Silná ochrana pro firemní prostředí
nejen proti internetovým hrozbám

Antivirové/ AntiSpyware řešení v dnešní době nesmí chybět na žádném počítači.

Nejen s operačním systémem Microsoft, ale i Linux a Mac OS. Antivirový klient zajišťuje ochranu proti pravidelně se vyskytujícím novým hrozbám virů, červů, Spyware, Trojských koní, Rootkitů nebo Ransomware. Klient slouží také jako personální firewall kontrolující bezpečnostní politiku a povolený síťový provoz. Kontroluje spuštění nepovolených aplikací a připojování nepovolených hardware zařízení. Hlídá tak bezpečnostní zásady společnosti. Zajišťuje svou aktualizaci a posílá data o dění na klientovi na centrální server pro vyvolání protireakcí a upozornění. Antivirový klient musí být v systému co nejmenší zátěží a zároveň zajišťovat 100% ochranu.

Co řešení přináší

Antivirus na klientech chrání proti stále narůstajícímu počtu hrozeb pomocí různých detekčních nástrojů pro ochranu na koncových zařízeních. Cílem je, aby zařízení, které je využíváno pro potřeby společnosti nebylo v ohrožení, aby hrozbu detekovalo, upozornilo na ni a bránilo šířením nákazy na další firemní prostředky.

Moduly firewallu je možné aplikovat dle politik pro vynucení bezpečnostní politiky společnosti, a to jak interně tak mimo připojení do korporátní sítě.

Definování zakázaných aplikací a povolených hardware zařízení umožnuje ochranu nejen proti hrozbám z internetu, ale také z přenosných médií.

Centrální správa antivirových klientů vynucuje dodržování politiky nastavení klientů, zajišťuje přehled o dění a vytváří reporty.

Aplikační antivirové řešení je vytvořené přímo pro ochranu aplikací jako jsou MS Exchange, MS Sharepoint, na ochranu před soubory, které jsou pro OS skryté, a tak je není možné klientským antivirem zachytit.

Antivirus na webové bráně společnosti zajistí ochranu ihned na vstupu do infrastruktury bez ohrožení neaktualizované stanice uživatele apod.

Hlavní cíle produktu

Produkt musí umět chránit prostředí proti všem známým i neznámým typům útoků. K tomu slouží moduly rozpoznávající nákazu jak na základě virových definic, tak podle analýzy chování. Antivirové produkty jsou dnes zpravidla na stejné úrovni detekce virů z virových definic. Mnoho výrobců antivirových programů spolupracuje na sdílení nově objevených hrozeb ve Virus Information Aliance (VIA). Cílem je vždy vytvořit detekční vzorek do definic na novou hrozbu co nejrychleji, aby se ochrana dostala k zákazníkům využívajícím produkt společnosti v co nejkratším čase.

CO PRODUKT UMÍ NABÍDNOUT NAVÍC

Univerzálnost řešení pro možné nasazení do společností o jednotkách počítačů až po sítě v řádu desetitisícových jednotek.

Antivirový program je většinou v infrastruktuře aplikován na každý operační systém klientských OS a Serverů, proto je nezbytná přehledná centrální správa. Nasazení antivirové ochrany s centrální správou umožní mj. splnit některé z požadavků GDPR (nařízení EU), jako je:

- zajištění důvěrnosti, integrity a dostupnosti osobních údajů (OÚ)
- zohlednění rizik zpracování OÚ, mezi něž patří např. ztráta, resp. únik nebo kompromitace, neoprávněný přístup k OÚ, a také neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných OÚ
- odolnost systémů a služeb zpracování OÚ

Centrální správa musí zajišťovat

- Zjišťování stavu na klientovi, sběr logů, reporty
- Definici vzdálené automatizované úlohy, jako je aktualizace virových definic nebo aktualizace nových verzí antivirového software
- Odesílání rozdílového aktualizačního souboru pro minimální zátěž infrastruktury
- Nastavení upozornění na události, jako zastaralé aktualizace, virové hrozby a jiné události
- Rozdělení rolí, skupin klientů, oddělené chování dle umístění či typu připojení klienta
- Možnost replikací mezí více servery
- Detekci klientů bez antivirové ochrany
- Jednoduché způsoby migrace
- Jazykovou lokalizaci na klientských stanicích

Antivirový klient musí zajišťovat

- Rychlé a výkonné zabezpečení na fyzických i virtuálních systémech
- Ochranu proti virům, Spyware, Rootkitům, Trojským koním, červům aj.
- Chytrou detekci proti neznámým hrozbám
- Firewall s možnostmi různých profilů dle připojení VPN, Firemní síť, internet aj.
- Ochranu před síťovými hrozbami - Intrusion Prevention System
- Ochranu proti neoprávněným zařízením (definování povolených CD, DVD, USB, monitoring zápisu souborů na USB apod.)
- Ochranu proti spouštění společností nepovolených souborů (zákaz spouštět programy, a to například omezením na externí média)
- Definování míst pro aktualizace tak, aby zatížení sítě při distribuci definic bylo minimální
- Plnohodnotné jazykové verze v českém jazyce a světových jazycích
- Podpora operačních systémů MS Windows, iOS, Linux (vždy záleží na konkrétních edicích dle konkrétní verze SW)