CLOUD WEB APPLICATION FIREWALL

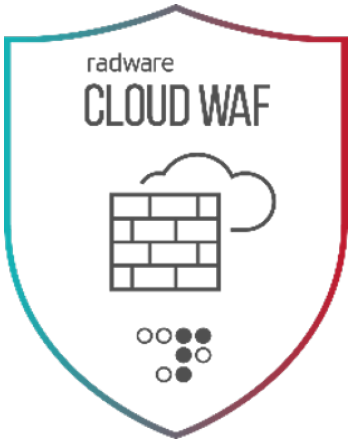
secured by radware

Nejvyšší ochrana webových aplikací

S masivním nárůstem on-line ekonomiky a e-governmentu dochází ke zvyšování závislosti na této formě komunikace. Současně s růstem závislosti roste významně i bezpečnostní riziko webových aplikací, které tuto formu ekonomiky podporují a vytvářejí.
Nezabezpečené webové aplikace jsou bránou k interním systémům, resp. pomocí stále více používaného API k systémům třetích stran.
Dynamický vývoj aplikací s sebou nese i nárůst zranitelností, který je dán především těmito skutečnostmi:

- Aplikace jsou sestaveny z více vrstev/komponent/frameworků, z nichž každá může obsahovat, a s vysokou pravděpodobností skutečně obsahuje, řadu vlastních zranitelností.
- Agilní přístup k vývoji a tlak na rychlost vývoje vede ke snížení času a hloubky testování bezpečnostních funkcí. Preferována je především funkčnost.
- Odstraňování známých zranitelností v kódu na všech vrstvách a implementace oprav je poměrně zdlouhavý proces, který nechává Váš business dlouho v ohrožení.
- Velmi těžce se do aplikace zabudovávají pokročilé analytické nástroje, které na základě behaviorální analýzy zajišťují ochranu například proti 0-day útokům.

Co se může stát?



- Zcizení/modifikace dat
- Modifikace obsahu
- Znepřístupnění webu
- Krádež/převzetí účtů
- Porušení regulatorních požadavků
- Další

Jak chráníme

Cloud WAF společnosti Radware poskytuje ochranu několika způsoby:

- Ochrana proti DDoS útokům – případný útok je zachycen a filtrován v cloudu a k vám se dostává jen legitimní provoz zbavený nežádoucích dat.
- Negativní bezpečnostní model – zajišťuje ochranu proti známým hrozbám. O aktualizaci a správu signatur útoku se nonstop stará profesionální ERT (Emergency Response Team), takže jste proti novým hrozbám chránění dříve, než vůbec zjistíte, že nějaká nová hrozba existuje.
- Pozitivní bezpečnostní model – originální koncept společnosti Radware umožní naučit se legitimní chování vaší aplikace a blokovat tak vše, co není povoleno. Vaše ochrana se vyvíjí spolu s vaší aplikací za spolupráce s ERT týmem. Tím se minimalizuje riziko false-positive alertů a buduje se ochrana proti 0-day útokům. Současně je zajištěna plná ochrana proti OWASP TOP10.
- Ochrana před boty – dnešní botnety dokážou simulovat lidské chování a mohou mít dopad nejen na bezpečnost (např. útoky typu credential stuffing), ale i rovnou na obchod (automatické porovnávaní cen, vytváření falešných účtů, objednávek atd.). Radware Bot Manager dokáže rozpoznat, zda je daný požadavek generován botem nebo člověkem a aktivity špatných botů blokovat.

Jen firewall nestačí

Běžný Firewall zjistí, že mluvíte německy, Next Generation Firewall ověří gramatickou správnost, ale pouze Web Application Firewall pochopí, o čem skutečně mluvíte.

Řešení Web Application Firewall v žádném případě nenahrazuje klasický Firewall ani Next Generation Firewall a naopak žádné z těchto řešení nenahrazuje, resp. nepokrývá ochranu, kterou Vám poskytuje WAF.

Rychlá implementace

Velkou předností je skutečně rychlé nasazení s minimální zátěží na interní IT a bez potřeby dalších investic do vzdělávání vlastních specialistů.

Jak taková implementace vypadá:

Krok	Popis	Čas
Přidání SSL certifikátu	Tento krok je nezbytný pro HTTPS aplikace	Okamžitě
Přidání aplikace (webu)	Nastavení parametrů aplikace včetně odkazu na certifikát (pokud je použitý)	Typicky do 30 minut
Přesměrování aplikace	Je potřeba aktualizovat DNS záznam, který zajistí přesměrování aplikace do Cloudu.	Rozšíření DNS záznamů trvá v jednotkách hodin, max. 48 hodin
Aplikace je nyní chráněna proti DDoS útokům a známým hrozbám	Po uplatnění změny DNS záznamů začne fungovat Radware negativní bezpečnostní model	Ihned po uplatnění DNS záznamů
Učící fáze	WAF se začíná učit legitimní chování aplikace	Doba trvání závisí na způsobu a složitosti aplikace. U běžných aplikací 1 až 2 týdny
Kontrola/schválení naučených zásad	Naučené pravidla chování jsou recenzována pracovníkem ERT týmu společnosti Radware, schváleny klientem. Dochází k zapnutí pozitivního bezpečnostního modelu	Po koordinace trvá revizní schůzka asi hodinu v návaznosti na složitost aplikace

Co získáte

Nasazením cloudového řešení WAF společnosti Radware, získáte špičkové zabezpečení svých webových aktivit s podporou profesionálního týmu, který s nástrahami kyberprostoru bojuje nepřetržitě. Odpadají vám náklady na školení vlastního personálů. Současně dostáváte průběžně zpětnou vazbu o zranitelnostech, které je potřeba postupně řešit v rámci standardního vývoje aplikací, bez nutnosti nekoncepčních záplat. Můžete se tak soustředit na vlastní podnikání a nechat nejlepší odborníky svého druhu bdít nad bezpečností vašich webových aplikací.