MIÉRT PROXEDO API SECURITY?

1. **API forgalom mélységi vizsgálata (DPI)**
2. **Egyéni biztonsági házirend kikényszerítése**
3. **Pozitív biztonsági modell (Positive Security Model)**
4. **Rugalmas, magasan képzett szenior mérnökcsapat**
5. **A proxy technológia úttörői**
6. **Magyar fejlesztés – 'Tiszta' kódbázis**

PROXEDO
API SECURITY

„A Gartner becslései szerint 2022-re az API-támadások lesznek a leggyakoribb olyan támadások, amelyek a vállalati alkalmazásokat érintő adatlopásokhoz vezetnek."

VÉDELEM AZ API-TÁMADÁSOK ELLEN

A kihívás

Manapság az API-k több tízezer webes és felhőalkalmazást, mikroszolgáltatást, valamint mobil- és IoT-eszközt kötnek össze, ezáltal biztosítják a gépek közötti zavartalan kommunikációt. Az API-k száma rendkívüli mértékben növekszik. Ezeken a felületeken elképesztő mennyiségű bizalmas adat megy keresztül: személyes azonosítók, pénzügyi- és egészségügyi adatok és vállalati titkok egyaránt. Az API-k tehát kiskapuként használhatók a vállalati rendszerekbe való bejutáshoz. Ennek eredményeként az API-infrastruktúrák elterjedése komoly biztonsági kockázatokat jelent.

A támadók az API-kat veszik célba

Az API-k használatából eredően a veszélyeztetett bizalmas adatok mennyisége gyors ütemben növekszik, ezáltal az API-k egyre inkább a támadók elsődleges célpontjává válnak. A sebezhető, hibás API-k felkutatásával képesek bejutni a bizalmas adatokat tároló háttérrendszerekbe. És ezek a támadások egyre sikeresebbek. A közelmúltban történt nagyobb adatlopások közül sok esetben az API-k sebezhetőségét használták ki – gondoljunk csak a Salesforce.com, a T-Mobile, a McDonald's és az Egyesült Államok Posta-szolgálatának esetére. Ez a probléma tehát mérettől és iparágtól függetlenül minden vállalatot érint.

Az API-fejlesztők nem a biztonságot tartják elsődleges szempontnak

A legtöbb alkalmazásfejlesztési projekt esetében a biztonság helyett elsősorban a funkcionalitás, a felhasználói élmény és a határidők számítanak. Számos ilyen projektből hiányzik a biztonsági követelmények részletes meghatározása. A fejlesztők nem a támadók fejével gondolkoznak. API-szabványok hiányában "best effort" alapon gondoskodnak csak a biztonságról. Ebből kifolyólag a nyilvános API-k egyedi biztonsági réseket tartalmaznak, ez pedig kockázatot jelent a vállalkozásra nézve, és lehetőséget kínál a támadók számára.

API-kockázatokkal van tele az OWASP is

A gyenge védelemmel ellátott API-k 2017-ben bukkantak fel először az OWASP (Open Web Application Security Project) top 10-es listáján. 2019-re a listát már az API-kkal kapcsolatos biztonsági kockázatok uralták, sőt az OWASP egy API Security TOP 10 nevű speciális listát is közzétett nemrég.

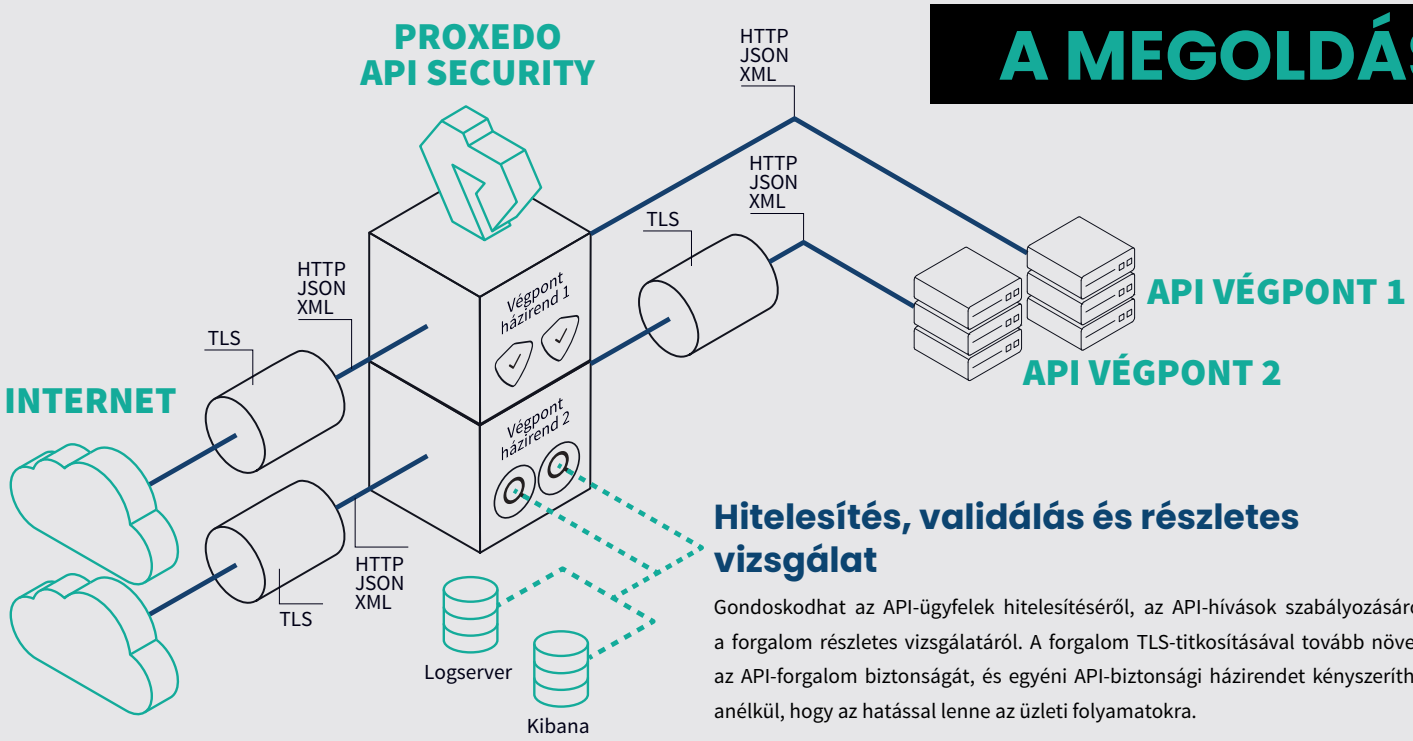
A hagyományos alkalmazásbiztonsági megoldások nem elegendőek

Napjainkban az API-támadások egyre összetettebbek, célozottabbak, amelyek könnyedén megkerülik a hagyományos védelmi rendszereket. A népszerű webes alkalmazás-tűzfalak (WAF-ok), vírusvédelmi, illetve egyéb, alapszintű biztonsági eszközök NEM KÉPESEK az ilyen támadások észlelésére. A fejlett API-támadások csak speciálisan erre a célra fejlesztett megoldásokkal akadályozhatók meg. Azok a vállalatok, amelyek ezzel nincsenek tisztában, hamis biztonságérzet mellett kockára teszik a központi rendszereikben tárolt adataikat.

BALASYS

info@balasys.hu

Proxedo API Security (PAS) mintaarchitektúra



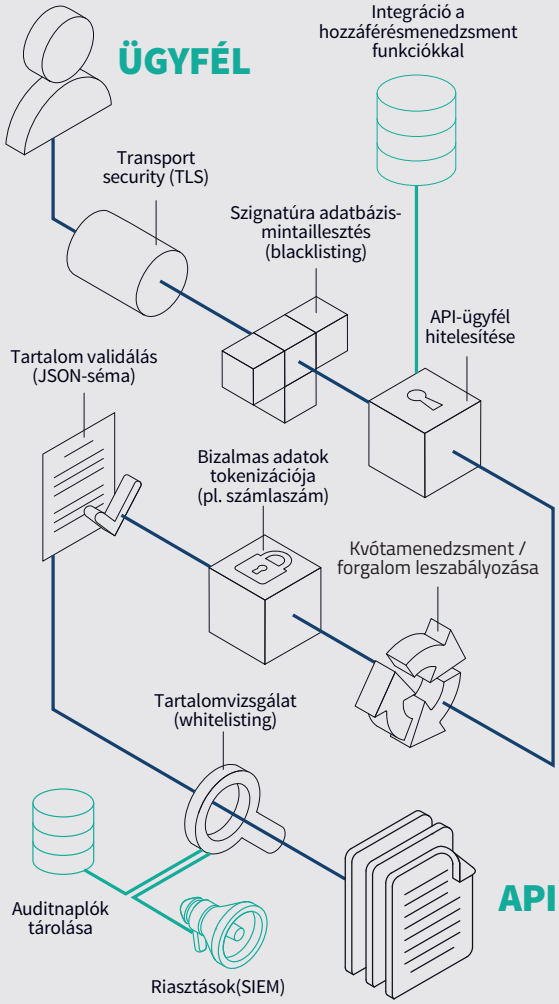
A MEGOLDÁS

Hitelesítés, validálás és részletes vizsgálat

Gondoskodhat az API-ügyfelek hitelesítéséről, az API-hívások szabályozásáról és a forgalom részletes vizsgálatáról. A forgalom TLS-titkosításával tovább növelheti az API-forgalom biztonságát, és egyéni API-biztonsági házirendet kényszeríthet ki anélkül, hogy az hatással lenne az üzleti folyamatokra.

A tartalom validálása révén gondoskodhat arról, hogy az API-végpontok bejövő és kimenő forgalma megfeleljen a megadott követelményeknek. Ezáltal azt is biztosítja, hogy csak az engedélyezett adatok juthassanak át az átjárón. A megoldás emellett támogatja a testreszabható biztonsági naplózást, és az adatok SOC/SIEM-rendszerekbe való továbbítását is, így javítva szervezete biztonsági felügyeleti és riasztási képességét.

A PAS egy szignatúra adatbázissal is folyamatosan összehasonlítja a HTTP(S) forgalmat, hogy azonosítsa a támadási mintákat. Ezzel megvédheti a webes szolgáltatásait az ismert internetes fenyegetésekkel szemben.



Hatékony API-biztonsági eljárásrend kialakítása

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 kompro- misszumok 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 Proxedo API Security legfőbb célja, hogy védelmet nyújtson vállalata számára az API-támadások ellen. A legjobb biztonsági gyakorlatokat kiterjeszti az API-kra irányuló támadások ellen. A megoldás biztosítja, hogy csak az engedélyezett adatok juthassanak át a hálózati határponton, és megakadályozza, hogy a nem megfelelő vagy potenciálisan rosszindulatú kérések elérjék a vállalati rendszereket, illetve hogy kiszivárogjanak a bizalmas adatok onnan.

Proxedo API Security Termékoldal

Próbaverzió kérése

BALASYS