**Technické specifikace**

**Integrace, konfigurace prvků WAN ČOI**

# Současný stav

Současná komunikační infrastruktura WAN ČOI je rozdělena takto:

* Vnější perimetr: komunikace z veřejné sítě do WAN ČOI,
* LAN a VLAN segment Praha: určený pro uživatele ústředního inspektorátu a regionálního inspektorátu „Praha“,
* Datové centrum: segment pražské sítě,
* Pobočky-inspektoráty ČOI: (viz. kap.4) umístěné v různých lokalitách ČR, komunikující s Datovým centrem v Praze dedikovanou MPLS sítí přímo bez mezilehlých FW.

Všechny výše popsané segmenty jsou logicky propojeny centrálním FW Fortinet, který na základě bezpečnostních pravidel řídí prostup mezi popsanými segmenty a přístup do nich včetně přístupu k jednotlivým centrálním systémům a aplikacím.

Jednotlivé přepínače v síti WAN ČOI pracují primárně na L2 vrstvě a nijak se nepodílí na řízení přístupu do sítě, pouze na L2 segmentaci v centrální lokalitě Praha. Menší dislokované lokality používají jednu plochou L2 síť pro veškerý provoz.

Dohled nad provozem v síti probíhá jednak na centrálním FW a také na centrálním prvku „sw-pha-core“ pomocí analytické bezpečnostní sondy Extreme Networks PVFC180 k němu připojené. Data nejsou korelována, protože se nesbíhají v žádném společném logovacím nástroji.

Administrátorský přístup na síťová zařízení je prováděn pomocí lokálních účtů. Aktuálně není používán žádný centrální nástroj pro logování a reporting v rámci celé sítě WAN ČOI.

Na základě závěrů externích auditů kybernetické bezpečnosti, Studie proveditelnosti SOC ČOI a požadavků zákona a vyhlášky o KB byla zahájena realizace koncepčního řešení výše popsaného stavu implementací nástrojů výrobce Extreme Networks v podobě těchto licencí:

* XMC Advanced pro 50 přepínačů (obecně zařízení o osmi a více portech) a 500 AP,
* Analytická licence pro monitoring provozu, která simultánně sleduje 50k spojení,
* XMC licence v dané verzi také obsahuje 500 NAC licencí pro řízení přístupu do sítě a 50 GIM licencí pro správu guest uživatelů a IoT zařízení.

# Požadavky na služby

V rámci předmětu tohoto bodu plnění jsou požadovány následující služby:

1. dodávka technického projektu včetně harmonogramu prací, kdy technický projekt bude obsahovat řešení bodů 2.1 až 2.4.

2. implementace dle závěrů technického projektu, školení

Všechny výše požadované služby jsou požadovány v rozsahu:

* stanovení bezpečnostních pravidel v prostředí nasazených produktů Extreme Networks (HW, SW),
* Integrace perimetrového FW Fortigate 500 D do XMC Extreme Networks,
* Přechodu na protokol 802.1X,
* Segmentace stávající sítě WAN ČOI.

## Stanovení bezpečnostních pravidel

Požaduje se nastavení bezpečnostních pravidel na úrovni portů provozovaných switchů v centru (Extreme Summit X460) a na pobočkách (Extreme Summit X440). Bezpečnostní pravidla nastavit v návaznosti na segmentaci sítě (bod 2.4) zejména pro zvlášť exponovaná zařízení a uživatele. V tomto smyslu bude určeným rolím přiřazen logický segment sítě, kdy po autentizaci uživatele nebo zařízení dojde ke konfiguraci síťového portu VLAN tak, aby tento reflektoval požadovanou politiku.

Analýza provozu v jednotlivých pobočkách bude prováděna přímo na úrovni provozovaných switchů. Pokud jde o nastavení pravidel a analytiku provozu prováděnou v centrální lokalitě požadujeme využití analytické sondy Extreme PVFC180, která je v současnosti v provozu. V rámci návrhu řešení je nutno mít na paměti výkon dané platformy a tomu uzpůsobit množství bezpečnostních pravidel při zapnuté telemetrii dat.

Datový LAN provoz ve všech lokalitách ČOI probíhá jak v drátové tak bezdrátové síti. Prioritou nastavení pravidel je dosažení požadované úrovně bezpečnosti provozu a dostupnosti centrálních aplikací.

## Integrace perimetrového FW Fortigate 500 D do XMC Extreme Networks

Integrace Fortinet FW do XMC pokryje jak možnost řídit centrálně bezpečnostní politiku z jednoho bodu, v tomto případě z nástroje XMC spolupracujícího s NAC, tak i integraci logování provozu z FW do XMC. K tomu bude nutné provést potřebnou konfiguraci na obou stranách (FW, XMC) v rozsahu:

* Konfigurace SNMP,
* Konfigurace logování,
* Konfigurace Radius serverů,
* Konfigurace bezpečnostní politiky.

Po vzájemné integraci obou prvků pak bude možné z XMC nejen řídit bezpečnostní politiku, ale také sledovat analytická data provozu v síti poskytnutá FW a jím reportované logy. Dalším cílem integrace je, aby FW mohl v případě detekce hrozby na perimetru sítě zasahovat do konfigurace přístupové vrstvy a zabránit dalšímu šíření případné hrozby.

Všechna data, jak analýza provozu, tak logy, a to i ze zbylých zařízení v infrastruktuře, by pak mohly být směrovány do XMC a zde hodnoceny a notifikovány určeným osobám.

## Přechod na protokol 802.1X

Na všech přepínačích je požadován přechod na protokol 802.1X. Konfiguraci přepínačů předpokládáme realizovat podle předem připravených šablon, jednotné metodiky a testovacích scénářů včetně provedení implementačních testů, monitoringu průběhu autentizace uživatelů a provozovaného HW. Všechny požadované úkony musí být provedeny bez dopadů na probíhající ostrý provoz.

## Segmentace stávající sítě WAN ČOI

Navazuje na zavedení technologie 802.1X s cílem provedení logické segmentace WAN ČOI dané určením rolí uživatelů, provozovaného HW a jednotlivých provozovaných systémů. Skupiny uživatelů a k nim asociované role by měly být definovány minimálně v rozsahu:

* Interní uživatelé ČOI (ethernet připojení):
* Administrátoři
* Zaměstnanci
* Uživatelé v terénu (VPN připojení) – inspektoři, režim home office apod.
* Externí dodavatelé IT služeb
* Návštěvnící

Těmto rolím budou přiřazeny bezpečnostní politiky, které po autentizaci uživatele (stroje) nakonfigurují síťový port přepínače v rozsahu stanovené bezpečnostní politiky (např. omezí přístup uživatelů na zdroje ve vnitřním perimetru sítě, omezí objem jejich provozu apod). S tím souvisí i možnost autentizace při přístupu do WAN ČOI využitím osobního certifikátu. V případě návštěvníků řešit možnost autentizace prostřednictvím návštěvnického portálu po schválení odpovědným zaměstnancem ČOI, případně vydáním časově omezeného přístupu. Jako suplikant koncových stanic zvážit použití nativního nástroje Microsoft Windows. Pokud by stanice používaly jiný OS, navrhnout s NAC jiný kompatibilní SW.

Skupiny provozovaného HW a k nim asociované role budou definovány minimálně v rozsahu:

* HW – provozované servery,
* HW – aktivní prvky,
* HW – tiskárny,
* HW – pracovní stanice,
* HW – bezdrátová síť (Access pointy)
* HW – uzavřené místnosti (servrovny)
* HW – dočasná zařízení (např. návštěvy s vlastním NTB)

Autentizace se, v případě těchto zařízení, může řešit buď skrze MAC adresu, nebo, pokud to zařízení umožňuje, certifikátem vydaným pro tato zařízení.

## Školení

Požaduje se 1 denní školení pro 10 účastníků v rozsahu implementovaných opatření a souvisejících změn oproti současnému stavu.

# Podpora

Požaduje se 2 letá podpora ve smyslu:

1. modifikace nastavených bezpečnostních pravidel, vytvoření nových,
2. případné vynucené změny řešení integrace FW – XMC,
3. případných změn v konfiguraci switchů v rámci technologie 802.1X,
4. případných změn konfigurace nastavené segmentace WAN ČOI.

# Seznam lokalit a pověřených osob

|  |  |  |  |
| --- | --- | --- | --- |
| Lokalita | Odpovědná osoba | E-mail | Telefon |
| Ústředí ČOI,  Praha 2, Štěpánská 567/15 | xxxxxxxxxxxxxxxxx | xxxxxxx | xxxxxx |
| Ústředí ČOI,  Praha 2, Štěpánská 567/15 | xxxxxxxxxxxxxxxxx | xxxxxx | xxxxxx |
| Brno,  tř. Kpt. Jaroše 1924/5 | xxxxxxxxxxxxxxxxx | xxx | xxxxx |
| České Budějovice,  Mánesova 3 | xxxxxxxxxxxxxxxxx | xxx | xxxxx |
| Hradec Králové,  Jižní 870/2 | xxxxxxxxxxxxxxxxx | xxx | xxxxxx |
| Liberec,  nám. Dr. Edvarda Beneše 585 | xxxxxxxxxxxxxxxxx | xxx | xxxxx |
| Olomouc,  Krapkova 3 | xxxxxxxxxxxxxxxxx | xxx | xxxxxx |
| Ostrava-Třebovice,  Provozní 1 | xxxxxxxxxxxxxxxxx | xxx | xxxxxx |
| Plzeň,  Houškova 33 | xxxxxxxxxxxxxxxxx | xxx | xxxxxx |
| Ústí nad Labem,  Prokopa Diviše 6 | xxxxxxxxxxxxxxxxx | xxx | xxxxx |

Aktuální seznam pověřených osob (stav ke dni podpisu smlouvy).