10 lépés a vállalati vírusvédelem telepítése során

Utolsó frissítés dátuma: Budapest, 2020. 01. 10.

A G DATA 35 éve partner a vírusvédelemben. 1985-ben cégünk alapítója és jelenlegi ügyvezetője, Kai Figge mutatta be a világ első vírusirtó koncepcióját, majd két évvel később ő és társa, Frank Kühn készítették el a legelső antivírust Atari ST rendszerre. Az elsők között készítettünk vírusirtót MS DOS és Windows rendszerre is.

A vírusvédelem az elmúlt 35 év alatt rengeteget fejlődött, és mára komplex technológiák halmazát jelenti, amelyek egymással együttműködve védelmezik a klienseket. Szokás ezt új generációs vírusvédelemnek is nevezni, de a marketingcímkéken túllépve a lényeg az, hogy a hagyományos szignatúraalapú és heurisztikus védelmet ma olyan dedikált technológiák egészítik ki, mint a mesterséges intelligenciát használó DeepRay, a fizetések biztonságát garantáló BankGuard vagy a zsarolóvírusok ellen védelmet nyújtó G DATA Zsarolásvédelem.

Ezekről a technológiákról bővebben tájékozódhat blogunkban, például ebben a cikkben.

Ennek az óriási fejlődésnek egyik következménye, hogy a vállalati vírusvédelem összetett alkalmazás, amelyet körültekintően érdemes telepíteni és beállítani.

Gyors útmutatónkban néhány fontos tudnivalót szedtünk össze, így jelen útmutató tanulmányozása nem helyettesíti a teljes kézikönyv elolvasását.

Tartalomjegyzék

Tudnivalók a telepítés előtt

Előző vírusvédelem eltávolítása

A vírusirtó szoftverek jogi okok miatt nem távolítják el versenytársaik termékeit. Ezért a telepítés előtt az előző vírusvédelmet Önnek kell eltávolítania.

Előfordul, hogy a Windows ezt nem képes maradéktalanul végrehajtani, ezért minden vírusvédelmi gyártó kiad egy saját eltávolító alkalmazást (removal tool). Ez a G DATA esetében az AV-Cleaner. **Az előző vírusirtójának eltávolító eszközével ellenőrizheti, hogy az előző védelem eltávolítása maradéktalanul megtörtént.** Szinte minden esetben szükség van a gépek újraindítására is.

Ütköző alkalmazások eltávolítása

A vírusirtó szoftverek működését jellemzően akadályozzák a különböző kiegészítő védelmi megoldások, mint például egy kémprogramvédelmi alkalmazás. Ilyen ütköző alkalmazás lehet egy kéretlenül települt böngészőkiegészítő is.

A vírusirtók működését emellett megzavarhatják a különböző “rendszer-optimalizáló” alkalmazások, amelyek körültekintés nélküli lefuttatása akadályozhatja a gépre telepített alkalmazások - így a vírusvédelem - működését.

Hálózati kommunikáció

A G DATA kliensek és a központi menedzsment alapértelmezés szerint a hálózati neveik alapján tartják egymással a kapcsolatot, úgy, hogy a kliensek keresik a szervert annak neve alapján a hálózaton. Amennyiben azt szeretné, hogy a kliensek a szerver IP-címe vagy FQDN neve alapján keressék a szervert, ezt még a kliensek telepítése előtt érdemes konfigurálnia, mivel ha a kliensek telepítése után módosítja a szerver nevét, a már telepített kliensek nem fogják megtalálni a szervert a hálózaton (csak miután mindegyiken egyesével vagy AD segítségével megváltoztatja a beállításokat). Ugyanez igaz a szerver újratelepítésére: ha a szerver neve megváltozik, ezt az összes kliensen módosítani kell.

Hardver- és szoftverkövetelmények

Kérjük, ellenőrizze a kézikönyvben a G DATA telepítéséhez szükséges hardver- és szoftverkövetelményeket. A központi menedzsment telepítése on-site telepítés esetében adatbázist igényel. A G DATA telepít adatbázist (SQL Express), vagy dönthet úgy, hogy egy már meglévő SQL adatbázist használ. Az SQL Express és az SQL adatbázisok használata igényli a .NET keretrendszer telepítését, kérjük, hogy ezekről tájékozódjon a kézikönyvben.

Telepítés és frissítés

A G DATA vállalati termékei egy központi menedzsment részből, valamint az ehhez csatlakozó kliensekből állnak. A szervert kiegészítheti alhálózati szerver (a terhelés elosztására) és tükörszerver (a folyamatos rendelkezésre állás biztosításához). A kliensek közé soroljuk a PC- és notebookeszközöket, a levelezőszervereket (Exchange és Linux Mail Gateway), a mobilklienseket és a fájlszervereket is. G DATA-klienst telepíthetünk arra a szerverre is, amelyen a G DATA központi menedzsmentje fut - ez fogja megvédeni az adott gépet. Fontos, hogy a szerverekre telepített kliensvédelmet mindig körültekintően kell beállítani, mivel az – különösen levelezőszerverek esetében – befolyásolhatja a szerver teljesítményét. **Ezért szerverek esetében különösen fontos a kivételek meghatározása.**

A G DATA védelmének telepítése során a helyes sorrend a következő: elsőként telepítjük a központi menedzsmentet, ezután a Start menübe telepített Internet Update alkalmazás segítségével, a G DATA Administrator elindítása nélkül regisztráljuk a szoftvert, majd frissítjük a szignatúrákat, valamint a programkomponenseket. Ha elvégeztük a központi menedzsment telepítését, beállítottuk az adatbázist és frissítettük a szignatúrákat, valamint a programkomponenseket, akkor következhet a kliensek telepítése. Ezt célszerű nem a telepítő CD-ről, hanem a központi menedzsmentből közvetlenül, vagy a központi menedzsment segítségével létrehozott telepítőcsomag segítségével elvégezni.

Fertőzött gépek kezelése

Amennyiben egy számítógépen fertőzést gyanítunk, ezt a kliensvédelem telepítése előtt érdemes már megtisztítani. Ehhez használhatjuk a G DATA Indítólemezt (G DATA Boot Medium). Így a kliensvédelmet már a megtisztított kliensre fogjuk telepíteni.

Technológiák aktiválása

FONTOS, hogy a G DATA vállalati termékében a lakossági termékektől eltérően alapértelmezés szerint nincs minden védelmi technológia aktiválva.

Ennek oka, hogy vállalati környezetben létezhetnek olyan speciális alkalmazások, amelyeket a különböző vírusvédelmi technológiák blokkolnak - jellemzően azért, mert azok kártevőkhöz hasonlóan viselkednek, vagy nem rendelkeznek megfelelő tanúsítvánnyal.

Ilyen például a G DATA Zsarolásvédelem (Anti-Ransomware) és a G DATA Sérülékenységvédelem (Exploit Protection).

Ezeket a technológiákat külön kell aktiválni a maximális védelem biztosításához, de ezt körültekintéssel és lépcsőzetesen érdemes megtenni – azaz nem egyszerre a hálózat egészében.

Tesztelés és konfigurálás

Az előző pontban említett speciális vállalati alkalmazások miatt fontos lehet, hogy a vírusvédelmet ne egyszerre aktiváljuk a hálózat egészén. Ez különösen kiterjedt hálózatok esetében fontos. Érdemes elkészíteni/lemásolni olyan tipikus konfigurációkat, amelyek a hálózatban jelen vannak, és a vírusvédelmet ezeken tesztelni – megvizsgálva a kompatibilitást a vállalatnál használt egyedi alkalmazásokkal.

A tapasztalatok és tesztek alapján kell beállítani a kivételeket. Fontos, hogy a kivételeket külön-külön kezeljük a kézi indítású víruskeresésre, az állandó vírusvédelemre és a webes védelemre. A bevezetés során lehetőség van igénybe venni a G DATA

terméktámogatásának segítségét is: amennyiben egy alkalmazásra a vírusvédelem téves riasztást ad, azt lehetőség van fehérlistáztatni.

Exchange szerverek esetében nem javasolt egyszerre használni a G DATA Exchange Plugint és a kliens portszűrését, mivel ez a levelek dupla átvizsgálását jelenti.

Szerverek esetében ügyelni kell a megfelelő kivételek meghatározására.

A konfigurálás során el kell dönteni, hogy a felhasználóknak milyen jogosultságot adunk meg, ügyelve arra, hogy amennyiben a felhasználók végezhetnek víruskeresést, úgy arra is jogot adunk, hogy a megtalált és kártékonynak jelölt fájlokat megtisztítsák. Ez könnyen járhat például azzal, hogy egy felhasználó törli saját lokális .pst archívumát, mivel nem tájékozott arról, hogy ez milyen következményekkel jár a gépén.

Ne felejtsük el létrehozni és beállítani a különböző jelentéseket és értesítéseket sem, amelyek tájékoztatják a rendszergazdákat a különböző hálózati eseményekről.

Hibaelhárítás

A vírusvédelem működésében tipikusan az alábbiak okozhatnak fennakadást, ezért ha a telepítőcsomag telepítése nem sikerül, vagy a kliens és a szerver között nincs kapcsolat, az alábbiakat érdemes első körben ellenőrizni.

Jogosultság hiánya

A kliensre történő távoli telepítéshez jogosultság szükséges. Az azonos tartományi rendszergazdafióknak mindkét gépen léteznie kell.

Hiányzó tanúsítvány

Korábbi operációs rendszereken előfordulhat, hogy a G DATA aláíró tanúsítványát a Windows még nem ismeri. Ilyen esetben a tanúsítványt importálni kell a kliensvédelem telepítéséhez.

Frissítések hiánya

Előfordulhat, hogy a kliensvédelem telepítése a Windows-frissítések hiánya miatt nem hajtható végre.

Hálózati hibák

A leggyakoribb oka a hibáknak, hogy a kliens és a szerver között nincs hálózati kapcsolat (ezt Telnet segítségével tudja ellenőrizni, a kommunikációs portok leírását pedig magyar nyelvű tudásbázisunkban megtalálja a https://tamogatas.virusirto.hu címen).

Elnevezésből származó hibák

Szintén gyakori hibázási ok, hogy a szerver *nevét* a kliens nem találja meg a hálózaton, akár a rossz szintaktika miatt, akár azért, mert a szerver átnevezésre került. A kliens a szerveren egyedi AES kulccsal azonosítja magát, amelyet a telepítéskor kap meg. A szerver megjegyzi, hogy melyik klienshez melyik AES kulcs tartozik.

A telepítés után a klienst engedélyezni (authenticate) kell a szerveren, csak ezután tudja letölteni a frissítéseket.

Amennyiben a kliens az Active Directoryban átnevezésre kerül, a szerver nem fogja visszaengedni. Ezért a kliens átnevezése előtt fontos, hogy tájékozódjunk a megfelelő lépésekről.

Más alkalmazások maradványai

Szintén gyakori hibaok, hogy a kliens telepítését vagy működését egy harmadik alkalmazás vagy annak maradványa blokkolja. Ilyen lehet sorrendben:

- Előző vírusirtó szoftver
- Kémprogramvédelmi alkalmazás vagy biztonsági böngészőkiegészítő
- Rendszer-optimalizáló alkalmazás

Hiba esetén meg kell győződnie arról, hogy harmadik fél által gyártott alkalmazás vagy annak maradványa nem blokkolja-e a G DATA működését. Az előző vírusvédelmi szoftver hivatalos eltávolító eszközét érdemes lefuttatnia.

Debuggolás

Amennyiben a fenti lépések nem hoznak eredményt, a klienst debuggolni kell. Ehhez a tudásbázisunkban talál segítséget. A debug logok mellett szükség lesz a telepítési naplófájlok, valamint az MsInfo fájl beküldésére is. Ezeket megoszthatja egy linken, hogy a terméktámogatási munkatársaink le tudják azokat tölteni.

Két fontos cikk a nemzetközi tudásbázisban:
Kliens és szerver közötti kommunikációs hiba elhárítása
Kliens debuggolása kommunikációs hiba esetében

G DATA eszközök

A G DATA különböző speciális eszközöket biztosít a hatékony működtetéshez, amelyeket tudásbázisunkból tölthet le.

A **G DATA AV-Cleaner** minden G DATA alkalmazást eltávolít egy számítógépről, a szerverkomponenseket is beleértve. Lehetséges, hogy az AV-Cleaner használata során a gépet többször újra kell indítania.

A **G DATA Activity Monitor** azt mutatja meg, hogy a G DATA milyen folyamatokat vizsgál a gépen. Ez az eszköz használható olyankor, ha teljesítménnyel kapcsolatos problémákat tapasztalunk.

A **G DATA Indítólemez** az operációs rendszer kívülről történő átvizsgálására szolgál, és aktív, a számítógép használatát megakadályozó vírusfertőzés esetén használható.

Kézikönyvek és tudásbázis

G DATA vállalati termékek kézikönyve
G DATA vállalati termékek működését ismertető referencia útmutató
G DATA magyar nyelvű tudásbázis

Hibajegy nyitása

Hibajegyet ezen az oldalon tud nyitni. Kérjük, hogy a hibajegyet minél több adattal töltse ki, beleértve az operációs rendszer verziószámát, a G DATA kliens verziószámát, valamint a hibát bemutató képernyőképet is.

A magyar nyelvű terméktámogatást a tamogatas@virusirto.hu címen tudja igénybe venni.

A magyar ügyfélszolgálat a +36 1 782 4246-os telefonszámon érhető el, hétköznaponként, munkaidőben reggel 10 és délután 16 óra között.

A nemzetközi ügyfélszolgálat (angol vagy német nyelven) a +36 1 999 6709 nem emelt díjas, budapesti telefonszámon érhető el, 0-24 órában, mindennap.

Biztonság a vírusvédelmen túl

A G DATA Endpoint Protection szoftver a vírusvédelmen túli biztonságot is nyújt a **Házirendkezelő** segítségével.

Az **Application Control modul** használata ajánlott szervereken. Fehérlista módban csak és kizárólag azok az alkalmazások futhatnak, amelyeket előre engedélyeztünk. Minden egyes engedélyezni kívánt alkalmazást fel kell vennünk az engedélyezettek közé ahhoz, hogy futni tudjon. Ez a mód a lehető legkevesebb teret adja a kártékony alkalmazások elindulásának.

Klienseken, feketelista módban pedig azoknak az alkalmazásoknak a futását tiltjuk, amelyeket a feketelistára felvettünk. Ebben segít a szoftverleltár funkció is, a kliensekre telepített szoftverek listájából azonnal a feketelistára szervezhetjük a nem kívánt alkalmazásokat.

A biztonságot növeli emellett a **külső eszközök letiltása,** valamint a **kategória alapú webszűrő** használata is.