Popis východiskovej situácie

Mesto Senica poskytuje svoje služby pre viac ako 20 000 obyvateľov, pričom na zabezpečenie svojich povinností používa niekoľko informačných systémov.

Dôležitosť kybernetickej bezpečnosti je z tohto pohľadu vysoká, nakoľko dopad potencionálneho kybernetického incidentu na naše mesto by zasiahol veľké množstvo obyvateľov. Kľúčové identifikované informačné systémy, ktorých ohrozenie by malo významný vplyv na poskytovanie základnej služby, resp. by výskyt incidentu spôsobil vážny výpadok informačných systémov verejnej správy:

* isvs\_10862 Komplexný informačný systém mesta Senica,
* isvs\_10863 Informačný systém personalistiky a miezd mesta Senica

Podporné systémy:

* Virtual server
* ActiveDirectory
* Centrálna bezpečná tlač
* Backup
* Syslog
* NAS
* Firewall

Na základe výsledkov vykonanej analýzy súladu s dotknutou legislatívou bol stanovený zoznam kľúčových aktív, bola vykonaná klasifikácia informácií a kategorizácia sietí a informačných systémov, boli identifikované možné hrozby, ako aj pravdepodobnosť ich výskytu. V kontexte už prijatých opatrení vznikli odporúčania, ktoré opatrenia je potrebné zaviesť, resp. modifikovať už existujúce tak, aby bola zabezpečená ochrana aktív v zmysle platnej legislatívy.

Z prijatej bezpečnostnej politiky vyplynula teda potreba zavedenia mnohých opatrení, ktoré sa priebežne zavádzajú. Mnohé opatrenia už boli realizované, napríklad zavedenie prísnejších autentifikačných pravidiel, či zabezpečenie priestorov dodatočnými prostriedkami fyzickej ochrany; stanovenie prísnejších pravidiel pre prístup ku kamerovým záznamom, zavedenie povinnosti častejšej zmeny hesiel, segmentácie siete, šifrovanie záloh, fyzický presun záloh do inej zabezpečenej budovy(mestská polícia), aplikácia pravidiel na dané porty a aplikácie, nasadenie aplikačného firewallu IPS. tzv. Next Gen Firewall a pod. Taktiež sa štatutárny orgán zaviazal podporovať kontinuálny rozvoj kybernetickej a informačnej bezpečnosti, najmä s ohľadom na nové trendy, hrozby, či technológie.

Prijatá politika informačnej bezpečnosti je záväzná pre všetkých zamestnancov, vyžaduje ich účasť a podporu. Táto politika určuje rámec riadenia informačnej bezpečnosti tak, aby boli informačné aktíva dostatočne chránené pred hrozbami, ako sú prerušenie/zlyhanie služby, ohrozenie informácií a majetku (aktív), chyby, podvody, vydieranie, prírodné pohromy a pod., či už ide o hrozby interné alebo externé, neúmyselné alebo zámerné.

Dotknuté systémy:

* isvs\_10862 Komplexný informačný systém mesta Senica,
* isvs\_10863 Informačný systém personalistiky a miezd mesta Senica,
* isvs\_10864 Webový portál mesta Senica,
* isvs\_10865 Systém elektronickej pošty mesta Senica

Verejný obstarávateľ nakúpil nasledovné HW a SW prvky pre bezpečnosť IKT infraštruktúry:

1. LOGmanager-M od spoločnosti LOGmanager
2. 2 ks firewall Palo Alto Networks PA-450 od spoločnosti Palo Alto Networks
3. 130 antivírusových licencií Endpoint Security Complete od spoločnosti Symantec

Bude potrebné všetky tieto prvky implementovať v prostredí infraštruktúry verejného obstarávateľa.

### Implementácia centrálneho logovacieho systému od výrobcu LOGmanager, zariadenie LOGmanager – M:

* Zber požiadaviek, nastavenie a konfigurácia systému v IT prostredí obstarávateľa;
* Konfigurácia Windows a Linux systémov pre zasielanie logov do systému;
* Inštalácia Windows agentov
* Vypracovanie komunikačnej matice protokolov, ktoré používa systém LOGmanager.
* Overenie funkčných a výkonových parametrov Windows agentov;
* Predvedenie vytvorenia a uloženia vlastných dashboardov a reportov;
* Predvedenie nastavenia značkovania udalostí a vytvárania upozornení s limitom alebo koreláciou;
* Nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom;
* Konfigurácia správneho parsovania logov zo všetkých systémov
* Zaškolenie obsluhy a správy systému pre roly administrátor, supervízor, operátor.
* Vypracovanie inštalačnej a prevádzkovej dokumentácie

**Rozsah: 20 MD**

### Implementácia Firewallu 2x Palo Alto Networks PA-450

* Analýza aktuálneho riešenia
* Fyzické osadenie HW a upgrade firmvérov;
* Konfigurácia vysokej dostupnosti (High Availability – HA) do režimu active-passive;
* Migrácia pravidiel z aktuálneho riešenia a ich revízia;
* Konfigurácia a migrácia FW pravidiel z „port-based“ na „application-based“;
* Nasadenie security profilov na FW pravidlá.
* Konfigurácia SSL dekrypcie
* Integrácia FW s Active Directory cez protkol kerberos over HTTP
* Konfigurácia dual ISP zapojenia
* Konfigurácia aktuálneho riešenia dvojfaktorovej autentifikácie OKTA s GlobalProtect VPN cez SAML protokol.
* Vytvorenie best-practices analýzy firewallu a jeho konfigurácie. Prezentácia analýzy objednávateľovi, vypracovanie plánu zmien a nasadenie zmien vyplývajúcich z tejto analýzy.
* Zaškolenie v prípade nových funkcií.
* Konfigurácia Palo Alto Networks Panorama VM do infraštrukúry.
* Integrácia FW s Panorama VM.
* Migrácia FW pravidiel do Panorama.
* Konfigurácia DLP add-onu.
* Analýza dokumentov a ich umiestnení v prostredí.
* Definovanie DLP politík
* Definovanie detekčných patternov a implementovanie patternov do firewallu.
* Testovanie DLP detekcie v monitoring móde, identifikácia false-positive/false-negative detekcií.
* Nasadenie OCR detekcie
* Nasadenie DLP do produkčného režimu.
* Nadenie AIOps free riešenia s FW.
* Odsegmentovanie PROD a TEST prostredí. Vyrobenie nových VLAN a konfigurácia detailných application-based FW pravidiel a security profilov.
* Osegmentovanie zálohovacieho riešenia od produkčných serverov. Vypracovanie detailných application-based FW pravidiel potrebných pre zálohovanie.
* Základné zaškolenie.
* Vypracovanie inštalačnej a prevádzkovej dokumentácie

**Rozsah: 35 MD**

### Implementácia Ochrany koncových staníc 130x Symantec Endpoint Security Complete

* Úplné nasadenie všetkých modulov ochrany koncových bodov, EDR a ochrany AD na všetky určené zariadenia a systémy;
* Migrácia pravidiel a politík zo stávajúceho riešenia ochrany koncových bodov;
* Nasadenie Antivírovej ochrany na koncové stanice a servery Windows a Linux.
* Nasadenie IPS ochrany na koncové stanice.
* Nasadenie Adaptive protection ochrany na koncové stanice do režimu block.
* Nasadenie exploit protection na koncové stanice.
* Nasadenie AD Threat protection na koncové stanice.
* Nasadenie Device control-blokovanie USB zariadení na koncových staniciach.
* Nasadenie EDR funkcionality. Zapnutie incident pravidiel a email notifikácií.
* Testovanie;
* Základné zaškolenie.
* Vypracovanie inštalačnej a prevádzkovej dokumentácie

**Rozsah: 20 MD**

### Pravidelné služby bezpečnostného analytika

* Zber údajov a udalostí – zber bezpečnostných a prevádzkových záznamov z rôznych zariadení nachádzajúcich sa v IT infraštruktúre organizácie.
* Normalizácia zozbieraných údajov – predspracovanie údajov za účelom zjednotenia rôznych formátov.
* Korelácia – posúdenie vzťahov medzi jednotlivými údajmi a udalosťami.
* Log management – uchovávanie log/auditných záznamov, ich komprimácia a indexácia.
* Monitoring používateľov a jednotlivých častí IT infraštruktúry – sledovanie neobvyklého správania sa používateľov a administrátorov, detekcia potenciálnych a reálnych bezpečnostných incidentov a neobvyklých aktivít voči pravidlám a/alebo minulému stavu.
* Audit a reporting – generovanie reportov o činnosti a bezpečnostnej kondícii IT infraštruktúry.
* bezpečnostné udalosti z firewallov, VPN, IDS, IPS a databáz,
* sieťové udalosti zo switchov, routerov, serverov a ďalších zariadení,
* sieťové aktivity a komunikáciu až na úrovni Layer 7,
* aktivity v cloude, Informácie zo SaaS a IaaS prostredia, ako sú Office365, SalesForce.com, Amazon Web Services (AWS), Azure a Google Cloud,
* dáta o používateľoch a aktívach, teda informácie zo systémov na riadenie prístupov a identít,
* informácie zo skenerov zraniteľností,
* udalosti koncových zariadení, ako je Windows event Log, Sysmon a podobne,
* aplikačné logy, či už ide o štandardné ERP, alebo vlastné aplikácie,
* informácie o hrozbách, ako je napríklad IBM X-Force®.
* Security Operations Center – SOC bude zaisťovať komplexnú centralizáciu riadenia bezpečnostných udalostí a incidentov, s cieľom minimalizovať reakčnú dobu na incident a škody z nej vyplývajúce.
* Pomocou SIEM budú konzultanti SOC nepretržite monitorovať bezpečnostné incidenty a budú zodpovední za reakciu, ak sa zistí.
* Detekcia - identifikuje sa, prípadne sa príjme, notifikácia o potenciálne škodlivom chovaní v chránenej infraštruktúre.
* Analýza - určí sa, či sa jedná o bezpečnostnú udalosť alebo o bezpečnostný incident, ktorý môže mať negatívny dopad na nami chránenú infraštruktúru – analýza.
* Investigácia - cieľom skúmania daného bezpečnostného incidentu bude zistiť konkrétne dopady a cestu, ktorou sa útočníkovi podarilo preniknúť do infraštruktúry.
* Reakcia - Okamžitou reakciou sa minimalizuje dopad bezpečnostných incidentov.
* Kontrola a zavedenie nápravných opatrení a reporting zistených skutočností na zvýšenie informovanosti – post incident aktivity.
* Vyhodnocovanie DLP incidentov a reportovanie High severity incidentov
* Aktualizácie bezpečnostnej dokumentácie

**Rozsah: 26 MD**

Špecialista pre bezpečnosť informačných systémov

* Pravidelné testy zraniteľností

**Rozsah: 66 MD**

Školiteľ pre IT systémy

**Rozsah: 8 MD**