1. **Testreszabható biztonsági szabályzat**
2. **Átfogó TLS és VPN támogatás**
3. **Adatmaszkolás**
4. **Rugalmas és professzionális mérnöki támogatás**
5. **Rendkívül szigorú biztonsági követelmények implementálása**
6. **Egyedi, proxy alapú technológia**
7. **Magyar fejlesztésű kódbázis - "Clean code"**

PROXEDO
NETWORK SECURITY

"A governance, kockázat és megfelelőségi eszközökkel kapcsolatos beruházások összege 50%-kal fog emelkedni 2026-ra a jogi és megfelelőségi részlegeken"

– A Gartner 2023. szeptemberi "Gartner Legal Risk & Compliance Practice" előrejelzésében.

HÁLÓZATI VÉDELEM ÉS TITKOSÍTÁS

A kihívás

TLS-titkosítás – A kétélű kard

A titkosítás az egyetlen módja annak, hogy adatai biztonságban legyenek a hálózaton adatmozgatás közben. A TLS (Transport Layer Security) protokoll használata nem csak az adatbiztonság és a bizalmasság védelmét biztosítja, hanem - sajnos - a rosszindulatú tevékenységek elrejtésére is alkalmas. A támadók ugyanis egyre inkább a titkosítás felé fordulnak, hogy elrejtsék tevékenységüket. Az adatok kiszivárgása, a Command and Control (C&C) rosszindulatú kommunikációja és a rosszindulatú letöltések mind az SSL/TLS titkosított forgalmat használják, ezért extra védelemre van szükség annak használata mellett is (!). Nincs hiány a nagy nyilvánosságnak örvendő exploitokból sem, amelyekben a támadók a HTTPS-forgalomban rejtőzködtek. Gondoljunk csak a British Airways Magecart adatszivárgására, ahol a HTTPS-forgalmat használták a különböző fizetési oldalakról kiszivárgott hitelkártyaadatok elfedésére. A jogsértés 380 000 ügyfelet érintett.

Az alkalmazáskiszolgálók nem rendelkeznek megfelelő titkosítással

Az alkalmazáskiszolgálók, beleértve a legtöbb levelező-, fájl- és távoli hozzáférés-kiszolgálót, nem tudnak kielégítő TLS-beállításokat biztosítani, vagy egyáltalán nem rendelkeznek TLS-támogatással. Még az Apache és az NGINX, a legelterjedtebb webkiszolgálók is nehezen támogatják a fontos TLS-funkciókat. Titkosítási szempontból ezen szerverek jelentős sebezhetőségeit a kriptográfiai könyvtárakban találhatjuk meg. Ez a probléma egy dedikált TLS-eszközt igényel, amely képes felügyelni a forgalom biztonságát és titkosítását.

Nem biztonságos SSL/TLS verziók

Az SSL/TLS családban hat protokoll létezik: Az SSL v2, SSL v3, TLS v1.0, TLS v1.1, TLS v1.2 és TLS v1.3. Az utolsó kettő kivételével az összes többi verzió elavult, sok esetben már nem biztonságos, így nem ajánlott használni. A gyakorlatban azonban még mindig szükség van rájuk, így számos webkiszolgálóban és üzleti alkalmazásban hatalmas biztonsági rések maradnak.

Emberi tényező – A legnagyobb adatvédelmi kockázat

Számos biztonsági elemző állítja, hogy az emberi hiba jelenti a legnagyobb kihívást az adatvédelem és az adatbiztonság terén. Nem is beszélve az emberi kíváncsiságról, a személyes adatokkal való visszaélésről és a szándékos kiszivárogtatásról. Másrészt, egy IT-biztonsági rendszergazda számára megterhelővé válhat az évente megjelenő, szó szerint több ezer patch kezelése, ami azt jelenti, hogy az adatvédelem és adatbiztonság fenntartásához szükséges erőfeszítések folyamatosan nőnek.

BALASYS

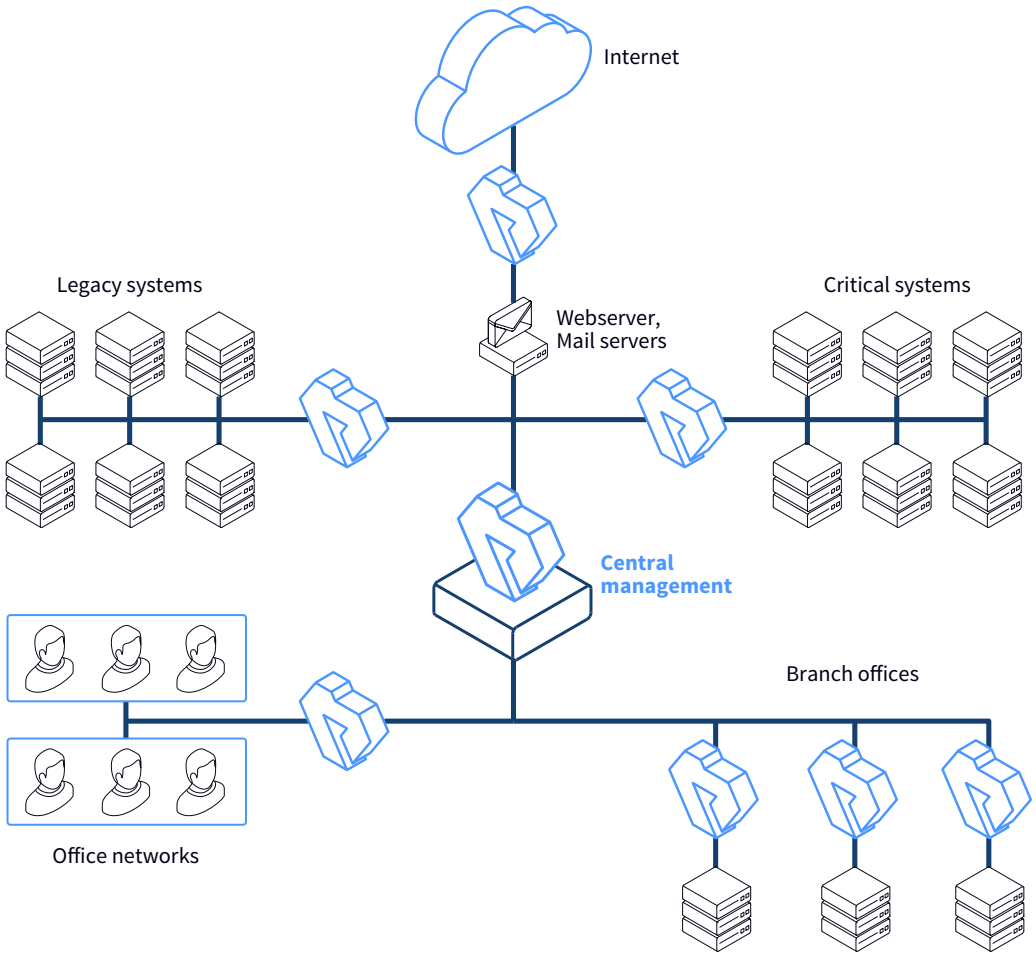
info@balasys.hu

Rugalmas TLS-konfiguráció a PNS segítségével

MEGOLDÁS

A PNS egy rendkívül rugalmas, többcélú biztonsági átjáró, amellyel a legapróbb részletekig ellenőrízhető a vállalati hálózati forgalom, így védelmet nyújt a legkifinomultabb belső és külső támadások ellen is. A PNS minden részletre kiterjedő mély csomagvizsgálatot (Deep Packet Inspection - DPI) biztosít a normál és a titkosított hálózati kommunikációban is, továbbá a forgalom szűrésére és a tartalom módosítására is képes. A PNS olyan rugalmas architektúrával és szkriptelhető konfigurációval rendelkezik, amellyel bármilyen szigorú IT-biztonsági szabályzattal rendelkező vállaltnál alkalmazható, a Zero Trust alapelveit is beleértve.

A PNS-t használó ügyfeleink olyan egyedi hálózatbiztonsági problémák megoldására képesek, amelyeket a tűzfalak nem képesek kezelni.



A hálózat mélységi védelme a PNS használatával

BALASYS

info@balasys.hu

ELŐNYÖK

A PSN segít, hogy az Ön vállalata is megfeleljen a legújabb adatvédelmi és titkosítási követelményeknek. Biztosítja a megfelelő TLS-beállításokat vállalkozása számára, többek között:

- Biztonságos protokollok és legújabb titkosítási készletek érvényesítését;
- Teljes tanúsítási láncok megvalósítását;
- Privát kulcsok védelmét;
- Elősegíti egyéb ismert problémák enyhítését.

A biztonsági intézkedések központilag is bevezethetők, ami leegyszerűsíti a folyamatot, hiszen így nem szükséges az összes kiszolgálón vagy kliensen telepíteni a megfelelő titkosítást.

A HTTPS-forgalom alapos vizsgálatán túl a PNS átveszi a biztonsági feladatokat az alkalmazáskiszolgálóktól, így azok az elsődleges feladataikra koncentrálhatnak. Ez nagymértékben növeli webkiszolgálói megbízhatóságát és biztonságát, ezáltal növelve az ügyfelek elégedettségét.

Bővebb információ

A PNS weboldala

Próbaverzió igénylése

Árajánlat kérése

BALASYS

A forgalom titkosítása

A PNS teljes ellenőrzést biztosít a TLS (a HTTP biztonságos rétege, IMAP, SMTP, FTP stb.) csatornái felett. A PNS volt az egyik első olyan informatikai biztonsági termék, amely támogatta a legújabb, TLS 1.3 protokollt.

A PNS képes a titkosítás következetes végrehajtásának biztosítására olyan érzékeny rendszerek előtt, amelyek nem feltétlenül támogatják a TLS-t. Lehetővé teszi a titkosítási irányelvek rugalmas konfigurálását a kommunikáló felek felé, ami tovább javítja az interoperabilitást. Képes titkosítani alapvetően nem titkosított vagy más eszközök által csak rendkívül ritkán titkosítható legacy internetes protokollokat is. A különböző hostokról érkező kapcsolatokra különböző biztonsági szabályzatok alkalmazhatók. Ez azt jelenti, hogy a „leggyengébb láncszemet" általában támogató beállítások alkalmazásának szükségessége elavult, és a legmagasabb biztonsági szabványokat is megvalósíthatja, miközben kizárja az bizonytalan tényezőket.

Átfogó VPN-támogatás

A PNS támogatja az IPSec (IKEv1 és IKEv2) és az OpenVPN megoldásokat, amelyek különböző módszereket használnak a privát forgalom interneten keresztüli átvezetésére. A site-to-site és a road warrior VPN-ek is támogatottak a távoli fiókok/felhasználók és a vállalat központi rendszerei közötti kommunikáció biztosításához.

Szelektív TSL csatorna vizsgálat

Bizonyos adatvédelmi forgatókönyvekben tilos a TLS-ellenőrzés. Ezekben az esetekben a PNS képes biztosítani, hogy a kívánt kommunikáció titkosított maradjon, és senki ne vizsgálhassa meg a forgalmat. Például a felhasználók online banki tevékenységéhez kapcsolódó adatforgalom soha nem kerül ellenőrzésre.

Adatmaszkolás a megfelelőség teljesítéséhez

A PNS elősegíti az érzékeny adatok védelmét, például az adatok anonimizálásával, amelyet számos adatvédelmi szabvány, többek között a GDPR is megkövetel. Az adatok anonim módon továbbíthatók külső partnerei számára, így érzékeny adatai még abban az esetben is védve vannak, ha illetéktelen kezekbe kerülnének egy - sajnos rendkívül gyakori - adathalász támadás során.

Az adatmaszkolás lehetővé teszi a biztonsági kockázatokra vonatkozó információk elrejtését és a legacy alkalmazások sebezhetőségeinek kezelését is. Például eltávolíthatja a bannereket, vagy más, az alkalmazásokra jellemző információkat az infrastruktúrára vonatkozó érzékeny információk elrejtése érdekében.

Nyilvános kulcsú infrastruktúra

A PNS nyilvános kulcsú infrastruktúra-rendszert kínál a felek közötti biztonságos kommunikációhoz szükséges tanúsítványok és kulcsok kényelmes és hatékony kezelésére. A megoldás beállítható úgy, hogy a tanúsítványok és a CRL-ek (Certificate Revocation Lists - tanúsítvány-visszavonási listák) rendszeres elosztását automatikusan elvégezze, így biztosítva, hogy érvénytelen vagy visszavont tanúsítványt ne lehessen használni. A nyilvános kulcsú infrastruktúra-rendszer képes a TLS- és VPN-kapcsolatok privát kulcsainak, ügyféltanúsítványainak kezelésére és a TLS- és VPN-kapcsolatok aláírási kérelmeinek kezelésére is, továbbá segít megbízható hitelesítésszolgáltatóként (Certificate Authority) működni.