Obsah

[Technická specifikace 2](#_Toc190257965)

[**Popis projektu a společná kritéria** 2](#_Toc190257966)

[Realizace perimetrového a centrálních firewallů a Sandbox 3](#_Toc190257967)

[NEXT GENERATION FIREWALL 3](#_Toc190257968)

[Požadavky na technologii 3](#_Toc190257969)

[Implementace 9](#_Toc190257970)

[SANDBOXING 10](#_Toc190257971)

[Požadavky na technologii 10](#_Toc190257972)

[Integrace 12](#_Toc190257973)

[Implementace 12](#_Toc190257974)

[VYSOKÁ DOSTUPNOST – WAF 13](#_Toc190257975)

[Požadavky na technologii 13](#_Toc190257976)

[Implementace 16](#_Toc190257977)

[Nástroj pro sběr a korelaci událostí a logů – log management 17](#_Toc190257978)

[Požadavky na technologii 17](#_Toc190257979)

[Implementace 18](#_Toc190257980)

[Systém pro správu privilegovaných účtů - PAM 20](#_Toc190257981)

[Požadavky na technologii 20](#_Toc190257982)

[Implementace 21](#_Toc190257983)

[Realizace nástroje pro řízení přístupu na síti - NAC 22](#_Toc190257984)

[Požadavky na technologii 22](#_Toc190257985)

[Implementace 25](#_Toc190257986)

[Vícefaktorový ověřovací systém včetně centralizované správy identit 26](#_Toc190257987)

[Vybudování PKI , Zavedení systému jednotného přihlašování a dvou faktorové autentizace 26](#_Toc190257988)

[Realizace systému pro řízení uživatelských identit 34](#_Toc190257989)

[Podmínky technické podpory (SLA) a rozvoje řešení 38](#_Toc190257990)

v1.0

# **Technická specifikace**

## **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.
* Automatizace – scénáře pro abstrakci práce s technologiemi formou snadno použitelných předpřipravených akcí pro operátory bez nutnosti manuálního zásahu do konfigurace jednotlivých technologií.

V rámci analýzy bude definována bezpečnostní politika v návaznosti na potřeby zadavatele včetně kvantifikovatelných parametrů typu Recovery Time Objective (RTO), Recovery Point Objective (RPO), přičemž hodnoty těchto parametrů budou definovány v rámci projektu v části Analytické práce v oblasti bezpečnosti a dalších, které vycházejí z vyžadované metodiky. Na základě těchto parametrů musí být nastaveny a integrovány dodané technologie, včetně tvorby automatizačních scénářů tak, aby bylo možné splnit mezní limity těchto parametrů. Požadavky na kapacitu, interoperabilitu se známými technologiemi a otevřenost protokolů vychází z předběžné analýzy prostředí a zohledňuje požadavky na míru integrace a automatizace, která je očekávána v rámci projektu.

Ke každé technologii (aktivitě dle obchodních podmínek) 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.).

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60měsíců, a to v režimu NBD 5x9; 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.

# Realizace perimetrového a centrálních firewallů a Sandbox

## NEXT GENERATION FIREWALL

Řešení pro ochranu uživatelského a síťového provozu. Zajištění ochrany pomocí realizace parametrového a centrálních firewall technologie v režimu active-active a active-passive s odpovídajícími funkcionalitami a požadavky pro ochranu provozu dle specifikace. Ochranu před zero-day malware zajišťuje dedikovaná HW appliance, jenž je s firewall řešením integrována pro kontrolu webového a e-mailového provozu. Řešení musí být homogenní, tj. všechny komponenty jsou od stejného výrobce a společně tvoří funkční celek požadovaných parametrů, včetně jednotné administrátorské konzole.

## Požadavky na technologii

|  |  |
| --- | --- |
| **NGFW č.1** | |
| **Obecné požadavky na NGFW platformu** |  |
| HW appliance o maximální velikosti 1U | ANO / NE |
| Podpora režimu vysoké dostupnosti active/active a active/passive | ANO / NE |
| Podpora duálního napájení (dva zdroje a přívodní kabeláž je součástí každého dodaného zařízení) | ANO / NE |
| Minimálně 4x 10 GbE SFP+ a 8x 1 GbE SFP sítová rozhraní | ANO / NE |
| Minimálně 16x 1 GbE RJ45 síťová rozhraní | ANO / NE |
| Samostatné porty RJ45 pro mgmt, HA a konzolové připojení a USB port | ANO / NE |
| Integrované TPM řešení nebo jeho ekvivalent | ANO / NE |
| **Výkonové požadavky** |  |
| Minimální propustnost NGFW pro IPv4 provoz je 35 Gbps (UDP komunikace a paket velikosti 512B) | ANO / NE |
| Kapacita současně navázaných spojení NGFW je alespoň 3 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 120 000 | ANO / NE |
| Propustnost NGFW pro IPSEC VPN je alespoň 30 Gbps bez licenčního omezení počtu sestavených spojení | ANO / NE |
| Propustnost NGFW při zapnuté funkci SSL inspekce využívající IPS inspekci je alespoň 2,5 Gbps | ANO / NE |
| Propustnost NGFW při zapnuté funkci aplikační kontroly je alespoň 6,5 Gbps | ANO / NE |
| Propustnost NGFW při zapnuté funkci IPS inspekce a současném logování provozu je alespoň 5 Gbps | ANO / NE |
| Propustnost NGFW při paralelně provozovaných funkcích stavového FW, IPS, aplikační kontrole a logovaní (obecně popisovaná kombinace funkcí pro NGFW zařízení) je alespoň 3 Gbps | ANO / NE |
| Maximální udávaná latence NGFW (pro UDP provoz nebo průměrná hodnota) je 9 μs | ANO / NE |
| **Funkční požadavky** |  |
| Jedná se o řešení dnes označované jako NGFW s integrovanou grafickou a CLI správou umožňující kompletní obsluhu zařízení | ANO / NE |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46 | ANO / NE |
| Podpora režimů explicitní a transparentní proxy | ANO / NE |
| 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 | ANO / NE |
| Podpora lokální databáze a vzdálené databáze (radius, IDAP, tacacs+, saml, kerberos) pro ověřování uživatelů | ANO / NE |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu | ANO / NE |
| 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 | ANO / NE |
| Podpora funkcí VPN brány ‐ IPsec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přistup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní́ platformy a zároveň NGFW podporuje portálový́ režim pro bezklientský přístup. | ANO / NE |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3 | ANO / NE |
| 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. | ANO / NE |
| Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků | ANO / NE |
| 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. | ANO / NE |
| 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 | ANO / NE |
| Možnost definice zakázaných slov pro vyhledávání na internetu | ANO / NE |
| Schopnost inspekce protokolu QUIC | ANO / NE |
| Možnost využít výrobcem udržovanou databázi internetových služeb při definici bezpečnostní politiky | ANO / NE |
| Podpora kategorizace stremovaných videí a kanálů jako například YouTube | ANO / NE |
| Podpora ZTNA bezpečného přístupu | ANO / NE |
| 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 | ANO / NE |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času | ANO / NE |
| 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 | ANO / NE |
| Podpora režimu nasazení v režimu WCCP (WCCP v2) | ANO / NE |
| Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy | ANO / NE |
| Podpora ICAP rozhraní pro obousměrnou integraci s externími servery | ANO / NE |
| Podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP) | ANO / NE |
| Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6 | ANO / NE |
| Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace) | ANO / NE |
| Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení | ANO / NE |
| Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí | ANO / NE |
| funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně zpracovávat před jeho zahozením | ANO / NE |
| Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace | ANO / NE |
| Možnost filtrovat Java applety, ActiveX prvky, cookie soubory ve webovém provozu | ANO / NE |
| NGFW může zároveň plnit funkci bezdrátového kontroleru pro bezdrátové přístupové body od stejného výrobce | ANO / NE |
| Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz | ANO / NE |
| **Další požadavky** |  |
| 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. | ANO / NE |
|  |  |
| **NGFW č.2** | |
| **specifikace FW** |  |
| min. 6x 10 GbE SFP+ port | ANO / NE |
| min. 8x 1 GbE SFP port | ANO / NE |
| min. 16x 1 GbE RJ45 port | ANO / NE |
| samostatné RJ45 porty pro mgmt, HA a připojení konzoly | ANO / NE |
| HW appliance (VM app. ani software řešení není akceptovatelné) | ANO / NE |
| podpora režimu vysoké dostupnosti min. active/active a active/passive, cluster o dvou fyzických zařízeních | ANO / NE |
| duální napájení | ANO / NE |
| montáž do 19" RACK, výška max. 1U | ANO / NE |
| **výkonové požadavky** |  |
| min. 75 Gbps propustnost pro IPv4 provoz (UDP komunikace s pakety s velikostí 512 B) | ANO / NE |
| min. 7 000 000 současně navázaných spojení | ANO / NE |
| min. 500 000 nových spojení za sekundu | ANO / NE |
| max. 5μs latence pro pakety o velikosti 64 B | ANO / NE |
| min. 55 Gbps celková propustnost IPSEC VPN (paket 512 B a šifrování AES256-SHA256) | ANO / NE |
| min. 3.5 Gbps propustnost SSL VPN | ANO / NE |
| min. 8 Gbps propustnost funkce SSL inspekce | ANO / NE |
| min. 26 Gbps propustnost při využití aplikační inspekce | ANO / NE |
| min. 6000 CPS u spojení kontrolovaných pomocí SSL inspekce | ANO / NE |
| min. 5 Gbps propustnost funkce IPS | ANO / NE |
| min. 9 Gbps propustnost funkcí next generation firewallingu (stavový firewall, IPS, analýza aplikací) | ANO / NE |
| min. 8 Gbps propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem) | ANO / NE |
| min. 4000 současně připojených uživatelů SSL VPN | ANO / NE |
| min. 2000 souběžně navázaných site-to-site IPSEC tunelů | ANO / NE |
| **funkční požadavky** |  |
| integrované konfigurační rozhraní pro plnou administraci (grafické i CLI), bez licenčního omezení na počet administrátorů | ANO / NE |
| logická segmentace HW s použitím tzv. virtuálních kontextů v min. počtu deseti současně běžících kontextů v ceně zařízení, každý kontext musí pracovat izolovaně, možnost interně propojit jednotlivé kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty | ANO / NE |
| podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46 | ANO / NE |
| možnost nasazení ve všech z následujících režimů: L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline) | ANO / NE |
| ověřování identity uživatelů (MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On | ANO / NE |
| podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů | ANO / NE |
| ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu | ANO / NE |
| funkce QoS, traffic shaping a SD-WAN min. 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 | ANO / NE |
| funkce VPN brány – IPsec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran), SSL VPN pro klientský přistup s podporou tunelového režimu včetně̌ zdarma dostupného klienta pro osobní počítače i mobilní́ platformy, podpora portálového režim pro bezklientský přistup | ANO / NE |
| podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3 | ANO / NE |
| antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků | ANO / NE |
| funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (mobile malware) | ANO / NE |
| detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén) | ANO / NE |
| ochrana před rychle se šířícími kampaněmi škodlivého kódu (virus outbreak) | ANO / NE |
| sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby) | ANO / NE |
| funkce rozpoznávání min. 4000 populárních sítových aplikací na základě jejich charakteristiky provozu na apl. vrstvě, pravidelná aktualizace signatur aplikací, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace | ANO / NE |
| možnost definice zakázaných slov pro vyhledávání na internetu | ANO / NE |
| podpora funkce Safe Search pro populární vyhledavače | ANO / NE |
| funkce kategorizace webových stránek (web filtering) s podporou kategorizace na skupiny (pracovní zájmy, osobní zájmy, hazard, pornografie, sdílená uložiště, stránky se škodlivým kódem, nově registrované domény atd.), výrobcem aktualizovaná databáze s pokrytím českého internetu, definice časových kvót pro uživatele a kategorie webu, akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii | ANO / NE |
| kategorizace stremovaných videí a kanálů min. pro platformu Youtube a Vimeo | ANO / NE |
| 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 | ANO / NE |
| možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času | ANO / NE |
| funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp. | ANO / NE |
| podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN | ANO / NE |
| podpora režimu nasazení v režimu WCCP (WCCP v2) | ANO / NE |
| podpora konfig. PAC souborů pro režim nasazení explicitní proxy | ANO / NE |
| podpora ICAP rozhraní pro obousměrnou integraci s ext. servery | ANO / NE |
| podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP) | ANO / NE |
| podpora statického a dynamického směrování min. OSPF a BGP | ANO / NE |
| podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace) | ANO / NE |
| podpora IPAM funkcionality pro správu přidělených IP adres | ANO / NE |
| podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí | ANO / NE |
| analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace | ANO / NE |
| možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu | ANO / NE |
| integrovaná funkce bezdrátového kontroleru pro AP | ANO / NE |
| integrovaná funkce centrální mgmt. platformy pro přepínače | ANO / NE |
| funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěžě (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí | ANO / NE |
| funkce SSL offloading a SSL inspekce pro rozkládaný provoz | ANO / NE |
| **transceiver** |  |
| 4ks SFP+ moduly | ANO / NE |
| Standard 10GBase-LR, IEEE 802.3ae | ANO / NE |
| Přenosová rychlost 10 Gbps | ANO / NE |
| Typ konektoru LC duplex | ANO / NE |
| Vlákno SM, vlnová délka 1310nm | ANO / NE |
| Funkce hot-plug, aouto negotiation, link status, digital monitoring | ANO / NE |
| přenosová vzdálenost maximálně 10 km | ANO / NE |
| **další požadavky** |  |
| 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. | ANO / NE |

## Implementace

Nasazení firewallu předpokládá perimetrovou ochranu infrastruktury Zadavatele včetně všech definovaných ochran uživatelského provozu, oddělení IT a OT infrastruktury, případně využití aplikačních ochran pro další segmenty v rámci interní infrastruktury, a to zejména technologií datových center.

## SANDBOXING

Řešení pro ochranu uživatelského provozu a eliminaci hrozeb pomocí emulace pro potenciálně rizikové soubory. Ochrana bude vynucena pro veškerý mailový provoz, selektivně pro webový provoz a pro průběžnou kontrolu dokumentů na sdílených uložištích. Přípustné je pouze řešení ve formě dedikovaných appliance, tak aby data nebyla zasílána mimo infrastrukturu provozovatele.

## Požadavky na technologii

|  |  |
| --- | --- |
| **Sandbox** | |
| Obecný požadavek | ANO/NE |
| Je poptáváno řešení ochrany před zero-day škodlivým kódem, viry a malware (založeném na principu tzv. sandbox) ve formě HW /SW appliance. Dodávané řešení musí být plně a obousměrně integrováno s dodávaným NG firewallem a bezpečnou emailovou bránou za podmínky plné technické podpory výrobce (pro případ řešení potíží). Plnou integrací se rozumí nativní integrace, umožňující obousměrnou komunikaci mezi firewallem/AS&AV (antispam/antivir) řešením a platformou sandbox (předávání souborů pro kontrolu, předávání detailních informací o kontrole zpět na firewall/mailovou bránu. Součástí nabídky a dodávky musí být podpora výrobce a předplatné pro veškeré požadované funkce na dobu 5 let a 24x7 podporu výrobcem | ANO/NE |
| HW požadavky | ANO/NE |
| HW appliance využivající proprietární operační systém pro analýzu zkoumaných vzorků | ANO/NE |
| Alespoň 3 instance pro sandboxing OS Windows včetně licencí Microsoft jako součást dodávky řešení | ANO/NE |
| Alespoň 1 instance pro sandboxing souborů pro MS Office prostředí jako součást dodávky řešení | ANO/NE |
| Funkční požadavky | ANO/NE |
| Podpora operačních systémů pro sandboxing: Windows 7-11, MacOS, Linux, Android, systémy průmyslového řízení; výrobce udržuje a aktualizuje skenovací sandboxing OS | ANO/NE |
| Plnohodnotná, výrobcem podporovaná a obousměrná integrace s nabízeným modelem firewallu a dalšími nabízenými bezpečnostními prvky | ANO/NE |
| Možnost integrace s interními systémy pomocí dokumentovaného API, podpora funkce API musí být součástí nabídky | ANO/NE |
| Odchozí komunikace ze sandboxovacích image musí do internetu odcházet přes dedikované síťové rozhraní | ANO/NE |
| Podpora režimu clusterování s cílem dosažení vysoké dostupnosti a navyšování výkonosti v budoucnu | ANO/NE | |
| Inspekce vzorků založená na vícevrstvá ochrana před škodlivým kódem – kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandboxing (spuštění v reálném operačním systému) a umělé inteligence (AI)/strojového učení (ML). Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat. | ANO/NE | |
| Možnost vytvořit a pro sandboxing používat vlastní konfiguraci operačního systému, včetně̌ konkrétních aplikací odpovídající́ konfiguraci v chráněné síti, který bude naimportován do platformy Sandbox a využíván pro inspekci | ANO/NE | |
| Detailní́ konfigurace politiky pro kontrolu, kontrola v různých typech OS, možnost kontroly jednoho souboru v různých operačních systémech zároveň, možnost definice vybraných aplikaci v různých typech OS. | ANO/NE | |
| Ochrana proti zjištění běhu v sandbox prostředí (anti evasion techniky) | ANO/NE | |
| Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloud služba (s výjimkou těch, u kterých to nedovoluje legislativa) | ANO/NE | |
| Detekce komunikace s C&C centry | ANO/NE | |
| Podpora detekce přístupu na kompromitované URL | ANO/NE | |
| Funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture, a v případě projevu malware v GUI také screenshoty či video záznam), podpora reportingu v MITRE ATT&CK formátu pro analýzu SoC, podpora STIX 2.0 formátu | ANO/NE | |
| Podpora kontroly minimálně následujících typů souborů a aplikací: MS Office, Adobe Acrobat Reader, Adobe Flash Player, MS Internet Explorer, Mozilla Firefox, Google Chrome, Java, MS .NET Framework, Visual C++, Python; spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např.  .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh,Mach, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip | ANO/NE | |
| Podpora sandboxingu průmyslových řídících protokolů a aplikací: tftp, modbus, s7comm, http, snmp, bacnet, ipmi | ANO/NE | |
| Podporora reportování ve standardních formátech (HTML, CSV, PDF, XML, …) | ANO/NE | |
| Automatická aktualizace signaturových databází odhalených hrozeb včetně funkce sdílení těchto signatur na nabízenou platformu firewallů a dalších bezpečnostních komponent | ANO/NE | |
| Přímé obousměrné propojení s nabízenou platformou firewallů a dalších bezpečnostních komponent | ANO/NE | |
| Podpora logování na externí nástroje a SIEM | ANO/NE | |
| Podporované režimy nasazení minimálně: napojení na bezpečnostní prvky stejného výrobce, sniffer režim (odposlech a rekonstrukce sítového provozu min. pro protokoly http, smtp, pop3, imap, ftp, mapi, im, smb), sanboxing souborů uložených na dostupných sítových discích, příjem souborů k sandboxingu pomocí API, podpora rozhraní typu ICAP. | ANO/NE | |
| Výkonové požadavky | ANO/NE | |
| Kapacita inspekce neznámého kódu pomocí paralelního běhu s využitím až 14 skenovacích image operačního systému Windows na jedna sandbox appliance | ANO/NE | |
| Výrobcem udávána propustnost min. 10000 souborů za hodinu při aplikaci pre-filteringu před samotným sandboxingem a využití plné kapacity sandboxu | ANO/NE | |

## Integrace

Automatizační procesy, jež jsou požadovány a budou součástí Solution Designu musí zahrnovat změny bezpečnostní politiky firewall formou změn bez nutnosti manuálního zásahu správce. Řešení musí být takto konfigurovatelné i přes API rozhraní. Minimální množina automatizačních postupů pro firewall:

• Změna filtračních pravidel reflektujících riziko koncového zařízení či síťového segmentu (zablokování, restrikce na administrátorský prostup, povolení do původního stavu),

• konfigurace IPS profilu,

• založení VPN prostupu či jeho zablokování,

• nastavení nového uživatele pro SSL VPN či jeho zrušení,

• schopnost záchytu síťové komunikace ve formě PCAP pro požadované rozhraní,

• odpojení síťových rozhraní či skupin rozhraní při kritickém scénáři

## Implementace

Nasazení firewallu předpokládá perimetrovou ochranu infrastruktury Zadavatele včetně všech definovaných ochran uživatelského provozu, oddělení IT a OT infrastruktury, případně využití aplikačních ochran pro další segmenty v rámci interní infrastruktury, a to zejména technologií datových center.

Události ze sandbox appliance musí být korelovány v jednotném managementu společně s firewall řešením, které tuto integraci zajišťuje. K sandbox řešení se může připojit paralelně několik instancí firewallu a využívat výkon dle aktuálních realtime provozních požadavků bez nutnosti rekonfigurace.

# VYSOKÁ DOSTUPNOST – WAF

WAF řešení pro kontrolu provozu jednotlivých aplikací s možností průběžné úpravy kontrolovaných dat dle požadavků.

## Požadavky na technologii

|  |  |
| --- | --- |
| **Požadavky** | |
| **MINIMÁLNÍ POŽADAVKY** |  |
| zařízení typu WAF (zařízení typu NGFW s integrovanou funkcí WAF není akceptovatelné) | ANO/NE |
| HW appliance o maximální velikosti 1U a podporou alespoň 4x 1Gb RJ-45 a 4x 1Gb SFP konektivity | ANO/NE |
| Interní datové SSD uložiště o velikosti alespoň 400 GB | ANO/NE |
| Propustnost plnohodnotné WAF inspekce nad protokolem HTTP min. 500Mbps (výkonová hodnota musí být doložena oficiálním produktovým listem výrobce) | ANO/NE |
| licenčně neomezená podpora režimu vysoké dostupnosti active/passive a active/active | ANO/NE |
| Podpora funkce synchronizace konfigurace mezi dvěma samostatnými WAF prvky v režimu vysoké dostupnosti | ANO/NE |
| Licenčně neomezený počet chráněných serverů a aplikací | ANO/NE |
| Podpora HTTP v1.0, v1.1 a TLS v1.0 - 1.3 | ANO/NE |
| Nativní podpora HTTP/2 | ANO/NE |
| Integrovaný průvodce/wizzard pro nejčastější typy konfigurací | ANO/NE |
| **POŽADOVANÉ BEZPEČNOSTNÍ FUNKCE** |  |
| Požadujeme podporu následujících režimů nasazení WAF: Reverse proxy, Transparentní režim, Transparentní proxy režim (řešení je schopné filtrovat i modifikovat provoz v transparentním režimu nasazení) a pasivní režim (konfigurace na SPAN portu switche), WCCP | ANO/NE |
| Ochrana před OWASP TOP10 hrozbami | ANO/NE |
| Validace protokolu http (dle RFC) | ANO/NE |
| Podpora funkce strojového učení (machine learning) - dvoúrovňová detekce anomálií a hrozeb za pomoci databáze vzorků výrobce a za pomoci strojového učení | ANO/NE |
| Podpora funkce ochrany API rozhraní s podporou schémat OpenAPI, XML a JSON | ANO/NE |
| Ochrana před klasickými typy útoků na web aplikace (XSS, SQL injection, Cross site request forgery, session hijacking, cookie poisoning, …) | ANO/NE |
| Signatury pro ochranu před útoky na známé webové aplikace | ANO/NE |
| Ochrana před útoky typu brute-force | ANO/NE |
| Ochrana před útoky na OS & webserver | ANO/NE |
| Ochrana před útoky typu L7 DoS/DDoS | ANO/NE |
| Podpora geolokační databáze, automaticky aktualizované výrobcem | ANO/NE |
| Podpora reputační DB pro IP adresy | ANO/NE |
| Rozpoznání a ochrana před přístupem automatizovaných klientů/nástrojů (skenery, crawlery, skripty, …) včetně využití funkce strojového učení | ANO/NE |
| Funkce user tracking & scoring (uživatel je identifikován, jeho chování je následně dlouhodobě sledováno a je mu dynamicky upravována reputace na základě reálného chování. Při překročení hraničních hodnot je provedena předdefinovaná akce.) | ANO/NE |
| Pokročilá ochrana před false positive IPS alerty pomocí ML s automatickým a opakovaným učením se na provozu | ANO/NE |
| Syntax based detection (signatura popisující útok je kombinována s inteligentní analýzou specifického/nestandardního chování s cílem minimalizovat množství false positives např. u SQL injection) | ANO/NE |
| Antivirová/antimalware kontrola (kontrola uploadovaných souborů) | ANO/NE |
| AV kontrola integrovaná do WAF appliance (nikoliv jako externí zařízení/služba) | ANO/NE |
| Ochrana před škodlivým kódem (malware, ransomware, trojské koně, atp.) včetně ochrany před polymorfním kódem | ANO/NE |
| Signaturová databáze udržovan výrobcem a automaticky aktualizovaná | ANO/NE |
| Plná integrace s platformou sandbox pro ochranu před pokročilým malware, která bude s WAF plně funkčně integrovaná (řešení SandBox není součástí řešení) | ANO/NE |
| Předdefinované politiky pro nejznámější aplikace (MS Exchange, MS SharePoint, OWA, WordPress) | ANO/NE |
| Všechny signatury udržované výrobcem a automaticky aktualizované | ANO/NE |
| Ochrana proti únikům dat - DLP | ANO/NE |
| Detekce použití kompromitovaných přístupových údajů a zabránění autentizace takovými přístupovými údaji | ANO/NE |
| Možnost využití Cloud SandBox prostředí výrobce WAF pro analýzu přenášeného provozu | ANO/NE |
| Ochrana API | ANO/NE |
| **POŽADAVKY NA AUTENTIZAČNÍ MECHANISMY** |  |
| Podpora autentizace klientským SSL certifikátem | ANO/NE |
| Podpora dvoufaktorové autentizace (radius access-challenge response) | ANO/NE |
| LDAP, RADIUS, SAML, Kerberos, HTTP Basic | ANO/NE |
| Podpora SSO (single sign on) pomocí Kerberos a HTTP Basic / HTML Form | ANO/NE |
| **SÍŤOVÉ FUNKCE** |  |
| Podpora IPv4 i IPv6 | ANO/NE |
| Požadované algoritmy pro L7 load balancing: Round Robin, Weighted Round Robin, Least Connection, URI hash, Host hash, Domain hash, Source IP hash | ANO/NE |
| Požadované metody pro LB persistence: Source IP, http header, URL parameter, Insert cookie, Rewrite cookie, Persistent cookie, Session ID (ASP, PHP, JSP, SSL) | ANO/NE |
| Požadované metody pro kontrolu stavu serverů (healthcheck metody): ICMP Ping, TCP, TCP half open, TCP SSL, HTTP, HTTPS | ANO/NE |
| URL rewriting | ANO/NE |
| Content routing | ANO/NE |
| HTTPS offloading, HTTPS inspekce | ANO/NE |
| Komprese HTTP | ANO/NE |
| Object caching | ANO/NE |
| **SKENOVÁNÍ ZRANITELNOSTÍ** |  |
| Vulnerability scanner integrovaný do WAF appliance (možnost interní bezpečnostní kontroly vlastních web aplikací) | ANO/NE |
| Výstup ve formátu PDF | ANO/NE |
| Definice automaticky aktualizované výrobcem | ANO/NE |
| Možnost automatického importu výsledků auditu pomocí externích nástrojů a následné automatické tvorby bezpečnostní politiky (tzv. virtual patching) | ANO/NE |
| Minimální podpora těchto nástrojů: Acunetix, HP WebInspect, IBM AppScan, Qualys | ANO/NE |
| **POŽADAVKY NA MANAGEMENT** |  |
| Plnohodnotná správa pomocí grafického rozhraní a CLI | ANO/NE |
| Management rozhraní provozované přímo na bezpečnostním prvku (bez nutnosti instalovat samostatný management server) | ANO/NE |
| Správa pomocí web browseru, bez nutnosti instalovat management aplikaci | ANO/NE |
| Podpora SNMP včetně MIB souboru dodávaného výrobcem | ANO/NE |
| Otevřené API pro inzegraci do stávajícího management prostředí | ANO/NE |
| Virtualizace na úrovni mgmt rozhraní (možnost omezit přístup administrátorů pouze na vybraná pravidla resp. chráněné servery) | ANO/NE |
| **POŽADAVKY NA PODPORU VÝROBCE** |  |
| Podpora výrobce v režimu 24x7 na systém i bezpečnostní konfiguraci je součástí nabídky WAF, po dobu 5 let | ANO/NE |

## Implementace

Zadavatelem jsou dále požadované implementační práce v minimálním rozsahu:

* Fyzická montáž zařízení
* Konfigurace síťového prostředí (VLAN, IP, routing)
* Nastavení parametrů HA
* Základní konfigurace virtuálních serverů (až 50)
* Případné komprese a cacheování
* Základní vytvoření bezpečnostních politik
* Konfigurace základních parametrů negativního bezpečnostního modelu dle využitých platforem
* Základní konfigurace
* Nastavení parametrů learning módu (po uplynutí 1 měsíce aktivního learning módu)
* Vyhodnocení událostí a incidentů learning módu
* Úprava hodnot learning módu
* Úprava blocking settings pro jednotlivé položky
* Zapnutí blocking módu
* Nastavení ochrany proti volumetrickým útokům DDoS
* Nastavení ochrany proti bruteforce
* Napojeni na provozní monitoring

# Nástroj pro sběr a korelaci událostí a logů – log management

Systém musí být schopen shromáždit provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpět.

## Požadavky na technologii

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

## Implementace

* Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, akceptačních testů, pilotního testování.
* Konzultace se Zadavatelem a finalizace politiky.
* Instalace centrální správy.
* Instalace dalších komponent (například skenery nebo další potřebné servery).

**Požadované řešení:**

Implementacie dohledového open source systému Zabbix nebo plně srovnatelného pro sledování dostupnosti a výkonnosti komponent IT infrastruktury v Nemocnici TGM Hodonín.

Součástí implementace bude také nastavení pravidel hodnocení shromážděných dat, prahových hodnot alertů, nastavení notifikací na odpovědné pracovníky (e-mailové notifikace, SMS notifikace, případně mobilní aplikace), eskalace notifikací a tvorba reportů. Součástí řešení bude instalace SMS brány pro zasílání SMS notifikací ideálně pomocí naší telefonní ústředny a též zobrazení stavu/alertů na širokoúhlé TV na zdi nad stolem IT techniků.

Součástí dodávky bude i zaškolení pracovníků zadavatele.

**Základní požadovaní komponenty ke sledování:**

|  |  |  |
| --- | --- | --- |
| **Typ zařízení** | **Počet zařízení** | **Sledovaný parametr** |
| Switche | 2 | Dostupnost |
|  |  |  |
| ESXi server | 1 | Dostupnost, využití zdrojů |
| Diskové pole | 1 | Dostupnost, využití zdrojů |
| WiFi Controler | 1 | Dostupnost |
| Firewally | 2 | Dostupnost |
| Vybrané síťové tiskárny | 3 | Dostupnost |
| Multifunkční zařízení Minolta c224e | 1 | Dostupnost |
| LAN převodní pro SW Kredit | 1 | Dostupnost |
| Platební terminál | 6 | Dostupnost |
| UPS APC | 5 | Dostupnost, teplota, stav baterií |
| CT Router | 1 | Dostupnost |
| Převodník LAN-RS232 | 6 | Dostupnost |
| VPN Router Zyxel ZyWALL USG 20 | 1 | Dostupnost |
| PACS server | 1 | Dostupnost, využití zdrojů (RAM, HDD, CPU, síťový provoz) |
| Windows server 2016, 2008 | 21 | Dostupnost, využití zdrojů (RAM, HDD, CPU, síťový provoz) |
| SQL Server 2016, 2014, 2008 | 4 | Dostupnost, využití zdrojů |
| AD | 2 | Dostupnost |
| DHCP | 2 | Dostupnost |
| DNS | 2 | Dostupnost |
| WWW (intranet WordPress) | 1 | Dostupnost |
| Síť Internet | 1 | Dostupnost |
| Konzole antiviru ESET | 1 | Dostupnost |
| SW Veeam |  | Provedení Jobu záloh |
| Mail server IceWarp | 1 | Dostupnost, IMAP, SMTP |

# Systém pro správu privilegovaných účtů - PAM

Nasazení systému, který zajistí správu privilegovaných účtů a monitoring privilegovaných relací. Tento systém zajistí logování všech relací, logování aktivit administrátorů, možnost dohledání zadaných a vykonávaných příkazů a možnost pozastavit, uzamknout nebo terminovat relaci. Dodávané řešení pro správu privilegovaných uživatelských účtů musí splňovat alespoň následující funkce a parametry.

## Požadavky na technologii

|  |  |
| --- | --- |
| **Systém pro správu privilegovaných účtů** | |
| **MINIMÁLNÍ POŽADAVKY** |  |
| Podpora virtualizační platformy Vmware a HyperV | ANO/NE |
| Podpora vTPM | ANO/NE |
| Podpora minimálně 20 privilegovaných účtů | ANO/NE |
| Podpora HA režimu active-pasive (pro případ pozdějšího rozšíření, nyní HA není předmětem poptávky) | ANO/NE |
| Podpora integrace se SIEM/SYSLOG v podobě možnosti exportu logů | ANO/NE |
| Správa řešení z jednotné webové konzole | ANO/NE |
| Podpora importu certifikátů pro potřeby přístupu k management rozhraní – import ze souboru a protokolem SCEP | ANO/NE |
| Podpora import CA certifikátu interní CA | ANO/NE |
| Podpora automatické zálohy konfigurace v případě změny konfigurace nebo periodicky – nahrání konfigurace na FTP, SFTP nebo HTTP/S server | ANO/NE |
| Možnost zachytávat packety s definovanými filtry a následky exportu do nástroje typy Wireshark | ANO/NE |
| Podpora protokolu SNMPv3 | ANO/NE |
| Podpora 2FA autentizace – mobilní aplikace, hardwarový token nebo email | ANO/NE |
| Podpora ověřování přes protokol LDAP | ANO/NE |
| Podpora ověřování přes protokol Radius | ANO/NE |
| Podpora ověřování přes protokol SAML | ANO/NE |
| Podpora reportingu – statistiky využíváni systému | ANO/NE |
| Podpora zasílání upozornění na email při změně konfigurace, kritických systémových událostech atd. | ANO/NE |
| Podpora přístupové proxy pro protokoly SSH, RDP, VNC, SFTP, SMB a HTTP | ANO/NE |
| Podpora SSH filtru – filtrování SSH příkazů | ANO/NE |
| Podpora nahrávání relace ve formě videa a uložení záznamu | ANO/NE |
| Možnost umožnit přístup k cílovému systému bez znalosti skutečného hesla | ANO/NE |
| Podpora periodické změny a verifikace hesla na cílovém systému | ANO/NE |
| Podpora DLP – definice vlastních pravidel | ANO/NE |
| Podpora spouštění nativních aplikací při přístupu k cílovému systému (Putty, Windows RDP atd.) | ANO/NE |
| Podpora schedulingu – časových oken, kdy je přístup umožněn nebo zakázán | ANO/NE |
| Podpora schvalování přístupů (minimálně 2 schvalovatelé) | ANO/NE |
| Agent pro koncovou stanici (pokud je vyžadován) musí být poskytován zdarma nebo musí být zahrnut v ceně řešení | ANO/NE |
| **POŽADAVKY NA LICENCE A PODPORU VÝROBCE** |  |
| Podpora výrobce na nabízené řešení funguje v režimu 24/7 a je součástí dodávky s platností po dobu 60 měsíců | ANO/NE |

## Implementace

Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.

Návrh politiky způsobu řízení privilegovaných účtů. Konzultace se Zadavatelem a finalizace politiky.

Instalace centrální správy.

Instalace dalších komponent (například skenery nebo další potřebné servery).

Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení SMTP reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.

Vytvoření skenovacích úloh.

Načítaní všech privilegovaných účtů a zařízení na platformách Windows, Linux, databáze, síťová zařízení, bezpečnostní technologie a automatizace vyhledávání zařízení / účtů a jejich automatické členění do skupin dle sítí a účelu zařízení / účtů.

Nastavení skupin a oprávnění uživatelů a administrátorů PAM, nastavení a přiřazení přístupových politik skupinám uživatelů, nastavení politik hesel podle skupin zařízení.

Vytvoření provozní dokumentace – popis běžných operativních aktivit, upgradu agentů a komponent, instalace a odinstalace (manuální i hromadné), troubleshooting.

Realizace akceptačních testů.

Školení pro administrátory řešení.

# Realizace nástroje pro řízení přístupu na síti - NAC

Nasazení nástroje, který́ bude řídit přístup 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).

## Požadavky na technologii

|  |  |
| --- | --- |
| **Nástroj pro řízení přístupu na síti** | |
| **MINIMÁLNÍ POŽADAVKY** |  |
| Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána) | ANO/NE |
| Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance | ANO/NE |
| Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami | ANO/NE |
| Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné) | ANO/NE |
| Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem | ANO/NE |
| Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky | ANO/NE |
| 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 | ANO/NE |
| 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. | ANO/NE |
| Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě | ANO/NE |
| Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting | ANO/NE |
| Všechny požadované funkce pokrývá jeden typ licence a je možné dodatečně zvýšit počet licencí v systému | ANO/NE |
| Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů | ANO/NE |
| **POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ** |  |
| Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN) | ANO/NE |
| 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 | ANO/NE |
| 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 | ANO/NE |
| 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 | ANO/NE |
| Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS | ANO/NE |
| Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standardních Radius atributů | ANO/NE |
| Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL | ANO/NE |
| Podpora 802.1x | ANO/NE |
| Podpora MAB autentizace | ANO/NE |
| Podpora tvorby lokálních účtů a lokální autentizace | ANO/NE |
| Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě | ANO/NE |
| Podpora funkce RADIUS proxy | ANO/NE |
| Integrace s certifikační autoritou | ANO/NE |
| 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 | ANO/NE |
| Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP | ANO/NE |
| Podpora captive portál v rámci autentizační brány s plně editovatelným prostředí | ANO/NE |
| Minimálně 5 různých captive portálů | ANO/NE |
| Podpora tzv. sponzorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email | ANO/NE |
| NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovní přístupové vrstvy v případě zjištění bezpečnostního incidentu | ANO/NE |
| Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty | ANO/NE |
| Podpora integrace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW | ANO/NE |
| Podpora alespoň RSSO komunikace s NGFW | ANO/NE |
| Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele | ANO/NE |
| **POŽADAVKY NA ENDPOINT COMPLIANCE** |  |
| Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici | ANO/NE |
| Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě) | ANO/NE |
| Kontrola stavu AV na stanici | ANO/NE |
| Kontrola stavu registrů | ANO/NE |
| Kontrola existence konkrétních souborů v lokálním filesystému | ANO/NE |
| Ověření domény | ANO/NE |
| Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, … | ANO/NE |
| Ověření verze a patch na úrovni operačního systému | ANO/NE |
| Podpora sběru informací o instalovaných aplikacích na endpointech | ANO/NE |
| Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál | ANO/NE |
| Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance | ANO/NE |
| **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 | ANO/NE |
| **NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ** |  |
| Možnost napojení autentizační brány na SMS nebo email bránu promocí konektoru přímo z GUI | ANO/NE |
| **POŽADAVKY NA LICENCE A PODPORU VÝROBCE** |  |
| Licence pro min. 1500 endpointů | ANO/NE |
| Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let | ANO/NE |

## Implementace

Vytvoření dokumentu Solution Design s popisem architektury, jednotlivých komponent, návrhu hromadného rolloutu agentů (bude-li použito), akceptačních testů, pilotního testování.

Návrh politiky způsobu řízení privilegovaných účtů. Konzultace se Zadavatelem  
a finalizace politiky.

Instalace centrální správy.

Instalace dalších komponent (například skenery nebo další potřebné servery).

Konfigurace centrální správy, vytvoření uživatelů a skupin, nastavení reportingu, vytvoření nebo úprava dashboardů po domluvě s administrátory Zadavatele. Volitelně nastavení SSO.

# Vícefaktorový ověřovací systém včetně centralizované správy identit

## Vybudování PKI , Zavedení systému jednotného přihlašování a dvou faktorové autentizace

|  |  |
| --- | --- |
| **Vybudování PKI + Zavedení systému jednotného přihlašování a dvou faktorové autentizace** | |
| **Funkční požadavky na systém** |  |
| Systém musí být koncipován pro provoz a licenčně pokrýt minimálně 2000 uživatelů (tzn. umožní přiřadit minimálně 2000 uživatelům autentizační prostředky (neomezené množství) a spravovat digitální certifikáty (neomezené množství)). Serverový agent je požadován umožnit připojit neomezený počet koncových zařízení. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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). | ANO/NE |
| 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). | ANO/NE |
| Dodané hybridní čipové karty budou v počtu 1000 ks s bezkontaktní částí typu: Mifare Classic 1K EV1 (S50) | ANO/NE |
| K dodaným čipovým kartám je požadována dodávka kompatibilních čteček čipových karet v počtu 1000 ks. | ANO/NE |
| Dodané hybridní čipové karty budou ve formátu ID-1 (velikost bankovní karty). | ANO/NE |
| Vlastnosti kontaktního čipu a PKI aplikace: | ANO/NE |
| Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty | ANO/NE |
| Privátní klíč uložený na kartě nelze z karty vyexportovat | ANO/NE |
| Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS na zařízení schválené ministerstvem vnitra | ANO/NE |
| Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu. | ANO/NE |
| Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu anebo mohou být na kartu importovány | ANO/NE |
| Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12 | ANO/NE |
| Podporované jsou minimálně kryptografické algoritmy: |  |
| o Symetrické: 3DES, AES | ANO/NE |
| o Hash: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. | ANO/NE |
| o RSA: 1024, 2048 bitů, 4096 bitů | ANO/NE |
| o Eliptické křivky: P-224, P-256, P-384, P-521 | ANO/NE |
| Vícefaktorová (multifaktorová) autentizace (dále jen MFA) bude umožňovat Zadavateli využívat minimálně následující metody a kombinace faktorů: |  |
| o Smartcard logon (kombinace přihlášení PIN+Certifikát X.509) | ANO/NE |
| o Mobilní aplikací (možnost kombinace následujících možností: | ANO/NE |
| Možnost nastavit přihlášení s následující kombinací faktorů pro vybrané uživatele: Hardwarový PIN v kombinaci s Otiskem prstu a certifikátem X.509. Nezbytná podmínka: bezkontaktní přihlášení na základě perimetru. | ANO/NE |
| Možnost nastavit přihlášení s následující kombinací faktorů pro vybrané uživatele: Mobilní tel. (Mobilní aplikace) : VAR1: PUSH notifikace + Otisk prstu, VAR2: QR kód + TOTP (časově omezený) + Otisk prstu (včetně možnosti offline). | ANO/NE |
| Systém musí pomocí hybridních čipových karet nebo mobilní aplikace zajistit 2 faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZoKB. | ANO/NE |
| Systém je provozovatelný na systémech založených na open source (bez nutnosti kupovat licence): Operační systém, Databázový systém a případně další vrstvy systému. | ANO/NE |
| 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. | ANO/NE |
| Systém zajistí kompatibilitu s oficiálními ovladači karet / tokenů bez nutnosti instalovat jiný SAC / Middleware vyráběný jinou stranou než výrobce. | ANO/NE |
| Systém umožní pomoc uživatelům s uzamčeným čipem pomocí šifrovaném PUKU bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. | ANO/NE |
| Systém umožní uživateli změnu PIN bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním. | ANO/NE |
| 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) | ANO/NE |
| 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. | ANO/NE |
| V rámci recyklace nesmí opustit kvalifikovaný prostředek prostředí organizace, být zasílán třetím stranám, případně používat pro účely recyklace PIN čipové karty. | ANO/NE |
| Systém musí uchovávat všechny informace o uživateli a jeho „přiřazené" čipové kartě tak, aby byl schopen je zprostředkovat dalším systémům v rámci možných integrací. | ANO/NE |
| 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. | ANO/NE |
| Operátor musí být osoba s důvěryhodným přístupem k systému. Pro operátora jako osobu vydávající platí stejná povinnost přihlášení k nástroji operátora prostřednictvím čipové karty. | ANO/NE |
| Operátor nemůže vydávat čipové karty uživatelům bez vlastního autentizačního prostředku zajišťujícího vícefaktorovou autentizaci jeho osoby. | ANO/NE |
| 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. | ANO/NE |
| Systém musí obsahovat roli Administrátor, který spravuje celky jako: Správa administrátorů, správa uživatelů, správa serverů, správa skupin, zobrazení tokenů, auditního logu | ANO/NE |
| 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 anebo v globálním pohledu, a to bez nutnosti technických znalostí. | ANO/NE |
| Integrace synchronizace uživatelů z AD a jejich role, na základě, které je dále řešen nárok na výdej obsahu na autentizační prostředek. | ANO/NE |
| Definice práv na základě členství v AD skupinách: Umožňuje přidělit oprávnění uživatelům a skupinám na základě jejich členství v AD DS. | ANO/NE |
| Delegování administrátorských oprávnění: Poskytuje možnost vytvářet různé kombinace oprávnění, které určují úrovně administrativního přístupu. Flexibilní delegování práv na konkrétní činnosti nebo nástroje. | ANO/NE |
| 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). | ANO/NE |
| Systém zajistí evidenci a správu serverových a aplikačních certifikátů. Pomocí nainstalovaného „serverového agenta" monitoruje instalované serverové certifikáty a zajišťuje notifikace o stavu serverových certifikátů včetně jejich expirací. Tato funkce musí být dostupná pro všechny infrastrukturní zařízení Objednatele (Load Balancer, Firewall, VPN koncentrátor atd.). Podporované systémy: Linux, Windows Server 2016 a novější. Dále by systém měl poskytovat možnost tvořit skupiny serverových techniků a delegovat jejich oprávnění pro monitoring servisních činností. | ANO/NE |
| Serverový agent by dále být schopen najít automaticky dostupné certifikáty z konfiguračních souborů nebo databází těchto programů: Nginx, Apache, Microsoft Certificate Store (Webhosting,Personal) | ANO/NE |
| Serverový agent by dále měl umožnit načtení certifikátů z vybraných souborů, a to i těch, které jsou šifrovány pomocí passphrase. Heslo v konfiguračním systému musí být šifrováno. | ANO/NE |
| Serverový agent musí být instalovatelný s minimálními vstupními parametry (například vygenerovaný bash skript na linux, MSI instalátor s vygenerovaným příkazem do CMD) | ANO/NE |
| Serverový agent musí být propojen se serverem pro evidenci certifikátů a musí zasílat veřejný obsah všech nalezených certifikátů. | ANO/NE |
| Serverový agent musí obsahovat auto update funkci a musí zajistit, že stažená aktualizace je od důvěryhodného poskytovatele (například formou podpisů). | ANO/NE |
| Serverový agent by dále měl být umožnit jednoduchou správu konfigurace přes konfigurační soubor a CLI aplikaci. | ANO/NE |
| Centrální evidence musí obsahovat modul pro evidenci serverů a seznamu veřejných certifikátů. Musí obsahovat seznam expirací, historii smazaných certifikátů, detekci chyb a případné navržení nápravy. | ANO/NE |
| Centrální evidence serverových certifikátů musí obsahovat přehledný dashboard s čísly serverů které nekomunikují, servery, které mají certifikát, servery, kterým brzy exspiruje certifikát a servery s exspirovaným certifikátem (který nebyl smazán z konfigurace / serveru). | ANO/NE |
| Centrální evidence serverových certifikátů musí obsahovat možnost si vložit adresu na webový server a pravidelně sledovat daný server stejně, jako kdyby byl instalován agent (sledování SSL certifikátu, který Web vrací, sledování dostupnosti připojení). | ANO/NE |
| Centrální evidence serverových certifikátů musí obsahovat možnost evidence techniků na úrovni skupin serverů anebo na konkrétní server. | ANO/NE |
| Centrální evidence serverových certifikátů musí obsahovat možnost notifikací, které budou zasílány určeným osobám nebo skupinám na základě jejich rolí a práv. Níže je přehled notifikací pro jednotlivé role: |  |
| o Správce serverů | ANO/NE |
| o Servery bez přiřazeného technika | ANO/NE |
| o Nepotvrzené servery | ANO/NE |
| o Nekomunikující servery | ANO/NE |
| o Technik serverů | ANO/NE |
| o Blížící se expirace serverového certifikátu | ANO/NE |
| o Nekomunikující servery | ANO/NE |
| o URL je nedostupná | ANO/NE |
| o Žádné certifikáty na serveru | ANO/NE |
| Systém musí obsahovat “Autoupdate službu” pro klientskou, operátorskou aplikaci a serververového agenta. Služba zajistí aktualizaci nových verzí (bez nutnosti zásahu administrátora). | ANO/NE |
| Celý životní cyklus kvalifikovaného prostředku musí být spravován v rámci systému. Organizace nesmí být nucena posílat kvalifikované prostředky fyzicky do prostoru třetích stran. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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. | ANO/NE |
| 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). | ANO/NE |
| 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) 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). | ANO/NE |
| Systém bude kompatibilní se všemi typy zařízení (čipové karty/tokeny) u kterých jeho dodavatel poskytne součinnost. | ANO/NE |
| Dodané HW prostředky musí být plně otevřený i jiným systémům, jenž vydávají na takový HW obsah, a to s otevřenou dokumentací pro další integrace. | ANO/NE |
| Dodané HW prostředky musí být plně funkční i po ukončení používání SW balíku pro centrální vydávání obsahu. | ANO/NE |
| 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. | ANO/NE |
| 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“). | ANO/NE |
| Výše zmíněné části musí být na sobě nezávislé. Tzn. jejich správa a přístupy včetně přístupových oprávnění musí být na sobě nezávislé. | ANO/NE |
| 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. | ANO/NE |
| Z bezpečnostních důvodů je vyžadováno, aby čipová karta byla plně v souladu s vydaným “Security Target”. 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. | ANO/NE |
| 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: |  |
| o eIdentity | ANO/NE |
| o I.CA | ANO/NE |
| Systém musí zvládnout následující minimální požadavky: | ANO/NE |
| o bezheslová multifaktorová autentifikace pro sdílené stanice. | ANO/NE |
| o automatické odhlášení po vzdálení od stanice (v případě použití zařízení s perimetrem) | ANO/NE |
| o automatické odhlášení při vysunutí fyzického zařízení (karta / token). | ANO/NE |
| o nastavitelné 1 až 3 faktory včetně biometrie | ANO/NE |
| o podpora pro bezdotykové přihlášení/odhlášení do/z PC, VPN, Vzdálené plochy | ANO/NE |
| o Podpora pro logický vstup: | ANO/NE |
| o Doménová autentifikace přes X.509 certifikáty | ANO/NE |
| o Bezkontaktní část – Podpora pro fyzický vstup (parkovací systém, docházka, tiskový systém, stravování) použitím 1 až 3 faktorů včetně biometrie (v případě použití zařízení nezaložený na karte / sub-tokenu). | ANO/NE |
| Systém musí být kompatibilní s bezpečnostními prostředky typu klíčenek, které umožňují drátovou a bezdrátovou komunikaci pro účely zabezpečeného přihlášení se do účtu uživatele pro řešení MFA (PIN/Otisk prstu) a musí umožňovat nastavení bezhleslového a bezdotykového přihlašování do operačního systému. Pozadavek Zadavatele je, aby Dodavatel nacenil 300ks těchto zařízení. Bezpečnostním požadavkem je, aby tyto zařízení disponovaly funkcionalitou Hardware PINu. | ANO/NE |
| Klíčenka v rámci dodaného systému musí splnit následující vlastnosti: |  |
| o Podporované a certifikované HW zařízení pro Microsoft infrastrukturu bez nutnosti instalace ovladačů a softwaru atd. na koncových stanicích | ANO/NE |
| o Nativně podporované Windows 7 a vyšší, nativně podporované Apple zařízeními | ANO/NE |
| o Certifikované pro FIDO infrastrukturu a Passkeys | ANO/NE |
| o S možností podpory pro samo registraci a obnovu (zapomenuté, ztracené přihlašovací údaje) | ANO/NE |
| o S možností podpory přihlášení/odhlášení do starších aplikací (automatické vyplňování jména/hesla) | ANO/NE |
| o S možností podpory eIDAS 2.0 QES certifikátů | ANO/NE |
| V rámci sjednoceného přihlašování musí dodaný systém zajistit automatické přihlášení do stanice Windows 10/11: |  |
| o STAPRO - Fons Enterprise | ANO/NE |
| o STAPRO - Openlims | ANO/NE |
| o ARBES - Feis | ANO/NE |
| o FaRMIS - FARMIS2 | ANO/NE |
| o Mail IceWarp | ANO/NE |
| Systém musí dokázat vynutit a zajistit pro vybrané autorizované aplikace další přihlašovací faktor pomocí passkeys,, T-OTP,. | ANO/NE |
| Systém musí a bude umožňovat konfiguraci různých typů MFA, včetně biometrických metod a aplikací generujících kódy. | ANO/NE |
| Systém musí využívat čipové karty i pro účely uchovávání a správu hesel – Password management s možností automatického vkládání login a heslo do webového prohlížeče. | ANO/NE |
| Systém musí a bude umožňovat pomocí uživatelské aplikace podepisovat PDF dokumenty, ukládat jednotlivé podpisové vzory do šablon pro opakované použití bez nutnosti nastavení viditelného podpisu při každém jednotlivém vytváření podpisu, podle druhů a kategorie dokumentů. Šablona musí umožnit přidat časové razítko a vodotisk s náhledem PDF dokumentu v této klientské aplikaci. | ANO/NE |
| Umožnění šifrování dat na uživatelských zařízeních s použitím uložených certifikátů. | ANO/NE |
| Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let | ANO/NE |

## Realizace systému pro řízení uživatelských identit

|  |  |
| --- | --- |
| **Realizace systému pro řízení identit** | |
| **Funkční požadavky na systém** | ANO / NE |
| IdM bude automaticky načítat informace o identitách ze zdrojového systému (personálního systému Avensio SW). | ANO / NE |
| V při načítání budev IdM implementován ochranný mechanismus, který přeruší import v případě, že je detekováno příliš velké množství změn, přičemž tento počet bude konfigurovatelný. | ANO / NE |
| IdM systém bude automaticky zakládat účty v řízených (cílových) systémech dle pracovních pozic a definovaných pravidel. | ANO / NE |
| Při nástupu zaměstnanců je požadováno, aby IdM získávalo data předem a včas informovalo příslušné administrátory systémů o potřebě založit účty tam, kde nebude realizováno přímé napojení. | ANO / NE |
| IdM musí umožňovat použití jednorázového časově omezeného hesla, které si uživatel musí při prvním přihlášení změnit. | ANO / NE |
| V rámci projektu bude do IdM importována matice rolí pro jednotlivé pozice v organizační struktuře zadavatele. | ANO / NE |
| IdM musí umožnit distribuci hesla vhodným způsobem tak, aby heslo nebylo v čitelné podobě dostupné nikomu jinému, než je samotný uživatel – například zaslání na sms nebo e-mail. | ANO / NE |
| IdM umožní automaticky aktivovat a deaktivovat identity při změně stavu zaměstnance v HR systému. | ANO / NE |
| Identitám importovaným do IdM systému budou automaticky zakládány účty v řízených (cílových) systémech dle nastavených pravidel, která budou vycházet z procesů popsaných v analýze. | ANO / NE |
| Při konci nebo přerušení pracovněprávního vztahu, případně uzamčení uživatele zajistí IdM znepřístupnění všech přímo napojených systémů a včas informuje příslušné administrátory systémů o potřebě zrušit účty tam, kde nebude realizováno přímé napojení. | ANO / NE |
| IdM bude poskytovat funkcionalitu administrátorského zámku pro okamžité zablokování aktivní identity a všech jeho účtů. | ANO / NE |
| Pro Microsoft Active Directory bude implementován automatický provisioning a IdM tedy bude účty v tomto systému řídit přímo. | ANO / NE |
| Pro Nemocniční informační systém (NIS) STAPRO – Fons Enterprise bude implementován automatický provisioning a IdM tedy účty v pro tento systém bude řídit přímo. | ANO / NE |
| Pro Laboratorní informační systém STAPRO – Openlims bude implementován automatický provisioning a IdM tedy účty v pro tento systém bude řídit přímo. | ANO / NE |
| Napojení ostatních systémů na IdM bude realizováno na základě výstupů z analytické fáze projektu dle dostupných možností daného systému. | ANO / NE |
| Pro komponenty poptávaného systému bude implementován automatický provisioning a IdM tedy účty v pro tento systém bude řídit přímo. | ANO / NE |
| U všech přímo napojených cílových systémů umožní IdM režim simulovaného zápisu, kdy nebudou do napojeného systému propagovány žádné změny (read-only), ale zamýšlené úpravy budou pouze logovány. | ANO / NE |
| IdM bude kromě specifických konektorů dodaných jako součást řešení disponovat minimálně těmito konektory: |  |
| o      Microsoft Active Directory konektor, | ANO / NE |
| o      CSV konektor, | ANO / NE |
| o      REST konektor, | ANO / NE |
| o      LDAP konektor, | ANO / NE |
| o      JDBC konektor, | ANO / NE |
| o      skriptovatelný konektor (univerzální programovatelný konektor), | ANO / NE |
| o      offline konektor pro manuální realizaci přístupů. | ANO / NE |
| IdM bude podporovat tzv.rekonciliaci řízených systémů, tedy proces, v rámci kterého jsou porovnány skutečné účty s jejich předpokládaným stavem vypočteným IdM systémem. | ANO / NE |
| Na základě výsledků rekonciliace může IdM spustit buď automatickou akce v podobě opravy nebo notifikovat administrátory. | ANO / NE |
| IdM umožní spuštění plné rekonciliace, tedy rekonciliace pro všechny identity. | ANO / NE |
| IdM umožní změnovou synchronizaci, která zajistí pouze aktualizaci změněných údajů (pokud to cílový systém umožní). | ANO / NE |
| IdM umožní spuštění rekonciliace 1 konkrétní identity. | ANO / NE |
| Plnou i změnovou rekonciliaci umožní IdM spustit jak ručně, tak jako plánovanou úlohu. | ANO / NE |
| Rekonciliaci 1 konkrétní identity musí umožní IdM spustit pouze ručně. | ANO / NE |
| S využitím rekonciliace a režimu simulovaného zápisu umožní IdM vygenerovat compliance report pro každý systém s přímým napojením, ze kterého bude vidět: |  |
| o      seznam orphan účtů (účty bez vlastníka, tzv. „mrtvé duše“), | ANO / NE |
| o      nesoulad namapovaných účtů, | ANO / NE |
| o      chybně povolené účty, | ANO / NE |
| o      chybně zakázané účty, | ANO / NE |
| o      chybné hodnoty v atributech účtu, | ANO / NE |
| o      chybějící účty pro aktivní zaměstnance. | ANO / NE |
| IdM musí zaznamenávat do auditního logu veškeré události spojené s identitami i jejich účty v cílových systémech. A to jak změny a akce prováděné administrátory nebo uživateli, tak i všemi automatizovanými úlohami. | ANO / NE |
| Auditní logy IdM musí být k dispozici systému pro bezpečnostní monitoring (SIEM) a události musí být možné vyčítat těmito metodami: |  |
| o      syslog, | ANO / NE |
| o      CSV soubor, | ANO / NE |
| o      JSON soubor, | ANO / NE |
| o      JDBC. | ANO / NE |
| Součástí IdM systému je notifikační engine, který umožňuje odesílat e-mailové notifikace na základě definovaných událostí. | ANO / NE |
| IdM systém umožňuje definovat role, které se skládají ze sady oprávnění v řízených systémech (např. skupiny v LDAPu). | ANO / NE |
| IdM systém umožňuje definovat role ze skupiny jiných rolí (vnořené role). | ANO / NE |
| Přiřazením role IdM uživateli, získá uživatel oprávnění v řízeném systému odpovídající sadě oprávnění této role, případně sady oprávnění všech vnořených rolí. | ANO / NE |
| Pokud IdM uživatel nemá žádnou roli, která by mu přiřazovala oprávnění v konkrétním řízeném systému, nebude takový uživatel disponovat aktivním účtem v tomto systému. | ANO / NE |
| IdM umožňuje definovat pravidla, na základě, kterých jsou uživatelé automaticky přiřazováni do rolí (resp. odebíráni z rolí). | ANO / NE |
| Součástí systému je workflow engine, který umožňuje definovat a spouštět schvalovací procesy pro přidělování a odebírání rolí nebo zakládání a úpravu IdM objektů (např. změna definice role, založení nové identity, ztotožnění uživatele). | ANO / NE |
| Workflow engine IdM umožňuje definovat víceúrovňové schvalování, ve kterém jako schvalovatel figuruje buďto konkrétní uživatel, nebo skupina uživatelů/členové role/vlastníci role/správci aplikace. | ANO / NE |
| O požadavku na schválení bude IdM notifikovat schvalovatele e-mailem. | ANO / NE |
| O schválení požadavku bude IdM notifikovat žadatele e-mailem. | ANO / NE |
| IdM musí podporovat tzv. automatické schvalování – pokud je žadatel zároveň schvalovatel, není toto schvalování vyžadováno a je automaticky označeno jako schválené. | ANO / NE |
| V případě zamítnutí žádosti je schvalovatel vyzve IdM uživatele k vyplnění textové poznámky s důvodem zamítnutí. Důvod zamítnutí pak bude součástí notifikace, která bude odesílána žadateli, zároveň bude trvale uložena u zamítnutého požadavku. | ANO / NE |
| IdM bude v rámci dodávky implementovat minimálně 2 druhy workflow – běžné schvalovací workflow a workflow pro citlivá práva se schválením pověřenou osobou. | ANO / NE |
| IdM řešení bude publikovat celkem 2 oddělená webová uživatelská rozhraní: |  |
| ●      Administrátorské rozhraní | ANO / NE |
| ●      Uživatelské rozhraní | ANO / NE |
| Toto musí být zajištěno dvěma samostatně přístupnými rozhraní, nikoliv pouze formou oprávnění, aby umožnila definovat pro každé rozhraní odlišná přístupová pravidla (pravidla na firewallech). | ANO / NE |
| Pokud se kdokoliv přihlásí do uživatelského rozhraní IdM, není žádná z funkcí administrátorského rozhraní technicky dostupná. | ANO / NE |
| Administrátorské rozhraní umožní kompletní správu konfigurací systému bude přes něj možné zobrazit všechna data v IdM systému i účty v napojených aplikacích. | ANO / NE |
| Uživatelské rozhraní umožní všem IdM uživatelům základní self-service zahrnující: |  |
| o      kontrolu hodnot vlastních atributů, přiřazených rolí a vlastních řízených účtů, | ANO / NE |
| o      podání žádosti o přiřazení role, | ANO / NE |
| o      změnu vlastního hesla (včetně hesel účtů v řízených systémech), | ANO / NE |
| o      reset hesla. | ANO / NE |
| Uživatelé, kteří figurují jako schvalovatelé rolí (vlastník role, security manažer, nadřízený atp.) budou smět v uživatelském rozhraní IdM provádět navíc: |  |
| o      schválení/zamítnutí žádosti o roli, | ANO / NE |
| o      přehled žádostí ke schválení, včetně těch, které byly již odbavené, | ANO / NE |
| o      přehled podřízených uživatelů (atributy, role). | ANO / NE |
| Operátoři IdM budou mít v uživatelském rozhraní IdM dále k dispozici: |  |
| o      zamčení/odemčení identity, | ANO / NE |
| o      vynucení rekonciliace 1 konkrétní identity. | ANO / NE |
| Uživatelé s definovanými oprávněními budou mít v uživatelském rozhraní IdM sekci správy externistů, kde bude možné spravovat jejich identity a přiřazovat role. | ANO / NE |
| IdM poskytne funkce a procesy pro evidenci externistů a správu životního cyklu jejich identit. Změny budou propagovány do řízených systémů na příslušné uživatelské účty. | ANO / NE |
| Systém bude umožňovat řídit oprávnění v rámci všech webových rozhraní IdM systému prostřednictvím tzv. IdM admin rolí. | ANO / NE |
| IdM systém umožňuje přihlášení uživatele jedním z následujících způsobů: |  |
| o      přihlášení prostřednictvím lokálního IdM hesla a loginu přiřazeného k identitě, | ANO / NE |
| o      přihlášení pomocí SSO. | ANO / NE |
| IdM umožní definovat politiky hesel, které určují složitost hesla. Tyto politiky lze přiřazovat jednotlivým systémům tak, že jsou při změně hesla aktivně vynucovány. | ANO / NE |
| V uživatelském rozhraní umožní IdM generování reportů. A to minimálně v rozsahu: |  |
| o      report uživatelů a jejich oprávnění v aplikaci XY; | ANO / NE |
| o      report rolí/oprávnění uživatelů; | ANO / NE |
| o      non-compliance report - přehled rozdílů mezi stavem uživatelských identit a oprávnění v IdM a cílových systémech. | ANO / NE |
| Veškerá citlivá data musí být v IdM adekvátním způsobem zabezpečena kryptografickými metodami, které zajistí pouze autorizovaný přístup. Ochrana dat musí být zaručena během celého jejich životního cyklu, tedy jak při jejich vzniku, přenosu, tak i jejich uchovávání. | ANO / NE |
| Součástí dodávky je předání kompletních zdrojových kódů aplikace, včetně veškerých použitých knihoven, závislostí, build skriptů a instalačních instrukcí. Dodavatel je povinen dodat také technickou dokumentaci. | ANO / NE |
| Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let | ANO / NE |

# Podmínky technické podpory (SLA) a rozvoje řešení

Tento požadavek je součástí Servisu Díla. 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 pro okamžitou komunikaci 24 h denně
* 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. 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 | 4 hodiny |
| Závažný | 60 minut | 8 hodin |
| Běžný | 1 den | 3 dny |
| Minoritní | 3 dny | „best effort“ |

Podpora je poskytovaná v českém jazyce ve formě Helpdesk 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.

V rámci části 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 180 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.