Management,
  - Nástroje pre DLP – Data Leak Prevention,
  - Nástroje na maskovanie, anonymizáciu dát (Data Masking),
  - Nástroje na šifrovanie dát, dátových prenosov, komunikácie, prostriedky šifrovej ochrany,
  - Nástroje na riadenie retencie dát (Data Retention),
  - Ostatné nástroje pre ochranu dát, dátových prenosov a komunikácie,
- Budovanie bezpečnostného povedomia:

- Nástroje pre zvyšovanie bezpečnostného povedomia (napr. e-learningové kurzy, edukačné videá, publicita a propagácia kybernetickej bezpečnosti)

Jednotlivé nástroje môžu spĺňať aj viacero z uvedených vlastností (napr. NGF Firewall s integrovaným sieťovým IDS/IPS a anti-malware nástrojom a pod.). Rovnako je možná implementácia viacerých bezpečnostných nástrojov so vzájomne sa podporujúcimi a doplňujúcimi vlastnosťami (nie však ich duplikácia).

Technologická architektúra

Predpokladá sa, že budúci stav technologickej architektúry jednotlivých žiadateľov bude rôzny v závislosti od predkladaného projektu a jeho cieľov. Preto sú nižšie uvedené len príklady technologických riešení, ktoré môžu žiadatelia zaviesť, resp. inovovať:

- šifrátory a kryptografické riešenia (v súlade s aktuálnymi normami),
- virtualizačný SW na koncových zariadeniach,
- špeciálny HW koncových zariadení,
- perimetrové sondy,
- virtuálne dátové úložisko,
- diskové pole s redundanciou,
- riešenie pre load balancing.

Minimálne požiadavky na zdroje logov, ktoré SOC musí po implementácii projektu zberať a vyhodnocovať:

Anti-virus/Anti-malware (Windows servers) - môže byť súčasťou XDR/EDR
Anti-virus/Anti-malware (Linux) - môže byť súčasťou XDR/EDR
Anti-virus/Anti-malware (Workstations) - môže byť súčasťou XDR/EDR
CMDB
Sieťová komunikácia (Netflow/NDR) - NDR kapabilitu môže obsahovať aj XDR
Web content filter / Proxy
Vzdialené pripojenie do siete & VPN
Windows Domain Controllers (Single sign-on (SSO) and identity access management)
XDR/EDR (laptops/workstations/servers)
Multi Factor Authentication (MFA)
UNIX/Linux OS logs (idealne pokryte XDR-EDR)
Skener zraniteľností

Vzhľadom na vysokú komplexitu projektov zameraných na budovanie bezpečnostných dohľadových centier v oblasti KIB sa očakáva, že projekty budú realizované nie len prostredníctvom aktivity Nákup HW a SW a služieb, ale aj ďalšími aktivitami (analýza a dizajn, implementácia, testovanie a nasadenie) v realizačnej fáze projektu podľa vyhlášky 85/2020 Z. z. o riadení projektov.