Požadavky na kybernetickou bezpečnost pro ICS systémy

Tento dokument rozšiřuje obecné požadavky na IT bezpečnost uvedené v dokumentu Pravidla chování třetích stran – IT bezpečnost publikovaný na adrese: http://www.veolia.cz/cs/pravidla-chovani-tretich-stran

Fyzická bezpečnost

V rámci fyzické bezpečnosti je vyžadováno **alespoň jedno z níže uvedených opatření pro všechny stroje terminálů**:

- Umístění zařízení v místnosti s kontrolovaným a řízeným přístupem (tj. velín s nepřetržitou obsluhou), nebo
- Umístění zařízení v uzamykatelné rozvaděčové skříni. Vhodným doplňkem v tomto případě je i montáž čidla otevření dveří rozvaděčové skříně, při otevření dveří se vyvolá alarm pro informování obsluhy včetně zápisu záznamu do logu.

Síťová bezpečnost

V optimálním případě je zařízení umístěno v bezpečné zóně – vyhrazeném síťovém segmentu odděleném firewallem s restriktivní politikou prostupů. Zařízení nemá přístup do Internetu.

Prostupy do a z vyhrazeného síťového segmentu jsou pro:

- Technologické účely (např. komunikace s řídícím systémem, předání plánů provozu, komunikace s nadřazenými systémy)
- Vzdálený přístup dodavatele pro servisní účely a při nasazování / upgrade systému (VPN)
- Obecně nesmí být na firewallu povolena jiná než potřebná komunikace pro funkci SCADA IS nebo diagnostiku

Synchronizace času – NTP

V rámci Veolie je preferováno nastavení synchronizace času na NTP servery Veolie.

Hardening

Mezi hardeningová opatření (Server, Workstation) patří:

- Nastavení bezpečnostních parametrů (politik) Windows (lokální politiky, případně využití doménových politik při zařazení zařízení do domény).
- V případě zařazení zařízení do domény musí být aplikován **AD Tier Model**
- Minimalizace uživatelských oprávnění dle rolí.
- Povolení pouze potřebných služeb. Ostatní služby budou zastaveny.

- Disablovat protokoly SSL 2.0 a SSL 3.0 případně pokud je to možné i TLS 1.0 a 1.1
- Účet Guest je zakázán
- Zákaz protokolu SMB ver. 1.0 Pro servery, u nichž není z důvodu zpětné kompatibility tento protokol nutno použít.
- Vypnutí NetBIOS over TCP/IP (ve vlastnostech aktivní síťové karty v TCP/IP4 na záložce WINS zvolit: Disable NetBIOS over TCP/IP)
- Restrict anonymous shares (Jedná se o vypnutí možnosti anonymního přihlášení na server. Pro vypnutí je potřeba v registrech změnit hodnotu klíče RestrictAnonymous z 0 na 1 na cestě HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\)
- Vypnutí LLMNR (**LLMNR** (UDP/5355, Link-Local Multicast Name Resolution) dokáže pomocí broadcastů přeložit jména okolních počítačů bez DNS serveru. Pokud jsou v síti používány DNS servery je protokol zbytečný. V opačném případě je možné jej ponechat zapnutý)
- Pokud existuje jiný vzdálený přístup na pracovní stanici (Workstation), je požadováno zakázání nativního RDP

V podmínkách terminálů Veolia je požadováno **zejména SW blokování portů USB v režimu „mass storage device" pro „běžné uživatele"** – tj. v závislosti na úrovni přihlášení.

Politika hesel: Je žádoucí, aby se **heslo všech uživatelů pravidelně měnilo** – vzhledem k nepřetržitému chodu terminálů však není vhodné tuto změnu vynucovat pravidlem s „tvrdou periodou", ale preferovanou variantou je zajistit tuto změnu organizačním opatřením – změna bude provedena vždy při profylaktice terminálu prováděné dodavatelem, případně v domluvených pravidelných cyklech.

Doplňující požadavky na hardening jsou upřesněny vždy na základě konkrétního zařízení.

Požadavky na OS a SW

S ohledem na skutečnost, že podpora ze strany Microsoft pro starší operační systém Windows 7 byla ukončena k 14. lednu 2020 a pro Windows 10 byla ukončena 14. října 2025, všechny stanice jednotlivých zařízení Veolia budou používat

- **OS Windows 11**

pro technologické zařízení je preferován

- **Windows 10 Enterprise 2021 LTSC**
- **Windows 11 Enterprise 2024 LTSC**
- **Serverový OS Windows Server 2022**
- **Serverový OS Windows Server 2025**

Databázové systémy preferujeme open source, systémy MS SQL a Oracle nejsou preferovány z licenčních důvodů.

Aktualizace OS a SW

Aktualizace aplikačního SW (mimo SW od Microsoft) budou prováděny pracovníky servisní organizace.

Aktualizace OS Windows a dalšího SW Microsoft – WSUS Veolia. Budou prováděny s využitím WSUS (Windows Server Update Services) Veolia, přičemž pro zařízení dodavatele se vytvoří samostatná WSUS skupina. Skupina slouží pro přehled všech připojených zařízení dodavatele, neslouží však pro distribuci aktualizací na základě konkrétních požadavků, nebo zařízeních dodavatele.

Z WSUS budou skupině poskytovány veškeré aktualizace ze strany Veolia, na zařízeních si poté dodavatel již sám vybere z jeho strany otestované a ověřené aktualizace a provede jejich stažení a instalaci.

Veolia je pouze schopná na základně feedbacku zablokovat požadovanou aktualizaci pro danou skupinu.

Aktualizace OS Windows a dalšího SW Microsoft – Patch management dodavatele. Aktualizace jsou testovány na straně dodavatele a uvolňovány jen aktualizace, které nebudou mít negativní vliv na funkčnost systémů. Za tyto aktualizace, jejich instalaci a následnou funkčnost systémů ručí dodavatel.

Pro testování zranitelností svých systémů používá Veolia mj. sken prostřednictvím SW Nessus. Systém musí být rezistentní proti skenům zranitelností i za provozu. Stejný sken může kdykoliv spustit útočník.

Antivir

Veolia v současnosti využívá na svých informačních systémech **antivirus ESET**. Tento antivirus je pro technologická zařízení nastaven tak, aby neohrožoval jejich funkčnost.

Dodavatel však může dodat přesné specifikace pro další úpravu nastavení, podle jeho potřeb.

Veolia dodá licence a instalační balíčky pro jednotlivé zařízení a vytvoří v rámci centrálního nastavení samostatný profil (skupinu) pro zařízení daného dodavatele.

V rámci tohoto antivirového řešení se zavádí blokace a správa USB portů.

Pokud systém dodavatele nepodporuje tento antivirus (nemá jej plnohodnotně otestován pro bezchybný chod svého systému) je možné po domluvě a předešlém schválení zavedení vlastního antivirového řešení.

Toto řešení však musí mít pravidelnou aktualizaci antivirových databází.

Zálohování

Veškerá zařízení musí být pravidelně zálohována.

Veolia preferuje použití SW **Veeam.** Zálohy lze provádět za běhu systému, a to periodicky nebo ad-hoc správcem zařízení dle potřeby. Obnovu lze provést za běhu systému nebo off-line s využitím bootovacího backup SW na USB. Zálohy jsou prováděny na datové uložiště NAS, které je k tomuto účelu na každé lokalitě určené. Offline zálohy jsou následně prováděné na externí USB HDD v pravidelném intervalu jednou měsíčně.

Centrální sběr logů a dohledový systém

Veolia využívá centrálního sběru logů ze zařízení do svého SIEM (Security Information and Event Management) systému.

Buďto se logy vyčítají SIEMem ze stanic a serverů pomocí lokálního účtu, nebo zařízení odesílají logy do SIEMu. Veškerá zařízení musí být připojena na centrální SIEM Veolia.

Řízení zranitelností (Vulnerability Management)

Veolia využívá Qualys jako nástroj pro řízení zranitelností. Veškeré servery a stanice musejí být zadány v systému Qualys a musí být na nich vytvořen lokální administrátorský účet Qualys pro možnost pravidelného autorizovaného skenování.

Vzdálený přístup

Vzdálený přístup je umožněn prostřednictvím personalizovaných uživatelů z řad servisní organizace pomocí VPN GlobalProtect clienta přes centrální monitorované jump servery Veolia.

Požadavky pro výběr aktivních prvků LAN v systémech SCADA

Mezi aktivní prvky LAN patří routery, switche, firewally a další zařízení, která potřebují pro svůj chod nebo vzdálenou správu operační systém nebo firmware (ať již standardizovaný nebo proprietární)

Aktivní prvky musí odpovídat následujícím požadavkům:

- výrobky určené pro podnikový segment, tzn. enterprise, nikoliv tzv. SOHO
- renomovaný výrobce s dlouholetou zkušeností, zastoupením a podporou na českém trhu
- plánovaná podpora výrobku po dobu morální životnosti, nejméně 5 let od uvedení do provozu (podporou výrobku se rozumí vyvíjení a rozšiřování funkcionality operačního systému nebo firmwaru a především vydávání oprav bezpečnostních chyb odhalených v průběhu životního cyklu výrobku - tzn. min 5 let do tzv. data End of Life/EoL a End of Support/EoS)
- vzdálená správa/přístup a konfigurace musí být možná pomocí šifrovaného spojení (např. protokoly https, ssh, scp, sftp)
- bude se jednat o aktivní prvky, pro které bude moci odběratel/uživatel zajistit např. formou servisní smlouvy konfiguraci odpovídající požadavkům Veolia, záplatování a obsluhu, pokud toto nebude zajištěno samotným dodavatelem
- produktová řada a typy budou předmětem jednání a schválení zástupci IT VEČR před jejich dodáním

Před každou realizací projektů je potřebná konzultace s oddělením KyB ohledně upřesnění požadavků na bezpečnost.

Účinnost od 12.1.2026