WEB APPLICATION FIREWALL
OCHRANA VAŠICH WEBOVÝCH APLIKACÍ

PŘEDSTAVENÍ

Ochránit vstupní bod (perimetr) sítě je důležité a obtížné. Pokud použijete firewall či IPS, musíte k webu nechat otevřený přístup. Ačkoli řada bezpečnostních produktů dokonale rozumí komunikaci na síťové a transparentní vrstvě, **pouze Web Application Firewall (WAF) rozumí i struktuře a logice konkrétní aplikace**, která je pokaždé jedinečná. Tato funkcionalita o to víc přichází ke slovu v době, kdy je již prakticky vše dostupné přes webové rozhraní. Dobrý WAF nabízí nejen maximální bezpečnost, ale i snadnou implementaci. Musí být schopen naučit se veškeré informace o konkrétní aplikaci sám, následně vyhodnotit rizika a vytvořit přesná pravidla.

PŘÍNOSY ŘEŠENÍ

- Skutečná ochrana webových aplikací na základě znalosti protokolu i logiky aplikace.
- Výrazné snížení rizikovosti aplikací (možnosti kompromitace), zajištění vysoké dostupnosti aplikací.
- Snadné nasazení díky schopnosti naučit se logiku aplikace z provozu.
- Ochrana webů bez nutnosti jakkoliv zasahovat do samotné aplikace (v mnoha případech zásah do kódu ani není možný).
- Možnost doplnit řadu důležitých vlastností – opět bez zásahu do kódu aplikace (autentifikace uživatele, integrace s AD/RADIUS serverem, SSO, povolení přístupu na základě geolokace).
- Ochrana před automatickým stahováním dat a provozem z robotů (scraping, botnety, brute force útoky atd.).
- Detailní přehled provozu nad sledovanými aplikacemi, snížení nákladů pro nasazení jejich nových verzí.
- DDoS ochrana.
- Zajištění shody v souladu s GDPR, PCI 3.1, HIPPA atd.

CO SE BEZ NĚJ MŮŽE STÁT?

- Zcizení dat (např. pomocí SQL injection) – **poškození firmy nebo zákazníků.**
- Modifikace obsahu webu – **ztráta reputace nebo finanční ztráta.**
- Znepřístupnění webu – **finanční ztráta.**

ZAUJALO VÁS TOTO ŘEŠENÍ?

ZREALIZUJEME KOMPLEXNÍ PROOF OF CONCEPT NA MÍRU.