**Technická specifikace plnění**

Obsah

[Popis projektu a společná kritéria 2](#_Toc190929206)

[ID001 - Zabezpečení síťové infrastruktury (NAC/802.1x) + Zabezpečení perimetru NGFW 3](#_Toc190929207)

[Firewall technologie 3](#_Toc190929208)

[implementace 9](#_Toc190929209)

[Aktivní prvky core switch a POE switch 10](#_Toc190929210)

[Management A Obecné technické požadavky 11](#_Toc190929211)

[Core přepínače 13](#_Toc190929212)

[přepínače s 48 porty s PoE 14](#_Toc190929213)

[přepínače s 24 porty s PoE 15](#_Toc190929214)

[implementace 17](#_Toc190929215)

[WiFi přístupový bod 18](#_Toc190929216)

[implementace 21](#_Toc190929217)

[NAC - Realizace nástroje pro řízení přístupu na síti 22](#_Toc190929218)

[implementace 27](#_Toc190929219)

[Analýza a ukládání logů 28](#_Toc190929220)

[implementace 30](#_Toc190929221)

[ID002 - Zvýšení redundance a zabezpečení primárního datového 30](#_Toc190929222)

[Specifikace aplikačního serveru 31](#_Toc190929223)

[SERVER BACKUP 39](#_Toc190929224)

[SERVER BACKUP - časové zámky 47](#_Toc190929225)

[Diskové Pole 55](#_Toc190929226)

[NAS 59](#_Toc190929227)

[UPS - páteřní prvky 60](#_Toc190929228)

[Zálohovací software 61](#_Toc190929229)

[licence 62](#_Toc190929230)

[implementace 63](#_Toc190929231)

[ID003 - Ochrana koncových stanic ENDPOINT 63](#_Toc190929232)

[implementace 65](#_Toc190929233)

[ID004 - Analýza sítového provozu ( ochrana integrity sítě školy) 65](#_Toc190929234)

[implementace 83](#_Toc190929235)

[ID005 - MFA + SSO ochrana identity uživatelů 83](#_Toc190929236)

[implementace 92](#_Toc190929237)

[TISKÁRNA – potisk čipových karet 93](#_Toc190929238)

[Podmínky technické podpory (SLA) a rozvoje řešení 93](#_Toc190929239)

## Popis projektu a společná kritéria

Projekt je koncipován jako ucelené řešení bezpečnosti Zadavatele, nikoliv jako dodávka technologií. Skládá se z následujících provázaných celků:

* Technologie – souhrn řešení pro jednotlivé oblasti bezpečnosti, jež je tvořena konkrétními produkty s výkonnostními parametry.
* Integrace – způsob kooperace a míra provázanosti technologií tak, aby tvořily funkční celek s maximální přidanou hodnotou pro bezpečnost daného prostředí.

Ke každé technologii (aktivitě ) bude vypracován Cílový koncept (Solution Design dokument), který popíše přesné zapojení do stávající infrastruktury, popis systémové konfigurace a provozní konfigurace, včetně integrací a veškeré interoperability s dalšími technologiemi. Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu. Solution Design musí být vzájemně odsouhlasen.

Konfigurační parametry dané definicí procesů a opatření musí být následně aplikovány na všechny technologie v rámci dodávky projektu a dále na existující technologie, které to dovolují (např. komunikační protokoly včetně úrovně zabezpečení, síla hesla, atp.).

DR (Disaster Recovery) plán jakožto jeden z poptávaných výstupů v rámci analytických prací definuje participaci jednotlivých technologií při obnově primárních procesů organizace a určuje formu a rychlost obnovy chodu technologie. Toto musí být reflektováno v popisu obnov technologií a jejich návazností formou detailní provozní dokumentace. Pro účely DR je dále požadováno, aby měly všechny dotčené systémy nastaven adekvátní plán zálohování dat a systémové konfigurace, přičemž bude podle připravených scénářů docházet k pravidelným testům obnovy. Podle typu řešení lze využít formu snapshotu ve virtuálním prostředí, automatického provisioning procesu skrze automatizační scripty a šablony, případně rekonfigurace HW zařízení přes OOB (out of band) rozhraní.

Schopnost dané technologie zajistit konzistenci systémové konfigurace a procesovaných dat při zálohování a obnově je společným požadovaným kritériem pro všechny technologie v rámci dodávky.

Všechny technologie využívající certifikáty musí používat Public Key Infrastructure (PKI) definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60měsíců, a to v režimu NBD 5x8; preferovány jsou trvalé (perpetual) licence, v případě, že trvalá licence není k dispozici, pak subscription s plnou funkcionalitou na dobu minimálně 60 měsíců.

V případě potřeby pořízení dodatečných licencí po dobu nezbytně nutnou pro účely implementace/testování, musí být tyto součástí nabídky dodavatele a řádně naceněny v rámci položkového rozpočtu na separátním řádku jako samostatná položka.

# ID001 - Zabezpečení síťové infrastruktury (NAC/802.1x) + Zabezpečení perimetru NGFW

Základní obecný prvek bezpečnosti je nasazení NGFW, který doposud ve škole není nasazen. Zvýší se obecně bezpečnost pro všechny IS ve škole. NAC + 802.1x zajistí bezpečný provoz všech IS ve škole, díky zcela jasně dané definici přistupujících uživatelů do dítě, dojde ke zvýšení bezpečnosti a ochrany IS. Pro použití IS je zcela kruciální dobré síťové prostředí, které díky nasazení nových aktivních prvků a technologií tento stav zajistí. Páteřní propojení budou posíleny z 1G na 10Gb a uživatelsky na 1Gb

### Firewall technologie

|  |  |  |
| --- | --- | --- |
| **NGFW** | |  |
| Požadovaný počet : 2 |  |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| HW appliance o maximální velikosti 1U |  |  |
| Podpora režimu vysoké dostupnosti active/active a active/passive |  |  |
| Podpora duálního napájení (dva zdroje a přívodní kabeláž je součástí každého dodaného zařízení) |  |  |
| Minimálně 2x 10 GbE SFP+ |  |  |
| Minimálně 8x 1 GbE RJ45 síťová rozhraní |  |  |
| lokální úložiště min 100GB založené na nerotační technologii (SSD disk) |  |  |
| Integrované TPM řešení nebo jeho ekvivalent |  |  |
| Výkonové požadavky | ANO/NE |  |
| Minimální propustnost NGFW pro IPv4 provoz je 25 Gbps (UDP komunikace a paket velikosti 512B) |  |  |
| Kapacita současně navázaných spojení NGFW je alespoň 3 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 120 000 |  |  |
| Propustnost NGFW pro IPSEC VPN je alespoň 25 Gbps bez licenčního omezení počtu sestavených spojení |  |  |
| Propustnost NGFW při zapnuté funkci SSL inspekce využívající IPS inspekci je alespoň 2,5 Gbps |  |  |
| Propustnost NGFW při zapnuté funkci aplikační kontroly je alespoň 6,5 Gbps |  |  |
| Propustnost NGFW při zapnuté funkci IPS inspekce a současném logování provozu je alespoň 4 Gbps |  |  |
| Propustnost NGFW při paralelně provozovaných funkcích stavového FW, IPS, aplikační kontrole a logovaní (obecně popisovaná kombinace funkcí pro NGFW zařízení) je alespoň 2 Gbps |  |  |
| Maximální udávaná latence NGFW (pro UDP provoz nebo průměrná hodnota) je 9 μs |  |  |
| Funkční požadavky | ANO/NE |  |
| Jedná se o řešení dnes označované jako NGFW s integrovanou grafickou a CLI správou umožňující kompletní obsluhu zařízení |  |  |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46 |  |  |
| Podpora režimů explicitní a transparentní proxy |  |  |
| Podpora ověřování identity uživatelů pomocí externích zdrojů s možností napojení na MS Active Directory, LDAP, Radius, Kerberos a práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On |  |  |
| Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů |  |  |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu |  |  |
| Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek |  |  |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); -  SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup. |  |  |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3 |  |  |
| Možnost logické segmentace zařízení s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty. |  |  |
| Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků |  |  |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče. |  |  |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace |  |  |
| Možnost definice zakázaných slov pro vyhledávání na internetu |  |  |
| Schopnost inspekce protokolu QUIC |  |  |
| Možnost využít výrobcem udržovanou databázi internetových služeb při definici bezpečnostní politiky |  |  |
| Podpora kategorizace streamovaných videí a kanálů jako například YouTube |  |  |
| Podpora ZTNA bezpečného přístupu |  |  |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů |  |  |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času |  |  |
| Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být alespoň jeden testovací HW/mobilní token a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN |  |  |
| Podpora režimu nasazení v režimu WCCP (WCCP v2) |  |  |
| Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy |  |  |
| Podpora ICAP rozhraní pro obousměrnou integraci s externími servery |  |  |
| Podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP) |  |  |
| Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6 |  |  |
| Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace) |  |  |
| Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení |  |  |
| Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí |  |  |
| funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně zpracovávat před jeho zahozením |  |  |
| Analýza a zabezpeční DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace |  |  |
| Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu |  |  |
| NGFW může zároveň plnit funkci bezdrátového kontroleru pro bezdrátové přístupové body od stejného výrobce |  |  |
| Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (Round-robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz |  |  |
| Další požadavky | ANO/NE |  |
| Součástí každého dodaného zařízení je podpora výrobce s možností kontaktovat podporu 24/7, vyměnit zařízení v režimu 8x5, licence pro spuštění požadovaných funkcí a výrobce umožňuje zdarma stáhnout VPN klienta kompatibilního s nabízeným NGFW. Vše s platností 5 let. |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **NGFW - implementace** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| fyzická montáž zařízení a propojení do stávající síťové infrastruktury |  |  |
| upgrade firmware na aktuální stabilní verzi doporučenou výrobcem |  |  |
| analýza stavu topologie a současné konfigurace |  |  |
| zapojení do clusteru, včetně možnosti rozložení zátěže na jednotlivé boxy |  |  |
| úprava konfigurace firewallu dle doporučení vyplívající z analýzy |  |  |
| optimalizace bezpečnostních profilů |  |  |
| migrace konfigurace všech funkcionalit implementovaných na stávajících firewallech včetně WiFi kontroléru |  |  |
| konfigurace hloubkové SSL inspekce |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 4 hodin |  |  |
| dokumentace skutečného provedení |  |  |
| rekonfigurace RDS, která byla pozdržena do doby upgrade centrálních firewallů |  |  |
| návrh topologie SD-WAN |  |  |
| konfigurace SD-WAN, dynamic routing (BGP, OSPF) v centru |  |  |
| konfigurace SD-WAN, dynamic routing (BGP, OSPF) vzdálených lokalit, rekonfigurace fw pravidel |  |  |
| implementace management nástroje a napojení všech prvků do managementu |  |  |

### Aktivní prvky core switch a POE switch

Cílem je modernizace počítačové sítě náhradou zastaralých prvků a zvýšení její kapacity doplněním nových prvků. Současně bude pro zvýšení úrovně zabezpečení počítačové sítě implementován systém řízení přístupu k síti NAC na bázi protokolu IEEE 802.1X s napojením na centrální databázi identit Active Directory. NAC bude implementován jako jednotný pro drátovou i bezdrátovou část sítě a dynamické zařazování koncových zařízení do VLAN na základě ověření, typu zařízení apod.

## Management A Obecné technické požadavky

|  |  |  |
| --- | --- | --- |
| **management platforma přepínačů** | |  |
| Obecné požadavky na management platformu přepínače | ANO/NE | Popis splnění požadavku |
| Efektivní správa poptávaných přepínačů z hlediska konfigurace, zabezpečení, logování, atd. pro zefektivnění jejich nasazení a následné správy |  |  |
| Může se jednat o fyzické i VM řešení (pro platformu ESXi) |  |  |
| Management platforma musí umožnit grafické znázornění fyzické a logické topologie spravovaných přepínačů |  |  |
| Management platforma musí umožnit zobrazení a vyhledávání koncových zařízení připojených ke spravovaným zařízením ve fyzické i logické topologii |  |  |
| Management platforma musí umožnit automatickou zálohu konfigurace přepínačů a možnost její migrace na nový přepínač v případě výměny přepínače |  |  |
| Management platforma musí umožnit poskytnout údaje o vytížení jednotlivých přepínačů jak z pohledu CPU a paměti, tak datových toků na jednotlivých portech |  |  |
| Management platforma musí umožnit kompletní síťovou i bezpečnostní konfiguraci přepínačů |  |  |
| Management platforma musí umožnit spravovat karanténu koncových zařízení vyvolanou administrátorem nebo automaticky na základě bepzčnostního incidentu |  |  |
| Management platforma musí umožnit hromadnou správu více přepínačů najednou pro akce jako je například upgrade jejich operačního systému a registrace jejich podpory |  |  |
| Management platforma musí umožnit administrátorský přístup pomocí SSH a HTTPS a také z ní je možné SSH přístup na samotné přepínače |  |  |
| Management platforma musí umožnit použití REST API pro konfiguraci a monitoring systému |  |  |
|  |  |  |
| Management platforma musí podporovat SNMP v1/v2c/v3 a Syslog včetně nativní integrace s poptávaným analyzátorem provozu |  |  |
| Management platforma musí umožnit RBAC pro administrátorský přístup |  |  |

|  |  |  |
| --- | --- | --- |
| **Obecné technické požadavky na poptávané přepínače** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| 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 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 |  |  |

## Core přepínače

|  |  |  |
| --- | --- | --- |
| **přepínače s 24 porty** | |  |
| Požadovaný počet : 2 |  |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| Minimálně 24x 1GE/2.5GE/5GE RJ45 ports a  4x 10GE/25GE SFP+/SFP28 port |  |  |
| Samostatný konzolový port, L3 mgmt port a USB port |  |  |
| Velikost maximálně 1RU |  |  |
| Minimální přepínací kapacita 440 Gbps |  |  |
| Propustnost minimálně 654 Mpps |  |  |
| Velikost bufferu pro zpracování paketů je alespoň 8 MB per port |  |  |
| Minimální velikost MAC tabulky alespoň 62000 záznamů |  |  |
| Minimální počet podporovaných VLAN alespoň 4000 |  |  |
| **Požadavky na podporu přepínačů výrobcem** | ANO/NE | Popis splnění požadavku |
| Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač |  |  |
| Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let. |  |  |

## přepínače s 48 porty s PoE

|  |  |  |
| --- | --- | --- |
| **přepínače s 48 porty s PoE** | |  |
| Požadovaný počet : 7 |  |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| Minimálně 48x10/100/1000 RJ-45, 4x10GE SFP/SFP+ |  |  |
| PoE budget až 740W a podpora 802.3aft/at na všech access RJ-45 portech |  |  |
| Samostatný konzolový port, L3 mgmt port a USB port |  |  |
| Velikost maximálně 1RU |  |  |
| Minimální přepínací kapacita 170 Gbps |  |  |
| Propustnost minimálně 250 Mpps |  |  |
| Velikost bufferu pro spracování paketů je alespoň 2MB per port |  |  |
| Minimální velikost MAC tabulky alespoň 32000 záznamů |  |  |
| Minimální počet podporovaných VLAN alespoň 4000 |  |  |
| **Požadavky na podporu přepínačů výrobcem** | ANO/NE | Popis splnění požadavku |
| Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač |  |  |
| Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let. |  |  |

## přepínače s 24 porty s PoE

|  |  |  |
| --- | --- | --- |
| **přepínače s 24 porty s PoE** | |  |
| Požadovaný počet : 3 |  |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| Minimálně 24x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+ |  |  |
| PoE budget až 370 a podpora 802.3aft/at na všech access RJ-45 portech |  |  |
| Samostatný konzolový port |  |  |
| Velikost maximálně 1RU |  |  |
| Minimální přepínací kapacita 120 Gbps |  |  |
| Propustnost minimálně 180 Mpps |  |  |
| Minimální počet podporovaných VLAN alespoň 4000 |  |  |
| Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky |  |  |
| Proudění vzduchu ze strany do zadní částí přepínače |  |  |
| Bez nutnosti aktivního chlazení přepínače |  |  |
| Podpora duálního firmwaru |  |  |
| Podpora sFlow pro IPv4 |  |  |
| Integrovaný nástroj pro packet capture |  |  |
| **Požadavky na podporu přepínačů výrobcem** | ANO/NE | Popis splnění požadavku |
| Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač |  |  |
| Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **SFP pro poptávané přepínače** | | |  |
| Minimální technické požadavky | | ANO/NE | Popis splnění požadavku |
| Požadovaný počet: Pro propojení nových switchů – minimální počet 30 ks |  | |  |
| 10G SFP+ Transceiver kompatibilní s nabízenými přepínači |  | |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Aktivní prvky core switch a POE switch** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| fyzická montáž zařízení a propojení do stávající síťové infrastruktury |  |  |
| upgrade firmware na aktuální stabilní verzi doporučenou výrobcem |  |  |
| analýza stavu topologie a současné konfigurace |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 2 hodin |  |  |
| dokumentace skutečného provedení |  |  |

## WiFi přístupový bod

|  |  |  |  |
| --- | --- | --- | --- |
| **WiFi přístupový bod** | | |  |
| Požadovaný počet : **25** | |  |  |
| Název a výrobce | **[doplní dodavatel]** | | |
| Minimální technické požadavky | | ANO/NE | Popis splnění požadavku |
| **Požadavky na řízení a správu přístupových bodů** | |  |  |
| Přístupové body musí být centrálně řízeny a spravovány řešením v podobě on-premise nástroje nebo cloud platformy | |  |  |
| Ideálně nástroj centrální správy umožňuje terminovat provoz SSID, v tunelovém režimu, s ohledem na možnou potřebu segmentace drátového a bezdrátového provozu | |  |  |
| On-premise varianta řešení centrální správy může být součástí jiného, v tomto projektu nabízeného, produktu stejného výrobce | |  |  |
| **řešení musí splňovat:** | |  |  |
| automatická nebo manuální autorizace přístupových bodů na základě auto discovery mechanismu | |  |  |
| jednotné management rozhraní, ze kterého lze spravovat přístupové body a případně i další produkty stejného výrobce | |  |  |
| jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID | |  |  |
| jednotné management rozhraní pro zobrazení stavu všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujících SSID včetně síly signálu interferujícího SSID vůči konkrétnímu přístupovému bodu | |  |  |
| možnost vyhledávání, v jednotném management rozhraní, konkrétních připojených zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno | |  |  |
| možnost automatické aktualizace operačního sytému přístupového bude po jeho připojení do sítě | |  |  |
| možnost automaticky registrovat přístupový bude na servisní portál výrobce | |  |  |
| možnost automatické karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti | |  |  |
| možnost hromadného upgrade firmware z jednotného management rozhraní | |  |  |
| Konkrétní technické požadavky na bezdrátový přístupový bod | |  |  |
| Formát zařízení: indoor s interními anténami | |  |  |
| Příslušenství k montáži na zeď/strop/T-Rail | |  |  |
| Počet rádií: minimálně 3 pro přenos v pásmech 2,4, 5 a 6GHz | |  |  |
| Podpora kanálů o šířce 160MHz v 6GHz pásmu | |  |  |
| Podpora BSS Coloring | |  |  |
| Minimálně 2x2 MIMO | |  |  |
| Dedikované Bluetooth/ZigBee rádio pro lokalizační služby | |  |  |
| Možnost provozu dvou rádií v pásmu 5GHz | |  |  |
| Alespoň 1x 10/100/1000 a 1x 1x 100/1000/2500 Base-T RJ45 Base-T RJ45 uplink porty s možností sestavení LAG | |  |  |
| 1x USB port 3.0 a 1x konzolový port RJ45 | |  |  |
| Možnost souběžně provozovat až 16 SSID | |  |  |
| Podpora Cellular Co-existence, TWT (Target Wake Time) | |  |  |
| Možnost spektrální analýzy přímo na AP | |  |  |
| Možnost zachytávání paketů na zařízení pro jejich analýzu | |  |  |
| Podpora napájení pomocí 802.3af | |  |  |
| Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az | |  |  |
| Kensigton lock na samotném AP | |  |  |
| **Požadavky na výrobcem** | | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let. | |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **WiFi přístupový bod** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| Zapojení do centrálního managementu |  |  |
| upgrade firmware na aktuální stabilní verzi doporučenou výrobcem |  |  |
| analýza stavu topologie a současné konfigurace |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 2 hodin |  |  |
| dokumentace skutečného provedení |  |  |

## NAC - Realizace nástroje pro řízení přístupu na síti

Cílem je, aby se k interní síti mohli připojit pouze autorizovaní uživatelé a zařízení, a aby se tak zamezilo nežádoucím připojením k síti. Cílem je zajistit co možná nejsnazší, ale dostatečně robustní, politikou řízený a prosazovaný přístup k síti a jejím zdrojům s ohledem na aktuální stav přistupujícího i již připojeného zařízení.

Centrálně definované politiky budou určovat způsob, typ, místo a rozsah přístupu pro konkrétní skupiny uživatelů a zařízení (případně v kombinaci). 802.1x politika bude řídit nejen přístup pro adekvátně ověřené skupiny uživatelů a kategorie zařízení, ale má být dalším stupněm kybernetické ochrany. Jejím sekundárním úkolem proto bude dohlížet momentální stav již připojených zařízení a bezprostředně reagovat na jeho nežádoucí změnu (např. vypnutí AV ochrany, nebo projev jiné hrozby).

|  |  |  |
| --- | --- | --- |
| **NAC** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| 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 dodatečně 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-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS |  |  |
| Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standartních 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 |  |  |
| Možnost integrace se stávající CA (certifikační autorita) |  |  |
| 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 portál v rámci autentizační brány s plně editovatelným prostředí |  |  |
| Minimálně 5 různých captive portálů |  |  |
| Podpora tzv. sponzorovaného 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 integrace 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 na úrovni 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 |  |  |
| 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 autentizační brány na SMS nebo email bránu promocí konektoru přímo z GUI |  |  |
| POŽADAVKY NA LICENCE A PODPORU VÝROBCE | ANO/NE | Popis splnění požadavku |
| Licence pro min. 1500 endpointů |  |  |
| Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **NAC** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| analýza stavu topologie a současné konfigurace |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 2 hodin |  |  |
| dokumentace skutečného provedení |  |  |

## Analýza a ukládání logů

|  |  |  |
| --- | --- | --- |
| **Analýza a ukládání logů** | | |
| Název a výrobce | **[doplní dodavatel]** | |
| základní technické požadavky | ANO/NE | Popis splnění požadavku |
| nástroj pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů |  |  |
| podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení |  |  |
| virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná alternativa) |  |  |
| možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu |  |  |
| alespoň 5TB alokovatelná kapacita dlouhodobého úložiště logů a alespoň 5GB minimální limit pro množství přijatých logů k analýze za jeden den (možnost navýšení limitů pomocí dodatečné licence) |  |  |
| minimálně 4x vNIC |  |  |
| možnost provozovat poptávané řešení jako prosté uložiště logů z dalších zařízení zákazníka bez jejich další analýzy |  |  |
| možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje |  |  |
| možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení |  |  |
| HTML/CSV/XML/PDF formát generovaných reportů s možností plánování pravidelné automatické tvorby reportů |  |  |
| možnost logické segmentace s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat |  |  |
| musí obsahovat předdefinované vzory reportů a umožňovat úpravu vzhledu generovaných reportů prvky zákazníka (loga, hlavička, …) |  |  |
| možnost zobrazení aktuálních logů z jednotlivých integrovaných NGFW zařízení v reálném čase |  |  |
| možnost zpětného zobrazení a analýzy logů z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb |  |  |
| požadavky na management | ANO/NE | Popis splnění požadavku |
| plnohodnotná správa pomocí grafického rozhraní a CLI |  |  |
| podpora SNMPv2 a SNMPv3 a REST API |  |  |
| samostatná sekce v grafickém rozhraní pro zobrazení zjištěných hrozeb |  |  |
| podpora přijímání syslogů ze zařízení třetích stran |  |  |
| možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením |  |  |
| další požadavky | ANO/NE | Popis splnění požadavku |
| podpora výrobce v režimu 24/7 na dobu min. 5 let |  |  |
| všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let musí být také součástí dodávky |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Analýza a ukládání logů- implementace** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| instalace zařízení a propojení do stávající síťové infrastruktury |  |  |
| upgrade firmware na aktuální stabilní verzi doporučenou výrobcem |  |  |
| analýza stavu topologie a současné konfigurace |  |  |
| akceptační testy a testovací provoz |  |  |
| implementace management nástroje a napojení všech prvků do managementu |  |  |
| implementace nástroje pro bezpečnostní analýzu logů z NGFW zařízení se schopnosti jejich korelace včetně možnosti ukládání logů |  |  |

# ID002 - Zvýšení redundance a zabezpečení primárního datového centra

IS je díky tomu možno provozovat ve vysoké dostupnosti a rovněž jej velmi efektivně zálohovat. Jedná se klíčový IS školy, který naplňuje potřeby žáků v rámci doplňujících služeb školy

## Specifikace aplikačního serveru

|  |  |  |
| --- | --- | --- |
| **Specifikace aplikačního serveru** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Požadovaný počet : 2 |  |  |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| Form Factor a vnitřní uspořádání | 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel. |  |
| CPU | Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. / AMD |  |
| [Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net](https://www.cpubenchmark.net/) |  |
| RAM | 8x 32GB na 5600MHz s možností osazení až 32 slotů. |  |
| Diskový subsystém | Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server disky: |  |
| Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně: |  |
| ·       2x 480GB M.2 SSD NVMe v RAID1 |  |
| Diskový řadič | ·       typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory) |  |
| ·       podpora RAID 0, 1, 5, 6, 10, 50, 60 |  |
| ·       podpora 12Gbps technologie rozhraní disků |  |
| ·       podpora Capacity Expansion (OCE) |  |
| ·       podpora RAID Level Migration (RLM) |  |
| ·       podpora SED disků a SSD disků |  |
| Síťové rozhraní | 1 x 1GbE port Base-T (RJ45) Dual Port |  |
| 1 x 10/25 GbE port Ethernet typu SFP28 Dual Port |  |
| 1 x 10 GbE port typu Base-T (RJ45) Dual Port |  |
| Napájení | Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium) |  |
| Interface | ·       3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0 |  |
| ·       2 x VGA (1 vpředu, 1 vzadu) |  |
| Rozšiřující sloty | ·       Min 3x PCIe Gen4/5 sloty volné pro budoucí použití |  |
| Kolejnice | ·       Zásuvné ližiny s ramenem pro vedení kabelů |  |
| Kompatibilita | ·       Microsoft® Windows Server® 2019/2022, x64 |  |
| ·       SUSE® Linux® Enterprise Server |  |
| ·       Red Hat® Enterprise Linux |  |
| ·       Canonical Ubuntu Server LTS |  |
| ·       VMware vSphere™ |  |
| Operační systém | ·       Windows Datacenter 2022 – licence na všechna jádra |  |
| Management a vzdálená správa | ·       samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru |  |
| ·       s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 |  |
| ·       monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách |  |
| ·       vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP |  |
| ·       management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů |  |
| ·       automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| ·       přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| ·       podpora multifaktorové autentizace, podpora MS AD a generického LDAP |  |
| ·       možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack |  |
| ·       data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace |  |
| ·       podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback |  |
| ·       podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu |  |
| ·       podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) |  |
| ·       management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora |  |
| ·       management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení. |  |
| ·       OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině |  |
| ·       OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home) |  |
| ·       možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| ·       vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| ·       management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru |  |
| ·       licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě |  |
| ·       management umožňuje monitoring spotřeby el. energie na úrovni serveru |  |
| ·       identifikace připojeného vzdáleného uživatele |  |
| ·       vzdálená identifikace serveru |  |
| Bezpečnostní funkce | ·       Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli |  |
| Podpora a servis | ·       Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. |  |
| ·       Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory. |  |
| Prodávající se zavazuje, že zařízení a veškeré jeho komponenty: |  |
| ·       pochází z autorizovaného obchodního kanálu výrobce |  |
| ·       je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení |  |
| ·       je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel |  |

## SERVER BACKUP

|  |  |  |
| --- | --- | --- |
| **SERVER BACKUP** | |  |
| Název a výrobce | **[doplní dodavatel]** | | |
| Požadovaný počet : 1 |  |  |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| Form Factor a vnitřní uspořádání | 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel. |  |
| CPU | Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD |  |
| [Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net](https://www.cpubenchmark.net/) |  |
| RAM | 8x 32GB na 5600MHz s možností osazení až 32 slotů. |  |
| Diskový subsystém | Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server osazený hot-plug disky: |  |
| 3x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive |  |
| Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně: |  |
| ·       2x 480GB M.2 SSD NVMe v RAID1 |  |
| Diskový řadič | ·       typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory) |  |
| ·       podpora RAID 0, 1, 5, 6, 10, 50, 60 |  |
| ·       podpora 12Gbps technologie rozhraní disků |  |
| ·       podpora Capacity Expansion (OCE) |  |
| ·       podpora RAID Level Migration (RLM) |  |
| ·       podpora SED disků a SSD disků |  |
| Síťové rozhraní | 1 x 1GbE port Base-T (RJ45) Dual Port |  |
| 1 x 10/25 GbE port Ethernet typu SFP28 Dual Port |  |
| 1 x 10 GbE port typu Base-T (RJ45) Dual Port |  |
| Napájení | Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium) |  |
| Interface | ·       3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0 |  |
| ·       2 x VGA (1 vpředu, 1 vzadu) |  |
| Rozšiřující sloty | ·       Min 3x PCIe Gen4/5 sloty volné pro budoucí použití |  |
| Kolejnice | ·       Zásuvné ližiny s ramenem pro vedení kabelů |  |
| Kompatibilita | ·       Microsoft® Windows Server® 2019/2022, x64 |  |
| ·       SUSE® Linux® Enterprise Server |  |
| ·       Red Hat® Enterprise Linux |  |
| ·       Canonical Ubuntu Server LTS |  |
| ·       VMware vSphere™ |  |
| Operační systém | ·       Windows Datacenter 2022 – licence na všechna jádra |  |
| Management a vzdálená správa | ·       samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru |  |
| ·       s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 |  |
| ·       monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách |  |
| ·       vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP |  |
| ·       management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů |  |
| ·       automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| ·       přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| ·       podpora multifaktorové autentizace, podpora MS AD a generického LDAP |  |
| ·       možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack |  |
| ·       data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace |  |
| ·       podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback |  |
| ·       podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu |  |
| ·       podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) |  |
| ·       management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora |  |
| ·       management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení. |  |
| ·       OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině |  |
| ·       OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home) |  |
| ·       možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| ·       vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| ·       management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru |  |
| ·       licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě |  |
| ·       management umožňuje monitoring spotřeby el. energie na úrovni serveru |  |
| ·       identifikace připojeného vzdáleného uživatele |  |
| ·       vzdálená identifikace serveru |  |
| Bezpečnostní funkce | ·       Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli |  |
| Podpora a servis | ·       Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. |  |
| ·       Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory. |  |
| Prodávající se zavazuje, že zařízení a veškeré jeho komponenty: |  |
| ·       pochází z autorizovaného obchodního kanálu výrobce |  |
| ·       je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení |  |
| ·       je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel |  |

## SERVER BACKUP - časové zámky

|  |  |  |
| --- | --- | --- |
| **SERVER BACKUP - časové zámky** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Požadovaný počet : 1 |  |  |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| Form Factor a vnitřní uspořádání | 2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel. |  |
| CPU | Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD |  |
| [Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net](https://www.cpubenchmark.net/) |  |
| RAM | 8x 32GB na 5600MHz s možností osazení až 32 slotů. |  |
| Diskový subsystém | Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server osazený hot-plug disky: |  |
| 4x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive |  |
| Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně: |  |
| ·       2x 480GB M.2 SSD NVMe v RAID1 |  |
| Diskový řadič | ·       typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory) |  |
| ·       typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory) |  |
| ·       podpora RAID 0, 1, 5, 6, 10, 50, 60 |  |
| ·       podpora 12Gbps technologie rozhraní disků |  |
| ·       podpora Capacity Expansion (OCE) |  |
| ·       podpora RAID Level Migration (RLM) |  |
| ·       podpora SED disků a SSD disků |  |
| Síťové rozhraní | 1 x 1GbE port Base-T (RJ45) |  |
| 1 x 10/25 GbE port Ethernet typu SFP28 |  |
| 1 x 10 GbE port typu Base-T (RJ45) |  |
| Napájení | Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium) |  |
| Interface | ·       3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0 |  |
| ·       2 x VGA (1 vpředu, 1 vzadu) |  |
| Rozšiřující sloty | ·       Min 3x PCIe Gen4/5 sloty volné pro budoucí použití |  |
| Kolejnice | ·       Zásuvné ližiny s ramenem pro vedení kabelů |  |
| Kompatibilita | ·       Microsoft® Windows Server® 2019/2022, x64 |  |
| ·       SUSE® Linux® Enterprise Server |  |
| ·       Red Hat® Enterprise Linux |  |
| ·       Canonical Ubuntu Server LTS |  |
| ·       VMware vSphere™ |  |
| Operační systém | ·       Windows Datacenter 2022 – licence na všechna jádra |  |
| Management a vzdálená správa | ·       samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru |  |
| ·       s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 |  |
| ·       monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách |  |
| ·       vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP |  |
| ·       management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů |  |
| ·       automatická instalace a obnova SSL certifikátu vestavěného serveru |  |
| ·       přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE |  |
| ·       podpora multifaktorové autentizace, podpora MS AD a generického LDAP |  |
| ·       možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack |  |
| ·       data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace |  |
| ·       podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback |  |
| ·       podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu |  |
| ·       podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) |  |
| ·       management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora |  |
| ·       management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení. |  |
| ·       OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině |  |
| ·       OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home) |  |
| ·       možnost přístupu přes dedikovaný USB port s emulací síťového připojení |  |
| ·       vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| ·       management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru |  |
| ·       licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě |  |
| ·       management umožňuje monitoring spotřeby el. energie na úrovni serveru |  |
| ·       identifikace připojeného vzdáleného uživatele |  |
| ·       vzdálená identifikace serveru |  |
| Bezpečnostní funkce | ·       Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli |  |
| Podpora a servis | ·       Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory. |  |
| ·       Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory. |  |
| Prodávající se zavazuje, že zařízení a veškeré jeho komponenty: |  |
| ·       pochází z autorizovaného obchodního kanálu výrobce |  |
| ·       je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení |  |
| ·       je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel |  |

## Diskové Pole

|  |  |  |
| --- | --- | --- |
| **Pole** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Požadovaný počet : 1 |  |  |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| Typ zařízení | ·        Diskové pole, v provedení do rack 19“ o maximální velikosti 2U. S blokovým přístupem. |  |
| ·        Multikontrolerové řešení s plně redundantní, vysoce dostupnou architekturou bez SPOF (Single Point of Failure), umožňující upgrade FW za provozu, řadiče v režimu Active-Active. S podporou SAS SSD a HDD disků a NL-SAS disků. |  |
| Diskový subsystém | ·        Minimálně osazeno disky 12x 1.92TB 2.5“ SAS SSD min. Disky min DWPD 1. |  |
| ·        Diskové pole musí podporovat výměnu všech HDD za běhu (tzv. hot swap) a podporovat global spare HDD, případně spare prostor |  |
| ·        Celková rozšiřitelnost datového úložiště minimálně na 270 disků, připojením pouze expanzních jednotek pro disky. |  |
| ·        Možnost připojovat expanzní jednotky na disky o velikostech 2,5“ a 3,5“ |  |
| RAID | ·        Diskové pole musí mít podporu pro RAID 1, 5, 6, 10 a distribuovaný erasure coding odpovídající RAID6 |  |
| Počet řadičů | ·        Min. 2 řadiče/kontroléry diskového pole |  |
| Cache | ·        Velikost operační paměti (cache) typu RAM - minimálně 32 GB a současně minimálně 16 GB na řadič pro data. |  |
| Back-end | ·        Typ připojení Back-endu pro expanzní police min. SAS 3.0 12 Gb/s, vyžadovány jsou minimálně dva SAS 3.0, 12 Gb/s porty na každý controller. |  |
| Front-end porty | ·        Počet a typ front-end portů – požadujeme minimálně 4x 32FC per controller. Vyžadujeme podporu přímého zapojení nabízeného pole s nabízenými servery. Součástí nabídky musí být i kompatibilní propojovací transceivery a kabely o minimální délce 2 m min. 2ks na každý server. |  |
| Napájení | 2 redundantní zdroje PDU koncovky |  |
| LUN | ·        Celkový počet LUNů na diskovém poli - min. 500. |  |
| ·        Podpora LUNů o min. velikosti 50 TiB |  |
| Požadované vlastnosti managementu diskového pole | ·        Min. 1ks GE Management port, na řadič |  |
| ·        Grafické uživatelské rozhraní včetně licence pro lokální správu diskového pole a příkazové řádky (CLI), mapování jednotlivých interních rolí a oprávnění na uživatelské skupiny v adresářové službě LDAP, výkonnostní statistiky, které lze exportovat v čitelném formátu (CSV/XML apod.) pomocí CLI nebo GUI |  |
| ·        Možnost zasílat události s různými severitami, které vznikají spontánně uvnitř pole za běžného provozu (např. chybové stavy, přihlášení uživatele apod.), pomocí standardních protokolů SMTP nebo SNMP |  |
| ·        Automatické hlášení poruch a problémů pomocí e-mailu, nebo automaticky na dohled dodavatele přes internet zabezpečeně |  |
| ·        Jednotná grafická konzole pro správu a monitoring serverů i diskového pole, s možností napojení do proaktivního monitoringu s prediktivní analýzou, v cloudového portálu výrobce. Tento portál přístupný i přes mobilní aplikace dostupné pro telefony iOS i Android. Pokud jsou vyžadovány licence musí být součástí řešení, minimálně po dobu platné podpory. |  |
| Funkce a licence | ·        Součástí musí být SW licencovaný v rozsahu pro maximální kapacitu pole, a to včetně rozšiřitelnosti kapacity): |  |
| ·        kompletní správa diskového pole, |  |
| ·        licence pro plně automatický sub-LUN tiering dat s 3 tier architekturou, |  |
| ·        licence pro snapshoty, klony, asynchronní replikaci, šifrování při použití SED disků a SSD cache musí být součástí |  |
| ·        dlouhodobý performance monitoring a reporting, a to až po dobu 6 měsíců, |  |
| ·        Thin Provisioning, |  |
| ·        zástupnost datových cest (multi-path) pokud pole nepoužívá standardní MPIO ovladače, |  |
| ·        kopírování jednotlivých LUNů v rámci pole i mezi jednotlivými diskovými poli, |  |
| ·        minimálně 1024 Snapshotů. |  |
| Záruka | Podpora na 5 let typu 24x7x365 s dobou zahájení opravy do 4h od nahlášení poruchy, oprava v místě instalace serveru, servis je poskytován výrobcem. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla. |  |

## NAS

|  |  |  |
| --- | --- | --- |
| **NAS (backup Office 365)** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| montaz | RACK |  |
| CPU | AMD Ryzen V1500B |  |
| Systémová paměť: | 32 GB DDR4 ECC SODIMM |  |
| Šachty pevného disku: | 8 |  |
| Maximální počet šachet pevného disku s rozšiřující jednotkou: | 12 |  |
| Hot-swap disk: | ano |  |
| Porty: | 4x RJ-45 1GbE LAN Port s podporou funkcí Link Aggregation / Failover 2x USB 3.2 Gen 1 1x eSATA  1x 10GbE  2x PCIe NVMe |  |
| HDD | 4x 16TB, 3.5", SATA, 7200 RPM - podpora vyrobce NAS |  |
| **Požadavky na podporu výrobcem** | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce na 5 let |  |  |

## UPS - páteřní prvky

|  |  |  |  |
| --- | --- | --- | --- |
| **UPS - páteřní prvky** | | |  |
| Požadovaný počet : 2 | |  |  |
| Název a výrobce | **[doplní dodavatel]** | | |
| Technický parametr | | Minimální technické požadavky | Popis splnění požadavku |
| montáž | | RACK |  |
| Kapacita výstupního výkonu [VA]: | | 3000 |  |
| Topologie: | | Line interaktivní |  |
| Typ křivky: | | Sinusoida |  |
| Jmenovité vstupní napětí [V]: | | 230 V |  |
| Typ připojení vstupu: | | British BS1363A, IEC-320 C20, Schuko CEE 7/EU1-16P |  |
| KOMUNIKACE A SPRÁVA | |  |  |
| Port rozhraní: | | RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB |  |
| Ovládací panel: | | diody zobrazují stav: napájení ze sítě : napájení z baterie : vyměnit baterii : přetížen |  |
| Zvukové upozornění: | | Upozornění na stav, kdy je systém napájen z baterie |  |
| **Požadavky na podporu** | | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce na 5 let | |  |  |

## Zálohovací software

|  |  |  |
| --- | --- | --- |
| **Zálohovací software** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Technický parametr | Minimální technické požadavky | Popis splnění požadavku |
| popis | **Min. na úrovni funkcí sw. Veeam** | |
| Zálohování na úrovni hypervisoru per VM | ANO |  |
| Agentové zálohování | ANO |  |
| Počet virtuálních strojů | **20** |  |
| **Požadavky na podporu** | **ANO/NE** | **Popis splnění požadavku** |
| Servisní a uživatelská podpora v délce 5 let |  |  |

## licence

|  |  |  |
| --- | --- | --- |
| **licence** | |  |
| Technický parametr | Minimální počet | Popis splnění požadavku |
| CSP Windows Server 2022 - 1 Device CAL EDU | 200 |  |
| CSP Windows Server 2022 Remote Desktop Services - 1 User CAL EDU | 15 |  |
| CSP Windows Server 2022 Datacenter - 16 Core EDU | licence na všechna jádra nabízených serveru |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Instalace serverové infrastruktury a zálohování** | | |
| Technický parametr | **Specifikace – minimální požadavek zadavatele** | Naplnění požadavku |
| Instalace | Instalace hypervisoru na servery |  |
| Instalace | Konfigurace síťového připojení |  |
| Instalace | Instalace a konfigurace diskového pole, |  |
| Instalace | Nastavení virtuálních strojů, předpokládáme 2xVM na produkčních serverech + virtualizace na backup server |  |
| Instalace | Instalace HDD do NAS, nastavení |  |
| Instalace | Zálohovací plány - návrh a konfigurace |  |
| Instalace | Konfigurace switchů |  |
| Instalace | Rozděleni VLAN |  |
| Instalace | migrace a nastavení |  |
| Instalace | akceptační testy a testovací provoz |  |
| školení | školení administrátorů v rozsahu 4 hodin |  |
| dokumentace | dokumentace skutečného provedení |  |

# ID003 - Ochrana koncových stanic ENDPOINT

v současnosti zalicencováno 120 zařízení stanice/servery licence ESET PROTECT Entry on-prem.

Zadavatel požaduje konkrétní produkt z důvodu zachování kompatibility, resp. navazujícího přechodu na vyšší verzi s funkcionalitou EDR.

ID licence: 33D-FPK-78C.

|  |  |  |  |
| --- | --- | --- | --- |
| **Ochrana koncových stanic a SVR** | | |  |
| Název a výrobce | **[doplní dodavatel]** | | |
| Požadovaný počet : 120 | |  |  |
| Minimální technické požadavky | | ANO/NE | Popis splnění požadavku |
| Správcovská konzole - Kybernetická platforma poskytující přehled o dění v síti a kontrolu nad ní. Může být nainstalována jako cloudové nebo lokální řešení. | |  |  |
| ochrana koncových zařízení | |  |  |
| Antivirus poskytuje ochranu před známými i novými hrozbami. Přístup založený na umělé inteligenci a prevenci | |  |  |
| Ochrana proti síťovým útokům | |  |  |
| Správa zařízení - Umožňuje omezení přístupu neautorizovaných zařízení, jako jsou USB flash disky nebo CD, k citlivým datům | |  |  |
| Anti-phishing | |  |  |
| Ochrana serverů - Ochrana dat v reálném čase pro všechny běžné servery. | |  |  |
| Ochrana mobilních zařízení proti hrozbám - mobilní zařízení s Androidem a iOS. Funkce antimalware, anti-theft a MDM. | |  |  |
| Šifrování celého disku | |  |  |
| Pokročilá ochrana před hrozbami - Proaktivní cloudová ochrana proti ransomwaru a dosud neznámým hrozbám se schopností automatické nápravy. | |  |  |
| Rozšířená detekce a reakce - umožňuje aktivní detekci hrozeb, efektivní identifikaci neobvyklého chování v síti a včasnou nápravu. Nástroj podporující využití XDR v cloudu. | |  |  |
| **Požadavky na podporu**  **výrobcem** | | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce na 5 let | |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Ochrana koncových stanic a SVR** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| migrace a nastavení |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 2 hodin |  |  |
| dokumentace skutečného provedení |  |  |

# ID004 - Analýza sítového provozu ( ochrana integrity sítě školy)

Analýza sítového provozu poskytne pro ochranu tohoto IS úplný a přesný přehled o dění ve vaší síti. V případě ohrožení provozu tohoto IS, lze tuto hrozbu detekovat. Použití této nejmodernější techniky detekce a dojde k bezprostřednímu řešení známých i neznámých hrozeb a problémů, kterým by mohla být síť vystavena. Analýza sítového provozu používá pokročilé techniky umělé inteligence a strojového učení, aby odhalil nebezpečí a slabá místa v infrastruktuře, která nelze detekovat klasickými bezpečnostními produkty. Zastaví útoky na školní síť, pomůže i obecně s moderními formami kybernetické kriminality i s nedostatky vedoucími k nestabilitě sítě. Jeho nasazení předchází finančním škodám na nedostupnosti IS, časovým ztrátám a zvýšeným nákladům na lidské zdroje či externí služby

|  |  |  |
| --- | --- | --- |
| **Analýza sítového provozu** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | Technický parametr | Popis splnění požadavku |
| Požadavky na monitorovací systém | | |
| Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream, cloudové FlowLogy). | Ucelený, škálovatelný NetFlow/IPFIX/FlowLogs monitorovací systém |  |
| Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s. | Podpora infrastruktury |  |
| Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. | Decentralizovaný monitoring lokalit s centrální správou |  |
| Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce). | Nezávislost na stávající infrastruktuře |  |
| Bezztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream). | Bezztrátový sběr flow statistik z více zdrojů |  |
| Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. | Ukládání statistik a vyhodnocování bezpečnostních hrozeb |  |
| Plná zákaznická podpora v českém jazyce. | Zákaznická podpora |  |
| Systém ověřený instalacemi v rozsáhlé síťové infrastruktuře (datové linky 10 Gbps a výše). Minimálně 10 instalací ve třech zemích světa. | Reference |  |
| Otevřené rozhraní a veřejně dokumentované API s možností integrace nástrojů i třetích stran. | Rozhraní pro integraci nástrojů třetích stran |  |
| Monitorovací systém sleduje aktivní relace všech uživatelů a umožnuje tyto relace ukončit. | Správa aktivních relací uživatelů s monitorovacím systémem |  |
| Během aktualizace systém zabraňuje uživatelským akcím, které by mohly narušit proces aktualizace. | Uzamčení rozhraní během aktualizací |  |
| Požadavky na kolektory NetFlow dat | | |
| Minimální technické požadavky | Technický parametr | Popis splnění požadavku |
| Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce. | Ukládání flow statistik |  |
| Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků. | Granularita vizualizace |  |
| Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP. | Podpora standardů datových toků |  |
| Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. | Hlavní funkcionalita |  |
| Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje. | Instalace |  |
| Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace. | Konfigurační šablony |  |
| Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | Zabezpečená vzdálená správa |  |
| Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. | Správa uživatelů a přístupových práv |  |
| Podpora autentizace vůči LDAP (Active Directory). | LDAP autentizace |  |
| Podpora autentizace vůči TACACS+. | TACACS+ autentizace |  |
| Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | Dohled |  |
| Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | Časová synchronizace |  |
| Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. | Podpora příkazové řádky |  |
| Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | DNS cache |  |
| Podpora IPFIX položek proměnlivé délky. | Podpora položek proměnlivé délky |  |
| Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions. | Podpora IPFIX rozšíření jiných výrobců |  |
| Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety. | Monitoring výkonu sítě |  |
| Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). Systém umožňuje extrahovat SNI (Server Name Indication) z HTTPS a QUIC protokolů. | Monitoring informací z aplikační vrstvy |  |
| Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů. | Monitorování rozšířených L3/L4 informací |  |
| Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů. | Automatická korekce časových známek |  |
| Systém je schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně šesti měsíců. | Kapacita datového úložiště |  |
| Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat. | Rozlišování rozdílných samplovacích poměrů pro každé rozhraní zdroje flow dat |  |
| Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik. | Přeposílání flow vč. možnosti samplingu a převodu formátu |  |
| Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011. | Spolehlivý a šifrovaný přenos IPFIX dat |  |
| Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. | Automatická identifikace zdroje flow statistik |  |
| Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat. | Identifikace výpadku dat |  |
| Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky. | Zálohování a obnova flow statistik |  |
| Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele). | Podpora pro uživatelské identity |  |
| Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). | Uživatelské rozhraní |  |
| Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů. | Předdefinované dashboardy |  |
| Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). | Sdílené dashboardy |  |
| Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem. | Vizualizace statistických dat |  |
| Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami. | Vizualizace výkonnostních metrik sítě |  |
| Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru. | Vizualizace výkonnostních metrik sítě |  |
| Systém umožňuje vizuálně porovnat současný průběh síťového provozu s historickými hodnotami. Porovnání probíhá pomocí časového intervalu, který lze flexibilně volit. Systém vypočítává procentuální změny pro jednotlivé časové intervaly a graficky vizualizuje nárůst nebo pokles síťového provozu. | Vizualizace historických trendů síťového provozu |  |
| Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. | Analýza dat a ad hoc výstupy |  |
| Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc bez nutnosti dotaz rozdělit dotaz na menší časové intervaly. Spuštění a vykonání dotazu není limitováno délkou časového intervalu nebo maximální dobou vykonávání dotazu. Dotazy, které se vykonávají dlouho, běží na pozadí a výsledky si uživatel může prohlídnout, jakmile je dotaz dokončen a výsledky jsou dostupné. | Analýza dat pomocí dotazů na dlouhé časové intervaly |  |
| Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. | Reporting |  |
| Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). | Řízení uživatelského přístupu |  |
| Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. | Top N statistiky |  |
| Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). | Filtrování a přizpůsobení výstupů |  |
| Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu. | Uživatelsky definovatelné alerty |  |
| Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.). | Uživatelsky definované pohledy na datový provoz |  |
| Možnost dohledat každý jednotlivý datový tok (flow záznam). | Drill-down |  |
| Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie. | Síťová topologie |  |
| Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení. | Monitoring aktivních zařízení na sítí |  |
| Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). | Automatická podpora geolokace |  |
| Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). | Otevřené rozhraní |  |
| Monitorování dostupnosti zdroje flow dat pomocí SNMP. | Monitorování dostupnosti zdroje flow dat |  |
| Požadavky na automatické vyhodnocování NetFlow dat | | |
| Minimální technické požadavky | Technický parametr | Popis splnění požadavku |
| Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP. | Podpora flow standardů |  |
| Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií. | Streamové zpracovávání flow dat |  |
| Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). | Otevřené rozhraní |  |
| Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí. | Škálovatelnost řešení |  |
| Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. | Deduplikace |  |
| Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. | Proxy korelace |  |
| Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. | Vzorkování na úrovni toků |  |
| Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků. | Správa zdrojů síťových toků |  |
| Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. | Identita uživatelů |  |
| Systém obsahuje vestavěnou databázi nejčastěji používaných SaaS aplikací a platforem na Internetu (1000 a více). Informace z databáze jsou používány k mapování aplikací na externí IP adresy. Informace o SaaS aplikacích a platformách je prezentována v UI u externích IP adres, pro které mapování existuje. | Mapování aplikací k IP adresám |  |
| Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. | Persistence doménových jmen |  |
| Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. Tyto metody detekují bezpečnostní události bez potřeby signatur. | Detekční pravidla a algoritmy nevyžadující signatury |  |
| Systém sbírá, ukládá a vizualizuje události z nástroje třetí strany - Suricata IDS. Události detekované na základě signatur pomocí Suricata IDS jsou korelovány s událostmi detekovanými pravidly a algoritmy nevyžadující signatury. | Analýza a korelace událostí detekovaných na základě signatur |  |
| Aktivita zařízení v síti je vyhodnocována a skórována číselným indexem, který umožňuje jednoduše identifikovat nejzávažnější zařízení z pohledu bezpečnostních hrozeb. Systém poskytuje pohled na zařízení seřazený podle indexu rizika. | Hodnocení zařízení mírou rizika |  |
| Systém poskytuje shrnující přehled, který obsahuje nejzávažnější bezpečnostní události a síťové zařízení, nově detekované hrozby a významné změny v monitorované síti z pohledu bezpečnosti. Toto shrnutí zjednodušuje prioritizaci práce bezpečnostního analytika. | Shrnutí bezpečnostní situace |  |
| Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. | Detekce síťových útoků |  |
| Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. | Detekce anomálií v síťovém provozu |  |
| Detekce NATů v síti s využitím rozšířených informací z L3/L4. | Detekce NATů |  |
| Detekce P2P sítí a VPN komunikace. | Detekce nežádoucích aplikací |  |
| Systém detekuje komunikace s různými SaaS aplikacemi a platformami (1000+) patřících do různých kategorií. Seznam SaaS aplikací a platforem je automaticky poskytován a aktualizován výrobcem. Uživatel si může libovolně vybrat, s jakými aplikacemi bude komunikace detekována a reportována jako událost. | Blacklistování aplikací |  |
| Systém umožňuje detekovat závadnou komunikací na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén. | Detekce náhodných domén |  |
| Systém umožňuje detekovat DNS přes HTTPS (DoH) komunikace a použití DoH serverů. | Detekce DNS přes HTTPS (DoH) komunikací |  |
| Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery. | Detekce TOR komunikace |  |
| Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků. | Analýza šifrovaného provozu použitím JA3 otisků |  |
| Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. | Detekce událostí na základě „Threat intelligence“ dat |  |
| Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti. | Podpora MISP platformy |  |
| Detekce nadměrné zátěže sítě, výpadků služeb,, nových a cizích zařízení připojených k síti. | Detekce provozních problémů |  |
| Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. | Detekce síťových anomálií |  |
| Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.). | Definice vlastních detekčních metod |  |
| Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí. | Vytváření událostí |  |
| Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). | Vyhledávání událostí |  |
| Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události. | Přímý přístup k události přes unikátní URL s využitím ID události |  |
| Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. | Interaktivní vizualizace událostí |  |
| Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP/HTTPS. | Integrace informací z jiných služeb |  |
| Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP. | Získávání doplňujících informací z adresářových služeb |  |
| Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. | Kategorie a komentáře |  |
| Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase. | Podpora MITRE ATT&CK frameworku a mapování na základě kontextu |  |
| Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku. | MITRE ATT&CK dashboard a vizualizace |  |
| Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. | Konfigurační průvodce |  |
| Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). | Konfigurace detekčních schopností |  |
| Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. | Definice závažnosti událostí |  |
| Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry. | Správa detekčních metod |  |
| Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí. | Různé pohledy na události podle uživatelských rolí |  |
| Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu. | Správa filtrů |  |
| Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. | Správa falešných poplachů |  |
| Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu. | Pozastavení platnosti pravidla falešných poplachů |  |
| Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu. | Dynamické definice falešných poplachů |  |
| Pravidla pro falešné poplachy je možné definovat pomocí čísel autonomních systémů (ASN) nebo pomocí plně kvalifikovaného doménového jména (FQDN), čímž lze označit provoz, který nebude zpracováván detekčními metodami. | Definice falešných poplachů pomocí ASN a FQDN |  |
| Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management. | Sledování změn konfigurace |  |
| Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. Součástí exportu musí být event ID, které jednoznačně identifikuje danou událost. | CEF export |  |
| Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. | SNMP Trap |  |
| Události je možné exportovat do formátu CSV pro další zpracování. | CSV export |  |
| Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. | Reporting |  |
| Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k e-mailovému reportu. | E-mailové notifikace |  |
| Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat. | Záchyt provozu v plném rozsahu |  |
| Na výskyt události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů. | Spuštění skriptu |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Nástroj pro ověřování identity uživatelů** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| nastavení |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 4 hodin |  |  |
| dokumentace skutečného provedení |  |  |

# ID005 - MFA + SSO ochrana identity uživatelů

Nasazení MFA + SSO je v rámci IS posílení Kybernetické ochrany. Uživatelům bude řešení umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci.

Řešení bude také poskytovat funkci automatického přihlášení SSO (Single Sign-On) do všech IS ve škole používaných.

Nasazení MFA jednoznačně posiluje bezpečnost provozovaného IS a nasazení SSO jednoznačně zrychluje a zefektivňuje uživatelskou práci s IS.

|  |  |  |
| --- | --- | --- |
| **Nástroj pro ověřování identity uživatelů** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| **Funkční požadavky na systém** |  |  |
| Systém musí být koncipován pro provoz a licenčně pokrýt minimálně 1000 uživatelů (tzn. umožní .přiřadit minimálně 1000 uživatelům autentizační prostředky (neomezené množství) a spravovat digitální certifikáty(neomezené množství)). |  |  |
| Systém zajistí, že vydávání interních certifikátů (X.509) i od akreditovaných CA (komerční, kvalifikované) bude zajištěn ve stejném uživatelském rozhraní, v rámci jednotného procesu a analogických funkcionalit v rámci zajištění správy jejich životního cyklu (následná obnova, revokace, atd.), stejně tak jako další druhy certifikátů, aby Zadavatel mohl systém využívat a provozovat pomocí méně kvalifikovaných zaměstnanců s menšími nároky na školení a úroveň dosaženého vzdělání. |  |  |
| Systém zajistí plnou správu PUK / Management key (dále klíč) pro tokeny zabezpečeným způsobem. Tyto kódy se nesmí tisknout a nejsou dostupné žádné osobě (viditelně). Systém tento klíč zabezpečeným způsobem eviduje a umožní jeho čtení pouze uživateli pomocí vlastní karty pro příslušné operace (s de-šifrovaným klíčem pracuje pouze daná aplikace pro vykonání práce s tokenem). Např: šifrováno klíčem na daném tokenu, klíč uložen v centrální databázi systému (bez tokenu nelze přečíst). |  |  |
| Systém je provozovatelný na systémech založených na open source (bez nutnosti kupovat licence): Operační systém, Databázový systém a případně další vrstvy systému. |  |  |
| Systém zajistí kompatibilitu s oficiálními ovladači karet / tokenů bez nutnosti instalovat jiný SAC / Middleware vyráběný jinou stranou než výrobce. |  |  |
| Systém umožní pomoc uživatelům s uzamčeným čipem pomocí šifrovaném PUKU bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. |  |  |
| Systém umožní uživateli změnu PIN bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. |  |  |
| Systém umožní uživateli resetovat zapomenutý nebo uzamčený PIN pro svoji kartu samoobslužným procesem bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.. Tento proces nejdříve ověří identitu uživatele před tím, než mu bude umožněno nastavení nového PINu. Ověření bude provedeno na základě e-mailu zaslaného ze systému. Email obsahuje bezpečný link pro ověření identity uživatele a následně dojde k dešifrování PUKu pro účely změny PIN / odblokování (uživatel PUK nevidí) |  |  |
| Workflow recyklace kvalifikovaného prostředku v systému obsahuje nejméně následující kroky: Systém musí vytvořit auditní záznam, že proběhla recyklace (recyklace automaticky obsahuje operace revokace certifikátů vydaných systémem a následné vymazání všech certifikátů a ostatních datových typů) na kvalifikovaném prostředku a byl nastaven nový defaultní PIN, PUK, digital signature PIN a PUK. |  |  |
| Systém musí uchovávat všechny informace o uživateli a jeho „přiřazené" čipové kartě tak, aby byl schopen je zprostředkovat dalším systémům v rámci možných integrací. |  |  |
| Systém musí obsahovat roli pro delegované osoby (například Operátor), která přiřazuje karty, vydává certifikáty a ověřuje identitu uživatelů. Přitom zajišťuje úkony spojené s vydáváním či správou životního cyklu kvalifikovaného prostředku pro uživatele. |  |  |
| Operátor musí být osoba s důvěryhodným přístupem k systému. Pro operátora jako osobu vydávající platí stejná povinnost přihlášení k nástroji operátora prostřednictvím čipové karty. |  |  |
| Operátor nemůže vydávat čipové karty uživatelům bez vlastního autentizačního prostředku zajišťujícího více-faktorovou autentizaci jeho osoby. |  |  |
| Systém musí obsahovat roli Administrátor, který spravuje celky jako: Správa administrátorů, správa uživatelů, správa serverů, správa skupin, zobrazení tokenů, auditního logu |  |  |
| Systém musí logovat operace spojené se správou životního cyklu certifikátu a kvalifikovaného prostředku včetně identifikace provádějící osoby - dále jako auditní log. Tento auditní log je možné vidět ve webovém rozhraní v detailu uživatele, tokenu a nebo v globálním pohledu a to bez nutnosti technických znalostí. |  |  |
| Systém zajistí podporu připojení dalších subjektů, přičemž jednotlivé subjekty musí být na sobě nezávislé a vzájemně nevidí na data ostatních subjektů, pokud k tomu nemají příslušné oprávnění a správu jednotlivých subjektů musí být možné delegovat na subjekty/uživatele nezávisle na sobě podle přidělených přístupových práv. |  |  |
| Notifikace systému musí být zasílány uživatelům (s možností nastavit notifikaci i operátorům) při blížící se expiraci certifikátu s možností nastavit časové limity při kterých se notifikace aplikují. |  |  |
| Systém bude kompatibilní se všemi typy zařízení (čipové karty/tokeny) u kterých jeho dodavatel poskytne součinnost. |  |  |
| Systém je kompatibilní s QSCD prostředky jako např: Thales (Gemalto) čipové karty a usb tokeny, které z bezpečnostních důvodů umožňují nastavit hodnoty PUKu pro kvalifikovanou a nekvalifikovanou část samostatně. |  |  |
| Systém musí obsahovat “Autoupdate službu” pro klientskou, operátorskou aplikaci a serververového agenta. Služba zajistí aktualizaci nových verzí (bez nutnosti zásahu administrátora). |  |  |
| Systém umožní zneplatnění certifikátu (revokace, pro interní a kvalifikované certifikáty) a recyklaci karty v rámci jedné organizace a jednoho systému bez použití uživatelského rozhraní 3. stran. |  |  |
| Systém umožní automatické obnovování certifikátů na PC uživatele bez zásahu (asistence) operátora. Operátor pouze schvaluje (povoluje) žádosti o obnovou. Samotná obnova musí proběhnout v režii uživatele pod jeho výhradní kontrolou v souladu s elDAS v rámci jednoho systému. |  |  |
| Systém umožní instalaci operátorské a klientské aplikace v podobě instalačních balíčků pro koncové zařízení (v podobě msi balíčku) a musí být podepsán CodeSignim certifikátem, který je akceptován Windows systémem. Dodavatel musí zajistit aktualizaci těchto aplikací v případě expirace aktuální verze znovu podepsat. |  |  |
| Systém obsahuje desktopové aplikace pro uživatele (klientská aplikace, pro automatické prodlužování, pomoc s PIN / tokenem) a operátora (vydávání certifikátů, přiřazování tokenů). Aplikace musí běžet na Windows 10/11. |  |  |
| Systém umožní vydání karty, vydání balíčku certifikátů (kvalifikovaný a komerční) v rámci Online napojení na CA v jednom systému bez použití uživatelského rozhraní 3. stran. |  |  |
| Požadavek na proces vydávání kvalifikovaných certifikátů mimo pracovní dobu. Proces vydání kvalifikovaného certifikátu by měl být zajištěn tak, aby byl dostupný v kterékoli době, ať už jde o standardní pracovní dobu úřadu nebo certifikační autority. Je klíčové, aby proces probíhal bez zbytečných prodlev, zajišťující kontinuitu služby a efektivitu řešení výdejů certifikátů. Pro efektivní realizaci tohoto požadavku je důležité využít automatizované procesy, které eliminují potřebu časově omezeného lidského schvalování, zatímco zůstanou zachovány všechny bezpečnostní a legislativní standardy. Tímto způsobem bude garantována dostupnost služby i v mimořádných časech a situacích. |  |  |
| Celý životní cyklus kvalifikovaného prostředku musí být spravován v rámci systému. Organizace nesmí být nucena posílat kvalifikované prostředky fyzicky do prostoru třetích stran. |  |  |
| V rámci recyklace nesmí opustit kvalifikovaný prostředek prostředí organizace, být zasílán třetím stranám, případně používat pro účely recyklace PIN čipové karty. |  |  |
| Reporting systému musí umožňovat generovat automaticky měsíční reporty obsahující minimálně předávací protokoly dle jednotlivých subjektů převzetí smluvní dokumentace CA, počty vydaných certifikátů dle subjektů a operátorů, počty revokovaných certifikátů dle subjektů a operátorů, počet uživatelů systému CMS dle subjektů. |  |  |
| Systém musí být připraven a umožnit v případě potřeby vydání balíčku certifikátů (kvalifikovaný a komerční) přímým online napojením minimálně alespoň dvě akreditované CA, aby měl zákazník možnost v případě nespokojenosti a přechod na jinou CA: |  |  |
| -        eIdentity |  |  |
| -        I.CA |  |  |
| Systém musí obsahovat integraci na Active Directory pro napojení a to zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) a to s podporou připojení AD na úrovni subjektů (každý subjekt v systému může mít vlastní AD). |  |  |
| Integrace synchronizace uživatelů z AD a jejich role, na základě které je dále řešen nárok na výdej obsahu na autentizační prostředek. Definice práv na základě členství v AD skupinách: Umožňuje přidělit oprávnění uživatelům a skupinám na základě jejich členství v AD DS. Delegování administrátorských oprávnění: Poskytuje možnost vytvářet různé kombinace oprávnění, které určují úrovně administrativního přístupu. Flexibilní delegování práv na konkrétní činnosti nebo nástroje. Automatická synchronizace identit: Zajišťuje, že identita uživatele v dodaném řešení odpovídá identitě v AD DS. Automatická synchronizace všech změn v AD DS (stav účtu, atributy, členství ve skupinách). |  |  |
| Systém vydává interní certifikáty pomocí šablon certifikátů v Active Directory Certificates Service díky přímé integraci zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) v a to v jednoduchém uživatelském rozhraní pouze pověřeným uživatelům (verifikace uživatele pomocí certifikátu) ve stejné aplikaci jako kvalifikované certifikát. A to s podporou připojení AD CS na úrovni subjektů (každý subjekt v systému může mít vlastní AD CS). |  |  |
| Systém musí pomocí hybridních čipových karet nebo mobilní aplikace zajistit 2 faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZoKB. |  |  |
| Vícefaktorová (multifaktorová) autentizace (dále jen MFA) bude umožňovat Zadavateli využívat minimálně následující metody a kombinace faktorů: |  |  |
| Smartcard logon (kombinace přihlášení PIN+Certifikát X.509) |  |  |
| Systém musí a bude umožňovat konfiguraci různých typů MFA, včetně biometrických metod a aplikací generujících kódy. |  |  |
| Možnost nastavit přihlášení s následující kombinací faktorů pro vybrané uživatele (750 uživ.): Mobilní tel. (Mobilní aplikace) : VAR1: PUSH notifikace + Otisk prstu, VAR2: QR kód + TOTP (časově omezený) |  |  |
| Čipová karta musí umožňovat uložení certifikátu z interní certifikační autority založené na produktech Microsoft. Pomocí tohoto certifikátu se držitel karty bude moci přihlásit do doménových počítačů (technologie Smartcard Logon). |  |  |
| Dodané kvalifikované prostředky - hybridní čipové karty budou v počtu 1000 ks s bezkontaktní částí typu: MifareDESFire 4K EV3 |  |  |
| K dodaným čipovým kartám je požadována dodávka kompatibilních čteček čipových karet v počtu 100 ks. |  |  |
| K dodaným čipovým kartám je požadována dodávka USB klávesnic s rozložením kláves čeština, numerická klávesnice, barva černá, min. délka kabelu 1.6 m s kompatibilní čtečkou čipových karet v počtu 150 ks. |  |  |
| Dodané hybridní čipové karty budou ve formátu ID-1 (velikost bankovní karty). |  |  |
| Vlastnosti kontaktního čipu a PKI aplikace: |  |  |
| · Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty |  |  |
| · Privátní klíč uložený na kartě nelze z karty vyexportovat |  |  |
| · Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS na zařízení schválené ministerstvem vnitra |  |  |
| · Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. |  |  |
| · Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu a nebo mohou být na kartu importovány |  |  |
| · Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12 |  |  |
| Podporované jsou minimálně kryptografické algoritmy: |  |  |
| · Symetrické: 3DES, AES |  |  |
| · Hash: SHA-1, SHA-256, SHA-384, SHA-512. |  |  |
| · RSA: 1024, 2048 bitů, 4096 bitů |  |  |
| · Eliptické křivky: P-256, P-384, P-521 |  |  |
| Dodané HW prostředky musí být plně otevřený i jiným systémům, jenž vydávají na takový HW obsah a to s otevřenou dokumentací pro další integrace. |  |  |
| Dodané HW prostředky musí být plně funkční i po ukončení používání SW balíku pro centrální vydávání obsahu. |  |  |
| Kryptografický obsah čipové karty musí být logicky oddělen na část pro uložení komerčních certifikátů včetně šifrovacích klíčů (dále „komerčních ID“) a na samostatnou část pro uložení kvalifikovaných certifikátů a jim příslušných šifrovacích klíčů (dále „kvalifikovaných ID“). |  |  |
| Výše zmíněné části musí být na sobě nezávislé. Tzn. jejich správa a přístupy včetně přístupových oprávnění musí být na sobě nezávislé. |  |  |
| Přístup k části s komerčními ID musí být chráněn uživatelským heslem a administrátorským heslem. Tato hesla budou nezávislá (tj. oddělená) na uživatelském hesle a administrátorském hesle pro přístup do části s kvalifikovanými ID. |  |  |
| Z bezpečnostních důvodů je vyžadováno, aby čipová karta byla plně v souladu s “Security Target” vydaným výrobcem čipové karty. Cílem tohoto požadavku je vyloučení jakýchkoliv zásahů do obsahu, funkce či nastavení kryptografického čipu třetí stranou, které by mohly potenciálně zpochybnit shodu dodaných čipových karet s kartami výrobce, které prošly certifikací Common Criteria a jsou platně zapsány na evropský seznam QSCD prostředků. |  |  |
| V rámci sjednoceného přihlašování (SSO) musí dodaný systém zajistit automatické přihlášení do stanice Windows 10/11: |  |  |
| -       Informační systém školy – studenti a zaměstnanci - Štefl software |  |  |
| - Informační systém - Avensio - zpracování mezd - RSM Payroll Centre CZ s.r.o. |  |  |
| -       Informační systém - Helios Fenix - Účetní software a evidence majetku |  |  |
| -       Informační systém  - Docházka (žáci + zaměstnanci), JobAbacusPro, GACC s. r. o |  |  |
| -       Informační systém  - EDUBAS |  |  |
| Systém musí dokázat vynutit a zajistit pro vybrané autorizované aplikace v rámci SSO další přihlašovací faktor pomocí passkeys,, T-OTP,. |  |  |
| **Požadavky na podporu** | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let |  |  |

## implementace

|  |  |  |
| --- | --- | --- |
| **Nástroj pro ověřování identity uživatelů** | |  |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| nastavení |  |  |
| akceptační testy a testovací provoz |  |  |
| školení administrátorů v rozsahu 4 hodin |  |  |
| dokumentace skutečného provedení |  |  |

## Tiskárna – potisk čipových karet

|  |  |  |
| --- | --- | --- |
| **Nástroj pro ověřování identity uživatelů** | |  |
| Název a výrobce | **[doplní dodavatel]** | |
| Požadovaný počet : 1 |  | |
| Minimální technické požadavky | ANO/NE | Popis splnění požadavku |
| Velikost karty: CR-80, formát ISO 7810, typ ID-1 |  |  |
| Tloušťka karty: 10 – 50 mil (0,25 – 1,27 mm) |  |  |
| Tloušťka karty pro laminaci: 30 mil (0,76 mm) |  |  |
| Tisková oblast na celou plochu karty CR-80 (bez okrajový tisk) |  |  |
| Rozlišení 300 DPI |  |  |
| Barvy |  |  |
| Rychlost tisku min 225 karet / hodina dual-sided printing |  |  |
| Kapacita vstupního zásobník 250 karet |  |  |
| Kapacita výstupního zásobníku 100 karet |  |  |
| SW ovladače pro Windows® 10 / 11 / Server 2016 a vyšší |  |  |
| USB 2.0 a Ethernet rozhraní s interním tiskovým serverem |  |  |
| **Požadavky na podporu** | **ANO/NE** | **Popis splnění požadavku** |
| Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let |  |  |

# Doplňující požadavky zadavatele

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 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 5 let. 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.

# Podmínky technické podpory (SLA)

Tento požadavek je součástí Servisu Díla. 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 primárně vzdáleným připojením. Výjimku tvoří činnosti nerealizovatelné vzdáleným připojením a vynucují si realizaci v místě zadavatele.

Dále uvedené požadavky se neuplatní ve vztahu k HW, u kterých je výše v technické specifikaci stanoven speciální požadavek. Dodavatel se zavazuje poskytovat zadavateli služby v režimu 24x7 v minimálním rozsahu:

* telefonická hot-line podpora prostřednictvím přiděleného tel. kontaktu pro okamžitou komunikaci 24x7 pro kritické incidenty
* Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 24x7 (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).
* telefonická, e-mailová a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 16 hod.
* diagnostika a odstraňování poruch systému
* profylaxe - preventivní prohlídka systému v rozsahu
* kontrola stavu nainstalovaných updatů a hotfixů
* kontrola a analýza chybových logů systémového SW, stejně tak aplikačního programového vybavení
* kontrola vytíženosti systémových zdrojů
* sběr zpětné vazby od administrátorů systému

Dodavatel se zavazuje zadavateli, že jakékoliv vady plnění Servisu díla či jeho části, budou odstraněny na náklady dodavatele. 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 garantuje zadavateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

|  |  |  |
| --- | --- | --- |
| Kategorie incident | Lhůta odezvy (IRT) | Lhůta vyřešení (TRT) |
| Kritický | 60 minut | 12 hodin |
| Závažný | 60 minut | 2 dny |
| Běžný | 1 den | 7 dní |
| Minoritní | 3 dny | Best effort |

Podpora je poskytovaná v českém jazyce ve formě Help-desk podpory a v případě kritického incidentu telefonické podpory. Jednotlivé úkony/akce dle specifikace podpory jsou definovány následovně.

**Lhůta odezvy (IRT)**

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikace po dobu, kdy je zpětně kontaktovaný dodavatelem nebo je incident přijat do řešení. Lhůta odezvy může být také označována jako reakční doba.

**Doba vyřešení (TRT)**

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikaci po dobu, kdy dodavatel vyřešil popsaný incident.

**Priority**

Zaručená lhůta odezvy na vzniklé incidenty se dělí dle jejich priority. Priorita je dána kritičností vzniklého incidentu v návaznosti na požadovanou funkčnost produktu:

* Kritický incident – Nefunkčnost způsobená dodanou technologií, Nefunkčnost/nedostupnost řešení
* Závažný incident – Nefunkčnost některé z komponent, která nedovoluje vykonávat požadovanou činnost. Vážné chyby řešení ovlivňující provoz objednatele.
* Běžný incident – Nefunkčnost některé z komponent, která nemá přímý dopad na dostupnost objednatele, vážné konfigurační chyby.
* Minoritní incident – Chyby v konfiguraci, Chyby řešení neovlivňující provoz objednatele, Nefunkčnost komponent minoritního charakteru.

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 deseti (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.

# Podmínky rozvoje řešení

V rámci části rozšířené servisní podpora (Služby rozvoje) je požadován rozvoj a údržba díla, tedy činnosti, které nejsou součástí SLA podpory. Cena za Služby rozvoje je pro účely porovnatelnosti nabídek vypočtena jako součin Ceny za jeden člověkoden (MD) práce (implementace) bez DPH a předpokládaného Počtu člověkodní rozsahu 30 MD za období 5 let. Předpokládaný počet člověkodní (MD) je stanoven pouze pro účely hodnocení nabídek v zadávacím řízení. Zadavatel není povinen předpokládaný počet člověkodní (MD) služeb rozvoje vyčerpat.