## 1. Pokročilá AntiSpam ochrana

Systém zajišťuje ochranu v prostředí e-mailového kanálu, kde předpokládáme nejvyšší riziko průniku škodlivého kódu.

Je poptáváno řešení na ochranu emailové komunikace (bezpečná emailová brána) fungující jako VM appliance (proprietární operační systém výrobce včetně všech funkcí) v prostředí VMWare ESXi. Řešení určené pro jiný druh hypervizoru, jako HW appliance, anebo jako software není přípustné. Součástí musí být podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 5 let

* HW požadavky
* Podpora 4 sítových rozhraní v rámci síťového prostředí hypervisoru
* Podpora Citrix XenServer, VMware ESXi, KVM, MS HyperV
* VM appliance alokuje min. 1 vCPU
* VM appliance alokuje min. 4 GB paměti
* VM appliance alokuje min. 1 TB diskového prostoru
* Funkční požadavky
* Možnost nasazení v režimu MTA gateway nebo transparentní režim
* Možnost nasazení v režimu vysoké dostupnosti (včetně sdílený fronty) pro budoucí rozšíření
* Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky (NG Firewall, sandbox) za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách (škodlivém kódu) sandboxovací technikou.
* Ochrana proti škodlivému kódu, nevyžádané elektronické poště a uniku citlivých dat
* Podpora víceúrovňové detekce nevyžádané pošty (IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza)
* reakce na detekovaný spam minimálně: přidání tagu, přidání hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce
* Možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky)
* Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant škodlivého kódu
* Podpora IPv6
* Podpora VLAN
* Plnohodnotná́ integrace s LOG serverem a SIEM platformou.
* Plnohodnotná́ integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně̌ dostupnosti MIB souboru dodávaného výrobcem).
* Výkonové požadavky
* Propustnost min. 25 000 emailů za hodinu při průměrné velikosti email ~100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu
* Podpora ochrany minimálně 20 emailových domén
* Licenčně nezávislý model na počtu uživatelů, mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek)

## 2. Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech

Plánované řešení je Endpoint Detection & Response, které bude provozováno na koncových stanicích a serverech a bude zajišťovat preventivní ochranu před škodlivým kódem, kybernetickými útoky a zároveň analyzovat aktivity na těchto systémech.

* Managment v cloud prostředí
* Hybridní možnost nasazení (kombinace on-prem a cloud)
* Systémové vlastnosti a správa řešení
* Podpora OS Windows 10/11
* Podpora Windows Server 2019 a novější
* Podpora Mac OS 13, 14, 15
* Podpora Linux OS Ubuntu 22.04, Ubuntu 24.04, Red Hat 9 nebo novější, CentOS Stream 9
* Podpora mobilních systemu Android, iOS
* Lokální administrátorské účty
* Administrátorské účty z LDAPu
* Napojení na SIEM/Syslog
* Plnění standardu GDPR (odstranění citlivých uživatelských údajů)
* Rozdělení koncových stanic do skupin
* Oddělené politiky pro skupiny koncových stanic
* Možnost vytvoření předkonfigurovaného instalačního balíčku
* Instalace agenta bez uživatelské interakce
* Možnost globálního preventivního nebo simulačního módu vynucování politik
* Možnost sledovat a shlédnout aktuální status aktivit na daném endpointu včetně bezpečnostních událostí
* Obousměrná a výrobcem podporovaná integrace s dalšími nabízenými bezpečnostními prvky, především NG Firewall, za účelem sdílení provozně telemetrických informací a informací o odhalených hrozbách
* Podpora nastavení poštovního serveru pro zasílání varování a chyb systému
* VPN a Zero Trust Security
* Funkce automatického připojení do VPN před přihlášení uživatele do Windows
* Možnost autentikace klientů pomocí RADIUSu, LDAPu, TACACS+, certifikátem nebo ověřením oproti lokální databázi na endpoint manageru
* SSL-VPN funkcionalita
* IPsec VPN funkcionalita
* Zero Trust Security funkcionality
* Předávání telemetrických informací z koncové stanice na centrální management server za účelem ochrany, následná možnost dynamického tagování klientů a tvorby politik v NGFW Firewallu obsahující dané tagy
* Antivirus
* Moderní antivirový engine s využitím strojového účení
* Součásti řešeni musí být Sandbox technologie
* Možnost připojení na sandboxu výrobce nebo přes ICAP protokol
* Periodický a ad-hoc sken stanic
* Ochrana aplikací a uživatele
* Aplikační Firewall
* Web filtering, možnost řídit přístup uživatelů k internetu na základě URL kategorii
* URL kategorie by měli mát alespoň tyto akce pro řízení přístupu uživatele: Blokace, Varování, Povolit a Monitorovat
* Možnost zapnuti Safe Search
* Možnost synchronizace Web Kategorii s platformou NG firewallu nebo centrálního managmentu
* API-based a Inline CASB funkcionality
* Vulnerability scan a možnost automatické opravy těchto zranitelností
* Přehled instalovaných aplikací na koncových stanicích
* Klasifikace a reputační ohodnocení aplikací
* Vyhodnocení zranitelností aplikací a odkaz na CVE
* Zákaz síťové komunikace zranitelných aplikací (virtuál patching)
* Definice politik pro zákaz síťové komunikace na základě reputace
* Definice politik pro zákaz síťové komunikace na základě výrobce
* Zákaz spouštění konkrétních aplikací
* Detekce útoků a malware
* Behaviorální analýza bez použití signatur
* Grafický agregovaný přehled detekovaných událostí s možností forenzní analýzy
* Detekce a mapování útoků dle MITRE ATT&CK framework
* Ochrana před exfiltrací
* Ochrana před ransomware
* Možnost preventivního nebo simulačního módu per politika
* Podpora definice výjimek pro konkrétní procesy
* Podpora definice výjimek na základě chování (application flow)
* Odpověď na detekované útoky
* Definice playbooků
* Možnost izolace koncové stanice pomocí agenta
* Terminace detekovaného procesu
* Odstranění persistentních dat vytvořených detekovaným procesem
* Odstranění původních detekovaného souboru
* Notifikace emailem, SIEM/syslog
* Možnost napojení na ticketovací systém pomocí API
* Možnost zablokování uživatelského účtu kompromitovaného uživatele
* Možnost resetu hesla kompromitovaného uživatele
* Možnost připojení na kompromitovanou stanici pomocí remote shell, možnost zadávat systémové příkazy
* Kontrola zařízení
* Kontrola USB zařízení dle jejich typu
* Detekce IoT zařízení v lokální síti pomocí agenta koncové stanice
* Proaktivni vyhledávání hrozeb
* Proaktivní vyhledávání hrozeb (Threat Hunting)
* Možnost rozšíření threat hunting databáze
* Zaznamenávání a ukladání informaci o:
  + Zápisy na disku
  + Zápisy do registrů
  + Síťová spojení
  + Systémové procesy
  + Systémové logy
* Tvorba a ukládání vlastních IOC
* Možnost konfigurace zaznamenávaných informací
* Možnost tvorby výjimek ze zaznamenávaných událostí
* IOC poskytované výrobcem
* Periodické spouštění IOC
* Definice akcí v případě pozitivního nálezu
* Identifikace MITRE ATT&CK taktik a technik

Agregovaná data pro rychlou orientaci

## 3. Hardeningové politiky

Předmětem zakázky je návrh, konfigurace a implementace centralizovaných security baselines (souborů bezpečnostních politik) pro prostředí Windows Server a Windows Desktop. Tyto politiky budou vycházet z doporučení Microsoft, Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), a budou doplněny o interní know-how a osvědčené postupy z praxe. Výsledkem bude jednotné nastavení bezpečnostních parametrů umožňující řídit a kontrolovat, co je na cílových stanicích a serverech povoleno či zakázáno.

Rozsah a hlavní oblasti nastavení

Politiky se zaměří na klíčové oblasti bezpečnosti, zejména:

* Používání výhradně moderních protokolů a šifer.
* Řízení oprávnění a uživatelských privilegií.
* Bezpečné ukládání a přenos uživatelských tajemství (credentials).
* Ochranu privilegovaných účtů.
* Logování činností operačního systému a jeho komponent.
* Ochranu firemních dat před neautorizovaným odesíláním dat do Microsoftu.

Výstupy

* Security baselines pro Windows Server 2016 a vyšší.
* Security baselines pro doménové řadiče Windows Server 2016 a vyšší.
* Security baselines pro Windows 10 a Windows 11.
* Politiky pro řízení šifrovacích sad v OS Windows Server a Windows Desktop.
* Politiky pro správu a řízení hesel lokálních administrátorů v OS Windows Server a Windows Desktop.
* Auditní politiky na míru podle MITRE ATT&CK frameworku pro Windows Server a Windows Desktop.

## 4. Nástroj pro řízení rizik

Jednoduchý a uživatelsky přívětivý nástroj pro analýzu rizik. Nástroj umožní udržovat vazby mezi primárními a podpůrnými aktivy a celkovou správu aktiv, dále správu hrozeb, zranitelností a správu rizik. Součástí nástroje bude modul pro asset management, který zajistí evidenci stanic, serverů, software a nemocniční přístrojové techniky, výstupem bude aktualizovaný seznam zařízeni. Dále bude součástí IPAM (IP Address Management), nástroj pro řízení IP adres. Tento nástroj slouží ke správě adresního prostoru, zajišťuje plánování, sledování a řízení použitého IP adresního prostoru v síti.

Licenční pokrytí software včetně aktualizací a podpory na 60 měsíců.

Minimální počet evidovaných assetů je 5000.

## 5. Systém pro správu a monitoring administrátorských přístupů

Systém bude zajišťovat správu a monitoring privilegovaných účtů používaných v organizaci. Tato komponenta zároveň zajišťuje rotaci hesel, čímž je sníženo riziko kompromitace privilegovaného účtu. Zavedení PAM systému pro všechny důležité IS a KS a onboarding všech privilegovaných účtů použitých v těchto systémech. PAM by měl být zařazen do BCM analýzy a DR plánu a musí existovat vhodný způsob pro přístup na spravované IS a KS v případě výpadku PAMu. PAM by měl být v základu implementován v HA/DR režimu a celá jeho architektura by měla být navržena s ohledem na kritičnost tohoto systému. Systémy zařazené v PAM – např. Active Directory, databáze, virtualizace, zálohovací systémy, servery.

* Řešení bude poskytovat správcovský přístup na cílový systém prostřednictvím privilegovaných účtů, ke kterým má uživatel přístup dle bezpečnostní politiky. Účty a systémy, ke kterým nemá práva přístupu, nebudou pro uživatele viditelné.
* Řešení bude umožňovat víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém.
* Správcovský přístup na cílový systém bude zprostředkován pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace zadavatele MS SQL Management Studio, WinSCP ), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP, SAML a RADIUS).
* Řešení musí umožňovat silnou autentizaci přistupujících uživatelů pomocí multifaktorové autentizace - MFA. MFA musí být nedílnou součástí nabídky řešení, může se jednat jak o nativní nástroj PIM/PAM řešení, tak MFA nástroj třetí strany.
* Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V záznamech je možné zpětně vyhledávat využitím metadat, které budou mimo jiné minimálně obsahovat:
  + u RDP relací spuštěné aplikace a události
  + u SSH relací jednotlivé příkazy
  + u Webových aplikací klik na jednotlivé odkazy,
  + u ostatních typů relací alespoň stisky kláves
* Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI dodávaného řešení.
* Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditorem), který v případě potřeby má možnost sledovanou relaci ukončit.
* Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data pořízení, uživatele a spuštěného příkazu.
* Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (například LDAP, Radius server, SAML atp.).
* Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi.
* Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě tak, aby k nim měl přístup pouze oprávněný uživatel.
* Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení i pro HA a DR.
* Řešení musí být dimenzované minimálně pro 110 cílových systémů a neomezený počet přihlašovaných uživatelů (interní správci a externí dodavatelé).

Licenční pokrytí software včetně aktualizací a podpory na 60 měsíců

## 6. Systém pro vzdálený privilegovaný přístup

Systém sjednocující vzdálený přístup na privilegované účty a efektivně minimalizuje používané technologie vzdáleného přístupu (TeamViewer, vypublikované RDP a další). Řešení musí vzdáleným administrátorům a externistům poskytovat přístup do interní sítě na privilegované účty pomocí vypublikované webové konzole, v rámci, které je možné vybrat, na jaké systémy a pomocí jakého privilegovaného účtu se může vzdálený administrátor / externista připojit. Takové řešení nezbytně předpokládá vysoce zabezpečenou hardwarovou nebo virtuální appliance na okraji perimetru sítě s vypublikovanou webovou konzolí do internetu. Spojení mezi externím uživatelem a řešením PAM musí být plně šifrované. Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem – je využit princip tzv. „jump/proxy serveru“. Řešení musí být navrženo tak, aby používalo pouze dedikovaný protokol a pomocí něj se dostávalo na koncová aktiva.

* Podpora virtualizační plaformy Vmware, KVM, Hyper-V, Azure, AWS, GCP, Alibaba Cloud
* Podpoda vTPM
* Systémové vlastnosti a správa řešení
* Podpora minimálně 5 privilegovaných účtů
* Podpora HA režimu active-pasive
* Podpora integrace se SIEM/SYSLOG v podobě možnosti exportu logů
* Správa řešení z jednotné webové konzole
* Podpora importu certifikátů pro potřeby přístupu k management rozhraní – import ze souboru a protokolem SCEP
* Podpora import CA certifikátu interní CA
* Podpora automatické zálohy konfigurace v případě změny konfigurace nebo periodicky – nahrání konfigurace na FTP,SFTP nebo HTTP/S server
* Možnost zachytávat packety s definovanými filtry a následky exportu do nástroje typy Wireshark
* Podpora protokolu SNMPv3
* Podpora 2FA autentizace – mobilní aplikace, hardwarový token, SMS, email
* Podpora ověřování přes protokol LDAP
* Podpora ověřování přes protokol Radius
* Podpora ověřování přes protokol SAML
* Podpora reportingu – statistiky využíváni systému
* Podpora zasílání upozornění email při změně konfigurace, kritických systémových událostech atd.
* Řízeni privilegovaných účtů
* Podpora přístupové proxy pro prokotoly SSH, RDP, VNC, SFTP, SMB a HTTP
* Podpora definice vlastních protokolů (typů koncových zařízení)
* Podpora SSH filtru – filtrování SSH příkazů
* Podpora nahrávání relace ve formě videa a uložení záznamu. Možnost poslat tyto videa na externí uložiště
* Možnost umožnit přístup k cílovému systému bez znalosti skutečného hesla
* Podpora periodické změny a verifikace hesla na cílovém systému
* Podpora antivirové kontroly souborů přenášených protokolem HTTP a SSH
* Podpora DLP – definice vlastních pravidel
* Podpora spouštění nativních aplikací při přístupu k cílovému systému (Putty, Windows RDP atd.)
* Podpora definice vlastních nativních aplikací a parametrů
* Podpora schedulingu – časových oken, kdy je přístup umožněn nebo zakázán
* Podpora schvalování přístupů (minimálně 2 schvalovatelé)
* Podpora reverzní gateway service mode. Klient muže začít session přímo s klientské stanice
* Agentless mode pro web based secrets minimalně pro tyto launchers: Web SSH, Web RDP, Web VNC, Web SFTP, Web SMB, Web Telnet
* Podpora Zero Trust přístupu – kontrola stavu koncové stanice a definice pravidel pro přístup minimálně na základě následujících parametrů :
  + kontrola kritických a vážných zranitelností
  + kontrola antiviru a jeho aktuálnosti
  + kontrola lokálních firewallu
  + zalogováni do domény
  + verze operačních systému
* Agent pro koncovou stanici (pokud je vyžadován) musí být poskytován zdarma nebo musí být zahrnut v ceně řešení
* Celá dodávka musí obsahovat všechny komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.