Web Application Firewall

Web Application Firewall chrání webové stránky a webové aplikace před útočníky, kteří využívají zranitelná místa aplikace nebo protokolů ke krádeži dat nebo ke změně vzhledu webových stránek organizace.

Chrání před útoky na webové aplikace a útoky typu odepření služby (denial of service, DoS). Na rozdíl od tradičních síťových firewallů nebo detekčních systémů průniku (IDS), které jednoduše propouštějí HTTP, HTTPS nebo FTP provoz do webových aplikací, Web Application Firewall funguje jako obousměrný proxy tohoto provozu. Kontroluje, zda provoz neobsahuje útoky, izoluje webové servery od přímého přístupu hackerů. Kromě toho Web Application Firewall eliminuje útoky prováděné záměrnými změnami dotazů aplikací (např. znemožňuje úpravy cookies).

Na rozdíl od detekčních systémů průniku, které analyzují pouze binární vzorky, Web Application Firewall přejímá veškerý provoz místo webového serveru. Dekóduje komunikaci a odstraňuje/dropuje nepovolené znaky či dotazy a normalizuje data. Dále systémy umožňují ochranu proti zneužití citlivých údajů. Ze všech dnes hlášených útoků je zhruba sedmdesát procent cíleno na aplikační vrstvu.

Přínosy našich služeb

- Výrazné snížení rizikovosti aplikací (možnosti kompromitace),
- zajištění vysoké dostupnosti aplikací,
- snížení nákladů pro nasazení nových verzí aplikace,
- detailní přehled provozu nad sledovanými aplikacemi.

Diferenciace:

- Analýza vhodného řešení a návrh nasazení WAF

  Analýza stávajících potřeb aplikací, detailní návrh vhodného řešení v souladu s nároky na infrastrukturu a oddělení jednotlivých aplikací.

- Implementace zvoleného WAF řešení

  Implementace analýzou zvoleného řešení, dle detailních návrhů.

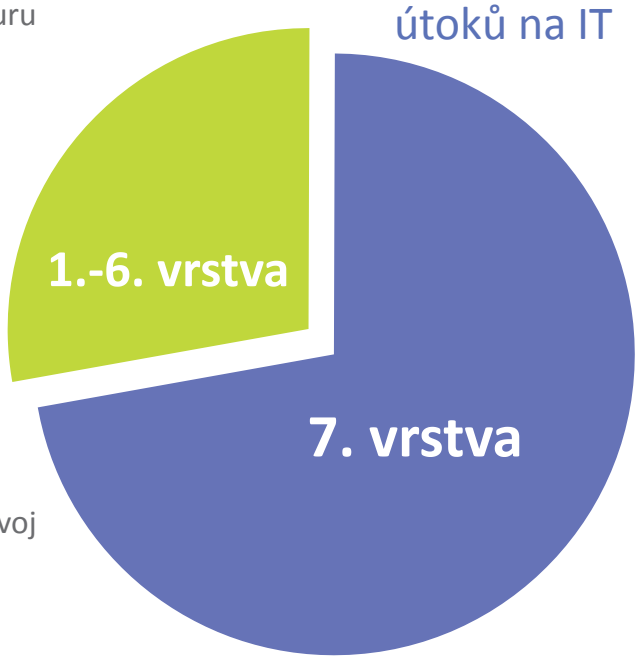
- Support/rozvoj WAF řešení

  Support/rozvoj WAF řešení v úrovni kontaktu s výrobcem, řešení nestandardních událostí, případně celková podpora zajištění funkce WAF řešení.

- Pronájem WAF řešení (jako služby)

  Může obsahovat jak implementaci, tak support/rozvoj dle parametrů smlouvy o pronájmu.

Poměr zaznamenaných útoků na IT

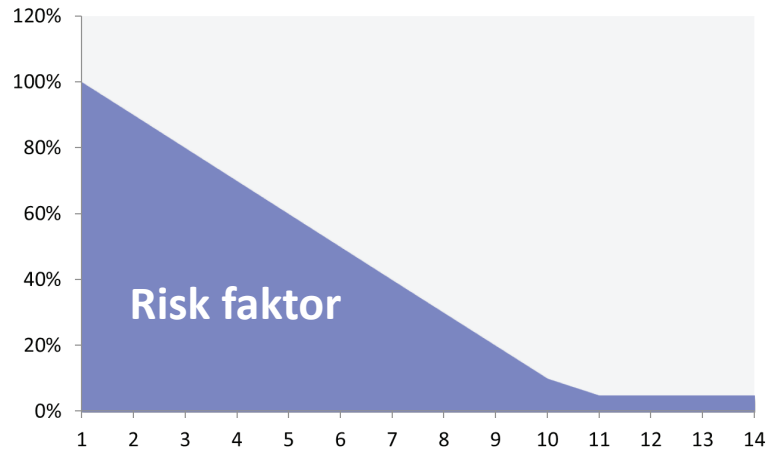


Metodika, nástroje, technologie

Přístup k analýze či nasazení WAF řešení vychází z best practices uváděnými výrobci jednotlivých WAF řešení. V případě analýzy či nasazení na aplikace s nejasnou nebo složitou strukturou je využito shodných metod jako pro provádění penetračních testů. Tyto výsledky jsou pak dalším jasným vodítkem budoucí konfigurace a budoucího designu.

Příklad z naší praxe

Zákazník požadoval snížení rizik v zákaznickém portále za udržení minimálně stejné úrovně dostupnosti. Jedná se o zákaznický portál s živým vývojem, který tuto aplikaci stále inovuje. Již v předešlých případech nebyly nové verze aplikace dostatečně zabezpečeny proti kompromitaci. Cílem tedy bylo zajištění bezpečnosti a zároveň snížení rizik v období nasazení nových verzí aplikace. Tím v podstatě urychlení nasazení nových verzí.



Výsledkem byl zásadní pokles risk faktoru, protože více než 97% aplikace je chráněno již v momentě nasazení nové verze. Celý vývoj aplikace je tímto výrazně jednodušší a odpadají někdy i nekonečné fáze deploymentu aplikací.

Proč AEC?

Mnohaleté zkušenosti s identifikací úrovně bezpečnosti a vývoje webových aplikací. Podpora TOP výrobců (F5 Networks, Barracuda, ...), certifikovaný tým specialistů.

Reference

Česká pošta
Analýza nasazení WAF, analýza a detailní návrh designu a implementace do prostředí České pošty.

AEC, spol. s r.o.
Purkyňova 2845/101
612 00 Brno, Czech Republic
Phone: +420 530 507 200
Fax: +420 530 507 220

AEC, spol. s r.o.
European Business Center
Dukelských hrdinů 34
170 00 Praha 7, Czech Republic
Phone: +420 267 311 402
Fax: +420 266 177 155

AEC
DATA SECURITY

www.aec.cz