MIÉRT PROXEDO API SECURITY?

1. **Az API-forgalom részletes vizsgálata és szabályozása**
2. **Egyedi biztonsági szabályok kikényszerítése**
3. **Részletes biztonsági és auditnaplózás**
4. **Rugalmas, magasan képzett szenior mérnökcsapat**
5. **A proxy technológia úttörői**
6. **Magyar fejlesztés – 'Tiszta' kódbázis**

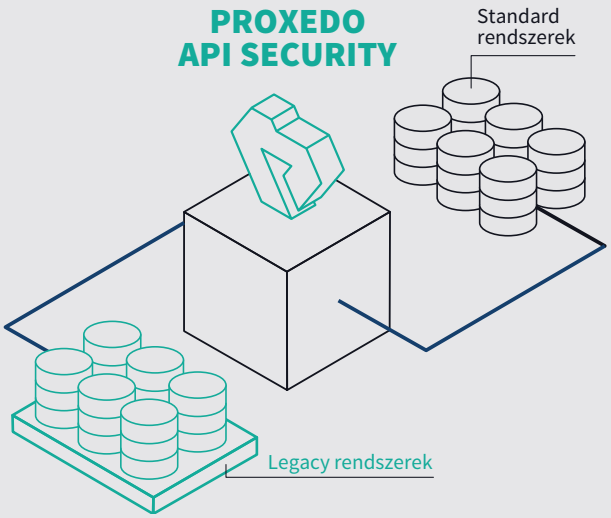
PROXEDO
API SECURITY

„A széles körben elterjedt WannaCry és NotPetya támadások a legacy operációs rendszerek ismert biztonsági réseit használják ki...”

– securityintelligence.com

LEGACY ALKALMAZÁSOK VÉDELME

A legacy infrastruktúrák sok iparágban továbbra is a vállalatok szerves részét képezik. Számos bank központi rendszere AS/400-as számítógépeken fut, teljes egészségügyi rendszerek épülnek Windows XP-re, jónéhány üzleti alkalmazás máig Linux RHEL4 operációs rendszeren fut, az ATM-ek többsége pedig a mai napig tíz évnél régebbi Windows-verziókkal üzemel – hogy csak néhány példát említsünk. Az egyedi (proprietary) szoftverek cseréje vagy frissítése költséges, sőt bizonyos esetekben szinte lehetetlen feladat, ezért csökkentenie kell azt a kockázatot, amelyet az API-kkal (Application Programming Interface-ekkel) ellátott legacy alkalmazásai jelentenek.



Legacy alkalmazások szegregációja és védelme

A kihívás

Régi infrastruktúra – új kockázat

A néhány éve még biztonságosnak számító rendszerek mára már bizonyítottan nem biztonságosak. A legacy rendszerek sok esetben elavult titkosítási protokollokat használnak, vagy érzékeny adatokat küldenek saját magukról (pl. verziószám, hibaüzenetek stb.). A szervezetek viszont gyakran nem fogadják meg a sebezhető rendszerek frissítésére vonatkozó iránymutatásokat, így rengeteg biztonsági rést hagynak kezeletlenül. Napjaink gyakori támadásainak (pl. WannaCry, NotPetya) jelentős hányada a legacy rendszerek ismert biztonsági réseit használja ki.

Kívülről elérhető belső alkalmazások

Ez a helyzet jóval gyakrabban áll elő, mint ahogy azt bármely cég be merné vallani. A belső használatra kifejlesztett webhelyeket a legritkább esetben tervezik a nyilvános webhelyekre vonatkozó biztonsági előírásoknak megfelelően. Az idő múlásával azonban a vállalati fúziók és felvásárlások, a partnerkapcsolatok és az üzleti nyomás hatására a belső alkalmazások az interneten keresztül is elérhetővé válnak. Az API-kon áthaladó, nem megfelelően védett, nyilvános forgalom komoly kockázatot jelent a vállalata számára.

A nem biztonságos legacy eszközök a teljes IT rendszert veszélyeztetik

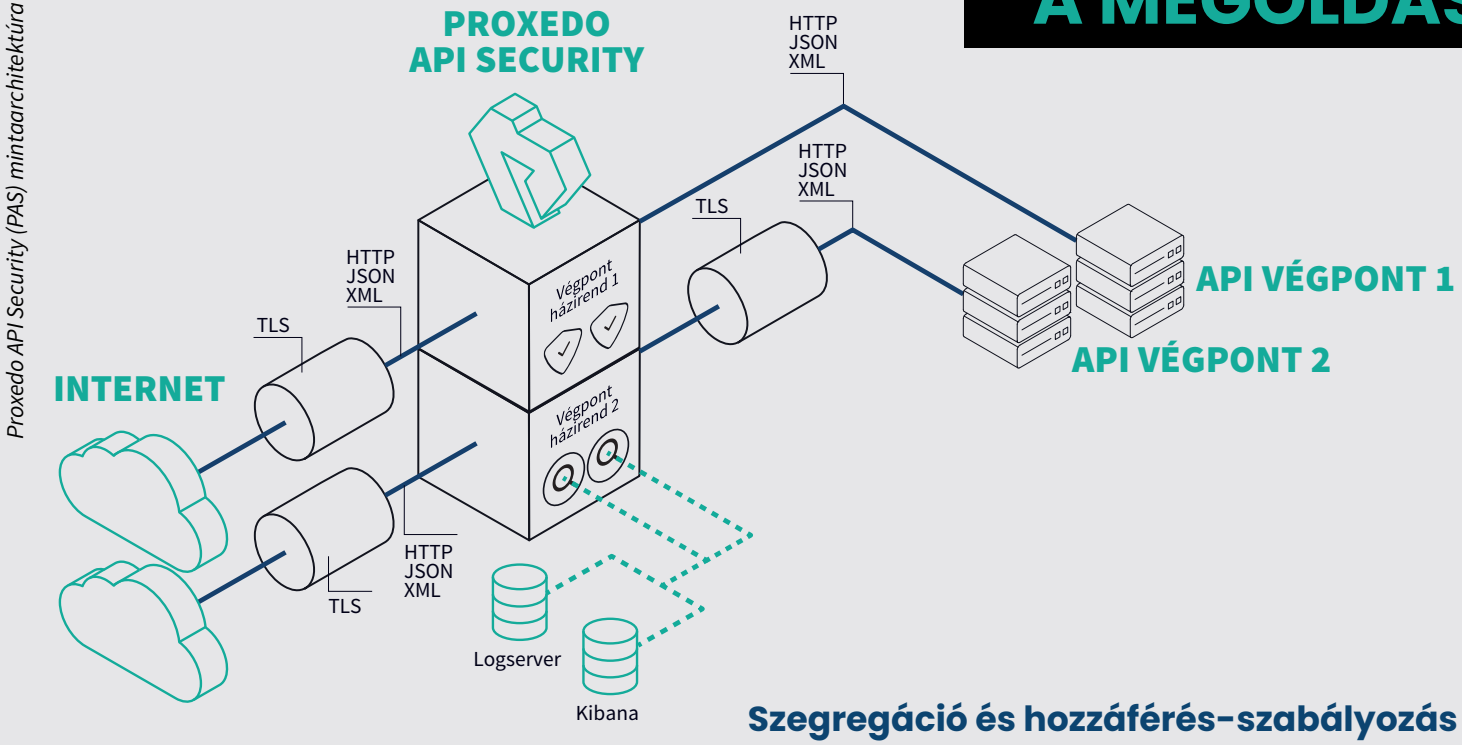
A legacy rendszerek megfelelő védelmének kialakítása kockázatos projekt, ahol nagy a kudarc esélye. Azonban például azok a Windows XP-t futtató eszközök, amelyek nincsenek frissítve, könnyedén kihasználhatók az adatközpontokba történő bejutáshoz. Vagy elég, ha csak a Microsoft Exchange 2013 nemrégiben nyilvánosságra hozott biztonsági résére gondolunk, amely lehetővé tette, hogy a támadók tartományi rendszergazdai jogosultságokat szerezzenek a Windows hálózatokban.

Ha a támadóknak sikerül hozzáférniük egy javítások és frissítések nélküli legacy számítógéphez, akkor egyenes út nyílik számukra a hálózat mélyére. A különféle (legacy és nem legacy) üzleti alkalmazások közötti komplex függőségi kapcsolatok miatt a támadók észrevétlenül mozoghatnak az infrastruktúrán belül.

BALASYS

info@balasys.hu

A MEGOLDÁS



Proxedo API Security (PAS) mintaarchitektúra

API biztonság a WAF-on túl

A Proxedo API Security egy speciális webes alkalmazás-tűzfal (WAF), amelyet az API-végpontok védelmére fejlesztettek ki. Egy rugalmas hálózatbiztonsági célmegoldás, amellyel szabályozhatja alkalmazásai adatforgalmát az API-támadások megelőzése érdekében. A Deep Packet Inspection (DPI) technológiának köszönhetően részletesen ellenőrizheti, titkosíthatja, és elemezheti az API forgalmát, mindezt kiegészítve egy szignatúra adatbázis-alapú védelemmel. Rugalmas architektúrájának köszönhetően vállalata kompromisszumok nélküli, egyedi API biztonsági házirendet kényszeríthet ki. A Proxedo API Security kifejezetten az API biztonságra összpontosít, így remekül kiegészíti a hagyományos WAF és API menedzsment eszközöket is.

ELŐNYÖK

A PAS képes a biztonsági kockázatot jelentő információk elrejtésére, és a legacy alkalmazások sérülékenységeinek kezelésére. A vállalata IT biztonsági és üzemeltetési csapatainak munkáját nagy mértékben segítheti a legacy rendszereket elérhetővé tévő API-k előtt megfelelően kialakított határvédelmi rendszer. A PAS használatával csökkentheti a felmerülő kockázatokat olyan esetekben, amelyekben egy rendszer frissítésére vagy javítására nincs lehetőség.

Proxedo API Security Termékoldal

Próbaverzió kérése

BALASYS

Szegregáció és hozzáférés-szabályozás

A Proxedo API Security képes arra, hogy elkülönítse a legacy rendszereket a többi rendszertől. Biztosítja, hogy a szóban forgó rendszerek ne legyenek közvetlenül elérhetők az internetről, és garantálja, hogy csak korlátozott és szabályozott módon lehessen velük kommunikálni.

Az API kliensek autentikációján túl, a forgalom validálása révén gondoskodhat arról, hogy a legacy alkalmazások bejövő és kimenő forgalma megfeleljen a megadott követelményeknek. Biztosíthatja, hogy csak az engedélyezett adatok juthassanak át a PAS biztonsági rendszerén, és megakadályozhatja, hogy a nem megfelelő vagy potenciálisan rosszindulatú hívások elérjék a legacy rendszereket, és a bizalmas adatok kiszivárogjanak.

Titkosítás és adatmaszkolás

A PAS képes a TLS-protokoll kezelésére, ezáltal biztosítja a titkosítás egységes megvalósítását olyan legacy rendszerek előtt is, amelyek nem feltétlenül támogatják a TLS-t. Sőt, az elavult titkosítási protokollok helyett a legfrissebb TLS-verzió kikényszerítésére is lehetőséget kínál. A PAS használatával központilag kezelheti az API-k TLS-beállításait, így gondoskodhat arról, hogy a konfiguráció a legkorszerűbb biztonsági követelményeknek is megfeleljen.

A PAS az API-forgalom bizonyos elemeinek módosításával biztosíthatja a legacy rendszereivel való kompatibilitást is. Lehetővé teszi a biztonsági rések elrejtését. Eltávolíthatja a hibaüzeneteket, a bannereket és a legacy alkalmazásaira vonatkozó egyéb érzékeny információkat is, ezáltal elrejtheti a háttérinfrastruktúra konfigurációs hibáit.

Felügyelet

A biztonsági felügyelet a legacy rendszerek esetében különösen fontos. A PAS részletes biztonsági és auditnaplózási funkciókat is támogat. A biztonság felügyeleti és riasztási képességek fejlesztése érdekében a releváns naplófájlokat SIEM/SOC-rendszerekbe továbbíthatja. A forgalomnaplózás és -monitorozás használatával még azelőtt észlelheti a legacy alkalmazásokra irányuló fenyegetéseket, mielőtt megtörténne az adatlopás.