# Nástroj pro ochranu před škodlivým kódem (MailGateway)

## Řešení ochrany SMTP komunikace

Simple Mail Transfer Protocol (zkratka SMTP) je internetový protokol určený pro přenos zpráv elektronické pošty (e-mailů) mezi přepravci elektronické pošty (MTA)

Ochrana SMTP komunikace bude realizována virtualizovaným řešení pro inspekci a zabezpečení příchozí a odchozí pošty v podobě samostatné SMTP brány (mail transfer agent) z veřejné sítě směrem ke stávajícímu SMTP serveru a opačně. Změnou DNS MX záznamu, dojde k přesměrování provozu na nové řešení bez nutnosti hlubšího zásahu do stávající topologie a infrastruktury.

## Specifikace minimálních požadavků technického řešení

#### MailGateway – 2x v HA režimu

|  |
| --- |
| **Platforma pro ochranu emailové komunikace** |
| MINIMÁLNÍ POŽADAVKY |
| **Obecné požadavky na platformu** |
| virtuální řešení pro platformu VMWare, KVM a Microsoft Hyper-V |
| podpora režimu vysoké dostupnosti (A-A, A-P). Pokud je vyžadována licence pro takové režimy fungování, musí být součástí dodávky. |
| požadujeme možnost přidělení minimálně šest virtuálních síťových rozhraní |
| podpora alokovatelné diskové kapacity až 4TB |
| požadovaná propustnost řešení je min. 220 000 email/h při využití souběžné inspekce pomocí antivirus a antispam profilů. referenční velikost kontrolovaného emailu je 100 kB. |
| řešení je schopno konfigurovat pro ochranu až 400 domén |
| pro každou doménu je možné nastavit až 50 inspekčních profilů |
| možnost nasazení v režimu gateway (MTA), server i transparent. Licence pro všechny požadované režimy provozu je součástí dodávky řešení. |
| v režimu server je možno vytvořit až 1500 schránek. Případná licence pro takový počet schránek je součástí nabízeného řešení. |
| certifikace řešení alespoň VBSpam a VB100 |
| **Bezpečnostní a síťové funkce** |
| podpora IPv4 i IPv6 |
| podpora SMTP autentizace min. pomocí protokolů LDAP, RADIUS, POP3 a IMAP |
| integrovaná funkce antivirové ochrany emailového provozu s podporou real-time ochrany před outbrake škodlivého kódu. Databáze antivirových signatur musí být udržována výrobcem nabízeného řešení a automaticky aktualizovaná |
| integrovaná funkce antispam ochran s možností kategorizace v emailu nalezených URL, IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza mailů, podpora systémů třetích stran (blacklisty), kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků s možností detekce a selekce newsletter emailů, podpora funkce tzv. bounce verification, podpora greylistingu. Všechny databáze potřebné pro provoz požadovaných funkcí jsou spravované a aktualizované výrobcem nabízeného řešení. |
| podpora nastavení limitů v rámci SMTP relací (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) |
| schopnost analýzy PDF dokumentů v příloze kontrolované zprávy |
| shodné možnosti nastavení a provedení kontroly příchozí i odchozí komunikace |
| granulární konfigurace pravidel (pravidla na základě IP adres a/nebo domén příjemce, možnost využití wildcard notace) |
| možnost využití zabudované geo databáze IP adres v rámci pravidel. Databáze je udržována udržovaná výrobcem nabízeného řešení. |
| podpora karantény s uživatelským přístupem umožňujícím běžné operace pomocí odděleného síťového rozhraní |
| podpora systémové karantény |
| podpora externího úložiště (šifrovaná komunikace, např. SFTP) |
| řešení a jeho dodané licence umožní provozovat TLS šifrování |
| řešení a jeho dodané licence umožní nastavit S-MIME |
| řešení a jeho dodané licence umožní nastavit DKIM, SPF a DMARC |
| řešení a jeho dodané licence umožní nastavit zabezpečení přenosu mailové komunikace pomocí IBE |
| funkce ochrany rate limiting, vyhodnocování lokálního skóre odesílatelů (na základě nedávné aktivity) s možností nastavení chování pro různé úrovně skóre |
| funkce zabezpečení dokumentů v příloze se schopností odstranění potencionálně nebezpečných prvků v dokumentu (makra, URL, …) včetně dokumentů MS Office a PDF při zachování původního typu dokumentu |
| automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel, za účelem provedení plné AV a AS kontroly |
| reakce na detekovanou hrozbu v podobě alespoň přidání tagu, přidání nové hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce |
| funkce opakované kontroly emailu ve chvíli jeho vyzvednutí z karantény |
| ochrana před škodlivými URL (výrobcem udržovaná databáze škodlivých URL). Možnost uživatelské volby nežádoucích webových kategorií (phishing, malware, adult material, ...) |
| URL click protection (vložené URL je přepsáno tak, aby byla provedena kontrola ve chvíli rozkliknutí odkazu uživatelem) |
| ochrana před útoky typu BEC |
| architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty |
| **Správa řešení** |
| plnohodnotná správa pomocí (HTTPs) a CLI (SSH) je součástí nabízeného řešení |
| možnost omezení administrátorských práv na definované domény |
| Integrované logování systémových událostí a průběhu inspekce provozu s možností zobrazení logů v GUI |
| podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do externího monitorovacího systému |
| podpora logování na externí log server (syslog) |
| podpora archivace (přístup do archívu pomocí protokolu IMAP) |
| podpora REST API pro možnost integrace management do stávající infrastruktury. Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky. |
| oddělení administrátorského a uživatelského přístupu do emailových schránek a karantény pře různá síťová rozhraní |
| **Požadavky na podporu řešení** |
| výrobce umožňuje kontakt podpory nabízeného produktu v režimu 24/7 a to telefonicky i elektronicky |
| nabízené řešení obsahuje všechny potřebné licence pro výše popsané a požadované funkce na dobu min. 2 let |
| všechny popsané funkce nabízeného řešení musí být možné ověřit ve veřejně dostupné produktové dokumentaci výrobce řešení |
| Součástí dodávky je instalace a konfigurace. |