1. **Transzparens, alkalmazásszintű proxy átjáró**
2. **Rendkívül szigorú biztonsági szabványok bevezetése**
3. **Egyedi, proxy alapú technológia**
4. **Rugalmas és professzionális mérnöki támogatás**
5. **Magyar fejlesztésű kódbázis – „Clean code"**

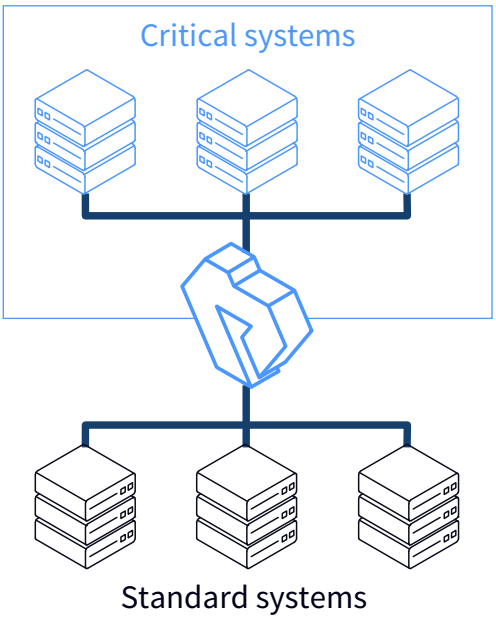
PROXEDO
NETWORK SECURITY

„Amikor egy kiberbûnöző jogosulatlan hozzáférést szerez egy hálózathoz, a hálózaton belüli további mozgásának korlátozására hatékony módszer lehet a szegmentálás vagy a zónákra bontás."

– Wikipédia

KRITIKUS RENDSZEREK ELKÜLÖNÍTÉSE ÉS VÉDELME

A kritikus informatikai infrastruktúrát a vállalkozás folyamatos működéséhez szükséges rendszerek és adatok alkotják. Ide tartoznak például a fizetési kártyafeldolgozó rendszerek, a számviteli rendszerek, az ERP és az ellátási lánc elosztórendszerei, a szellemi tulajdon és az ügyféladatbázisok.



Az üzleti szempontból kritikus szerverek mélyreható védelme

A kihívás

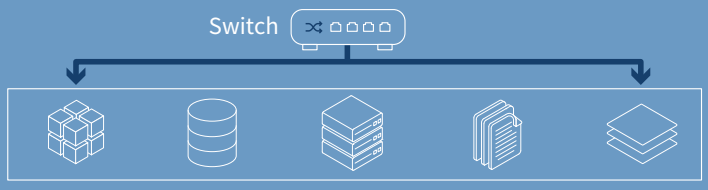
Nincs szegmentálás – Nagy kockázat

A legtöbb szervezet még nem tette meg az összes szükséges lépést kritikus infrastruktúrájának védelme érdekében, így nem szegmentálták a hálózatot, nem használnak megfelelő módszereket a fenyegetések megelőzésére és észlelésére. Utólag, a különböző biztonsági követelményekkel rendelkező hálózatok között létrehozni a demilitarizált zónákat és átjárókat, pedig mindig kihívást jelent.

Az ábra egy olyan sík hálózatot mutat, amelyben mind az adminisztratív, mind a kritikus rendszerek ugyanabban a hálózati szegmensben helyezkednek el. A kritikus rendszerek felé, és annak irányából is, csekély ellenőrzéssel, vagy éppen minden ellenőrzés nélkül áramlik az információ. A kritikus rendszerek felhasználói hozzáférnek az internethez, a támadók pedig potenciálisan láthatják ezeket a rendszereket amikor egy egyszerű szkennelést hajtanak végre a hálózat felderítése során.

A támadók szeretik a sík hálózatokat

Ha a támadó hozzáfér egy munkaállomáshoz, onnan már távoli kapcsolatot létesíthet egy kiszolgálóval, feltérképezhet egy hálózati erőforrást, onnantól "jogszerűen" használhatja a hálózati adminisztrációs eszközöket az érzékeny információk megszerzéséhez vagy lefuttahat egy rosszindulatú kódot az adott szerveren. A megfelelően megtervezett és megvalósított hálózati szegmentálás és elkülönítés kulcsfontosságú biztonsági intézkedés az ilyen fenyegetések megelőzésében.



Szegmentálás nélküli sík hálózat

A szabályozások és szabványok megkövetelik az elkülönítést

A PCI-DSS és hasonló szabványok útmutatást adnak az adatok hálózaton belüli egyértelmű szétválasztásához, például a fizetési kártya-engedélyezési hálózat elkülönítésével a szolgáltatási pontoktól vagy az ügyfelek Wi-Fi-forgalmától. Egy megbízható IT-biztonsági szabályozás magában foglalja a hálózat több zónára történő szegmentálását, és a zónáról zónára történő átvitelre vonatkozó irányelvek szigorú betartását.

BALASYS

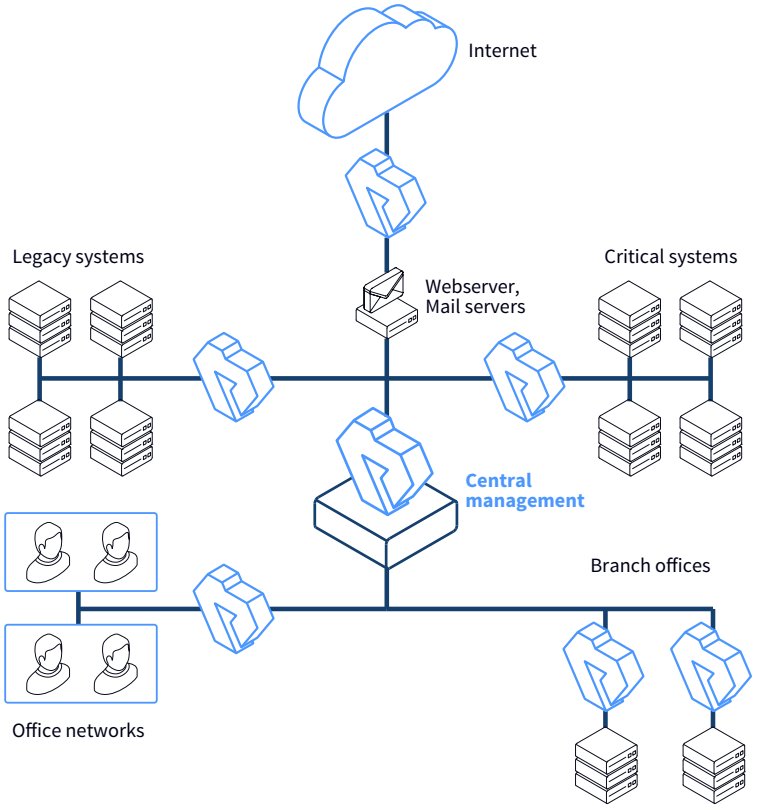
info@balasys.hu

MEGOLDÁS

Proxy átjáró a hálózat szétválasztásához

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 Proxedo Network Security architektúrája

ELŐNYÖK

A PNS segítséget nyújt egy kiforrott és elkülönített informatikai környezet létrehozásában, amely lehetővé teszi, hogy a vállalatok a prioritást élvező rendszerekre koncentrálhassanak biztonsági stratégiájuk kialakítása során. Emellett biztosítani tudja a feltört hostok vagy hálózatok időben történő elkülönítését a hálózati behatolást követően.

1. **Fokozott biztonság** - A hálózati forgalom elszigetelhető a hálózati szegmensek közötti kommunikáció megakadályozása érdekében.
2. **Továbbfejlesztett hozzáférés-szabályozás** - A felhasználók számára csak bizonyos hálózati erőforrásokhoz való hozzáférés engedélyezése.
3. **Továbbfejlesztett monitorozás** - Lehetővé teszi a gyanús informatikai események észlelését, és a kockázatok csökkentését.
4. **Jobb teljesítmény** – Az alhálózatonkénti kevesebb hostnak köszönhetően a helyi forgalom minimálisra csökken. A helyi alhálózat el tudja különíteni a broadcast forgalmat.
5. **Fejlett elszigetelés** – Hálózati hiba esetén annak hatása a helyi alhálózatra korlátozódik.

Bővebb információ

A PNS weboldala

Próbaverzió igénylése

Árajánlat kérése

BALASYS

Elkülönítés

A PNS képes elkülöníteni a kritikus rendszereket a többi, nem kritikus rendszerektől. Biztosítja, hogy ezek a rendszerek ne legyenek közvetlenül elérhetők az internetről, és garantálja, hogy a kritikus rendszerekkel zajló kommunikáció korlátozott és ellenőrzött legyen.

Minden részletre kiterjedő protokoll ellenőrzés

A PNS proxy szinten kezeli a hálózati kapcsolatokat. A hálózati kapcsolaton átmenő információk teljes egészében elérhetők az eszközön, amelyen részletes protokollvizsgálat és -validálás végezhető. Az átjáró felismeri az egyes protokollok tulajdonságait, és megszakítja a kapcsolatot azokkal, amelyek nem felelnek meg a sztenderd előírásoknak. Hozzáadható funkció a mélyreható tartalomszűrés.

Átfogó titkosítás

A PNS teljes körű kontrollt biztosít a TLS-titkosítású (korábban SSL) csatornák felett. A gyakorlatban ez azt jelenti, hogy a PNS-t használó ügyfeleink még a titkosított csatornákon keresztül zajló email- és webes forgalmat is ellenőrízni tudják. Emellett a PNS támogatja a nem titkosított és a legacy kriptográfiai protokollok korrekt titkosítását is.

A forgalom módosítása

A PNS képes a forgalom bizonyos elemeinek módosítására. Elrejthetők az ügyféladatok vagy az érzékeny infrastruktúra információk, és kezelhetők a legacy alkalmazások biztonsági rései. Például, eltávolíthatók a forgalomból a hibás konfigurációból adódó hibaüzenetek és bannerek, vagy a személyes adatok (pl. bankkártyaszámok) amelyet a megfelelőségi és adatvédelmi előírások betartása érdekében mindenképp meg kell tennünk.