VZMR „Dodávka 2 ks webových aplikačních firewalů (WAF) formou virtuální apiliance“

TECHNICKÉ POŽADAVKY ZADAVATELE	Příloha č. 1 výzvy
Implementační požadavky na WAF	ANO/NE
3 člověkodny na nasazení politik formou zaškolení obsluhy na vybrané www servery	ANO
Platnost licence	ANO/NE
plná funčnost min. 5 let(nové verze databáze zranitelností, reputačních IP, nové verze SW, apod.)	ANO
Kapacitní požadavky na WAF	ANO/NE
min. propustnost 200 Mbit/s	ANO
minimálně zabezpečit 10 webů	ANO
Funkční požadavky na WAF	ANO/NE
Technologie musí fungovat jako plně reverzní proxy	ANO
Technologii musí být možné nasadit jako virtuální appliance	ANO
Reputační databáze známých škodlivých IP adres aktualizovaná v reálném čase, kterou lze využít na zablokování provozu	ANO
Produkt není licenčně omezen na počet uživatelů	ANO
Podporuje shodu s regulacemi PCI DSS a HIPAA	ANO
Poskytuje automatizované nápravy zranitelností	ANO
Poskytuje komplexní ochranu proti příchozím útokům vč. OWASP Top 10	ANO
Disponuje vbudovaným cashingem, kompresí a TCP spoolingem	ANO
Pro webové aplikace umožňuje kontrolu přístupu na základě identity(např. možnost definovat logon page aplikace, chránit před brute force nebo MITB útoky)	ANO
Poskytuje ochranu proti SQL Injection, Cross-site scription, úprava cookies a formulářů	ANO
Poskytuje funkci XML Firewall (Ochrana XML DOS, Schéma/WSDL enforcement, Kontroly souladu WS-I)	ANO
Kontroluje JASON Payload a chrání proti Web scraping	ANO
Umožňuje validaci metadat polí formuláře	ANO
Poskytuje ochranu proti krádeži dat: čísla platebních karet, Identifikační čísla sociálního zabezpečení,Srovnání se zadaným vzorkem (regex)	ANO
Disponuje granulárními politiky pro HTML prvky	ANO
Umožňuje řízení uploadu souborů	ANO
řešení musí podporovat protokoly HTTP/S 0.9/1.0/1.1/2.0, WebSocket, FTP/S, XML, IPv4/IPv6	ANO
řešení musí podporovat nasazení v HA, SSL Offloading, Load balancing, Content routing	ANO
řešení musí mít správu založenou na rolích	ANO
řešení musí podporovat integraci s vulnerability scannerem	ANO
řešení musí podporovat REST API	ANO
Podporuje hypervizory minimálně: Vmware ESX/ESXi, MS Hyper-V	ANO
Podpora redundance dvou a více zařízení v režimech Active-Active/Active-Standby s automatickou synchronizací konfigurace	ANO
Podpora redundance dvou a více zařízení v režimech Active-Active/Active-Standby s automatickou synchronizací konfigurace popř. úprava provozu pomocí pravidel a politik vč. bulk mode editoru a/nebo JSON konfigurace	ANO
Agregace mnoho TCP spojení od různých uživatelů do jednoho spojení k serveru pro optimalizaci HTTP provozu– TCP Multiplexing	ANO
TCP optimalizace síťových flows např. při přístupu k aplikaci z mobilu.	ANO

Ukončení šifrovaného provozu SSL TLS 1.2, podpora TLS 1.3.	ANO
Dvoucestná SSL autentizace – serverový, klientský certifikát	ANO
Podpora minimálně těchto šifrovacích algoritmů: AES 256, SHA256, RSA klíče minimálně o velikosti 4096bit	ANO
Podpora SW utilit na troubleshooting např. tcpdump	ANO
Podpora různých typů load-balancingu(kruhová, podle počtu navázaných spojení, důležitosti serverů)	ANO
Zajištění "session persistence" na základě IP adresy, HTTP cookie	ANO
Podpora různých typů health monitoringu – ICMP, HTTP/HTTPS, HTTP/2.	ANO
Podpora modifikace provozu(vložení/přepsání HTTP hlavičky, modifikace URL, změna zdrojové IP adresy v L7 hlavičce, modifikace http obsahu)	ANO
Podpora HTTP/2 směrem k uživateli i k serveru	ANO
Možnost konfigurace Webového aplikačního firewallu za využití učícího se módu	ANO
Automatické nahrávání a aplikování nových signatur od výrobce	ANO
Automatické odlišení skutečných uživatelů od botnetů	ANO
Průběžná analýza stresu aplikace, analýza nestandardního chování tzv. behaviorální analýzy	ANO
Ochrana proti útoku typu Session Highjacking pomocí jednoznačné identifikace prohlížeče uživatele („fingerprintu" webového prohlížeče).	ANO
Ochrana dat a přihlašovacích údajů proti malware během zadávání do citlivých polí formuláře.	ANO
Výrobce produktu musí disponovat vlastní databází známých botů	ANO
Výrobce produktu musí disponovat vlastní technologií typu Cloud Based Machine Learning k detekci botů a pokročilých útoků	ANO