MULTISCAN ARCHITEKTÚRA KIALAKÍTÁSA

MIÉRT VAN SZÜKSÉG MULTISCAN KÖRNYEZETRE?

A hagyományos AV/AM eszközök kártékony kód felismerése időablakhoz kötött: csak azokat a kártékony kódokat ismerik fel az adott pillanatban, amelyek szignatúrája és lenyomata megtalálható az eszköz szignatúra-adatbázisában.
Egy-egy újabb malware vagy malware-variáns megjelenése után akár napoknak, heteknek kell eltelnie ahhoz, hogy az új szignatúra bekerüljön az üzemben lévő AV/AM eszközök adatbázisába.
Egyetlen – vagy akár két – motor sem ismerhet fel minden fertőzést az adott időpillanatban.
A legtöbb üzemeltető és biztonsági szakember találkozott már azzal, hogy az adott kártékony kódot a vállalat AV/AM eszköze nem ismeri fel, viszont egy másik AV/AM eszköz képes ellene védelmet nyújtani.
A jelenség oka az, hogy a különböző gyártók különböző reagálási idő mellett frissítik szignatúra adatbázisaikat. Amíg a vállalat AV/AM eszköze nem képes az új variáns vagy új malware felismerésére, a hálózat és a munkaállomások védtelenek az új variánsú kártékony kódokkal szemben.

MULTISCAN KÖRNYEZET KIALAKÍTÁSA A HATÁRVÉDELEMBEN

Multiscan környezetek kialakításával lehetővé válik a meglévő határvédelmi infrastruktúra (web szűrés, email szűrés) megerősítése, akár további 20, párhuzamosan működő AV/AM motorral. A multiscan környezet együttműködik a már üzem alatt lévő web- és e-mail védelmi eszközökkel. Az integráció célja nem a meglévő eszközök kiváltása, hanem a meglévő eszközök megerősítése, képességeiknek fokozása.

Kutatói célú elemzés

A multiscan környezet ICAP protokollon keresztül integrálódik a meglévő Web határvédelmi eszközhöz vagy proxy szerverhez. Minden webes forgalom vizsgálatra kerül, és a multiscan rendszer akár 20 AV/AM motorral vizsgálja át az adatforgalmat. Amennyiben fertőzést vagy kártevőt észlel valamely motor, az adott fájl letöltése blokkolásra kerül.

Multiscan környezet e-mail határvédelemben

A multiscan rendszer beépül az e-mail forgalomba. Lehetőség van csak a bejövő, vagy csak a kimenő levelek sokmotoros vizsgálatára is. A megvizsgált levelek és csatolmányok karanténba kerülnek, ha a motorok valamelyike fertőzést vagy rosszindulatú adattartalmat észlel.

Párhuzamos vizsgálatok

A multiscan környezet a kapott fájlokat (ICAP, SMTP, stb.) és objektumokat egy lépésben vizsgálja meg, tehát az egyes motorok nem egymás után, hanem egyszerre képesek ellenőrizni az adott objektumot vagy fájlt, így nem lép fel olyan késleltetés, amely zavarná a felhasználói élményt.

MULTISCAN KÖRNYEZET KIALAKÍTÁSA ADATTÁRAKHOZ ÉS PORTÁLOKHOZ

Legyen szó SharePoint-ról, vagy OpenText-ről, vagy bármely más adattárház vagy dokumentumkezelő alkalmazásról, minden esetben felmerül az a kérdés, hogy ha a vállalati adatvagyont ezekben a rendszerekben tároljuk, akkor hogyan tudjuk biztosítani azt, hogy az adattárban csak fertőzés és káros tartalom nélküli állományok és dokumentumok szerepeljenek?
A multiscan környezet vizsgáló szervere számos API felülettel rendelkezik és támogatja a legismertebb programozási nyelveket (C, Python, PHP, PERL, stb.), így bármely dokumentumkezelő vagy adattár rendszerhez hozzáilleszthető.
Amikor a felhasználó feltölt vagy elment egy dokumentumot az adattárban vagy dokumentumkezelőben, az állomány átadható vizsgálatra egy workflow-n keresztül a multiscan rendszernek, amely ellenőrzi és megvizsgálja a dokumentumot. Amennyiben a fájl tiszta, a dokumentumkezelő letárolhatja az állományt, míg fertőzött vagy kártékony tartalom esetén a tárolási folyamat megáll és a felhasználó értesítést kap a tárolni kívánt dokumentum fertőzöttségéről. Természetesen az ilyen blokkolásokról helyi vagy syslog naplóbejegyzés történik, így akár SIEM rendszerekkel is integrálható a megoldás.

MULTISCAN KÖRNYEZET WEBALKALMAZÁSOKHOZ, PORTÁLOKHOZ

A webalkalmazások gyakran biztosítanak adatfeltöltési lehetőséget – legyen az egy blog (pl. Wordpress) vagy akár üzletkötői portál, ahova a külső szerződéskötők töltik fel a kitöltött dokumentumokat és szerződéseket. A belső “office/trusted” hálózat és a portál backend között legtöbbször már nincs malware és vírusvédelem kialakítva, így a feltöltött dokumentumok nem kerülnek megfelelő malware és vírusvédelmi ellenőrzésre.
Nem csak adattárakhoz, de bármilyen webalkalmazáshoz hozzáilleszthető a multiscan környezet, amely képes REST API felületen csatlakozni. Az API felület a legtöbb programozási nyelvben felhasználható, így PHP, C, VB, Python, stb. nyelveken bármilyen külső alkalmazás hozzáilleszthető.
Minden egyes állományfeltöltés keresztülmehet a sokmotoros AV/AM malware vizsgálaton, illetve akár a portálról való fájl letöltések is vizsgálatra kerülhetnek. Amennyiben a fel- vagy letöltött állomány káros adattartalommal rendelkezik, a rendszer megakadályozza annak eltárolását és értesíti a felhasználót vagy az üzemeltetőt.