Všeobecné pravidlá pre partnerské firmy dodávajúce OT infraštruktúru a softvér

Verzia pre Verejné Obstarávanie

Verzia: 1.0

Dátum vydania: 04.03.2024

Vydal: Oddelenie rozvoja a prevádzky riadiacich systémov

Obsah

1 Účel dokumentu

Tento dokument ustanovuje pravidlá pre partnerské firmy dodávajúce OT infraštruktúru a softvér pre MH Teplárenský Holding, a.s. v rámci verejného obstarávania. Dokument je určený vedeniu partnerských spoločností, ich zamestnancom a subdodávateľom a slúži ako technický štandard MHTH

2 Všeobecné ustanovenia

Pravidlá uvedené v tomto dokumente, v prípade, že ich možno aplikovať na rozsah dodávky, sú povinné.

3 Použité skratky a pojmy

MHTH – MH Teplárenský Holding, a.s.
OT – Operational Technology
SW – Software
HW – Hardware
OS – Operating system
FW – Firewall
DMZ – Demilitarizovaná zóna
AD – Active directory
HMI – Human Machine Interface
Dodávateľ - partnerská firma dodávajúca OT infraštruktúru a softvér pre MH Teplárenský Holding, a.s.
DRP – Disaster Recovery Plan
NDA – Non-disclosure agreement. Zmluva o mlčanlivosti.
IS – Informačný systém
RS – Riadiaci systém
DRS – Dokumentácia realizácie stavby
ZoBOaNP - Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatváraná ako príloha hlavnej zmluvy

4 Sieťová infraštruktúra

Nová sieťová infraštruktúra sa pripája na existujúcu sieťovú infraštruktúru MHTH len v miestach na to určených a podľa definovaných pravidiel. Pripojenie do sieťovej infraštruktúry MHTH je možné len po podpise ZoBOaNP. Vytváranie ostrovných riešení je zakázané.

4.1 Switche

V rámci dodávky je možné dodať len manažovateľné L2/L3 switche s nasledujúcimi vlastnosťami:

- Rozhranie pre manažment cez SSH
- Podpora RSPAN
- Podpora SNMP V3 pre pripojenie na centrálny monitoring (viď Kapitola 15.2)
- Podpora RSTP
- Podpora štandardu 802.1x
- Podpora syslogu a napojenia na centrálne sledovanie logovacích hlásení (viď Kapitola 15)
- Podpora RADIUS servera pre manažment užívateľov

- Podpora „port security“ funkcionality
- Možnosť vzdialenej aktualizácie firmware
- Podpora protokolov CDP alebo LLDP
- Možnosť konfigurácie aspoň 250 rôznych VLAN
- Podpora agregácie liniek
- Downlink porty s rýchlosťou 100/1000Mbps
- Uplink porty s rýchlosťou 1000Mbps (v prípade predpokladaných prenosov veľkého objemu dát s rýchlosťou 10Gbps)
- Vyhotovenie, stupeň ochrany a celková odolnosť vyhotovenia switchu musia zodpovedať náročnosti prostredia, v ktorom bude switch umiestnený
- V prípade použitia switchu, pre zariadenia využívajúce industriálne protokoly (Profinet a pod.) je nutné aby bola zaručená ich natívna podpora samotným switchom
- Je možné dodať len zariadenia, na ktoré je od výrobcu deklarovaná podpora po dobu 5 rokov od dátumu odovzdania diela a zároveň počas tejto doby musí byť na zariadenia zakúpený support od výrobcu s možnosťou sťahovania nových verzií firmware ak ich výrobca neposkytuje bezplatne na stiahnutie

4.2 Routre

Dodávka routrov je zakázaná. Routovanie je zabezpečované existujúcimi zariadeniami vo vlastníctve MHTH. Každý prestup medzi oddelenými sieťami ide cez centrálny FW.

4.3 Firewally

FW a ich funkcionalita sú poskytované zo strany MHTH. Dodávka FW dodávateľom je zakázaná s výnimkou dedikovaných industriálnych FW.

4.4 Prevodníky

Zariadenia na prevod signálu z optického vlákna na metalický kábel resp. „vice versa“ môžu byť použité len v technológii pri koncových zariadeniach. Pre prepojenia v rámci serverovne alebo vyhradenej miestnosti musí byť ukončenie optického sieťového kábla priamo na switchi. Pre ostatné prepojenia musí byť ukončenie optického sieťového kábla v opto paneli v rozvádzači pomocou optického gbic korešpondujúcim typom portu a optického kábla. Môžu sa použiť iba gbic alebo DAC káble, ktoré sú podporované výrobcami na zariadeniach do ktorých sa budú pripájať. Prevodník musí byť v rozvádzači pevne uchytený.

4.5 Kabeláž

4.5.1 Optické sieťové káble

Dodávané optické sieťové káble musia spĺňať nasledovné požiadavky:

- Multi-mode kábel musí byť typu OM3 alebo vyšší. Konkrétny typ musí zohľadňovať požadovanú prenosovú rýchlosť a dĺžku kábla resp. komunikačnej trasy.
- Single-mode kábel musí byť typu OS1 pre vnútorné a OS2 pre vonkajšie použitie

Realizačné riešenie návrhu optickej siete musí prejsť schvaľovacím procesom zo strany MHTH v rámci schvaľovania DRS.

4.5.2 Metalické sieťové káble

Metalické sieťové káble musia byť kategórie Cat6 a vyššej.

4.6 Bezdrôtové siete

V rámci MHTH sa bezdrôtové lokálne siete v rámci aktuálne OT nepoužívajú. Vybudovanie novej bezdrôtovej siete v rámci dodávky je možné len v prípade, že nie je technicky možné zrealizovať fyzické pripojenie pomocou kábla.

4.6.1 WLAN

Nové infraštruktúry musia podporovať výhradne IP protokol verzie 4 alebo vyššej. Iné protokoly musia byť odfiltrované, aby sa do siete skupiny mohli dostať iba IP protokoly. Umiestnenie prístupových bodov a vysielací výkon musia byť zvolené tak, aby pokrývali iba želanú oblasť.
Používanie bezdrôtových extenderov/bridge-ov je povolené iba ak sú počas rádiového prenosu implementované šifrovanie pripojenia a techniky overovania rovnakej úrovne zabezpečenia ako na access pointe, ku ktorému sa extender/bridge pripája. Preklad sieťových adries (NAT) nie je na prístupových bodoch povolený.

4.6.2 Bluetooth

Používanie Bluetooth na komunikáciu medzi jednotlivými časťami OT systémov je zakázané.

4.7 Konfigurácia

Konfiguráciu dodávaných komponentov sieťovej infraštruktúry bude vykonávať MHTH v spolupráci s dodávateľom a na základe jeho špecifikácie odsúhlasenej v DRS. Konfigurácia musí zodpovedať bezpečnostným požiadavkám zo strany MHTH.

4.8 Zapojenie

Zapojenie sieťovej infraštruktúry, vrátane kabeláže, bude vykonávať dodávateľ podľa platnej projektovej dokumentácie. V prípade zapájania v serverovniach alebo vyhradených miestnostiach MHTH, bude toto zapojenie vykonávané pod dohľadom zodpovednej osoby, ktorú určí MHTH.

4.9 Zonácia a segmentácia

Zonáciu a segmentáciu sietí určuje MHTH na základe podkladov dodaných dodávateľom počas prípravy DRS. Podklady musia obsahovať sieťový diagram a typy a počty plánovaných pripojených zariadení. Riešenie musí byť navrhnuté s ohľadom na dobrú prax – PERA model. Akákoľvek komunikácia so sieťami mimo lokálnej OT siete musí prebiehať cez DMZ/Proxy, terminovaná je cez centrálny FW.

4.9.1 VLAN

VLAN a ich adresné rozsahy sú určené zo strany MHTH podľa špecifických potrieb systému definovaných dodávateľom. VLAN sa poskytujú v najmenšom možnom rozsahu s minimálnymi rezervami. VLAN sú navrhované tak, aby sieť bola rozdelená na čo najmenšie logické celky, čo musí byť reflektované aj v požiadavkách od dodávateľa. Všetky VLAN sú ukončené na centrálnom FW a sú navzájom izolované. V prípade nutnosti komunikácie medzi rôznymi VLAN pozri kapitolu 4.9.2.

4.9.2 Prestupy medzi VLAN

Prestupy medzi rôznymi VLAN sú možné len na základe schválenej komunikačnej matice. Komunikačná matica obsahuje minimálne:

- Zdrojovú a cieľovú IP adresu
- Konkrétne porty a služby ktoré majú byť otvorené
- Smer komunikácie
- Zdôvodnenie nutnosti komunikácie

Komunikačná matica obsahuje aj komunikácie medzi zariadeniami na rovnakom subnete. Komunikačnú maticu navrhuje dodávateľ v rámci prípravy DRS a schvaľuje ju MHTH v rámci procesu schvaľovania DRS na základe platných bezpečnostných štandardov. Komunikačná matica musí obsahovať najmenší možný rozsah portov a IP adries nutný na správnu funkcionalitu systému. Vzor komunikačnej matice bude poskytnutý na vyžiadanie.

5 Komunikačné rozhrania a protokoly

5.1 Všeobecné požiadavky

MHTH vyžaduje použitie zabezpečených protokolov na komunikáciu medzi jednotlivými systémami. Taktiež komunikácia medzi jednotlivými komponentami systému musí byť zabezpečená. Jedinou výnimkou je nutná komunikácia s existujúcimi systémami, ktoré nepodporujú použitie zabezpečených protokolov. To neplatí pre prípad keď daná komunikácia zabezpečuje prenos prihlasovacích údajov alebo informácii s vyššou klasifikáciou ako interné. V takom prípade je nutné realizovať zabezpečenie tohto spojenia vhodnými technickými prostriedkami.

5.2 Komunikačná schéma

Súčasťou ponuky musí byť aj bloková komunikačná schéma poskytujúca nasledujúce informácie o rozhraniach medzi jednotlivými súčasťami systému:

- Smer komunikácie komunikačného rozhrania
- Typ prenášaných dát
- Použitý protokol

5.3 Zoznam obmedzených protokolov

Služba/Protokol	**Popis**
FTP	Zakázané
Telnet	Zakázané
SMTP	Len pre interné e-mailové adresy za predpokladu použitia TLS/SSL s možnosťou overovania.
IMAP	Zakázané
POP3	Zakázané
HTTP	Zakázané. Potrebné nahradiť HTTPS
OPC DA	Zakázané. Potrebné nahradiť šifrovaným OPC UA.
MQTT	Len šifrované na porte 8883. Nešifrovaná komunikácia na porte 1883 je zakázaná.

6 Servery

6.1 Všeobecné požiadavky

Všetky servery v rámci dodávky musia byť virtualizované. Automatické spúšťanie vymeniteľného média („Autorun") musí byť deaktivované. Na každom serveri musí byť implementované automatické uzamknutie interaktívnej relácie po preddefinovanej dobe nečinnosti (maximálne 10 minút). Uzamknutie je možné odstrániť iba po riadnom overení používateľa. Automatické uzamknutie musí byť konfigurovateľné/vypínateľné za použitia administrátorského oprávnenia. Nastavenie automatického uzamknutia nie je vyžadované (aj keď funkcionalita samotná musí byť dostupná) pre „Kioskové" riešenia a pre relácie určené pre operátorov v nepretržitej prevádzke.
Pri fyzických serveroch nesmie byť žiadna značka (tag) alebo označenie obsahujúce citlivé informácie (napr. informáciu o ILO mgmt.), ktoré nesmú byť viditeľné neoprávneným osobám.

6.2 Sieťové rozhranie

Každý server môže disponovať, až na výnimky uvedené nižšie, len jedným sieťovým rozhraním. Ako komunikačný protokol je povolený len IP protokol verzie 4. Všetky ďalšie komunikačné protokoly musia byť vypnuté. Servery musia používať statické IP adresy. Na serveroch musí byť vypnuté smerovanie a nesmie byť zapnuté preposielanie paketov. Všetky nevyžadované sieťové rozhrania musia byť vypnuté.

Zoznam výnimiek pre viac sieťových rozhraní:

- Zabezpečenie redundantného pripojenia fyzického servera do siete. Takéto pripojenie je však možné len po jednej VLAN.
- Zabezpečenie aplikačnej redundancie pomocou dedikovanej VLAN. Táto VLAN nemôže byť použitá na iné účely.
- VLAN použitá na zabezpečenie redundancie medzi dvoma servermi musí byť úplne izolovaná.
- Zabezpečenie komunikácie pomocou industriálnych protokolov vyžadujúcich dedikované sieťové rozhranie (napr. Profinet)

6.3 Služby

Nainštalované a spustené služby môžu byť len tie, ktoré sú vyžadované pre prevádzku. Kontá služieb používané na tento účel musia mať pridelené minimálne oprávnenia tak aby služba mohla fungovať. Kontá služieb nesmú mať povolenia interaktívne sa prihlásiť na server.
Kontá s lokálnymi alebo lokálnymi správcovskými oprávneniami (koreňové, správcovské, kontá správcov domén atď.) sa nesmú používať na spúšťanie aplikácií.
Služby, ktoré vyžadujú overenie a požadujú aby boli meno a heslo uložené v nezašifrovanom texte sa nesmú používať a musia byť nahradené zabezpečenými službami. Protokoly sa musia používať v ich najbezpečnejších verziách v dobe nasadenia systému do prevádzky.
Konfigurácia povolených služieb servera musí byť jasne a zrozumiteľne zdokumentovaná. Pred uvedením do prevádzky a po inštalácii všetkých aplikácií MHTH skontroluje a zdokumentuje, či neobsahujú nepovolené služby. V prípade, že budú takéto služby identifikované musí ich dodávateľ, ešte pred uvedením diela do prevádzky, na vlastné náklady odstrániť.

6.4 Súborový systém

Oprávnenia systému súborov sa musia nastaviť podľa princípu najnižších oprávnení alebo „need-to-know".

Iba správcovia systému, správcovia kybernetickej bezpečnosti a systémové kontá môžu dostať právo na zapisovanie do súborov operačného systému servera.
Údaje musia byť udržiavané štruktúrovaným spôsobom, pričom systémové súbory a údajové súbory musia byť uložené v oddelených oblastiach.
Aplikácie musia byť nainštalované na inú partíciu ako je systémová, tak aby nemohlo dôjsť k jej neželanému zaplneniu.

6.5 Virtuálne servery

Virtuálne prostredie a inštaláciu virtuálneho servera zabezpečuje a vykonáva MHTH podľa špecifikácií dodaných dodávateľom.

Špecifikácia požiadaviek na virtuálny server v nasledovnom rozsahu musí byť už súčasťou ponuky:

- Typ a verzia operačného systému
- Počet vCPU
- Veľkosť RAM
- Veľkosť úložiska podľa jednotlivých partícií
- Počet sieťových rozhraní
- Požadované výnimky pre AV a FW
- Zoznam štandardných služieb a rolí servera, vrátane ich konfigurácie, ktoré majú byť nainštalované
- Zoznam inštalovaného SW vrátane databázových serverov vrátane ich verzií

6.6 Fyzické servery

Nakoľko všetky servery musia byť virtualizované, dodávka fyzických serverov nie je povolená.

7 Databázy a databázové servery

7.1 Všeobecné požiadavky

V prípade, že dodávaný systém potrebuje využívať databázy, tak tieto databázy musia byť umiestnené na databázovom servery ktorý určí MHTH. Použitie dedikovaného databázového servera je možné len v nasledovných prípadoch:

- Aplikačný SW vyžaduje pre bezproblémový beh inštaláciu na rovnaký server ako je databázový server a táto podmienka je uvádzaná výrobcom.
- Existuje technické obmedzenie, ktoré to neumožňuje, prípadne výrobca to nedovoľuje. V takom prípade musí byť musí byť obmedzenie v ponuke riadne zdokumentované a preukázané.

7.2 Preferovaný databázový server

V MHTH je ako databázový server preferovaný Microsoft SQL Server.

7.3 Databázy

V prípade, že súčasťou dodávky je aj databáza, ktorá môže bežať na externom databázovom servery, tak jej finálne umiestnenie určí MHTH počas procesu prípravy DRS, nakoľko pre niektoré typy databázových serverov existujú centrálne riešenia, ktoré sú uprednostňované pred stand-alone riešeniami. Umiestnenie

databázy bude ovplyvnené parametrami ako je požadovaná veľkosť a očakávaná záťaž read/write prístupov.

7.4 Databázové servery

Všetky databázové servery musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH. Všetky databázové servery sú spravidla virtualizované vo virtuálnom prostredí MHTH a inštalované na serverový operačný systém. Inštalácia databázového servera spolu s aplikačným SW na jeden server je povolená len v prípade, že ide o nutnú podmienku na bezproblémový beh aplikačného SW udávanú jeho výrobcom. Táto skutočnosť musí byť zdokumentovaná v ponuke a aj vo finálnej dokumentácii.

Špecifikácia požiadaviek na virtuálny databázový server v nasledovnom rozsahu musí byť súčasťou ponuky:

- Typ a verzia operačného systému
- Počet vCPU
- Veľkosť RAM
- Veľkosť úložiska podľa jednotlivých partícií
- Počet sieťových rozhraní
- Požadované výnimky pre AV a FW
- Zoznam štandardných služieb a rolí servera, vrátane ich konfigurácie, ktoré majú byť nainštalované

Databázové servery, ktorých licenčný model by vyžadoval licencovanie celého virtuálneho prostredia, nie sú povolené.

8 Klientské stanice

8.1 Sieťové rozhranie

Každá klientská stanica môže disponovať (až na výnimky uvedené nižšie), len jedným sieťovým rozhraním. Ako komunikačný protokol je povolený len IP protokol verzie 4. Všetky ďalšie komunikačné protokoly musia byť vypnuté. Procesne kritické klientské stanice musia používať statické IP adresy. Na staniciach musí byť vypnuté smerovanie a nesmie byť zapnuté preposielanie paketov. Všetky nevyžadované sieťové rozhrania musia byť vypnuté.

Zoznam výnimiek:

- Zabezpečenie redundantného pripojenia fyzickej klientskej stanice do siete. Takéto pripojenie je však možné len do jednej VLAN.
- Zabezpečenie aplikačnej redundancie pomocou dedikovanej VLAN. VLAN použitá na zabezpečenie redundancie medzi dvoma klientskými stanicami musí byť úplne izolovaná.
- Zabezpečenie komunikácie pomocou industriálnych protokolov vyžadujúcich dedikované sieťové rozhranie (napr. Profinet)

8.2 Služby

Nainštalované a spustené služby môžu byť len tie, ktoré sú vyžadované pre prevádzku. Kontá služieb používané na tento účel musia mať pridelené minimálne oprávnenia tak aby služba mohla fungovať. Kontá služieb nesmú mať povolenia interaktívne sa prihlásiť na server.

Kontá s lokálnymi alebo lokálnymi správcovskými oprávneniami (koreňové, správcovské, kontá správcov domén atď.) sa nesmú používať na spúšťanie aplikácií.
Služby, ktoré vyžadujú overenie a požadujú aby boli meno a heslo uložené v nezašifrovanom texte sa nesmú používať a musia byť nahradené zabezpečenými službami. Protokoly sa musia používať v ich najbezpečnejších verziách v dobe nasadenia systému do prevádzky.
Konfigurácia povolených služieb servera musí byť jasne a zrozumiteľne zdokumentovaná. Pred uvedením do prevádzky a po inštalácii všetkých aplikácií MHTH skontroluje a zdokumentuje, či neobsahujú nepovolené služby. V prípade, že budú takéto služby identifikované musí ich dodávateľ, ešte pred uvedením diela do prevádzky, na vlastné náklady odstrániť.

8.3 Súborový systém

Oprávnenia systému súborov sa musia nastaviť podľa princípu najnižších oprávnení alebo „need-to-know“. Iba správcovia systému, správcovia kybernetickej bezpečnosti a systémové kontá môžu dostať právo na zapisovanie do súborov operačného systému servera.
Údaje musia byť udržiavané štruktúrovaným spôsobom, pričom systémové súbory a údajové súbory musia byť uložené v oddelených oblastiach.

8.4 Databázové servery

Inštalácia databázových serverov na klientské stanice je zakázaná. Výnimku tvoria len databázové servery, ktoré sú neoddeliteľnou súčasťou aplikačného SW a sú súčasťou inštalačného balíka (vyžadované výrobcom aplikačného SW). Takáto výnimka musí byť riadne zdokumentovaná už vo fáze ponuky a preukázaná. Takáto inštalácia podlieha rovnakým pravidlám ako inštalácia na serverový operačný systém. Databázové servery musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH.

8.5 Operátorské stanice

Preferované riešenie vizualizácie riadiaceho systému pre operátorov na velíne je použitie virtuálneho terminálového servera. V prípade, že terminálový server nie je možné z technického obmedzenia uvádzaného výrobcom použiť, tak pracovné stanice poskytujúce túto službu musia byť virtualizované.

8.6 Tenkí klienti

Pre vytvorenie nových operátorských pracovísk je nutné použiť tenkého/zero klienta, ktorý bude sprostredkovávať zabezpečenú užívateľskú reláciu s príslušným serverom/pracovnou stanicou pomocou protokolu RDP alebo HTTPS. Preferovaná konfigurácia tenkého/zero klienta je stiahnutie si konfigurácie pri štarte zo siete (PXE Boot).

9 Software

9.1 Všeobecné požiadavky

Každý dodávaný SW musí byť legálny, v prípade open-source riešení zabezpečené legálne použitie pre komerčné účely, dodaný spolu s inštalačnými súbormi v použitej verzii, platnou dokumentáciou od výrobcu a podrobným návodom na inštaláciu vrátane potrebnej konfigurácie.

9.2 Operačný systém a firmware

Preferovaná je dodávka operačného systému na báze MS Windows alebo bežných komerčných distribúcií na báze Unix/Linux.

9.2.1 MS Windows

Všetky zariadenia s operačným systémom na báze MS Windows musia byť pripojené do Active Directory, ktoré určí MHTH. MS Windows musí byť dodaný v poslednej známej LSTC verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.2.2 Unix/Linux

Všetky zariadenia s operačným systémom na báze Unix/Linux musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH. Unix/Linux musí byť dodaný v poslednej známej LTS verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať. V MHTH je preferovanou distribúciou Debian alebo Ubuntu.

9.2.3 Iné OS

Všetky zariadenia s iným operačným systémom ako na báze MS Windows alebo Unix/Linux, musia umožňovať manažment užívateľov v Active Directory, ktoré určí MHTH. Operačný systém musí byť dodaný v poslednej známej stabilnej verzii a pred odovzdaním musí mať nainštalované všetky bezpečnostné a funkčné záplaty vydané výrobcom do dátumu odovzdania diela. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.2.4 Firmware

Dodávané komponenty obsahujúce firmware musia byť pri odovzdávaní diela aktualizované na aktuálnu stabilnú verziu FW s aplikovanými bezpečnostnými záplatami. Inštaláciu záplat vykoná dodávateľ a MHTH ju bude validovať.

9.3 Aktualizácie OS a firmware

OS a firmware, musí umožňovať aplikáciu bezpečnostných a funkčných aktualizácií, patchov a service packov vydaných výrobcom, bez toho aby to negatívne ovplyvnilo záruku na dodané dielo aj v prípade, že tieto aktualizácie nevykoná dodávateľ. Možnosť použitia centrálnej správy aktualizácií je preferovaná.

9.4 Aplikačný SW

Aplikačný SW musí byť dodaný v poslednej stabilnej verzii, alebo prípadne v takej verzii, aby výrobca garantoval jeho podporu (minimálne vydávanie bezpečnostných záplat) po dobu minimálne 5 rokov od dátumu odovzdania do prevádzky. Medzi aplikačný SW sa radia aj databázové servery.

9.4.1 Aktualizácie aplikačného SW

Aplikačný SW musí umožňovať aplikáciu bezpečnostných a funkčných aktualizácií, patchov a service packov vydaných výrobcom, bez toho aby to negatívne ovplyvnilo záruku na dodané dielo aj v prípade, že tieto aktualizácie nevykoná dodávateľ. Táto požiadavka sa týka aj patchovania OS na ktorom aplikačný SW beží a podporných služieb.

9.4.2 Human Machine Interface

Aplikačný SW poskytujúci funkcionalitu HMI alebo inej vizualizácie slúžiacej na sledovanie alebo riadenie výrobných procesov musí umožňovať tzv. „Kiosk mód“ kde prístup na operačný systém hosťujúci aplikačný

SW je umožnený len oprávneným používateľom. Neoprávnení používatelia nesmú mať možnosť akokoľvek interagovať s OS alebo inými aplikáciami.

9.4.3 Kompatibilita s hypervisorom

Dodávateľ musí garantovať kompatibilitu dodávaného aplikačného SW s hypervisorom používaným v MHTH, tak aby bola umožnená virtualizácia. Informácia o type a verzii bude poskytnutá úspešnému uchádzačovi po podpise zmluvy.

10 Hardware

HW musí byť dodaný v takej verzii aby jeho výrobca garantoval podporu a dostupnosť kompatibilných náhradných dielov po dobu minimálne 5 rokov od dátumu odovzdania do prevádzky pokiaľ nie je v Opise diela(Príloha A) požadované inak.

11 Antivírus a zabezpečenie

11.1 Všeobecné požiadavky

Všetky dodávané systémy musia byť v čo najvyššej možnej miere zabezpečené voči neoprávneným zásahom a zneužitiu.

11.2 Antivírus

Všetky servery a klientské stanice musia mať nainštalovaný antivírusový SW používaný v MHTH. V prípade, že pre správny beh dodávaného SW sú nutné výnimky v AV nastavení, tak je potrebné tieto výnimky uviesť už v ponuke. Informácia o type a verzii bude poskytnutá úspešnému uchádzačovi po podpise zmluvy.
Licencie pre AV zabezpečuje MHTH.

11.3 Lokálny Firewall

Lokálny firewall musí zostať aktivovaný a všetky pridané prestupy musia byť riadne zdokumentované a odsúhlasené MHTH. Pre zariadenia s operačným systémom na báze MS Windows bude použitý integrovaný firewall a pre zariadenia s operačným systémom na báze Unix/Linux je nutné použiť nftables alebo iptables alebo firewalld.

12 Zálohovanie

Podmienky dostupnosti a požiadavky na DRP sú definované v Opise diela (Príloha A).

12.1 Servery

Dodávateľ je povinný definovať plán záloh a údržby jednotlivých databáz tak, aby vyhovovala podmienkam dostupnosti a požiadavkám vyplývajúcim z DRP. Plán záloh a údržby bude súčasťou DRS.

Zálohovanie serverov bude vykonávané centrálnou službou v kompetencii MHTH. Pred uvedením do prevádzky je dodávateľ povinný v súčinnosti s MHTH validovať funkčnosť automatických záloh.

12.2 Klientské stanice

Dodávateľ je povinný definovať plán záloh a údržby jednotlivých klientských staníc tak, aby vyhovovala podmienkam dostupnosti a požiadavkám vyplývajúcim z DRP. Plán záloh a údržby bude súčasťou DRS.

Pred uvedením do prevádzky, musí dodávateľ poskytnúť MHTH aktuálne zálohy všetkých klientských staníc v elektronickej podobe v takom formáte aký bude odsúhlasený zo strany MHTH.

12.3 Databázy

Dodávateľ je povinný definovať plán záloh a údržby jednotlivých databáz tak, aby vyhovovala podmienkam dostupnosti a požiadavkám vyplývajúcim z DRP. Plán záloh a údržby bude súčasťou DRS.

12.4 Sieťové komponenty

Dodávateľ je povinný definovať plán záloh a údržby jednotlivých sieťových komponentov tak, aby vyhovovala podmienkam dostupnosti a požiadavkám vyplývajúcim z DRP. Plán záloh a údržby bude súčasťou DRS.
Zálohovanie konfigurácie sieťových komponentov je v zodpovednosti MHTH. Dodávateľ je povinný zabezpečiť nutnú súčinnosť.

12.5 Automatizačné komponenty

Automatizačné komponenty ako sú napríklad PLC, konfigurovateľné frekvenčné meniče a podobne musia umožňovať zálohovanie konfigurácie. V prípade, že na zálohovanie je nutný špecializovaný SW, tak musí byť (spolu s licenciou a ak je nutná aj dokumentáciou) súčasťou dodávky.
Dodávateľ je povinný definovať plán záloh a údržby automatizačných komponentov tak, aby vyhovovala podmienkam dostupnosti a požiadavkám vyplývajúcim z DRP. Plán záloh a údržby bude súčasťou DRS.
Pred uvedením do prevádzky, musí dodávateľ poskytnúť MHTH aktuálne zálohy všetkých komponentov v elektronickej podobe.

13 Časová synchronizácia

Všetky zariadenia a systémy sa musia vedieť synchronizovať pomocou protokolu NTP. Zdroj času určí MHTH.

14 Kryptografia

Kryptografické prostriedky sa používajú na zabezpečenie:

a) dôvernosti údajov,
b) integrity údajov,
c) autentizácie odosielateľa (digitálny podpis),
d) nepopierateľnosti vykonanej činnosti (non-repudiation).

Kryptografické prostriedky sa používajú najmä na ochranu citlivých údajov:

a) prenášaných cez nezabezpečené prostredie (napr. internetová alebo e-mailová komunikácia),
b) uložených na lokálnych diskoch (koncové stanice, zdieľané úložiská údajov a pod.),
c) prenosných zariadeniach (notebooky, tablety, smartfóny a pod.),
d) prenosných médiách (CD, DVD, USB a pod.).

Použitý šifrovací algoritmus musí byť vhodne zvolený tak, aby zabezpečil dostatočnú úroveň ochrany údajov. Úroveň zabezpečenia údajov vyplýva z ich citlivosti, resp. klasifikačného stupňa.

Výber použitej kryptografickej metódy závisí najmä na:

a) posúdení rizík spojených s ochranou aktíva,
b) požadovanej úrovni ochrany aktíva,
c) technických možnostiach prevádzkovaných systémov a
d) ekonomickej náročnosti opatrenia vzhľadom na hodnotu chráneného aktíva.

Minimálne požiadavky kryptografickej ochrany aktív podniku sú definované nasledovne:

a) šifrovací algoritmus symetrického šifrovania: AES-256,
b) šifrovací algoritmus asymetrického šifrovania: RSA,
c) dĺžka kryptografického kľúča RSA: najmenej 2048 bitov,
d) exspirácia kryptografického kľúča: 1 rok,
e) funkcia používaná na hashovanie: SHA-256.

Nasadenie kryptografických prostriedkov vykonáva:

a) zamestnanec dodávateľa v prípade externe vyvíjaného alebo nasadzovaného IS alebo RS,
b) špecialista/administrátor úseku informačných technológií MHTH v prípade interných aplikácií alebo nástrojov.

Správu nasadených kryptografických prostriedkov vykonáva špecialista/administrátor úseku informačných technológií MHTH.
MHTH požaduje dodržiavať min. Odporúčania dobrej praxe v oblasti kryptografických prostriedkov, uvedených tu:
https://www.nukib.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf

15 Bezpečnostné logovanie a monitoring

Systémy musia byť konfigurované tak aby logovali všetky bezpečnostne relevantné udalosti definované nižšie.
Systémy, ktoré logujú udalosti, sa musia synchronizovať prostredníctvom vopred dohodnutého referenčného času.
Logy musia byť chránené pred neoprávneným prístupom a modifikáciou.
Ak logy obsahujú klasifikované informácie, potom môže byť zabezpečený prístup len osobám disponujúcim potrebnou autorizáciou vlastníka informácie.

15.1 Logovanie udalostí

Logovacie zdroje musia byť nakonfigurované tak, aby sa logovacie hlásenia, dali vytvoriť minimálne pre nasledovné bezpečnostne závažné udalosti:

- úspešné a zamietnuté pokusy o prihlásenia ako aj odhlásenia pre administrátorské aj bežné účty
- vytvorenie, zmena, zablokovanie, odblokovanie a vymazanie účtov a rolí v aplikáciách,
- zmeny hesla a/alebo zmeny certifikátov,
- zmeny oprávnení (napr. používateľské práva, oprávnenia k objektom, členstvo v skupinách),
- spúšťanie a ukončovanie procesov,
- zmeny v časovej službe,
- zmeny v nastaveniach logovania (špeciálne deaktivovanie logovania).
- všetky ostatné udalosti, ktoré osoby zodpovedné za logovací zdroj považujú za dôležité,

- chyby vzniknuté na systéme.

Okrem bezpečnostne relevantných udalostí sa musí logovať vlastná funkcia logovacieho zdroja.
Všetky logy by mali byť zapisované do logovacieho mechanizmu operačného systému (Windows event log alebo Unix/Linux syslog).

15.1.1 Štruktúra logovacích hlásení

Logovacie hlásenia musia obsahovať nasledovné údaje o udalostiach: časovú značku, identifikačné znaky udalosti a opis bezpečnostne významnej udalosti.
Okrem toho by mali byť zahrnuté nasledovné udalosti: stupeň závažnosti udalosti, kategória (napr. informácia, chyba, výstraha, ...).
Logovacie hlásenia nesmú obsahovať heslá, ich „hashe“ alebo akúkoľvek formu autentifikácie používateľa.

15.1.2 Sledovanie logovacích hlásení

Dodávateľ je povinný v rámci projektu spolupracovať s Oddelením kybernetickej bezpečnosti, s ktorým sa dohodne na pripojení do systémov pre kontinuálne monitorovanie hrozieb, príp. zasielaní logov, ktoré sú vyprodukované dodávanými systémami na systémy, ktoré v rámci MHTH centrálne spracúvajú logovacie hlásenia. Realizácia týchto aktivít musí byť popísaná v DRS.

15.2 Centrálny monitoring

Servery, klientské stanice a sieťová infraštruktúra musia byť napojené na nástroj centrálneho monitoringu používaného v MHTH. Informácia o požiadavkách na spôsob pripojenia bude poskytnutá úspešnému uchádzačovi po podpise zmluvy.

15.2.1 Servery

Každý server bude monitorovaný príslušným klientom centrálneho monitoringu. MHTH poskytne základnú šablónu monitorovaných parametrov, ktorú dodávateľ upraví tak aby klient vedel vyhodnotiť všetky neštandardné stavy indikujúce poruchu alebo stavy smerujúce k poruche.

15.2.2 Klientské stanice

Každá klientská stanica bude monitorovaná príslušným klientom centrálneho monitoringu. MHTH poskytne základnú šablónu monitorovaných parametrov, ktorú dodávateľ upraví tak aby klient vedel vyhodnotiť všetky neštandardne stavy indikujúce poruchu alebo stavy smerujúce k poruche.

15.2.3 Sieťové komponenty

Všetky switche, routre a prípadne iné konfigurovateľné komponenty musia byť napojené na centrálny monitoring pomocou protokolu SNMP V3.

15.2.4 Ostatné komponenty

Pokiaľ niektorý s dodávaných systémových komponentov nie je uvedený v predchádzajúcich podkapitolách a umožňuje napojenie na centrálny monitoring pomocou protokolu SNMP V3, tak takýto komponent musí byť napojený tiež.

16 Access and identity management

16.1 Všeobecné ustanovenia

Vytváranie nových lokálnych servisných prístupov s oprávnením lokálneho administrátora (OS Windows) je v prípade použitia AD zakázané. Ak je v prípade použitia AD, nutné servisné konto s oprávnením lokálneho administrátora, tak je nutné použiť Group Managed Service Accounts (gMSAs). Vytváranie užívateľských lokálnych prístupov je prípade použitia AD zakázané. Heslá do zabudovaných lokálnych prístupov musia byť pred odovzdaním diela zmenené tak, aby ich jediným držiteľom bola zodpovedná osoba v MHTH. Dodávateľ nesmie mať po odovzdaní projektu prístup k týmto heslám. Vyžaduje sa princíp RBAC (Role-based access control), teda vytvárania rolí na základe špecifických požiadaviek na prístupové oprávnenia pre každú rolu zvlášť tak, aby každý užívateľ mal iba ten level oprávnení potrebných na vykonanie vyžadovaných pracovných činností.

16.2 Vytváranie používateľov a skupín v AD

Všetci používatelia a role v AD sú vytvárane zástupcom MHTH na základe požiadaviek dodaných zo strany dodávateľa, ktoré musia zodpovedať bezpečnostným štandardom MHTH.

16.3 Autentifikácia používateľov

Autentifikácia používateľov dodávaných systémov musí byť vykonávaná centrálne za pomoci Active Directory, ktoré určí MHTH. Všetky systémy ktoré to umožňujú, a na ktorých sa vyžaduje manažment používateľov musia, pre tento účel, používať Active Directory.

16.4 Autorizácia používateľov

Prístup k informáciám, ktoré dodávaný systém spracováva alebo ukladá musí byť nevyhnutne podmienený autentifikáciou a autorizáciou. Pre autorizáciu k dátam v rámci systému platia nasledovné pravidlá.

Autorizácia používateľov je vykonávaná na základe ich role, ktorú na danom systéme plnia. Tieto role sa delia na systémové a aplikačné role. Minimálne delenie rolí je nasledovné:

- Administrátor operačného systému

  Takýto účet je autorizovaný na vykonávanie administratívnych zásahov do systému. Takýto administrátor nesmie mať oprávnenie spravovať, resp. používať aplikácie, ktoré môžu byť prevádzkované na systéme.

- Používateľ operačného systému

  Táto rola môže byť pridelená používateľovi, ktorý má oprávnenie spravovať súbory a nastavenia aplikácie na úrovni operačného systému. Tento používateľ nesmie mať administrátorské oprávnenia na systém.

- Systémový používateľ

  Táto rola môže byť pridelená používateľovi, na základe ktorého sa v rámci operačného systému alebo v rámci aplikácie spúšťa služba, ktorá vyžaduje neinteraktívnu identifikáciu a autentifikáciu používateľa. Tento používateľ môže mať oprávnenie na vykonávanie administratívnych alebo aplikačných úloh, ktoré sa vykonávajú automaticky. Tento používateľ nesmie byť použitý na interaktívne prihlásenie do systému alebo aplikácie.

- Aplikačný administrátor

  Táto rola môže byť pridelená používateľovi, ktorý má oprávnenie spravovať aplikáciu. Takýto používateľ nesmie mať oprávnenie na bežné používane aplikácie. Taktiež nesmie mať oprávnenie na správu používateľov, rolí a oprávnení v rámci aplikácie

- Aplikačný administrátor oprávnení

  Táto rola môže byť pridelená používateľovi, ktorý má v rámci aplikácie oprávnenie spravovať používateľské účty a role, prideľovať a odoberať oprávnenia pre používateľov a role. Takýto používateľ nesmie mať oprávnenie na bežné používane aplikácie.

- Aplikačný používateľ

  Táto rola môže byť pridelená používateľovi, ktorý aplikáciu používa na účely, pre ktoré bola aplikácia vytvorená. Tento používateľ nesmie mať oprávnenia na správu aplikácie a ani na správu používateľov

Manažment jednotlivých rolí je na základe členstva užívateľských účtov v skupinách Active Directory.

17 Fyzické zabezpečenie a kontrola prostredia

17.1 Fyzické zabezpečenie

Všetky rozvádzače a skrine, v ktorých je umiestnená akákoľvek časť OT systému alebo infraštruktúry musia byť uzamykateľné a musia mať implementovanú signalizáciu prístupu/otvorenia dverí, tak aby bolo možné monitorovať každý prístup. Tato informácia musí byť zaslaná ako aj do lokálneho riadiaceho systému, tak aj do nadradeného riadiaceho systému ako alarm.

17.2 Kontrola prostredia

Všetky rozvádzače a skrine, v ktorých sú umiestnené switche alebo časti riadiaceho systému (riadiace jednotky a pod.) musia mať zabezpečené sledovanie a udržiavane prevádzkovej teploty v rozmedzí 15-35°C počas celoročnej prevádzky pokiaľ nie je výrobcom zariadenia požadovaný prísnejší interval teplôt. Taktiež musí byť zabezpečená ochrana proti vnikaniu prachu do uzatvoreného rozvádzača alebo skrine napríklad použitím vhodných filtrov a tesnení.
Informácia o porušení želaného teplotného rozsahu, poruche senzora a prípadnej poruche chladiaceho/ohrievacieho zariadenia (ak je použité) musí byť zaslaná ako aj do lokálneho riadiaceho systému, tak aj do nadradeného riadiaceho systému ako alarm.