

GFI MailSecurity

E-mail antivírus és tartalomszűrő Exchange/Lotus/SMTP
levelezőszerverekhez

Egy vállalat elektronikus levelezésének védelmekor a beérkező többszázezer levél közül ki kell tudni szűrni a veszélyes tartalmú vagy támadó szándékú leveleket úgy, hogy a folyamat közben az értékes és bizalmas levelek ne sérüljenek, ne kerüljenek a kiszűrt levelek közé. A kéréstlen levelek mellett a legtöbb problémát az e-mailben érkező vírusok és más rosszindulatú kódok okozzák, amelyek képesek akár lebénítani a levelezőszerveret. Talán még ennél is nagyobb veszélyt jelentenek azok az e-mailben terjedő kódok, amelyek megfertőzhetik a levelezőszerveret és bizalmas adatokat, leveleket küldenek tovább a világ bármely postafiókjába. A felsorolt veszélyforrásokra nem adnak megfelelő megoldást azok a programok, amelyek csak egy hagyományos vírusirtót használnak, mert a levelekben érkező trójai és exploit programok szabályos kommunikációját a hagyományos módszerekkel nem lehet felderíteni.

A levelezőszerveret csak egy integrált email tartalomszűrő és több motorral működő email antivírus szoftver tudja megvédeni. A GFI MailSecurity email tűzfalként tartja távol az levelekben érkező vírusokat és más kártékony, támadó jellegű tartalmakat.

Vírusellenőrzés több vírusirtóval

A GFI MailSecurity a bejövő leveleket akár 5 különböző vírusirtó segítségével ellenőrizheti. A több vírusirtó alkalmazása drasztikusan csökkenti a vírusok megszületése és felismerése között eltelt időt, ezáltal minimálisan csökkentve a fertőzés esélyét. A magyarázat nagyon egyszerű: egyik gyártó sem lehet mindig a leggyorsabb. A víruskitörésekre az egyes gyártók más-más válaszdővel reagálnak a vírusok típusa és a megjelenésük helyének függvényében. Több vírusirtó használata esetén nagyobb az esély arra, hogy ezek közül a programok közül legalább egy képes azonosítani és megállítani a legújabb vírusokat. Fontos még kiemelni, hogy minden vírusirtó egyedi keresési mechanizmussal rendelkezik. Egyesek nagy pontossággal találhatnak meg egy bizonyos vírust és annak variációit, míg egy másik antivírus motor más vírusokat képes azonosítani. Összefoglalva: a több vírusirtó nagyobb védelmet biztosít.

Norman, Kaspersky, BitDefender, McAfee és AVG anti-vírus motorok

A GFI MailSecurity két ICSA bizonyítvánnyal rendelkező elismert és erőteljes vírusirtó motorra támaszkodik. A fokozott biztonság érdekében azonban lehetőség van további három gyártó termékének integrálására is. A Kaspersky, McAfee és AVG víruskeresők külön-külön beállíthatók a két beépített vírusirtó program helyett vagy mellé, így akár egyszerre 5 megbízható antivírus motor védheti a levelezést. A Kaspersky, a McAfee és az AVG sok éves tapasztalata és világszerte elismert antivírus mérnökeinek kiváló munkája teszi még erőteljesebbé és megbízhatóbbá a GFI MailSecurity-t.

Spyware keresés

A GFI MailSecurity Trojan & Executable Scanner modulja felismeri a spyware és adware fájlokat. Az opcionális Kaspersky víruskereső motor további kiterjedt spyware, adware és trójai adatbázissal rendelkezik.

Trojan & Executable Scanner

A GFI MailSecurity Trojan & Executable Scanner analízálja a futtatható állományokat és egy beépített intelligencia segítségével képes megállapítani az állományok veszélyességi szintjét. Visszafejti a kódot és megvizsgálja, hogy mit szeretne tenni az adott program, és az eredményeket összeveti a tiltott tevékenységeket leíró adatbázissal. A kereső minden olyan programot karanténba helyez, amely gyanúsán viselkedik, ok nélkül próbál hozzáférni a modemhez, címjegyzékhez vagy a hálózathoz.

Csatolt állományok vizsgálata

A GFI MailSecurity tartalomszűrő szabályrendszere segítségével a felhasználók és csatolt állományok típusa alapján a beérkező állományok karanténba helyezhetőek. Például: minden csatolt futtatható alkalmazás a karanténba kerül, így csak ellenőrzés után férhetnek hozzá a felhasználók. A GFI MailSecurity tartalomszűrője csökkenti az adatszivárgás esélyét, felügyeli a kimenő levélforgalmat, és beavatkozik, ha visszaélést észlel (például ha egy alkalmazott adatbázist küld ki e-mailben).



HTML szkriptek eltávolítása automatikusan

A HTML és CSS formázású levelek küldésének lehetősége a hackerek és vírusok előtt is újabb kapukat nyitott, de a GFI MailSecurity képes ellenőrizni és kiszűrni a káros kódsorokat, így a címzetthez már csak a biztonságos tartalom érkezik meg.

Felhasználó szintű, szabályrendszer alapú tartalomszűrés

A felhasználó (címtár) és kulcsszó alapú, erőteljes tartalomszűrő és szabályrendszer gondoskodik arról, hogy a kétes tartalom előbb karanténba kerüljön, és csak ellenőrzés után jusson a felhasználókhöz.

Egyéni, RSS felügyelt karantén-szabályok

A karantén-elemek gyorsabb és egyszerűbb kezelését segíti a Microsoft Outlook Keresési mappákhoz hasonló szolgáltatás, mely a karantén mappákra is alkalmazható. Lehetőség van külön mappába gyűjteni a vírusgyanús leveleket és a gyanús mellékleteket tartalmazó leveleket későbbi ellenőrzés céljából, így hamarabb kerülhetnek a felhasználókhöz a levelek. Az RSS csatornák segítségével még egyszerűbbé válik a mindennapi munka, mert nem kell folyamatosan belépni és ellenőrizni az új elemeket a karanténban, hanem csak az RSS csatornákat kell szemmel tartani.

Directory Harvest védelem

A GFI MailSecurity Directory Harvest védelme megakadályozza a címlista feltérképezését, mert a rendszer a címtárban nem található címzett esetén nem küld hibáüzenetet a feladónak. A hibás címzetteknek küldött leveleket karanténba helyezi, ezzel biztosítva, hogy a későbbiekben visszakereshetők legyenek ezek a levelek.

Egyszerűsített karantén-menedzsment

A GFI MailSecurity számos eszközt kínál a karanténba került elemek kezelésére. A dedikált adminisztrációs kliens a megszokott Windows alkalmazások rugalmasságát biztosítja, míg a webalapú kliens a hálózat bármely pontján elérhető, így a karanténba került levelek azonnal elfogadhatók vagy elutasíthatók. Lehetőség van az Outlook Nyilvános Mappa szolgáltatásának használatára is, amellyel a karantén-menedzsment szétsztható az adminisztrátorok között.

Automatikus karantén-menedzsment

A Time-to-Live szolgáltatás segítségével a karanténban tárolt elemek automatikus törlését lehet elvégezni megadott paraméterek alapján (például: 14 napnál régebbi levelek). Ez a megoldás biztosítja, hogy a karantén által felhasznált szerver erőforrások (pl. karantén diszkerületek) jól méretezhetőek és karbantarthatóak legyenek.

Riportolási lehetőségek

A GFI MailSecurity ReportPack egy ingyenes, kiegészítő programcsomag, mellyel a vezetők részére bemutatató riportok készíthetőek. Az egyszerűen áttekinthető jelentések segítenek értelmezni és értékelni az alkalmazott szabályokat. Az előre definiált riportok módosítása révén új, egyéni riportsablonok készíthetők és óránkénti, napi, heti vagy havi ütemezésben, amelyek automatikusan le is kérhetőek.

Rendszerkövetelmények

- Windows 2000/2003 SBS, Windows XP
- Microsoft Exchange Server 2000/2003/2007/5.5, Lotus Notes, vagy más SMTP szerver
- Small Business Server alapokon, Exchange Server 2000 esetén SP2, Exchange Server 2003 esetén SP1 telepítés
- .NET Framework 2.0
- Microsoft Messaging Queueing Service
- IIS SMTP service

Díjak

