**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

**на специализирано устройство за защита на интернет базирани приложни среди,  
 за клиент - web браузър**

**Устройството трябва да притежава следните функционални възможности:**

- Да има възможност за анализ и защита на HTTP трафик с версии 0.9, 1.0 и 1.1;

- Да има възможност за анализ и защита на SSL криптиран HTTP трафик (HTTPS) с поддържка на криптиращи алгоритми TLS 1.0, 1.1 и 1.2;

- Да осигурява възможност да защитава минимиум срещу следните видове заплахи: „Cross Site Scripting“, „Cross Site Request Forgery“, „SQL Injection“, „Malicious Code Injection“;

- Да има възможност да анализира и защитава минимум следните протоколи: HTTP(S), AJAX, Web Services, XML, SOAP;

- Да поддържа автоматични методи на самообучение и самонастройка, чрез които се изграждат профили на нормално (типично) поведение на приложението и поведението на потребителите, чрез анализ на съдържанието на изградените сесии и в двете посоки – отвън навътре и отвътре навън;

- Да има възможност за автоматична актуализация на профила за използването на WEB приложението в случай на одобрени промени;

- Да има възможност за анализ на съдържанието в отговорите на заявки към WEB приложението и отчет за необичайно или извън рамките на нормалното поведение;

- Да има възможност за идентифициране на подозрително поведение на WEB приложението, според съдържанието на отговорите на WEB сървъра (напр. кодовете за грешка и т.н.);

- Да има възможност за валидиране на входните данни от даден потребител според специфични параметри за определено URL, чрез използването на предефинирани списъци от стойности;

- Да има възможност за разпознаване и рапортуване на инциденти, породени от потребители на WEB приложението;

- Да не налага промяна на архитектурата на защитаваните WEB приложения при внедряването на устройството;

- Да има възможност за работа в режим на симулация / мониторинг (т.е. без да блокира трафик) с цел избягване на нежелани грешки и блокиране на легитимен трафик , като режимът на симулация / мониторинг да може да се конфигурира отделно за всяко WEB приложение;

- Да поддържа метод на внедряване inline transparent (на пътя на трафика, без да променя трафика, който минава през него);

- Да има възможности за реализиране на функционалност Virtual patching (VP);

- Да притежава метод базиран на сигнатури за откриване и блокиране на заплахи и зловреден код;

- Да притежава метод базиран на поведението за откриване и блокиране на заплахи и зловреден код;

- Да получава актуална репутационна информация за заплахи от зловредни източници, като например: Malicious IP Addresses, Anonymous Proxies, TOR Networks, IP Geolocation, Phishing URLs, Comment Spammers и др.;

- Да има възможност за прилагане на политики по сигурност за блокиране на атаки без да променя трафика, който минава през него

- Да предоставя възможност за деактивиране или настройване на определени засечени инциденти/сигнатури/ правила – False possitive (FP)

- Да предоставя възможност за дефиниране на определени действия (напр. „Alert Only“ или „Block & Alert“) към всяко правило от политиката за сигурност;

- Да има възможност за централизиран мениджмънт през графичен потребителски интерфейс осигуряващ графична визуализация на информацията и механизъм за генериране на отчети;

- Да притежава предефинирани шаблони за отчети, възможност за създаване на собствени отчети както и възможност за експорт на отчетите в CSV или XLS(X) формат;

- Да позволява използване на роли, както и разделяне на права за различните роли при администрирането на устройството;

- Да има възможност за записване в журнални (log) файлове на всички дейности, извършени от потребители и администратори ;

- Да има възможност за записване в журнални (log) файлове на автоматичните системни дейности (като актуализация на версията на системата и т.н.);

- Да има възможност за генериране на SNMP комуникация, syslog-съобщения или известяване по имейл в случай на инцидент;

- Достъпът до устройството да се осъществява само по защитен (криптиран) комуникационен канал;

**Устройството трябва да притежава следните технически характеристики:**

- Да има пропускателна способност поне 100 Mbps ( ниво 7 OSI модел) за WEB Application Firewall;

- Да има поне четири мрежови интерфейса за обработка на трафика с пропускателна способност 1 Gb, които да поддържат следните режими на работа:

* Мостови (bridge)
* За подслушване (sniffing)
* Прокси

- Да има поне два мрежови интерфейса за управление с пропускателна способност 1 Gb

- Да има поне два Fail-Open bypass сегмента

- Да има оперативна памет поне 8 GB

- Да има RJ 45 сериен порт

- Да има поне два броя USB порта

- Да може да се монтира в 17” сървърен шкаф

- Да има работен температурен диапазон от 5 до 40 ºC

- Да има възможност за добавяне на второ резервиращо устройство