# Nástroj pro zabezpečení zdravotnických zařízení

## Řešení ochrany zdravotnických zařízení

Ochrana zdravotnický zařízení bude řešena jako soubor opatření a to:

1. zavedením klasifikace a segmentace zdravotnických zařízení s aplikací specifických pravidel pro vzájemnou komunikaci
2. implementací autentizace a autorizace (**AA**)zdravotnických zařízení v prostředí IT s přihlédnutím ke specifickým možnostem a vlastnostem těchto zdravotnických zařízení. Tato řešení navazuje a rozšiřuje implementaci aktivity „Realizace nástroje pro řízení přístupu na síti“ řešené v tomto projektu.
3. nasazení monitoringu datových toků s konfigurací zaměřenou na specifické komunikační protokoly Operačních Technologií (Operational Technology - **OT**), které, mimo jiné, využívají zdravotnická zařízení

**Zavedení segmentace, autentizace a autorizace zdravotnických zařízení**

Pokud zdravotnické zařízení podporuje AA prostřednictvím protokolu 802.1X použije toto ověřením, budou mu přidělena speciální přístupová práva dle definovaných politik odlišných od „standartních“ IT zařízení.

Většina zdravotnických zařízení neumí pracovat s protokolem 802.1X, proto bude nakonfigurováno ověření podle MAC adresy (MAB – MAC Authentication Bypass). Pokud je MAB úspěšný, zařízení opět dostane práva dle definovaných politik. Tyto politiky musí být nadefinovány striktněji než při AA pomocí protokolu 802.1X z důvodu hrozícího podvrhnutím MAC adresy.

***Politiky budou definovány minimálně pro tyto dva typy zdravotnických zařízení:***

*Zdravotnické zařízení podporující práci s Active Directory (AD) a podporují protokol 802.1X*

* zdravotnické zařízení MUSÍ být v doméně (AD)
* zdravotnické zařízení bude zařazeno v příslušné skupině nebo OU (organizační jednotka)
* zdravotnické má z AD vygenerovaný certifikát, který použije k přihlášení (zdravotnické zařízení, odstraněné z domény, nesmí být vpuštěny do počítačové sítě i v případě platnosti certifikátu).
* zdravotnické zařízení bude autentizováno na základě validního certifikátu a existenci objektu, daného zařízení, v AD
* zdravotnickému zařízení bude přidělena VLAN kde se dostane do OT sítě s omezeným přístupem na konkrétní zařízení

*Zdravotnická zařízení, které nepodporují protokol 802.1X*

* Zařízení bude definováno na AAA serveru (administrátorem nebo pověřeným zaměstnancem s velmi omezenými právy).
* Účet bude mít definovánu skupinu nebo přímo VLAN.
* Tyto zařízení budou mít dedikovanou(é) VLAN, případně speciální VLAN s omezením práv pomocí ACL (Access List).

Pokud se zařízení neumí provést AA ani pomocí MAC adresy je nutné nakonfigurovat, na vyjmenovaný port přepínače, „Port Security“ se statickou MAC adresou. Následně věnovat zvýšenou pozornost definici komunikačních politik tohoto zařízení a omezení komunikačních práv prostřednictvím ACL (Access List).

**Monitoring a analýza datových toků**

Je požadován monitoring a analýza datových toků pro zvýšení schopností detekce a ochrany před kybernetickými útoky v rámci OT a IT včetně analýzy datových toků. Je požadován nástroj pro zaznamenání síťového provozu a detekci útočníka v OT i IT části počítačové sítě s možností automatické reakce na vzniklý bezpečnostní incident.

V rámci provozního prostředí, s ohledem na MBS (minimální bezpečnostní standard), je požadována implementace monitoringu a analýzy datových toků pro zajištění schopnosti detekce hrozeb v rámci OT a IT části počítačové sítě a reakce na ně.

V rámci realizačního projektu je požadavkem dané řešení vybírat s ohledem na vzájemnou propojitelnost jednotlivých technologií. V rámci provozního prostředí se jedná o doporučený sběr a archivaci logů v rámci log managementu.

V rámci OT a IT části počítačové sítě bude řešení využito pro zaznamenání síťového provozu (síťová sonda) a pro uchování a analýzu dat (kolektor).

Vzhledem ke zdrojům virtualizačních serverů a předpokládanému objemu dat je požadováno využití virtuálního řešení kolektoru. Předpokládaná potřebná úložná kapacita na kolektoru je 2 TB při uchování obohacených dat po dobu 6 měsíců. Odhad reflektuje předpokládány rozvoj v rámci nemocnice a její infrastruktury. V OT části, počítačové, sítě bude nasazena HW sonda, pro sběr specifického síťového provozu (datových toků).

Řešení monitoringu a analýzy datových toků bude tedy jednotným celkem (složeným z dílčích HW a SW prvků) určeným pro zvýšení síťové bezpečnosti v rámci OT a IT části počítačové sítě.

## Specifikace minimálních požadavků řešení

Je požadováno komplexní škálovatelné řešení umožňující monitorování sítě jako systém pro monitorování výkonu, provozu a bezpečnosti počítačových sítí. Monitorovací systém musí umožňovat dlouhodobé podrobné monitorování veškerého provozu na počítačové síti OT a IT. Získané statistiky o provozu datové sítě musí umožnit sledovat a vyhodnocovat objemy a strukturu provozu v reálném čase, analyzovat příčiny provozních nebo výkonnostních problémů na straně sítě až po uživatele a jednotlivé aplikace, odhalovat vnitřní a vnější neznámé bezpečnostní hrozby a anomálie na základě analýzy chování sítě, uživatelů a zařízení. Je požadováno, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí nenarušoval sledovanou počítačovou síť. Ze strany sledované počítačové sítě nesmí být monitorovací systém detekovatelný.

Pro uložení a zpracování statistik bude využito specializovaného zařízení – kolektor.

Kolektor musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na zdravotní zařízení a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace.

Ukládání dat probíhá kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Je požadována plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie musí umožnit monitorování počítačové sítě prostřednictvím zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě nebo specializovaná prostředí průmyslových sítí.

Obecné vlastnosti řešení:

* Řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy).
* Řešení poskytne detekci anomálií na síti s podporou deduplikace, vzorkování na úrovni toků, identifikace uživatelů, persistencí doménových jmen.
* Minimální detekční mechanismy zahrnují detekci skenování portů, slovníkové útoky, útoky typu DoS (odmítnutí služby), útoky na síťové protokoly SSH, RDP, Telnet.
* Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikaci.
* Minimálně viditelnost OT protokolů
* Detekce P2P sítí a anonymizačních služeb (např. TOR).
* Detekce událostí na základě "Threat Intelligence" dat (komunikace s botnet C&C), detekce nadměrného zatížení sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti.
* Detekce NAT.
* Řešení musí být schopné analyzovat a vyhodnocovat události nejen na základě porovnání signatur, ale také na základě behaviorální analýzy.
* Řešení nesmí omezovat funkčnost, kvalitu ani narušovat bezpečnost ostatních zařízení/systémů v síti.
* Systém musí podporovat čtení a vyhodnocování informací z síťového provozu, zejména na aplikační úrovni ISO/OSI modelu resp. TCP/IP, s ohledem na možnost odhalení pokročilých útoků.
* Kromě výše uvedených IT protokolů a jejich vyhodnocování bude, toto řešení, v sobě integrovat monitoring datových toků a vyhodnocování protokolů, využívaných v OT prostředí, kterými jsou, tradiční průmyslové protokoly Modbus, PROFInet/PROFIbus, které využívají systémy SCADA.

### Popis požadovaných technologií

Všechny níže zmíněné technologie budou provozovány v počítačové síti OT a IT prostředí nemocnice. Je požadováno dodání technologie včetně hardware:

* *NetFlow/IPFIX dat HW sonda, 2-port 10/25G – 1 kus včetně 2ks transciever - 25GBase-LR SFP+:*

Sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivnit sledovanou síť. K síti budou připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí TAPu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Sonda bude navíc vybavená vlastní kolektorovou aplikací umožňující lokální ukládání a analýzu vlastních NetFlow/IPFIX dat.

* *Vlastnosti virtuálního 2TB kolektoru NetFlow dat – 1kus:*

Funkčnost kolektoru musí být možné dále rozšířit o systémy pro automatické vyhodnocování NetFlow/IPFIX dat, záchyt síťového provozu, monitorování výkonu aplikací a systémem pro ochranu proti DoS/DDoS útokům.

* *Automatické vyhodnocování NetFlow dat:*

Systém pro automatické vyhodnocování IP toků musí umožňovat automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém bude založen na pokročilých metodách tzv. behaviorální analýzy a umožnit odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostní ochranu koncových stanic, a pro které dosud není dostupná signatura. Detekované události musí být možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM.

### Záruka a implementace

Součástí dodávky souboru opatření zabezpečení zdravotnických opatření je kompletní implementace včetně záruky na 2 roky.