# Mateřská škola, základní škola a střední škola Vyškov, příspěvková organizace, Sídliště Osvobození 681/55, 682 01 Vyškov

# **TECHNICKÁ SPECIFIKACE**

**KYBERBEZPEČNOST**

Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

* 1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
  2. mají plnou záruku od výrobce,
  3. jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
  4. obsahují všechny nezbytné licence na používání příslušného softwaru,
  5. jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
  6. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením výrobce daného zařízení, nebo čestným prohlášením distributora, nelze-li prohlášení výrobce získat.

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

1. **nástroj pro ochranu integrity komunikačních sítí**
2. **nástroj pro ochranu koncových stanic**

**3) nástroje pro ochranu integrity komunikačních sítí**

**4) nástroj pro zajišťování úrovně dostupnosti informací**

* **Server 2 ks**
* **Server BACK UP - 1 ks**
* **BACK UP - časové zámky**
* **Diskové pole**

**5) nástroj pro ověřování identity uživatelů**

# 1) nástroj pro ochranu integrity komunikačních sítí

### FIREWALL – 1KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Provedení | Do racku 1U, včetně montážního kitu |
| Porty | min. 8x GE RJ45 a zaroveň min. 2ks SFP+ port   * Dedikovaný konzolový port – min 1x * USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x * Bluetooth Low Energy (BLE) |
| NGFW | Min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation\_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod. |
| Počet současných spojení | min. 1,5 miliónu |
| Propustnost SSL VPN | min. 1,4 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 25 klientů |
| Propustnost SSL inspekce | min. 2.6 Gbps |
| Propustnost firewallu | min. 27 Gbps pro pakety 512 bytů a větší |
| Propustnost NGFW | min. 2,5 Gbps |
| Propustnost IPS | min. 4.4 Gbps |
| Propustnost detekce škodlivého kódu | min. 2.1 Gbps |
| Logování | min. 7 dnů historie v zabezpečeném cloud prostředí |
| Zabezpečení VPN | Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace |
| Virtualizace | min. 5 virtuálních kontextů |
| Vysoká dostupnost | Podporují režimy Active/Passive i Active/Active se společnou konfigurací v případě zapojení druhého firewallu |
| Dualstack | podpora současného běhu IPv4 a IPv6 |
| Aplikační kontrola | detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S, …) |
| Antivir | Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd) |
| Kategorizace a blokace provozu | založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne |
| Antispam | antispamová a antivirová inspekce elektronické pošty |
| Sandbox | Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky) |
| Aktualizace | automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení |
| Ověřování uživatelů | LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu |
| Management a monitoring | HTTP/S, SSH, SNMP, syslog |
| Záruka | min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalvare, antispam, aplikační kontrola) |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### 2) nástroj pro ochranu koncových stanic

### Ochrana koncových stanic a SVR – 53KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| ANTIVIROVÉ ŘEŠENÍ PRO KONCOVÉ BODY A SERVERY | * - Podporované klientské platformy - OS: Windows, Linux, MacOS, Android, vše v českém jazyce * - Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. * - Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall. * - Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. * - Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému * - Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. * - Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:   o síťové protokoly,  o Flash Player,  o Javu,  o Microsoft Office,  o webové prohlížeče,  o e-mailové klienty,  o PDF čtečky…   * - Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě. * - Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…). * - Anti-phishing se schopností detekce homoglyph útoků. * - Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování. * - Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. * - Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. * - Kontrola souborů při zapisování na disku a extrahování archivačních souborů * - Detekce s využitím strojového učení. * - Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur. * - Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni. * - Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací. * - Lokální sandbox * - Modul behaviorální analýzy pro detekce chování nových typů ransomwaru * - Systém reputace pro získání informací o závadnosti souborů a URL adres. * - Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur. * - Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému. * - Skenr firmwaru BIOSu a UEFI. * - Skenování souborů v cloudu OneDrive. * - Podpora odečítače obrazovky pro zrakově postižené * - Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent * - Funkcionalita pro klienty MacOS – Personal Firewall, Device control, autoupgrade * - Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek * - Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem * - Podpora automatického vytváření dump souborů na stanici na základě nálezů * - Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze) * - Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). * Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví * Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP * Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích |
| INTEGROVANÁ CLOUDOVÁ ANALÝZA NEZNÁMÝCH VZORKŮ | * Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě * Sandbox umožňující spuštění vzorků malwaru pro:   Windows,  Linux   * Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů * Analýza neznámých vzorků v řádu jednotek minut. * Reporty poskytují i nízkoúrovňové informace o vzorku - informace o konkrétním problematickém chování, detailní informace o procesech, API * Optimalizace pro znemožnění obejití anti-sandbox mechanismy. * Schopnost analýzy rootkitů a ransomwaru. * Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. * Řešení pracuje s behaviorální analýzou. * Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru * Manuální odeslání vzorku do sandboxu. * Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu. * Neomezené množství odesílaných souborů. * Veškerá komunikace probíhá šifrovaným kanálem. * Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu * Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.) * Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB. |
| ŠIFROVÁNÍ CELÝCH DISKŮ | * Podpora platforem Windows a MacOS * Správa skrze centrální management * Unikátní technologie pro platformu Windows (nevyužívá se BitLocker) * Podpora Pre-Boot autentizace * Podpora TMP modulu * Podpora Opal samošifrovacích disků * Možnost definovat počet chybně zadaných pokusů * Možnost definovat složitost a délku autentizačního hesla * Možnost omezit platnost autentizačního hesla * Podpora okamžitého smazání šifrovacího klíče a následné uzamčení počítače * Recovery z centrální konzole |
| EDR ŘEŠENÍ | * - Možnost provozu centrálního serveru on-premise na platformě Windows Server   Možnost provozu s databázemi:   * MS SQL * MySQL. * - Možnost provozu v offline prostředí. * - Možnost logování činností administrátora * - Podpora EDR agenta pro prostředí Windows, Windows server, macOS a linuxové distribuce * - Možnost autentizace do managementu EDR pomocí 2FA   Možnost řízení managementu EDR a EDR agentů prostřednictvím API, a to jak pro:   * Přijímání informací z EDR serverů/agentů * Zasílání příkazů na EDR servery/agenty   EDR řešení podporuje vzdálené pouštění příkazů přímo z EDR konzole. U jednotlivých OS požadujeme plnou podporu funkcionalit:   * Powershell u OS Windows   Vzdálené spouštění příkazů umožňuje vynucení 2FA ověření daného uživatele.   * - Možnost izolace zařízení od sítě prostřednictvím EDR agenta přímo z konzole. * - Možnost tvorby vlastních IoC. * - Možnost škálování množství historických dat vyhodnocených v EDR, až 3 měsíce pro raw-data, 3 roky pro detekované incidenty * - Možnost aktivovat „učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům * Indikátory útoku pracující s behaviorální detekcí. * Indikátory útoku pracující s reputací. * Řešení umožnuje analýzu vektorů útoku.   Schopnost detekce:   * škodlivých spustitelných souborů * skriptů, * exploitů, * rootkitů, * síťových útoků, * zneužití WMI nástrojů, * bezsouborového malwaru. * Pokusů o dumpování přihlašovacích údajů uživatele * Schopnost detekovat laterální pohyb útočníka. * Schopnost ukončit infikovaný proces. * Možnost ruční analýzy procesů veškerých spustitelných souborů a DLL knihoven. * Možnost náhledu na spuštěné skripty použitých v daném incidentu * Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR * Možnost vytváření automatizovaného response úkonu v podobě izolace stanice, blokace konkrétní hash, odhlášení uživatele, restartování počítače pro jednotlivá detekční pravidla. * Možnost automatického vyřešení incidentu definovaných administrátorem * - Schopnost prioritizace vzniklých incidentů. * - Schopnost stažení problémového souboru. * - Schopnost zobrazení detekcí provedených antimalware produktem. * - Řešení je schopno generovat tzv. forest / full execution tree model. * - Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty. * - Provázání s technikami popsanými v knowledge base MITRE ATT&CK. * - řešení umožňuje fungovat v offline režimu, a to konkrétně jeho detekční pravidla + předem definované komplexnější incidenty/set detekčních pravidel po sobě jdoucích. * - Průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta * - Možnost definice vlastních komplexních „incidentů“ spojující v chronologickém pořadí detekci vybraných událostí * - pokročilý detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního detekčního mozku výrobce * - možnost exportu raw dat (veškerých dat) na externí úložiště, např. Azure Blob * - Možnost definice kontrolního součtu ve formátu SHA256 * - možnost filtrování určitého typu dat zpracovávaného a odesílaného z klientské stanice/server do centrální správy. * - u detekčních pravidel možnost definovat jako automatickou součást pravidla/remediace odeslat soubor na analýzu do cloudového sandboxu výrobce |
| MANAGEMENT KONZOLE PRO SPRÁVU VŠECH ŘEŠENÍ V RÁMCI NABÍZENÉHO BALÍKU | * - Webová konzole. * - Možnost instalace na Windows i Linux. * - Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box. * - Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. * - Možnost probuzení klientů pomocí Wake On Lan. * - Možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin. * - Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta * - Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu). * - Administrace v nejpoužívanějších jazycích včetně češtiny * - Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). * - Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA. * - Informace o aktuálně přihlášených uživatelích na daném zařízení * - Podpora štítků/tagování pro snazší správu a vyhledávání * - Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. * - Vzdálené získání zachyceného škodlivého souboru z klienta. * - Detekce nespravovaných (rizikových) počítačů komunikujících na síti. * - Instalace a odinstalace aplikací 3. stran. * - Vyčítání informací o verzích softwaru 3. stran. * - Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…). * - Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. * - Vzdálená odinstalace antivirového řešení 3. strany. * - Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. * - Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy * - Dynamické skupiny musí umět fungovat i v konkrétních časových slotech a uplatňovat podporované klientské úlohy * - Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy). * - Podpora SNMP Trap, Syslogu a qRadar SIEM. * - Podpora instalace skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…). * - Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu. * - Reportování stavu klientů chráněných jinými bezpečnostními programy. * - Schopnost zaslat reporty a upozornění na e-mail. * - řešení umožňuje odesílat notifikace o vybraných událostech prostřednictvím tzv. webhooků * - Možnost integrace s řešením třetích stran podporující MDM funkcionalitu (např. MS intune, Workspace One) * - Možnost definice kontrolního součtu ve formátu SHA256 * Možnost řízení managementu konzole a jeho komponent prostřednictvím API, a to jak pro: * Centrální správu samotnou * Komponenty antimalware řešení, jeho správy, politik a nastavení * EDR řešení, * Možnost exportu informací o detekcích, incidentech * Možnost úpravy detekčních pravidel EDR * správy zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů   Přidání zařízení do vzdálené správy pomocí:   * o synchronizace s Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů * o ruční přidání pomocí dle IP adresy nebo názvu zařízení, * o pomocí síťového skenu nechráněných zařízení v síti. |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### 3) nástroje pro ochranu integrity komunikačních sítí

## aktivní prvky – POE 48port – 3KS + MINIGBIC 4KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Základní vlastnosti | * Záruka výrobce na výměnu vadného HW platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení * Podpora výrobce pro řešení technických problému platná po celou dobu životnosti zařízení, minimálně 5 let od ukončení prodeje daného zařízení s dostupností 24/7 v případě zaplacené podpory výrobce. * Pravidelné a automaticky instalované bezpečnostní a funkční aktualizace sítových prvku po celou dobu platnosti placené podpory výrobce. * Veškerá konfigurace a monitoring všech síťových prvků, které jsou předmětem poptávky, musí probíhat jak centralizovaně, a to buďto pomocí samostatného centralizovaného switch kontroléru od stejného výrobce, nebo prostřednictvím cloudové webové aplikace nebo případně lokálně na daném zařízení přes příkazovou řádku/webové rozhraní daného přepínače. * Centrální administrativní rozhraní je kompatibilní pro přepínače i firewall * Automatická karanténa připojených koncových zařízení na základě detekce bezpečnostní hrozby řídícím NGFW. |
| Technické požadavky na agregační přepínače LAN | • L2 přepínač  • Rackmount provedení pro 19’’ rozvaděč  • Rozměr 1 RU  • 48x GE RJ45 portů celkem z toho všech 48 portů podporující PoE/PoE+ (802.3af/at)  • 4x 10GE SFP+ porty  • 1x RJ45 Sériový port pro připojení konzole  • Minimální výkon PoE/PoE+ 740W  • Minimální kapacita přepínání 170 Gbps  • Minimální paketový výkon přepínače 250 Mpps  • Minimální počet záznamů MAC tabulky 32 000  • Minimální počet MST Spanning tree instancí 15  • Packet buffer minimálně 2MB  • Maximální hloubka přepínače: 33 cm  • Zdroj napájení integrovaný v těle přepínače  • Airflow – Side to back |
| Funkční požadavky | * Podpora IEEE 802.3ad * Podpora IEEE 802.1q * Podpora IEEE 802.1ab * Možnost propojení s prvkem podporující IEEE 802.1s * Podpora IEEE 802.1w * Podpora ACL IPv4 * Podpora QoS pro IPv4 včetně 802.1p * Podpora 802.1x * Podpora MAB * Podpora Radius CoA * Podpora Radius Accounting * Podpora ARP inspekce * Podpora IGMP a DHCP snooping * Podpora Jumbo Frame o velikosti alespoň 9000B * Podpora SPAN * Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS * Podpora REST API pro konfiguraci a monitoring prvku * Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů * Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN |
| MINIGBIC – 4KS | * 10G SFP+ Transceiver SM |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

WIFI – 20KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Základní vlastnosti | * Formát AP: indoor s interními anténami v katefgorii WiFi 6E * WiFi s 3 rádii a 2 spatial streams * Příslušenství k montázi na zeď/strop/T-Rail * Počet rádií: minimálně 3 pro přenos v pásmech 2,4 a 5GHz a 5 GHz/ 6 GHz/skenovací rádio * Minimálně 2x2 MIMO * Dedikované rádio pro analýzu okolního provozu * Dedikované Bleutooth/ZigBee rádio pro lokalizační služby * Současná podpora 2,4 GHz, 5GHz a 6GHz pásma * Podpora standardů 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, * 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, * 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, * 802.3at, 802.3az, 802.3bz * 2x 10/100/1000 Base-T RJ45 uplink porty s možností sestavení LAG, min. jeden z portů podporuje i 2.5 GbE * 1x USB 3.0 * 1x seriový port * Počet SSID: min. 8 per rádio * Cellular Co-existence * Podpora BSS Coloring * Podpora TWT (Target Wake Time) * Spektrální analýza přímo na AP * Možnost zachytávání paketů na AP pro jejich analýzu * Provoz min. dvou rádií při napájení pomocí 802.3af * Obousměrná a výrobcem podporovaná integrace s wireless kontrolérem * Podpora výrobce na 60 měsíců * Kensigton lock * AP umožňují centrální správu jak z cloudu výrobce, tak z centralizovaného nástroje, který umožňuje současnou správu ostatních nabízených prvků stejného výrobce (přepínače, NGFW) |
| Záruka, servis | * HW záruka na 5 let |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

NAC – 1KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| OBECNÉ POŽADAVKY NA PLATFORMU | * Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána) * Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance * Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami * Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné) * Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem * Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky * Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB * Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky. * Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě * Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting * Všechny požadované funkce pokrývá jeden typ licence a je možné doatenčně zvýšit počet licencí v systému * Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů |
| POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ | * Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN) * Možnost detailní profilace připojeného zařízení a klienta a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy a to bez nutnosti dodatečného licencování této funkcionality * Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality * Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu * Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TEAP * Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí stadarttních Radius atributů * Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL * Podpora 802.1x * Podpora MAB autentizace * Podpora tvorby lokálních účtů a lokální autentizace * Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě * Podpora funkce RADIUS proxy * Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence * Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP * Podpora captive portálů v rámci autentizační brány s plně editovatelným prostředí * Podpora tzv. sponozorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email * NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovní přístupové vrstvy v případě zjištění bezpečnostního incidentu * Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty * Podpora integraace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW * Podpora alespoň RSSO komunikace s NGFW * Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele |
| POŽADAVKY NA ENDPOINT COMPLIANCE | * Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici * Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě) * Kontrola stavu AV na stanici * Kontrola stavu registrů * Kontrola existence konkrétních souborů v lokálním filesystému * Ověření domény * Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, * Ověření verze a patch levelu operačního systému * Podpora sběru informací o instalovaných aplikacích na endpointech * Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál * Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance |
| AUTOMATIZACE | * Možnost definovat playbook, nativně v GUI, který bude vykonávat automatické akce na základě definované události a následné akce dle aktuálního stavu (minimálně v podobě blokace portu, změny L2 segmentu, aplikace skriptu) * Řešení je možné obsluhovat pomcí výrobcem popsaných API volání * Možnost automatické tvorby tiketů v systému ServiceNow na základě definované události |
| REPORTING | * Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování |
| NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ | * Možnost napojení autetntizační brány na SMS nebo email bránu promocí konektoru přímo z GUI |
| POŽADAVKY NA LICENCE A PODPORU VÝROBCE | * záruka 3 roky v režimu 24x7 od výrobce řešení * Licence pro min. **500** endpointů |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

Analýza síťového provozu – 1KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Základní vlastnosti | **Systém pro analýzu síťového provozu**   * Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. * Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. * Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu. * Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. * Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému. * Aktualizace systému musí být možné provádět uživatelsky v off-line režimu.   **Zpracování a ukládání síťových toků**   * Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. * Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření. * Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 6 měsíců složené z SSD nebo NVMe disků. * Analýza aplikačních a systémových logů * Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.   **Uživatelské rozhraní**   * Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů. * Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně: * granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute), * granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), * vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, * vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.   **Automatické hlášení (alerty) a reporting**   * Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. * Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému. * Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.). * Je požadováno vytváření automatizovaných reportů v českém jazyce.   **Integrace systému**   * Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně: * syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat) * přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní * export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP * integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft Active Directory * integrace s firewallem pro automatické a manuální reakce vyvolané systémem   **Podpora EDR**   * Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce. |
| *Dodavatel stručně popíše způsob naplnění jednotlivých požadavků základních vlastností* |  |
| Požadavky na architekturu nasazení | * Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“. * Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap. * Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod. * Požadavky pro pokrytí IT prostředí * Je požadován 1x HW datový kolektor/sensor umožňující trvalý průtok 500Mbps pro alespoň 1500 monitorovaných IP adres s monitorovacím rozhraním 4x 1GbE. * Na zařízení je požadována dostupná historie dat minimálně 6 měsíců. |
| *Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na architekturu nasazení* |  |
| Požadavky na schopnost detekce bezpečnostních událostí | **Monitorování zařízení, segmentů sítě a využívaných síťových služeb**   * Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:  1. změna IP/MAC adresy hosta, 2. duplicitní IP/MAC adresa, 3. změna VLAN, 4. vytvoření nové podsítě, 5. připojení nového zařízení, 6. použití nebo vznik nové služby, 7. nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného komunikujícího zařízení, 8. přístup nového zařízení ke službě či zařízení 9. ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení.  * Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.   **Samostatné učení behaviorálních aktivit a detekce anomálií**   * Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. * Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:  1. odchylku od modelu pro přenos dat, toků a paketů, 2. odchylku od modelu pro počet komunikačních partnerů, 3. odchylku od modelu entropie na komunikačních portech, 4. odchylku od modelu pro počet síťových toků a využitých síťových služeb, 5. odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).  * Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.   **Identifikace neznámých hrozeb a podezřelých chování**   * Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:  1. průzkumné aktivity v síti, 2. detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, 3. detekce repetitivních vzorců chování na síti, 4. detekce botnetů a ovládání kompromitované stanice, 5. detekce příznaků těžení kryptoměn, 6. útoky hrubou silou a enumerace dat, 7. rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.   **Detekce na základě databáze známých hrozeb**   * Systém musí být schopen identifikovat hrozby a reportovat události na základě  1. detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik, 2. reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.  * Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb. * Uživatel musí být schopen importovat vlastní záznamy. * Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace. * Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc). * Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. * Příklad možné syntaxe detekčního pravidla: * alert tcp $HOME\_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”;)   **Analýza šifrované komunikace**   * Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.   **Asistované učení**   * Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:  1. IP adresa, 2. MAC adresa, 3. hostname, 4. segment sítě / podsíť, 5. lokalita – ASN, země apod. 6. směr komunikace – určení klienta, nebo serveru, 7. detekovaná událost – kategorie, název apod. 8. použité služby, protokolu, portu, 9. libovolné kombinaci výše popsaných.   Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii. |
| *Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na schopnost detekce bezpečnostních událostí* |  |
| Požadavky na zajištění síťové viditelnosti | **Vyhledávání, filtrování a vizualizace dat**   * Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. * Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:  1. podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN, 2. prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.  * Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů. * Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. * Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS. * Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry. * Systém musí umožnit uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi; využitím uživatelského datového filtru modifikovat vizualizační pohledy.   **Kontextuální informace**   * Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace:  1. jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie 2. hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu 3. IP geolokace 4. IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá 5. historie použitých MAC adresa a výrobce zařízení 6. operační systém a jeho historie na zařízení 7. uživatelem zadané poznámky a informace k zařízení 8. automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. 9. seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat. 10. seznam detekovaných bezpečnostních a provozních událostí daného zařízení.   **Zaznamenávání, ukládání a zpětná analýza plného provozu**   * Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací. * Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru. * Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru. |
| *Dodavatel stručně popíše způsob naplnění jednotlivých požadavků na zajištění síťové viditelnosti* |  |
| Další požadované oblasti využití | **Monitorování politik kybernetické bezpečnosti**   * Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:  1. monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase. 2. detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. 3. Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: 4. uživatelem definované podsítě na základě rozsahů IP adres 5. uživatelsky libovolně definovaných skupin zařízení 6. automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.   **Management bezpečnostních událostí a incidentů**   * Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:  1. spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele, 2. jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, 3. možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.), 4. možnost exportování dat do emailu, csv, pdf, syslogu a podobně, 5. možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.   **Detekce úniku dat**   * Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). * Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. * V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:  1. název souboru, 2. velikost souboru, 3. HASH souboru.   **Monitoring výkonu aplikací a sítě**   * Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:  1. přenosová rychlost sítě, 2. rychlost odezvy aplikace, 3. odezva systému z pohledu uživatele.  * Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:  1. všechny porty a služby TCP, 2. pro všechny kombinace služeb a zařízení.  * Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.   **Monitoring cloudových služeb**   * Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. * Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.   **Inventarizace sítě a grafická vizualizace topologie**   * Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení. * Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace. * Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele. * Systém umožňuje všechny inventarizační informace řadit dle různých parametrů. |
| *Dodavatel stručně popíše způsob naplnění jednotlivých požadavků pro další požadované oblasti využití* |  |
| Implementační služby | * Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.   Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele. |
| Záruka | * Záruka 36měsíců. |
| Akceptační podmínky | * Veškeré komponenty systému jsou řádně licencované * Bylo dodáno fyzické zařízení dle požadované technické specifikace. * Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu zadavatele. * Dochází k záznamu flow a zrcadleného provozu, informace jsou dostupné k zobrazení a dalšímu zpracování. * V systému jsou zavedeny všechny zadavatelem dodané podsítě. * Pro všechna zařízení v síti jsou okamžitě dostupné informace o zařízeních (název, mac adresy, IP adresa, uživatele, klientské služby, serverové služby, detekované události, … ) * Systém zobrazuje inventarizovanou grafickou topologii celé sítě, včetně počtu zařízení v jednotlivých segmentech sítě a jejich bezpečnostním rizikem. * Systém graficky znázorňuje skutečně přenesená data (In/Out) filtrovaná podle jednotlivých zdrojů flow nebo fyzických/logických interface. * Byla vytvořena a dodána provozní dokumentace. * Bylo provedeno školení v požadovaném rozsahu |
| Potvrzení | **Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky**   * jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce, * mají plnou záruku od výrobce, * mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce, * obsahují všechny nezbytné licence na používání příslušného softwaru, * jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt * jsou určeny pro provoz v České republice. * Tyto skutečnosti dodavatel doloží potvrzením výrobce nebo oficiálního distributora tohoto zařízení |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

## 4) Nástroj pro zajišťování úrovně dostupnosti informací

### Server 2 ks

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Provedení, příslušenství | * Rackové provedení, min. 1U. * Pro přístup ke všem komponentám serveru není nutné nářadí. * Barevně značené hot-plug vnitřní i vnější komponenty |
| CPU | * Minimálně 2x procesor každý o výkonu minimálně 22000 bodů dle <http://cpubenchmark.net/>, počet jader 8 (z důvodu případných licenčních nákladů) |
| RAM + HDD | * minimálně 256 GB RAM v provedení min. DDR5, min. 5600 MHz * Server musí disponovat alespoň 10x diskovou hotswap šachtou pro disky 2,5”, přístupnou zpředu. Požadujeme osazení min. dvěma SSD s kapacitou alespoň 480GB/KS s minimálně SATA 6Gbps rozhraním, min. 1DWPD |
| Vlastnosti | * typu SAS12 * podpora hot-plug disků SAS, SSD i SATA * podpora min. RAID - 0, 1, 5, 6, 10, 50, 60 * Cache řadiče alespoň 8GB se zálohováním proti výpadku napájení na dobu min. 72 hodin * Řadič nezabírá volné PCI-e sloty * 4 x 10/25GbE SFP28 * 1x Dual Port 32GB Fibre Channel karta * Redundantní napájecí zdroje 230V, max. 1100W (alespoň Platinum třída podle specifikace 80 Plus) * Možnost provozu při okolní teplotě stabilně až do 40°C (provoz chlazení čerstvým vzduchem) * 1 x přední, 2x zadní a 1x vnitřní USB port (alespoň jeden zadní a vnitřní s podporou USB3.0) * Interaktivní LCD display indikující základní informace o systému (min. IP adresa, model, chybové stavy, atd.), možnost nastavení IP konfigurace a čtení chybových stavů z out-of-band managementu, bez potřeby připojení monitoru a klávesnice * Dedikovaný RAID slot pro RAID kartu * OCP 3.0 slot * Zásuvné ližiny pro rack * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * VMware ESX 6.7 až 8.0 * RedHatEnterprise Linux 7 * RedHatEnterprise Linux 8 * RedHatEnterprise Linux 9 * SUSE Linux ES 15 * Ubuntu 20.04 LTS * Ubuntu Server 22.04 LTS |
| Management | * Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti: * web GUI a dedikovaná IP adresa, dedikovaný management LAN port s podporou VLAN * SW LAN adaptér pro management mapovaný prostřednictvím z předu přístupného USB portu, podpora přímého připojení USB kabelem z notebooku správce nebo servisního technika (není nutné zpřístupňovat management LAN) * Agent-less hardware FW update vč. možnosti rollback při neúspěchu * Podpora asistovaného OS Deploymentu * LifeCycle Log * sledování hardwarových sensorů (teplota, napětí, stav, chybové sensory) * erroralerty (server reset, kritické sensorové hodnoty, atd.) za použití email traps, paging, atd. * možnost failoveru management LAN portu na jinou síťovou kartu na desce serveru (LOM) * podpora IPv6 * podpora WS-MAN/SMASH-CLP * plná podpora a IPMI funkcionalita * vestavěný Unified Server Configurator GUI (není třeba asistenční/driverové nebo HW-test CD/DVD) * vzdálená konfigurace RAID, přímo v OOB managementu * server remote reset, reboot, power-on/off/cycle * power management a powercaping * integrace managementu do ActiveDirectory a dvoufaktorováauthentikace (TFA), encryption) * podpora RemotevirtualSerial support * BIOS recovery * Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru * Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashována proti zneužití (zerotouchdeployment) * Management serveru ukládá nastavení komponent do vyhrazené paměti, která je neoddělitelnou součástí chassis. Tato konfigurace je pak použitelná po výměně kterékoliv HW komponenty * Interaktivní čelní informační panel. Panel musí umožňovat kontrolu a nastavení parametrů out-of-band vestavěné správy systemu, včetně přiřazení IP adres a přístupu do HW logu * management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích |
| Záruka, servis | * Záruka na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, možnost rozšíření záruky min. na 7 let. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů adresně pro konkrétní zadané sériové či produktové číslo každého serveru. Možnost provázání managementu serveru pro online spojení technickou podporou výrobce a automatickým otevíráním servisních požadavků včetně automatického odeslání HW a OS logů pro následný troubleshooting proces. |
| Kompatibilita | * Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

SERVER - virtulizační platforma

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Funckionalita umožňující bezvýpadkovou migraci virtuálních strojů mezi jednotlivými fyzickými serverovými hostiteli za provozu zajišťující tak plynulou správu a údržbu IT * Funkcionalita, která automaticky nastartuje virtuální stroje při výpadku fyzického serveru na jiném produkčním serveru ze společného diskového prostoru nebo opětovně restartuje dotčený virtuální stroj např. při pádu OS * Funkcionalita, která bude umožňovat za běhu přidávat CPU a paměť virtuálním strojům bez jakéhokoliv přerušení provozu * Rozhraní umožňující zálohovacímu SW třetí strany provádět konzistentní plné, rozdílové a přírůstkové zálohy * Podpora operačních systémů Windows 2016 a novější, Linux * Licence musí pokrývat minimálně 32CORE (dva fyzické servery) s možností dalšího rozšíření |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

SERVER OS + CAL

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | 2 ks licencí 64-bitového serverového operačního systému v aktuální verzi   * Podpora min. 64 procesorových socketů * Podpora běhu v on-premise, hybrid a cloudovém prostředí * Podpora TPM 2.0 čipů * Podpora ochrany firmware před neoprávněným přepsáním * Podpora replikace úložišť * Vestavěná technologie serverové i desktopové virtualizace * Nativní podpora virtualizace sítí * Neomezený počet virtuálních serverů * Počet licencí bude určen počtem jader procesorů ve všech navržených virtualizačních serverech – min 2x16CORE * Operační systém musí být kompatibilní s již provozovanými aplikacemi. Aktuálně zadavatel provozuje operační systémy od společnosti MICROSOFT. * licence pro nabízené operační systémy umožňující využívat těchto systémů minimálně pro **53 zařízení** |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### Diskové pole

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * modulární, minimálně dvou řadičové hybridní diskové pole, řešení je koncipováno jako HW a SW od jednoho výrobce * škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do čtyř řadičové konfigurace a škálování kapacit pomocí expanzních jednotek. Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů * celková velikost cache/RAM v jednom řadiči je minimálně 32GB * celková nativní rozšiřitelnost je minimálně 400 disků, v případě nasazení více řadičů až dvakrát tolik disků. Jak je popsáno výše na řádku výkonnost, nelze toto řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů * podpora 2,5” nebo 3,5” disků technologie SSD/flash včetně rotačních disků a to současně: * enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 1 a vyšší * rotační disky minimálně na SAS 3.0 architektuře * podpora minimálně následujících režimů RAID - 1, 5, 6 nebo DRAID 1, 5 a 6 * minimálně **32TB hrubé kapacity na SSD**, maximální velikost jednoho disku 2TB * Nabízené řešení nesmí přesáhnout 2U * diskové pole obsahuje připojení diskového pole blokovým přístupem minimálně pomocí 16Gbit FC a 10Gbit iSCSI * jsou požadovány min. 4 porty 16Gb FC a 2 porty 10Gb iSCSI na řadič, tzn. minimálně 8x 16Gbit FC portů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole * vytváření virtuálních logických disků * thin provisioning (včetně detekce a reklamace prázdného prostoru) * komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu * deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence * možnost budoucího šifrování dat pro jakýkoliv typ disků a nabízenou kapacitu (licence nemusí být součástí dodávky) * možnosti budoucího nasazení inteligentní správy výkonnostních charakteristik (pro minimálně 3) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD), licence nemusí být součástí dodávky * podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. * Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky) * Microsoft VSS podpora * VMware VAAI, VVOL podpora, dále je požadován VASA provider přímo ve FW nabízeného diskového pole * IBM AIX 7.1, 7.2 a vyšší * IBM VIOS 2.2 a vyšší * Oracle Enterprise Linux 8.x a vyšší * Oracle DB 11.x a 12.x a vyšší * RHEL 6.x a vyšší * VMware 7 a vyšší včetně VAAI a VASA integrací * Windows server 2016 a vyšší * blokový, standard FCP a iSCSI * ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku * řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni * zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole) * možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: * snapshot se po určité době může automaticky stát klonem * inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu * reverzní snapshoty, tzn. lze provést zpětné přesunutí dat z klonu do původního originálního Volume * lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) * interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle * upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum * diskové musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. * vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí * podpora replikace do třetí lokality * SW pro redundantní datové cesty v ceně řešení * Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware * transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možnosti rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit * řešení obsahuje licence na neomezený počet připojení hostitelských serverů * Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních. |
| Záruka, servis | * Minimálně 5 let; v online režimu 24x7 s odezvou tentýž pracovní den včetně SW podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům apod a s garancí opravy do 24hod od nahlášení |
| Certifikace dodavatele, původ zboží | * Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“ |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### Datový rozvaděč centrální - 1 ks

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Datový rozvaděč (RACK) min. 42U/19“/ 1000mm hloubka * včetně vybavení (napájecí panel min 6x zásuvka, potřebná kabeláž, police atp) * Záruka 5LET |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### Datový rozvaděč podružný - 1 ks

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Datový rozvaděč nástěnný (RACK) min. 9U/19“ 390mm hloubka * včetně vybavení (napájecí panel min 6x zásuvka, potřebná kabeláž, police atp) * Záruka 5LET |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

NAS – 1KS + 4KS HDD

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Čtyřjádorový procesor v architektuře x86 64 bit s výkonem min: 4500 bodů v <https://www.cpubenchmark.net/cpu_list.php> * Systémová paměť 16 GB DDR4 2666 MHz * Pozice pro diskové jednotky   + 8 x 3,5" nebo 2,5" SATA HDD/SSD * Kompatibilita diskových jednotek   + 3,5" SATA jednotky pevných disků   + 2,5" SATA jednotky pevných disků   + 2,5" SATA SSD * Diskové jednotky vyměnitelné za provozu * Min.2x Gigabitový Ethernet port (RJ45) * 2x 10GbE SFP+ * USB port   + 2x USB 3.0 * Indikátory LED * Napájení/stav, LAN, HDD 1-8 * Systémové varování * Disky:   + 4x12T HDD stejný výrobce jako NAS a určen pro provoz v NAS   + rychlost přenosu dat 200 MB/s,   + vyrovnávací paměť 256 MB,   + rozhraní SATA III (6 Gb/s),   + rychlost 7 200 ot./min. * Záruka 5LET NBD |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

UPS – 2KS

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce a model | **[bude doplněno dodavatelem]** |
| Parametry | * Min. kapacita výstupního výkonu [W]: 2 700 * Jmenovité výstupní napětí [V]: 230 * 8x IEC 320 C13 (Záložní provoz na baterie) * Topologie: Line interaktivní * Zvukové upozornění: Upozornění na stav, kdy je systém napájen z baterie * Zřetelné upozornění na nízkou kapacitu baterie (dobu musí jít nastavit) * Port rozhraní: RJ-45 10/100 Base-T, RJ-45 Serial, rozšiřující slot, USB * Záruka 5LET |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

### Zálohovací SW – pro 5VM

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce, název, verze a licenční program | **[bude doplněno dodavatelem]** |
| Verze | * Zálohovací software v nejnovější verzi |
| Vlastnosti | * Trvala licence - PERPETUAL * Podporované platformy: VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Red Hat Virtualization, Microsoft Windows, Linux, macOS, IBM AIX, Oracle Solaris. * Podpora cloudových služeb: AWS, Azure, Google Cloud, Microsoft Entra ID, Amazon EC2, RDS, EFS, VPC, Azure VMs, SQL, Files, Google Cloud VMs, Cloud SQL.   Podpora databází a aplikací: Microsoft, Oracle, SAP HANA, PostgreSQL, MySQL,   * Podpora fyzických serverů: Windows, Linux, macOS, IBM AIX, Oracle Solaris. * Podpora nestrukturovaných dat: Objektové úložiště, NAS, souborové sdílené. * Podpora: 24/7/365 produkční podpora během celého období |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

## Implementace

Implementace analýzy síťového provozu:

* Instalace a konfigurace sondy a agentů pro dohled nad celý prostředím
* Instalace a konfigurace systému pro sběr dat a vyhodnocení
* Konfigurace monitorovacích politik na základě doporučení dané technologie a schválené projektové dokumentace
* Ověření monitorovacích pravidel, testovací provoz

Implementace serverového HW:

* Fyzická instalace serverového HW, aktualizace firmware, zahoření, provedení HW testů
* Konfigurace konzole pro vzdálenou správu a management
* Nasazení a konfigurace virtualizace
* Nasazení a konfigurace SW pro replikaci datového úložiště
* Instalace a konfigurace UPS
* Instalace prostředí a virtuálních systémů
* Migrace stávajícího prostředí virtuálních serverů na nový HW

Implementace síťových prvků a FW

* Instalace a fyzické rozmístění switchů a FW v definovaných lokalitách
* Konfigurace bezpečnostních politik na FW
* Konfigurace sítě a jednotlivých segmentů
* Fyzické propojení síťových prvků včetně přepojení celé sítě a klientských zařízení do nové sítě
* Kompletní konfigurace a nastavení NAC

Implementace zálohování a archivace:

* Instalace a konfigurace zálohovacího serveru
* Konfigurace zálohovacích politik pro zálohování serverové infrastruktury
* Ověření zálohovacích pravidel

Provedení závěrečných akceptačních testů, zpracování dokumentace a zaškolení

* Provedení testu výpadku jednoho fyzického nodu
* Provedení testu výpadku napájení
* Provedení testu obnovy libovolného serveru či dat ze zálohy
* Zpracování komplexní dokumentace popisující konfiguraci celého prostředí
* Zpracování komplexní bezpečnostní dokumentace dle požadavků bezpečnostních norem
* Zaškolení interní obsluhy správy sítě, zaškolení obsluhy dohledového centra podpory pro vyhodnocení bezpečnostních událostí.

5) nástroj pro ověřování identity uživatelů

## Pořízení a implementace nástroje pro multifaktorovou autentizaci a SSO

|  |  |
| --- | --- |
| **Parametr** | **Minimální požadavek** |
| Výrobce, název, verze a licenční program serverového OS | **[bude doplněno dodavatelem]** |
| Funkční specifikace | |  | | --- | | Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy rodiny Windows pro minimálně **17uživatelů** | | Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry, případně cloudy. | | Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v místním datovém centru a další virtuální stroj nebo stroje v cloudu, formou SaaS. Minimálně jeden virtuální stroj však musí být provozován v místním datovém centru organizace zadavatele. | | Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění. | | Řešení musí být integrováno na jednu nebo více instancí adresářových služeb Microsoft Active Directory Directory Services (AD DS). Identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Dodané řešení musí být možné integrovat na více samostatných AD DS bez nutnosti jejich propojení pomocí vztahů důvěryhodnosti (trustu), a dále musí být možné řešení integrovat na další adresářové (LDAP) služby jiných výrobců. | | Komunikace mezi jednotlivými komponenty řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna FIPS 140-2 validovaným šifrováním AES 256. | |
| Více-faktorová autentizace | Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty a předměty včetně karet NXP Mifare DesFire, bezkontaktní FIDO2 bezpečnostní karty a kontaktní FIDO2 USB klíče, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu). |  |  |
|  | Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí volitelně umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“). |  |  |
|  | Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, Omnissa Horizon). |  |  |
|  | Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci. |  |  |
|  | Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením minimálně: 1. koncová stanice s OS Windows, 2. mobilní zařízení s OS Android |  |  |
|  | Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních předmětů i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení. |  |  |
|  | Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů během pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským Active Directory účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |  |  |
| Single Sign-On (SSO) | Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací:   * INFORMAČNÍ SYSTÉM ŠKOLY (Bakaláři/EDUPAGE) * IS pro provoz školy (stravování, účetnictví, docházka, ACS atd) * O365   V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 120 a vyšší, Google Chrome verze 120 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolu SAML a pomocí protokolu OpenID Connect. |  |  |
|  | Řešení musí poskytovat funkci Single Sign-On do aplikací (popsaných v předchozím bodu) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |  |  |
|  | Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, dále pro virtualizované aplikace a server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, Omnissa Horizon). |  |  |
|  | Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje do jednotlivých aplikací a systémů musí být šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno. |  |  |
|  | Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP). |  |  |
|  | Řešení musí obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.). |  |  |
|  | Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací. |  |  |
| Čtečky karet – **20KS** | Požadované parametry stacionárních čteček bezkontaktních předmětů:   * Pracovní frekvence: 13,56 MHz * Podpora bezkontaktních karet/předmětů: rodina NXP Mifare® * Rozhraní: připojitelná přes USB * Typ: externí * Napájení: přes USB rozhraní * Formát: stolní * Přenos dat: zabezpečený, přes API (nesmí simulovat klávesnici)   Kompatibilita OS: Windows 10 a vyšší |  |  |
| Autentizační předměty – **17KS** | Požadované parametry bezkontaktních předmětů:   * Pracovní frekvence: 125 kHz a 13,56 MHz * Standardy bezkontaktních předmětů: EM4102/EM4200 a NXP Mifare® minimálně S50, 1kb * Formát: přívěšek (fob)   Provedení: plastový, mechanicky odolný, možnost potisku nebo gravírování |  |  |
| Implementace | Instalace a konfigurace SW pro dvoufaktorovou autentizaci a SSO  Konfigurace přístupu uživatelů  Pilotní ověření a ostré nasazení |  |  |
| Záruky a podpora | Záruka 36měsíců |  |  |
| *Další informace či odkazy dodavatele k nabízenému plnění*  *(nepovinné pole)* |  |

# Společné požadavky pro kapitoly 1 – 5

|  |
| --- |
| **Požadavek** |
| Uchazeč bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Uchazeč pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření. |
| Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu školy (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |
| Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. |
| Zákaznická dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) * informaci o způsobu řešení servisních požadavků |
| Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:   * instalace zařízení do standardní RACK skříně 19“ 42U * implementace Best Practice scénářů pro dané konfigurace * kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace * registrace záruk u výrobců * umístění do racku a zapojení kabeláže vč. jejího označení, * inicializace a konfigurace všech dodaných zařízení * nastavení IP adres * nastavení vysoké dostupnosti * konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu * zapojení do stávající LAN |

# Maintenance

MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenence dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat níže uvedené scénáře:

**Korekční údržba:** Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.

**Adaptivní údržba:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.

**Perfekcionistická údržba:** Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

# Provozní podpora

|  |
| --- |
| **Požadavek** |
| Podpora a servis pro dodaný HW a SW budou poskytovány po dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), nebude-li dohodnuto smluvními stranami jinak – dodavatel bude kalkulovat pro základní technickou podporu **2 hodiny/měsíc.** |
| Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. |
| Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |
| Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením. |
| Technická podpora bude zajišťována těmito způsoby:   * Telefonicky prostřednictvím přiděleného tel. kontaktu. * Prostřednictvím servisního e-mailu. * Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). * Prostřednictvím vzdáleného připojení na PC uživatele / server. |
| Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 16 hod. |
| Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). |
| **Postup při řešení incidentů – SLA**  Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk).  Součástí nahlášení požadavku Zadavatelem musí být:   * popis Incidentu nebo Požadavku, * jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu, * kontaktní osoba.   Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.  **Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 4 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 7:00 a 16:00 v pracovní dny.**  **Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.**  Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.  Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.  Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.  Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.  Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.  V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:   * v případě Incidentu specifikuje příčinu (pokud je známa), * vyzve iniciátora k ověření funkčnosti služby.   Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.  Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.  Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany. Záruky na servisní služby Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré HW opravy po dobu záruky budou bez dalších nákladů pro provozovatele. |