kaspersky BRING ON THE FUTURE

Kaspersky Security for Mail Server

Budování odolnosti vůči vektoru útoku číslo jedna

E-mail je v současnosti primární vektor útoku ohrožující IT zabezpečení firem. Útočníci hledají stále rafinovanější způsoby, jak proniknout do organizací prostřednictvím útoků na bázi e-mailů, což má za následek finanční a provozní ztráty, a také ztrátu dobrého jména. Tomuto vývoji musí firmy čelit budováním jak odolnosti, tak ochrany. Optimalizací své odolnosti a minimalizací zranitelných míst se můžete stát méně atraktivním nebo dokonce nenapadnutelným cílem útoku. A nejlepší pro nasazení protiopatření na posílení odolnosti je ta fáze, než se nevyžádaný e-mail dostane do kontaktu s uživatelem a jeho koncovým bodem.

V roce 2018 jsme zablokovali **téměř půl miliardy pokusů o phishingový útok – což je dvojnásobek** oproti předchozímu roku.

Securelist,
Spam a phishing v roce 2018

Vybudujte si odolnost u vstupního bodu pro útoky číslo jedna

Aplikace produktu Kaspersky Security for Mail Server pomáhají vybudovat odolnost vůči útokům na bázi e-mailu prostřednictvím:

Identifikace a filtrování podezřelých nebo nevyžádaných e-mailů na úrovni brány

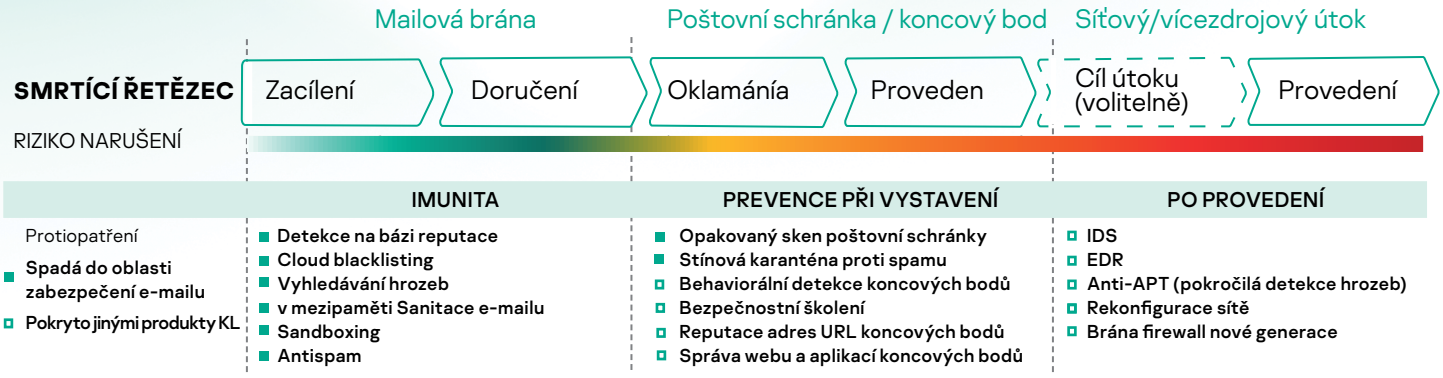
Většina mailových útoků se aktivuje až na úrovni koncových bodů – Kaspersky Security for Mail Server si klade za cíl zastavit je ještě předtím, než se dostanou tak daleko. Naše oceňovaná ochrana posiluje vaši odolnost detekcí a zachycením útoků hned v jejich počátku, než mohou narušit vaši bezpečnostní linii a pokračovat k vašim koncovým bodům a uživatelům.

Rychlé a přesné zpracování vyžádané komunikace

Klíčová role, kterou e-mail v podnikové komunikaci hraje, znamená, že zpracování zabezpečení musí probíhat rychle, agilně a přesně – aniž by byla ohrožena legitimní komunikace. Kaspersky Security for Mail Server nabízí nejefektivnější[1] technologie ochrany před všemi hrozbami na trhu, počínaje phishingovými e-maily a nevyžádanou poštou po útoky prostřednictvím firemních e-mailů (BEC) a ransomware s téměř nulovými falešně pozitivními výsledky, a zároveň umožňuje nepřerušovaný průchod legitimních e-mailů.

Přesunutí e-mailové ochrany za bránu

Uživatel musí být chráněný, mimo jiné sám před sebou – a firma musí být chráněna před následky neznalosti nebo chyb uživatele. Kaspersky Security for Mail Server deteku-je přítomnost škodlivého nebo nežádoucího obsahu na úrovni jednotlivých složek doručené pošty a odeslané pošty na serverech Microsoft Exchange – včetně malwa-ru, phishingových e-mailů a potenciálně nebezpečných příloh, v souladu ze zásadami nakonfigurovanými správcem. Aby bylo možné zabránit převzetí účtu nebo hrozbám zevnitř, vysoce doporučujeme ochranu na úrovni serveru poštovní schránky.



[1] https://www.kaspersky.co.uk/top3

Klíčové funkce

Vícevrstvá ochrana proti malwaru

Více vrstev zabezpečení aplikovaných prostřednictvím neurálních sítí s hloubkovým učením zastaví v postupu i ten nejsložitější malware na bázi e-mailů, včetně spearphishingu a cíleného ransomwaru. Behaviorální analýza, data reputace z cloudu a technologie na bázi signatur, heuristika a databáze signatur v kombinaci s lidskou odborností poskytují vrstvu za vrstvou oceňované detekce a úrovní prevence s minimem falešně pozitivních výsledků.

Sandboxing

Na ochranu i před tím nejvíce sofistikovaným, vysoce maskovaným malwarem jsou přílohy spouštěny v bezpečném emulovaném prostředí, kde jsou analyzovány s cílem zajistit, aby nebezpečné vzorky nepronikly do firemního systému. Vlastníkům Kaspersky Anti Targeted Attack umožňuje jeho plná integrace fyzickou detonaci ve vnějším prostředí izolovaného prostoru Sandboxu – čímž poskytuje mnohem hlubší úrovně hodnocení a dynamické analýzy. Cílený útok pak může být narušen zablokováním doručení jeho součástí.

Automatizovaný antispam (s reputací obsahu a zdrojové adresy)

Antispamový systém Kaspersky Lab využívá inteligentní technologie pro minimalizaci možnosti výskytu falešně pozitivních výsledků a přizpůsobení se změnám v celém spektru hrozeb, pod dohledem lidských odborníků. Globálně shromažďovaná data reputace jsou zpracovávána v cloudu a poskytují solidní základ pro efektivní detekci spamu.

Vícevrstvá ochrana proti malwaru

Více vrstev zabezpečení aplikovaných prostřednictvím neurálních sítí s hloubkovým učením zastaví v postupu i ten nejsložitější malware na bázi e-mailů, včetně spearphishingu a cíleného ransomwaru. Behaviorální analýza, data reputace z cloudu a technologie na bázi signatur, heuristika a databáze signatur v kombinaci s lidskou odborností poskytují vrstvu za vrstvou oceňované detekce a úrovní prevence s minimem falešně pozitivních výsledků.

Nejčastěji používaný malware obsažený v e-mailech

Nejčastější výsledek detekce, který mohli zákazníci Kaspersky v loňském roce zaznamenat, byl Win32. CVE-2017-11882, zneužívající známou chybu zabezpečení MSOffice.

Securelist,
Spam a phishing v roce 2018

Boj proti podvodům prostřednictvím firemních e-mailů (BEC)

Speciální systém detekce na bázi strojového učení, s algoritmickými modely pravidelně aktualizovanými o nové scénáře, zpracovává řadu nepřímých ukazatelů, čímž umožňuje systému zablokovat i ty nejpřesvědčivější falešné e-maily. Podpora mechanismů pro ověřování odesilatele, například SPF/DKIM/DMARC, pomáhá chránit před falšováním zdroje – což je obzvláště užitečné u scénáře útoků typu BEC.

Za branou – odolnost na úrovni poštovní schránky

Technologie na úrovni poštovní schránky zahrnují:

Opakované skenování e-mailu – řešení scénáře při zpožděné aktivaci phishingu adres URL

Stínová karanténa antispamu – ideální pro prostředí s nízkou tolerancí. Hraničně podezřelé e-maily mohou být ponechány v dočasné karanténě, dokud Kaspersky Security Network neshromáždí dostatek důkazů pro posouzení, zda je doručení jednoznačně bezpečné.

Prevence přenosu nebezpečného obsahu

Konfigurovatelný systém filtrování příloh Kaspersky dokáže odhalit maskování souborů běžně používané kyberzločinci za účelem identifikace potenciálně nebezpečných příloh. Funkce filtrování obsahu umožňuje správci nakonfigurovat speciální pravidla pro zabránění úniku dat.

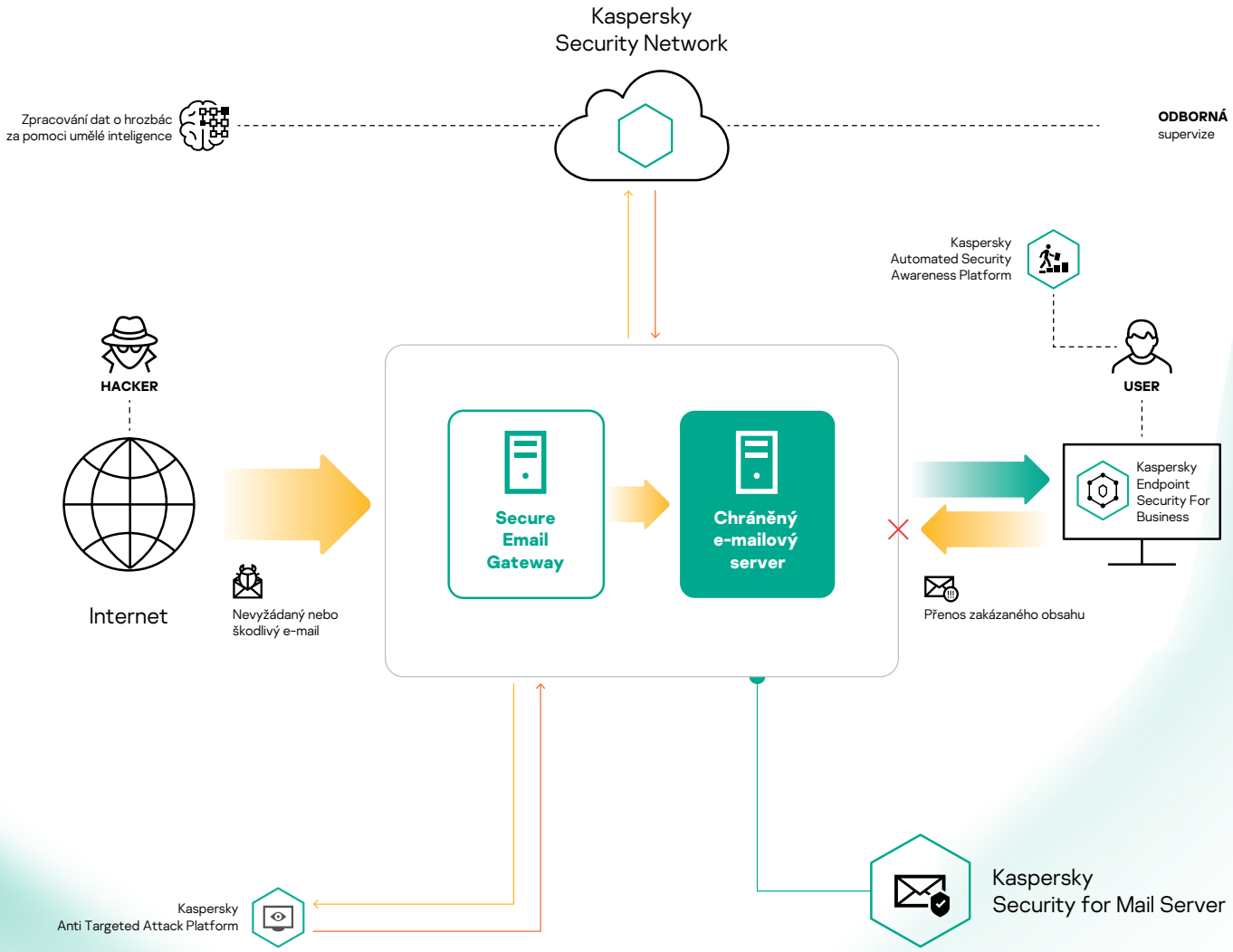
Integrovaná záloha

Pro zajištění, aby z důvodu dezinfekce nebo odstranění nedošlo ke ztrátě klíčových dat, mohou být původní zprávy uloženy do záložního úložiště, kde budou zpracovány správcem při nejbližší vhodné příležitosti. Pro podmíněné zálohování dat mohou být nakonfigurována zvláštní pravidla.

Správa a viditelnost

Přehledné, uživatelsky přívětivé webové rozhraní umožňuje správci sledovat úrovně ochrany firemní pošty pomocí následujících nástrojů:

- Flexibilní, avšak snadno použitelná konfigurace pravidel a zásad.
- Integrace Active Directory.
- Export událostí do vašeho systému SIEM.
- Diagnostika zdraví systému



Přidejte se k nám s Kaspersky Security for Mail Server:

Kaspersky Security for Mail Server je pouze jedním z řady produktů a řešení od Kaspersky Lab, vyvinutý interně, vycházející z více než 20 let cílevědomých odborných znalostí, vytvořený na bázi jednoho kódu a určený pro bezproblémovou integraci za účelem poskytnutí komplexní a nenapadnutelné bezpečnostní platformy.

Pokud již využíváte řešení zabezpečení, například Kaspersky Endpoint Security for Business, po instalaci Kaspersky Security for Mail Server si můžete být jisti, že ochrana vaší mailové brány funguje na stejné úrovni bezkonkurenční výkonnosti jako zbytek vašeho zabezpečení.

Pokud ne, nyní je vhodná příležitost na posílení vaší bezpečnostní linie a budování odolnosti instalací Kaspersky Security for Mail Server souběžně nebo místo vaší aktuální ochrany e-mailu.

Postup při

Kaspersky Security for Mail Server je prodáván jako samostatné cílené řešení nebo jako doplněk dostupný pouze pro zákazníky Kaspersky Endpoint Security for Business.

Zahrnuté aplikace

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Office 365

Licence

Kaspersky Security for Mail Server je k dispozici prostřednictvím:
- roční licence
- měsíčního předplatného

Můžete také zvážit...

Kaspersky Security for Microsoft Office365 – je speciálně navržen pro vyplnění mezer zabezpečení v cloudové nabídce společnosti Microsoft, včetně Outlook 365.

Kaspersky Security for Internet Gateway – doplňte ochranu bezpečnostní linie vašeho e-mailu stejně výkonným zabezpečením brány webu – rovněž dostupný jako součást řešení Kaspersky Total Security for Business.

Kaspersky Endpoint Security for Business – naše vlajková loď v oblasti řešení zabezpečení koncových bodů poskytující nejvíce testovanou a nejvíce oceňovanou ochranu koncových bodů na trhu.

Vyzkoušejte před nákupem Kaspersky
Security for Mail Server nyní s naší bezplatnou 30denní zkušební verzí.

Požádejte o hovor
Potřebujete ještě další informace? Požádejte o hovor za účelem objasnění všeho, co je třeba!

Kupte prostřednictvím důvěryhodného partnera
Jste připraveni k nákupu? Najděte si prodejce ve vaší oblasti,

Novinky v oblasti kybernetických hrozeb: www.securelist.com
Novinky v oblasti zabezpečení IT: business.kaspersky.com
Zabezpečení IT pro malé až střední podniky: kaspersky.com/business
Zabezpečení IT pro firmy: kaspersky.com/enterprise

www.kaspersky.com

Jsme prověření. Jsme nezávislí. Jsme transparentní. Zavázali jsme se k budování bezpečnějšího světa, ve kterém technologie zlepšují naše životy. Proto je zabezpečujeme, aby všichni lidé všude na světě mohli využívat nekonečné možnosti, které přinášejí. Pečujte o kybernetickou bezpečnost pro bezpečnější zítřky.

Zjistěte více na stránce kaspersky.com/transparency

Proven. Transparent. Independent.