Bezpečnostní rizika pro webové aplikace

a jejich eliminace pomocí webového aplikačního firewallu

Text: Bohumír Kotora, foto: Alex M. Videmannová

Vystavování podnikových aplikací do prostředí internetu se těší stále větší oblibě. Snadná dostupnost aplikace pro uživatele s sebou ovšem přináší také nejrůznější úskalí a bezpečností rizika. Stále více webových aplikací se stává terčem hackerských útoků technikami typu SQL injection, cross-site scripting, manipulací se soubory cookies aj., vedoucím k pokusům o poškození dobrého jména společnosti díky krádeži citlivých údajů nebo způsobením nedostupnosti provozované aplikace.

Většina organizací využívající informační technologie a systémy dnes bez větších problémů chrání svou infrastrukturu za pomoci technologií, jako jsou např. síťové firewally nebo next generation firewally a IDS. Tyto pojmy v současnosti nejsou cizí ani laické veřejnosti a naprostá většina přístupových bodů do Internetu je dobře zabezpečena.

Zcela odlišná situace je v oblasti aplikační bezpečnosti, tedy v implementaci bezpečnostních prvků a opatření, zejména do webových aplikací. Důvody pro současný negativní stav jsou dány především nízkým povědomím o možných chybách na straně aplikací. Zákazník většinou není schopen předložit přesné požadavky na vývoj aplikace a její bezpečnost, někdy chybí i zájem na prosazení konkrétních zásad bezpečnosti, ať už ve formě vnitřních standardů, nebo definovaných smluvních ustanovení.

Celkově se bezpečnost aplikační vrstvy řeší velmi intuitivně, eventuelně vůbec. Reálným dopadem jsou poměrně vážné bezpečnostní chyby v současnosti provozovaných aplikací.

Zabezpečení webové aplikace před útoky

Aby firemní data zůstala bezpečná a webová aplikace flexibilní, je důležité celý systém zabezpečit takovým nástrojem, který je schopen analyzovat a efektivně filtrovat veškerý provoz na HTTP/HTTPS/XML. Takovým nástrojem, který poskytuje rychlou a účinnou eliminaci rizik je určitě webový aplikační firewall (WAF). Chrání webové stránky a webové aplikace před útočníky, kteří využívají zranitelná místa aplikace nebo protokolů ke krádeži citlivých dat či změně vzhledu webových stránek organizace.

Podle údajů analytické společnosti Gartner Group jsou celé tři čtvrtiny bezpečnostních útoků vedeny právě na aplikační úroveň. Zařízení WAF na ni kontroluje všechny vstupy a výstupy dle předem stanovených pravidel. Kontrola proti známým útokům je zajišťována na základě signaturní detekce. Pro zajištění ochrany samotné logiky aplikace se uplatňuje model pozitivního zabezpečení. Namísto spoléhání se na známky útoku a technik porovnávání vzorců, model pozitivního zabezpečení zná „správné“ chování aplikace a blokuje jako škodlivé jakékoli odchylky od řádných činností aplikace. Toto je jediný přístup, který zajišťuje ochranu proti nepublikovaným rizikům.

Etický hacker z AEC komentuje svůj postup při prolamování zabezpečení zranitelné webové aplikace

Workshop AEC o zranitelnostech webových aplikací

Zabezpečení webových aplikací znamená pro bezpečnostní manažery tvrdý oříšek, jak co nejrychleji a s přijatelnými náklady řídit rizika související s provozem svých podnikových aplikací v prostředí webu. Týmy vyvíjející aplikace jsou často velice rozsáhlé a centralizace bezpečnosti je značně problematická. Komplexnost aplikací způsobuje, že bezpečnostní chyby v nich jsou často i několik měsíců skryté. „Základní chybou, jež zapříčiňuje výskyt zranitelností webových aplikací, je neznalost otázky jejich bezpečnosti ze strany vývojářů. Dodatečně se bezpečnost do tohoto prostředí dodává velice těžce,“ upozorňuje Maroš Barabas ze společnosti AEC, která pravidelně pořádá semináře zaměřené na ochranu webu a webových aplikací. Zúčastnili

Matej Kačic, Senior IT Security Consultant

Maroš Barabas, Head of Security Technologies Division

jsme se jednoho z nich, který byl věnovaný problematice zabezpečení webových aplikací a představení řešení od společnosti F5 Networks, která je v současnosti lídrem na trhu webových aplikačních firewallů.

V průběhu workshopu předvedli odborníci z AEC základní hackerské techniky a reakce vyvolané prostřednictvím WAF. Názorně tak demonstrovali chování tohoto nástroje v případě směrování útoku na webovou aplikaci, ale také schopnost prezentovaného řešení automatizovaně se učit z reálného provozu. Nechyběla ani modelová situace odstranění zjištěného problému zranitelnosti webu. Na pomoc byl přizván etický hacker (pentester), aby živě demonstroval nejčastější útoky na web, které skuteční hackeři podnikají. Oponenta mu dělal firemní expert společnosti AEC na WAF, který se staral o obranu v reakci na simulované útoky. Vzájemné dialogy probíhaly na dvou úrovních. Zpočátku útočník nejprve snadno kompromitoval pomocí několika útoků nechráněný web. Po zapnutí WAF ochrany pentester celý scénář zopakoval, ale tentokrát již byl jeho pokus neúspěšný. „Na základě zachycených útoků vznikne ucelený přehled zpráv a hlášení, se kterým analytik dále pracuje, aby zjistil, co se na webu dělo. Řešení od F5 Networks se tyto věci učí automaticky, přitom vytvoří pozitivní model, a to i v živém prostředí," popsal Maroš Barabas schopnosti použitého WAF nástroje.

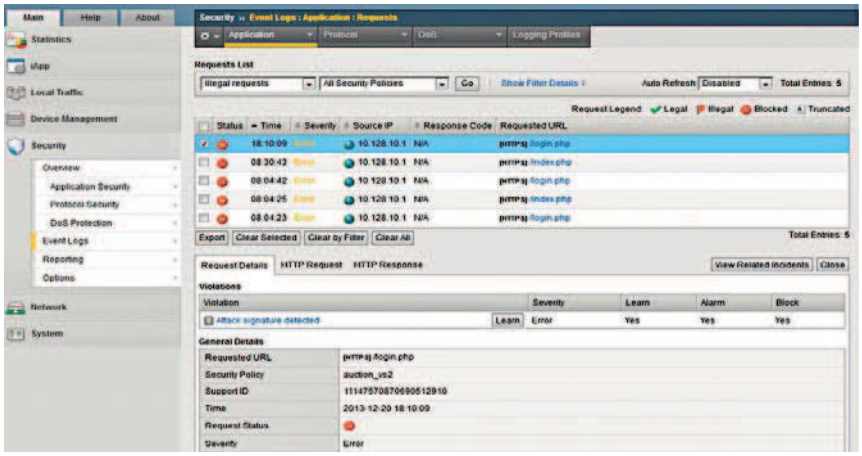
V průběhu workshopu byly představeny nejčastěji používané hackerské techniky a nástroje k prolomení webových aplikačních prostředí. Mezi ně patří např. technika SQL Injection, pomocí které lze pozměnit data v databázi, změnit logiku aplikace, infikovat ostatní uživatele aplikace, či užít kompromitované systémy aplikace k šíření útoku do interní sítě firmy. „Právě SQL Injection představuje nejzávažnější úroveň rizika napadení. Penetrační testy webových aplikací u klientů proto provádíme kontinuálně. Odstraňujeme odhalenou sníženou bezpečnost, školíme lidi. Jejich velká fluktuace otázce bezpečnosti rovněž škodí," dodává Maroš Barabas z AEC.

Oblíbenou, ale relativně méně významnou zranitelností je XSS (Cross-Site Scripting), která mění obsah webové stránky nebo její parametry URL (tzv. Reflected XSS) pro podvržení kódu uživateli napadené aplikace. Lze tak odcizit identity uživatelů, získat citlivá data, případně provést aktivity v zranitelné aplikaci pod identitou uživatele. V případě odcizení identity privilegovanému uživateli aplikace může dojít až k její úplné kompromitaci. „Útok pomocí Cross-Site Scripting je jeden z nejčastějších útoků, využívaný hackery," zmínil v průběhu workshopu přítomný pentester.

Útoky využívající zranitelnosti aplikací jsou komplikovanější, ale riziko z případného napadení je vysoké. Další z běžných chyb, je náchylnost formulářů (většinou formuláře přihlašovací, registrační, atd.) na brute-force útok. Z tohoto důvodu se specialisté ze společnosti AEC zaměřili i na ukázku zneužití chyby špatného ošetření vstupu ve formuláři.

Při podrobné analýze útoků, bylo poukázáno na fakt, že všechny předváděné útoky byly pomocí nástroje WAF od společnosti F5 Networks spolehlivě detekovány a blokovány. ■

Příklad detekce SQL injection pomocí signatur



Sledování uživatelských relací včetně zamaskování přístupových hesel