**Technické specifikace**

1. Aktuální stav

ČOI je správcem a provozovatelem aplikací zahrnutých do Informačního systému ČOI. Aplikace Mercurius, pokrývající oblast kontrolní činnosti ČOI, byla podle vyhlášky č. 317/2014 Sb. určena jako významný IS. Personální, ekonomický IS a spisová služba jsou provozovány podle zákona č. 365/2000 Sb. jako veřejné IS. Kromě těchto aplikací jsou provozovány ještě SW řešení menšího, lokálního významu. Pro oblast ICT má ČOI zpracován „Katalog služeb“, dále je zpracována „Informační koncepce“, v oblasti ICT jsou plněny úkoly v rámci schválené „Strategie ČOI na roky 2017 – 2021“. Aplikace IS ČOI jsou provozovány v Datovém centru ve Štěpánské 15, Praha 2. K těmto centrálním aplikacím přistupují zaměstnanci ČOI v rámci provozované WAN, případně vzdáleným VPN připojením.

Centrální aplikace jsou provozovány v prostředí MS produktů (operační, databázové, kancelářské, poštovní) s výjimkou aplikace Mercurius, která pracuje s DB Firebird SQL v.3. Virtualizace serverů je řešena na platformě Hyper-V. Z bezpečnostního SW jsou provozovány antivirové produkty firmy Symantec, dále produkty Carbon Black a Varonis. Je provozována správa identit na bázi produktu MidPoint, dále FortiManager pro správu firewalu a ICINGA pro monitoring sítě a infrastruktury ČOI. Pro interní audit SW je provozován AuditPro.

Pro správu sítě z pohledu získání přehledu, řízení a bezpečnosti jsou k dispozici produkty Extreme Networks. Jedná se o licence:

1. NMS-ADV-50 s produkty Extreme Management Center, Extreme Analytics a Extreme Control. Tyto produkty podle svých vlastností a určení budou využity k řízení a analýze provozu WAN ČOI, dále k zabezpečení důvěrnosti, dostupnosti a integrity provozovaných dat, k řízení přístupu k síti apod,
2. PV-FPM-50K – s určením pro analýzu datových toků na WAN ČOI,
3. IGE-50 s určením pro vyhodnocování síťové konfigurace, které nejsou v souladu s nastavenými pravidly (např. s GDPR).

Z pohledu provozovaného HW se jedná zejména o zařízení, komponenty:

1. Dell Poweredge VRTX chasis,
2. DELL servery (standalone),
3. Quantum Scala i3-i6 tape library LTO-7,
4. IBM disková úložiště, servery, blade centrum, zálohovací knihovna – vše před ukončením provozu,
5. Fortigate firewall, Fortianalyzer,
6. Bezpečnostní sonda SSA 180,
7. Aruba Wi-Fi,
8. UPS APC od 1,5kVA do 7,5kVA,
9. Aktivní, síťové prvky Extreme Summit 4xx,
10. Pracovní stanice, notebooky DELL.

2. Požadavky na obsah

Požadavkem je zpracování studie proveditelnosti SOC ČOI (Security Operation Center). Jako vhodné se jeví doplnění psaného textu grafickými obrázky z důvodů lepšího pochopení předkládaného návrhu. Návrh řešení musí zohlednit současné SW a HW komponenty, které ČOI provozuje z důvodů ochrany vložených investic. Svým obsahem musí pokrýt požadavky vyhlášky č.82/2018 Sb., o kybernetické bezpečnosti, zejména paragrafy:

§22 – Zaznamenávání událostí informačního a komunikačního systému, jeho
 uživatelů a administrátorů,

§23 – Detekce kybernetických bezpečnostních událostí,

§24 – Sběr a vyhodnocování kybernetických bezpečnostních událostí.

Návrh řešení pokrývající požadavky §22 - §24 bude členěn do etap:

1. **Analýza současného stavu.** Zde zejména popsat vhodnost, nevhodnost, slabá, silná místa současných technologií z pohledu stanoveného cíle, což je vybudování SOC ČOI. Navrhnout způsob, rozsah, parametry zaznamenávání událostí u VIS Mercurius („co a jak logovat“).
2. **Integrace licencí Extreme Networks vůči stávajícím objektům v síti ČOI.** Zde navrhnout a popsat Integrační scénáře, pravidla vůči Fortigate, SSA 180, Extreme Summit 4xx, Varonis, Carbon Black. Navrhnout, co je nutno z pohledu dosažení stanoveného cíle doplnit (dokoupit) a proč. Definovat nutná související opatření (např. přechod na komunikační protokol 802.1X) s možnými dopady na uživatele IS ČOI.
3. **Integrace produktu Extreme Networks vůči možným budoucím řešením typu SIEM** (viz §24 vyhlášky o KB). Zde pojmenovat, včetně odůvodnění, možná vhodná technická řešení typu SIEM. Navrhnout možnost a pravidla filtrace událostí (logů) na úrovni Extreme Networks směrem k SIEM z důvodů snížení objemu sledovaných událostí.
4. **Návrh provozu SOC ČOI.** Požaduje se popsat návrh opatření z pohledu zabezpečení provozu SOC ČOI včetně vyhodnocení jejich efektivnosti a udržitelnosti. Popsat případná rizika (např. změny zákona a vyhlášky o KB), jejich eliminaci z  pohledu provozu navrhovaného řešení. Navrhnout možný harmonogram realizace SOC ČOI. Z pohledu zabezpečení provozu navrhnout minimálně 3 varianty s vymezením slabých a silných stránek, případně rizik:

a)provoz SOC ČOI si zabezpečuje ČOI sama,

b) provoz SOC ČOI je nakoupen jako služba 3.strany. Zde zmínit hranici
 odpovědnosti (navrhnout základní opatření) mezi ČOI a 3.stranou,

c) provoz SOC ČOI představuje kombinaci obou předcházejících variant.