**ТЕНДЕРНАЯ ДОКУМЕНТАЦИЯ**

**СОДЕРЖАНИЕ:**

1. **Инструкция для участников тендера**
2. **Приложение №1 ГОТОВАЯ ФОРМА № 1 (КОНВЕРТ №2)**
3. **ПРИЛОЖЕНИЕ №2 ГОТОВАЯ ФОРМА № 2 (КОНВЕРТ №3)**
4. **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Инструкция для участников тендера

**Предмет тендера (закупки).**

* 1. ЗАО «Банк Компаньон» (далее Покупатель) приглашает Вас представить предложения на проводимый тендер **по выбору поставщика на поставку программного обеспечения Imperva WAF.**

**2. Квалификация участников тендера.**

* 1. Все Участники тендера включают в состав тендерной заявки следующую информацию и документы:

1. Подтверждение об отсутствии задолженностей (налоговой и соц. фонд.)
2. Подтверждение об отсутствии судебных разбирательств за последние два года.
3. Документы, подтверждающие квалификацию согласно запросу в приложении №1 к данной инструкции.

Гарантировать предоставление нижеперечисленных документов компании, выигравшей тендер:

1. Заверенные в установленном законом порядке копии с оригинала документов, определяющих юридический статус, место регистрации и основной вид деятельности (учредительные документы, свидетельство регистрации, копия устава, копия решения полномочного органа о назначении руководителя, копия паспорта руководителя, доверенность на лицо, имеющее право деятельности);
2. Информация о наличии/отсутствии просроченной задолженности по налогам, выплатам в Социальный фонд.

**3. Затраты на участие в тендере.**

3.1. Участник непосредственно несет все затраты, связанные с подготовкой и подачей своего тендерного предложения. Покупатель ни в каких случаях не несет каких-либо обязательств или какой-либо ответственности за такие затраты.

1. **Содержание тендерных документов Участника тендера.**

Тендерные документы передаются на электронный адрес: [tender@kompanion.kg](mailto:tender@kompanion.kg) **в архивированном документе (.rar) с установленным паролем в трех электронных конвертах.**

**Внимание! Согласно правилам информационной безопасности ЗАО «Банк Компаньон» максимальный размер электронных писем не должен превышать 20МБ. В связи с этим просим Вас разделять отправляемые файлы в случае превышения данного лимита.**

**Пароль (ключ) от электронного предложения на адрес:** [pass@kompanion.kg](mailto:pass@kompanion.kg) **с указанием наименования мероприятия.**

* 1. Участник тендера должен подготовить оригинал и копии прилагаемых готовых форм тендерного предложения. Ответственность за одинаковое содержание оригинала и копий готовых форм тендерного предложения несет участник тендера.
  2. Оригиналы готовых форм тендерного предложения — это документы в сканированном виде, которые подписаны лицом (лицами), имеющим(и) полномочия выступать от имени субъекта на подписание договоров, и заверены печатью.
  3. Копии готовых форм тендерного предложения заполняются аналогично оригиналу и не должны содержать подписей, печатей, наименований, адресов, телефонов и иной информации, указывающей на принадлежность к Вашей фирме. **Данные документы присылаются в формате word или excel.**
  4. В тендерном предложении не должно быть никаких исправлений, добавлений между строчками, подтирок или приписок.

**Содержимое 1-го конверта:** Квалификационная информация (см. пункт 2.1.), рекомендации, отзывы, резюме и др. документы, перечисленные в Техническом задании, кроме заполненных готовых форм (Готовая форма №1 и Готовая форма №2 – «Финансовое предложение»);

**Содержимое 2-го конверта:**

1. Готовая форма № 1 с печатью и подписью лица, имеющего полномочия подписывать договоры и тендерные документы **- в 1 (одном) экземпляре.**
2. Готовая форма №1 без идентификации фирмы-участницы (без названия, печати и подписи фирмы-участницы) – **в 1 (одном) экземпляре.**

**Содержимое 3-го конверта:**

1. Готовая форма № 2 (Финансовое предложение) с печатью и подписью лица, имеющего полномочия подписывать договоры и тендерные документы **- в 1 (одном) экземпляре.**
2. Готовая форма №2 (Финансовое предложение) без идентификации фирмы-участницы

(без названия, печати и подписи фирмы-участницы) – **в 1 (одном) экземпляре.**

Участник также представляет любые другие документы, которые Участник должен будет заполнить или подготовить в соответствии с требованием Покупателя. Данные документы могут быть запрошены как во время тендера, так и после его проведения в рамках работы с победителем.

* 1. Неполное представление запрашиваемой информации или же подача тендерного предложения, не отвечающего всем требованиям, изложенным в технической спецификации тендера и настоящей Инструкции, может привести к отказу от предложения Покупателем.

Внимание! Все три конверта должны быть помеченными номерами 1, 2, 3.

1. **Право покупателя принять любую тендерную заявку и отклонить все тендерные заявки.**
   1. Покупатель оставляет за собой право принять или отклонить любую тендерную заявку, а также отклонить все тендерные заявки и аннулировать процесс тендера в любой момент до определения победителя, не неся при этом никаких обязательств перед участниками и не будучи обязанным информировать участника или участников о причинах таких действий.
   2. Покупатель оставляет за собой право отклонить тендерную заявку участника, имеющего какие-либо невыполненные обязательства перед Покупателем, имевшего судебные разбирательства с Покупателем и иным требованиям, не удовлетворяющим Покупателя.

\*Кроме того Вы можете сообщить о злоупотреблении должностными обязанностями  со стороны сотрудников Банка, возникшем во время нашего с Вами взаимодействия или сотрудничества. Вы можете оставить голосовое сообщение с жалобой на короткий номер 8808, которое будет рассмотрено со стороны ответственного подразделения Банка.

|  |  |  |
| --- | --- | --- |
|  | **ПРИЛОЖЕНИЕ №1 ГОТОВАЯ ФОРМА № 1 (КОНВЕРТ №2)** | |
|  |  |  |
|  |  |  |
| **Квалификационные данные участника** | | |
| **№** | Квалификационное требование | Данные участника |
| **1** | Место регистрации компании |  |
| **2** | Основной Вид деятельности |  |
| **3** | Условия оплаты (указать) |  |
| **4** | Отсутствие незавершенных долговых обязательств, включая обязательства перед ГНС, СФКР и текущих судебных тяжб. |  |
| **5** | Срок поставки – до 17 мая |  |
| **6** | Соответствие техническому заданию |  |
| **7** | Предоставление авторизационного письма от производителя ПО (MAF) **(с переводом на русский язык)** |  |

**ПРИЛОЖЕНИЕ №2 ГОТОВАЯ ФОРМА № 2 (КОНВЕРТ №3)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
| **№** | **Наименование** | **кол-во** | **стоимость, сом** | | **Примечание** |
| **за ед.** | **всего** |  |
| 1 | Imperva WAF V2500 VA, AES | 2 |  |  |  |
| 2 | Imperva WAF VM 150 Management Server VA, AES | 1 |  |  |  |

*Внимание: для резидентов* ***Цены указываются в национальной валюте Кыргызской Республики (сомах) с включением всех налогов.***

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Общие требования**

1. WAF должен поставляться в формате программного комплекса в виде виртуальных машин для платформы виртуализации VMware и поддерживать версии ESX/ESXi 5.x, 6.x.

2. Общая пропускная способность по Layer 7 трафику каждой виртуальной машины должна быть до 500 Mbps, но не менее 100 Mbps.

3. Решение должно быть в лидерах Магического квадранта Гартнера не менее 7 последних лет

4. Решение должно иметь Common Criteria сертификацию

5. Вендор должен предоставить обучение по правильному развертыванию и управлению политиками WAF.

**Функциональные требования**

1. WAF должен поддерживать как позитивную, так и негативную модели безопасности.

a. Отрицательная модель безопасности будет определять известные сигнатуры атак.

i. Транзакции, содержимое которых совпадает с известными сигнатурами атак, блокируются. Все остальные разрешены.

ii. Отрицательная модель безопасности должна включать предварительно настроенный всеобъемлющий и точный список сигнатур атак.

iii. WAF должен разрешать модификацию или добавление сигнатур.

iv. WAF должен поддерживать автоматическое обновление списка сигнатур, обеспечивая полную защиту от новейших угроз.

v. Отрицательная модель безопасности должна позволять обнаруживать известные атаки на нескольких уровнях, в том числе на уровне сети, операционной системы, программного обеспечения веб-сервера и атак на уровне приложений.

b. Положительная модель безопасности предполагает, что разрешено все, что известно, а остальное блокируется.

i. Положительная модель безопасности должна включать в себя URL-адреса, каталоги, cookie, поля форм с параметрами и методы HTTP.

ii. С целью снижения трудоемкости настройки положительной модели безопасности, WAF должен обладать механизмом автоматического изучения и обновления структуры веб-приложения и его элементов.

1. Находясь в режиме обучения в течение ограниченного периода времени WAF запоминает параметры, вводимые легитимными пользователями в различные поля форм веб-приложения.
2. WAF должен обеспечивать непрерывное автоматическое изучение шаблона нормальной работы веб-приложения с учетом возможных запланированных изменений структуры и данных веб-приложения, и то же самое время обеспечивать активную блокировку отклонений от нормы.

a. Приемлемые значения параметров полей форм ввода записываются в профиль.

b. Записанные значения параметров используются в качестве критериев проверки легитимности запросов в положительной модели безопасности.

c. Режим обучения служит для создания модели структуры и элементов приложения (каталогов, URL-страничек, параметров, cookie) и ожидаемого поведения пользователя (ожидаемые диапазон изменения значений параметров, приемлемые символы, предназначен ли параметр для чтения или редактирования клиентом, является ли он обязательным или опциональным). Все это помогает автоматизировать настройку положительной модели безопасности.

d. Предусмотрена возможность изменения конфигурации профиля вручную администратором.

e. Механизм автоматического построения модели приложения (обучения) выявляет узкие места в профиле и предлагает соответствующие меры (изменения) для его оптимизации, например, преобразование URL в параметры и др.

1. WAF должен обнаруживать известные вредоносные источники автоматизированных атак и атак с использованием ботнетов, анонимных прокси, сетей TOR, фишинговых сайтов.
2. WAF должен уметь отслеживать удачные входы пользователей в веб-приложения и обогащать события безопасности соответствующей информацией
3. WAF должен обеспечивать возможность создание сложных политик безопасности, использующих в том числе данные внешних систем (например, Active Directory) посредством интуитивно понятного графического интерфейса, не требуя применения какого-либо языка программирования.
4. WAF должен обнаруживать и разрешать/блокировать запросы пользователей по географическому признаку.
5. WAF должен обеспечивать защиту программных интерфейсов приложений (Application programming interfaces, API).
6. WAF должен различать ботов от пользователей.
7. WAF должен уметь коррелировать события безопасности, чтобы отличать легитимные запросы от вредоносных.
8. WAF должен поддерживать пользовательские правила (политики) безопасности. У администраторов должна быть возможность создавать политики как для положительной, так и для отрицательной модели безопасности, а также создавать корреляционные правила, содержащие несколько критериев.
9. При развертывании в качестве прокси (прозрачный прокси или обратный прокси) WAF должен поддерживать цифровую подпись cookie, шифрования cookie, и перезапись URL.
10. WAF должен обладать интерфейсом интеграции со сканерами уязвимостей приложений с целью создания виртуальных патчей.
11. WAF должен устранять большинство из перечисленных в списке OWASP Top 10 уязвимостей веб-приложений. Перечень угроз OWASP Top 10 изложен в разделе “Список OWASP Top 10” данного документа.
12. WAF должен удовлетворять большинству из критериев WAFEC (www.webappsec.org).

**Требование к поддержке репутационных источников**

1. С целью предоставления дополнительного уровня безопасности необходимо, чтобы WAF обладал встроенными регулярно обновляемыми репутационными списками IPv4 адресов. Необходимо, чтобы у политик безопасности WAF была возможность блокировать источники по критерию принадлежности IPv4 адреса к таким репутационным спискам. Необходимо, чтобы WAF содержал репутационные списки по следующим категориям:

- Прокси-анонимайзеры

- Распостранители спама

- Geo-IP

- IP зловредной активности

- Фишинговые URL

- Узлы TOR.

2. Репутационный сервис должен поддерживать функционал Emergency Feeds для немедленной доставки обновлений в случае обнаружения критических уязвимостей.

3. Должен быть Forensic сервис для более детализированного просмотра информации об IP адресе.

**Требования по развертыванию и использованию**

1. WAF должен обладать возможностью развертывания в варианте in-line как прозрачный мост, обратный или прозрачный прокси-сервер. WAF также должен быть готов к развертыванию в режиме off-line как сниффер (пассивный сетевой монитор).
2. WAF должен поддерживать пассивный и активный режимы работы:

a. В пассивном режиме WAF позволяет администратору просматривать уведомления об атаках, об ошибках работы сервера, о других несанкционированных действиях.

b. В активном режиме WAF должен обладать возможностью блокировок атак.

c. При обнаружении атаки или любых несанкционированных действий WAF должен быть в состоянии принять соответствующие меры. Поддерживаемые действия должны включать возможность сбрасывать конкретные запросы и ответы, блокировать целые сессии TCP, запросы от конкретных пользователей приложений или с определенных IP-адресов. Для особо опасных атак WAF должен уметь блокировать все запросы от конкретного пользователя или с конкретного IP-адреса за заданный период времени.

d. В режиме пассивного сетевого мониторинга (сниффера) WAF должен быть в состоянии отправлять пакет TCP RST серверу приложений. Кроме того, WAF в режиме мониторинга может сообщать об аномальном поведении, но не предпринимать никаких ответных действий.

1. WAF должен обладать линейной пропускной способностью и латентностью в доли миллисекунд, чтобы не оказывать влияние на производительность веб-приложений.
2. WAF должен поддерживать среду виртуализации VMWare.
3. WAF должен быть в состоянии работать с HTTP и HTTPS (SSL) трафиком веб-приложений.
4. Для защиты SSL веб-приложений должна быть предусмотрена возможность импорта в WAF сертификатов и пар закрытый/открытый ключ веб-серверов.
5. Для защиты SSL веб-приложений WAF будет терминировать и расшифровывать клиентские соединения, инспектировать трафик на предмет соответствия политикам безопасности и, в зависимости от режима, может повторно его зашифровывать при соединениях с веб-серверами.
6. В режимах моста и сниффера WAF должен уметь расшифровать SSL трафик для проверки, не терминируя или изменяя HTTPS соединение.
7. WAF должен быть способен защищать веб-приложения, которые содержат XML контент. Защита XML должна быть эквивалентна защите веб-приложений с использованием механизма автоматизированного обучения (профилирования).
8. WAF должен поддерживать возможность работы в режиме высокой доступности (High availability).

**Требования к администрированию**

1. WAF должен иметь веб-интерфейс для администрирования.
2. WAF должен поддерживать функцию централизованного управления несколькими устройствами (шлюзами).
3. Конфигурация должна быть простой и интуитивно понятной.
4. Сервер управления должен поставляться в формате виртуальной машины для платформы виртуализации VMWare.

**Требования к поддержке интеграций**

1. WAF должен иметь возможность интеграции со сканерами уязвимостей:

* Beyond Security
* Acunetix
* Cenzic
* Denim Group
* HP Fortify WebInspect
* IBM AppScan
* Qualys
* Trend Micro
* Veracode
* WhiteHat"

1. WAF должен иметь возможность интеграции с системами управления событиями безопасности SIEM.
2. Решение должно интегрироваться со средами сервисных сетей на базе Envoy с использованием протокола gRPC, чтобы применять защиту как к трафику North-South, так и к трафику East-West в этих средах. Интеграция с решением должна выполняться через Sidecar прокси.
3. Решение должно поддерживать интеграцию с продуктами для обнаружения вредоносных программ, такими как FireEye (MPS), которая идентифицирует зараженные хосты на внутренних IP-адресах. Эта интеграция должна позволять администратору определять защитные действия от веб-активности, генерируемой зараженными хостами. В зависимости от уровня угрозы политики безопасности должны иметь возможность выполнять различные защитные действия, такие как аудит, оповещение или блокировка.

**Требования к мониторингу и отчетности**

1. WAF должен поддерживать:

a. Проверку и контроль HTTP трафик, включая HTTP заголовки, поля форм, а также передаваемые данные.

b. Проверку HTTP запросов и ответов.

c. Декодирование данных для представления в текстовом виде с целью последующей проверки.

d. Проверку для URL, форм, cookie, строк запроса, скрытых полей и параметров, методов HTTP, XML элементов и SOAP действий.

1. WAF должен поддерживать надлежащую отчетность и возможность журналирования:

a. Должен обладать возможностью формирования отчета о событиях с помощью стандартных механизмов, например, в системный журнал.

b. Уровни ведения журнала и фильтры должны устанавливаться администратором.

c. WAF должен быть в состоянии формировать табличные или предопределенные графические отчеты.

d. Эти отчеты должны быть доступны как по требованию, так и по расписанию и распространяться по протоколу SMTP.

e. Интерфейс управления WAF должен иметь графическую панель, информирующую о его состоянии и веб-активности.

1. WAF должен быть в состоянии идентифицировать пользователей веб-приложения. Механизм идентификации пользователей должен быть автоматизированным, не предусматривать внесения каких-либо изменений в существующее приложение или схему аутентификации приложения.

**Требования к архитектуре внедрения**

WAF должен поддерживать следующие варианты развертывания: Reverse Proxy, Transparent Bridge и Sniffer.

***Режим обратного прокси-сервера***

В данной топологии WAF должен действовать в качестве Reverse Proxy и терминировать HTTP/HTTPS соединения. При этом Reverse Proxy должен располагаться между веб-серверами и пользователями, осуществляя статическое преобразование внутреннего адреса веб-сервера во внешний, по которому пользователи обращаются к нему. В случае, когда WAF развернут в качестве обратного прокси, необходима переконфигурация сети:

Корректировка записей в DNS – те, что первоначально указывали на IP адреса веб-сервера должны указывать на IP адреса WAF.

Настройка межсетевых экранов таким образом, чтобы запретить непосредственный доступ по IP адресам веб-серверов.

Соответствующая настройка маршрутизации.

***Режим прозрачного моста***

В этой топологии, WAF должен действовать как прозрачный мост и не терминирует HTTP/HTTPS соединения. Весь трафик к защищаемым веб-серверам должен пройти через WAF (перехватывается и обрабатывается WAF). WAF проверяет трафик и блокирует вредоносный трафик. Весь остальной трафик проходит сквозь WAF без проверки (прозрачно).

***Режим пассивного мониторинга сети***

В данной топологии WAF должен быть подключен к SPAN порту коммутатора или к устройству Tap Ethernet. Веб-трафик не проходит через WAF, а поступает на его прослушивающие порты. В данной топологии WAF должен пассивно отслеживать и оповещать о событиях безопасности. При необходимости, в случае обнаружения нарушений правил защиты - сбрасывать TCP сессию путем отправки команды TCP Reset серверу.

**Список OWASP “Top 10”**

Open Web Application Security (OWASP) является открытым проектом, который разработал документацию и инструменты, чтобы помочь пользователям защитить свои веб-приложения и соответствующие службы. Целью проекта OWASP “Top 10” (список десяти наиболее часто встречающихся уязвимостей веб-приложений) является увеличение осведомленности о безопасности веб-приложений при помощи определения наиболее критичных рисков, угрожающих организациям. На проект “Top 10” ссылается множество стандартов, инструментов и организаций, включая MITRE, PCI DSS, DISA, FTC и множество других.

Ниже приводится список OWASP десяти наиболее часто встречающихся уязвимостей веб-приложений:

1)A1:2017-Injection

2)A2:2017-Broken Authentication

3)A3:2017-Sensitive Data Exposure

4)A4:2017-XML External Entities (XXE)

5)A5:2017-Broken Access Control

6)A6:2017-Security Misconfiguration

7)A7:2017-Cross-Site Scripting (XSS)

8)A8:2017-Insecure Deserialization

9) A9:2017-Using Components with Known Vulnerabilities

10) A10:2017-Insufficient Logging&Monitoring.

**WAF должен выявлять и блокировать атаки на вышеперечисленные уязвимости.**