Heurisztika vagy kellemetlen meglepetés?

Az esettanulmány készítésének időpontja: **2007. március**

NOD32 a GSK Computer Kft.-nél

A GSK Computer hálózatát 2006 nyarán komoly vírustámadás érte. A rendszerbe betörő kórokozót az akkor használt vírusirtó nem ismerte fel, és nem tudta megállítani, ezért a vállalat szakemberei új megoldást kerestek.

„A pusztán vírusdefiníciós adatbázis alapján, heurisztika nélkül működő vírusirtók ma már nem korszerűek."

Halász Attila,
a GSK Computer Kft. informatikai menedzsere

ThreatSense technology

NOD32 technology

we protect your digital worlds

eset

A GSK Computer Kft. a távkönyvelés, a kontrolling és a hitelkártyás fizetések feldolgozása mellett repülőjegyek számítógépes rögzítésével és rendszerezésével, valamint a jegyeladások ellenőrzésével foglalkozik. A vállalkozás fő szakmai partnere 1998 óta az olasz Alitalia légitársaság. A jelenleg 115 főt alkalmazó vállalkozás szakemberei egy komoly vírusfertőzés után döntöttek úgy, hogy a korábban használt antivírusrendszer helyett megbízhatóbbat keresnek.

A GSK Computer mintegy 130, homogén operációs rendszerrel rendelkező kliensgépből, Windows 2003-, Exchange-, valamint Linux-szerverekből felépülő hálózatát 2006 nyarán komoly vírustámadás érte. A rendszerbe betörő kórokozót az akkor használt – egyébként jó nevű – vírusirtó nem ismerte fel, és nem tudta megállítani. *„A vírus megtámadta a szerverünket, és a megosztásokon keresztül továbbterjedt az egész rendszerre”* – emlékezett vissza Halász Attila, a GSK Computer Kft. informatikai menedzsere. A kórokozó – 115 kilobájtnyi pluszkód hozzáadásával – majdnem minden végrehajtható fájlt használhatatlanná tett a megfertőzött számítógépeken. *„A támadás következtében másfél napra leállt az egyik szerverünk, amelyen egyébként kényes adatokat is tároltunk”* – mondta el a szakember. Az előrelátó szakemberek által konfigurált folyamatos biztonsági mentéseknek köszönhetően szerencsére komolyabb kár nem történt, így az adatbázisok sem sérültek meg.

Próbaverzió után élesben is NOD32

A GSK informatikai szakemberei a bekövetkezett fertőzést több gyártó antivírusszoftverének próbaverziójával kísérelték meg hatástalanítani. *„Két-három jó nevű terméket töltöttünk le, amelyek között ott volt a független víruslaboratóriumok tesztjein folyamatosan jól szerepelő NOD32 is”* – mondta el Halász Attila.

A letöltött szoftverek közül végül pont ez volt képes kisegíteni a céget a bajból. *„A próbaverziókat a szerverünkre töltöttük le, mert úgy gondoltuk, hogy a fertőzés gócpontjában kezdjük el irtani a vírust. Ám egyedül a NOD32 regisztrálta, hogy ezek az állományok manipulálva lettek”* – ismertette tapasztalatait a szakember.

Így a NOD32 segítségével sikerült elhárítani a fertőzést, a távoli elérésen alapuló programfuttatások helyreállítása azonban pluszmunkát és -időt igényelt, ami felhívta az informatikai menedzsment figyelmét arra, hogy a heurisztikus védelmet is biztosító, az új, ismeretlen kórokozók többségét felismerni képes antivírus-megoldás sokkal jobb védelmi teljesítményt nyújt, mint korábbi antivírusrendszerük. Ezért a GSK a harmincnapos próbaidő után felvette a kapcsolatot a vírusirtót forgalmazó Sicontact Kft. szakembereivel, és árajánlatot kért egy Windows- és Linux-környezetben egyaránt működő licenckonstrukcióra. *„Végül a százharminc gép NOD32-telepítését házon belül, távoli adminisztrációval pár nap alatt meg tudtuk oldani”* – mondta el a menedzser.

„Oldjuk meg magunk a problémát!”

A NOD32 egyik előnye, hogy a vírusirtó automatikusan – akár naponta többször – frissíti önmagát, amikor szükséges. *„A korábbi antivírusrendszerben erre egy bizonyos időintervallum volt meghatározva, egyéb esetekben az informatikusainknak külön kellett akceptálniuk, majd a rendszerbe integrálniuk a frissítéseket”* – emlékezett Halász, és hozzátette: *„Az internet elterjedésével ennek automatikusan kell megtörténnie, s ez megint csak a NOD32 mellett szól.”*

A GSK rendszerét azóta a NOD32 védi, de a vállalat hálózatát korábban megtámadó vírus néha még ma is felbukkan. A visszafertőzések abból a világméretű vállalati hálózatból érkeznek, amelyre partnerei miatt a cég csatlakozik, azonban a korábbi antivírusrendszerrel szemben a NOD32 mindig megfogja a vírusokat. *„Érdekes, hogy a korábbi vírusirtónk még most, hónapokkal a fertőzés után sem ismeri fel ezt a kórokozót”* – jegyezte meg a szakember. Az informatikai menedzser szerint azokban az esetekben, amikor a vállalati rendszerek között átfedések vannak, és egy cégnek más vállalatok hálózatában is dolgoznia kell, különösen fontos a biztonság. *„Nem várhatunk másokra, inkább oldjuk meg magunk a problémát, és alkalmazzunk mi olyan antivírusrendszert, amely megállítja a fertőzést! Csak ezután elemezgessük, mi is volt a baj!”* – tette hozzá Halász Attila.

Heurisztikus vírusvédelem

Más antivírusgyártóktól eltérően a NOD32 esetében az ügyfelek egy szolgáltatást licencelnek. Így a felhasználók nem csupán az adatbázis-frissítésekhez jutnak hozzá, hanem mindig a program – az antivírusmotor – legkorszerűbb változatát használhatják. *„Ez a vásárlás során lehetővé tette számunkra, hogy hosszabb távban gondolkodjunk. Azt tartottuk célszerűnek, hogy ha három évre megveszünk egy szolgáltatást, akkor az foglaljon magában mindent. A NOD32 esetében amikor programfrissítés van, azt mi is automatikusan megkapjuk”* – emelte ki a szakember. A GSK számára emellett különösen fontos, hogy a szoftver kedvező áron nyújt „pontos”, „korrekt” és „informatikusbarát” szolgáltatást. Továbbá a heurisztikus keresésen alapuló szűrésnek köszönhetően olyan vírusokat is észrevesz, amelyek az adott pillanatban még egyetlen antivírusszoftver vírusdefiníciós adatbázisában sincsenek benne. *„A pusztán vírusdefiníciós adatbázis alapján, heurisztika nélkül működő vírusirtók ma már nem korszerűek”* – hangsúlyozta Halász Attila, aki más vállalatoknak is azt ajánlja, hogy körültekintően válasszák ki, milyen antivírus-megoldás alkalmazása mellett döntenek.