Научная статья
Original article
УДК 004.424

БЕЗОПАСНОСТЬ ВЕБ КОНТЕНТА

WEB CONTENT SECURITY

Кобылко Андрей Эленович, аспирант, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kurinaaa@rambler.ru

Kobylko Andrey Elenovich, post-graduate student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kurinaaa@rambler.ru

Аннотация. Обеспечение высокой доступности. Многие веб-сайты и веб-приложения являются критически важными службами, которые должны работать круглосуточно и без выходных. Простои могут привести к нарушению SLA, потере доходов и ущербу для репутации.

Annotation. Ensuring high availability. Many websites and web applications are mission-critical services that need to run 24/7. Downtime can lead to SLA violations, loss of revenue and reputational damage.

Ключевые слова: Атака, информационная безопасность, веб-контент.

Keywords: Attack, information security, web content.

Оценка и выбор инструментов безопасности веб-сайта: полное руководство

Безопасность веб-сайтов — это практика защиты веб-приложений от широкого спектра киберугроз . Вот наиболее распространенные проблемы безопасности, с которыми сталкиваются группы безопасности, занимающиеся защитой веб-сайтов и веб-приложений:

Защита данных — веб-приложения обычно хранят конфиденциальные данные клиентов и организаций во внутренних базах данных. Если веб-приложение взломано, есть большая вероятность, что злоумышленники смогут скомпрометировать эти данные.

Контроль трафика веб-сайта. Владельцам веб-сайтов нужна видимость и контроль над тем, кто получает доступ к их веб-присутствию. Очень важно отличать хороший трафик от плохого — например, законных ботов от вредоносных ботов — и блокировать плохой трафик.

Защита доверия и репутации — веб-сайт является витриной для большинства предприятий. Если веб-сайт не работает, если домашняя страница повреждена или если злоумышленники скомпрометировали конфиденциальные данные клиентов, это может нанести серьезный ущерб бренду и репутации.

Защита посетителей веб -сайтов — онлайн-пользователи безоговорочно доверяют посещаемым ими веб-сайтам и веб-приложениям, с которыми они работают. Если злоумышленникам будет позволено красть сеансы или идентификационные данные посетителей или компрометировать их устройства, это доверие будет непоправимо подорвано.

Автоматизация безопасности — нехватка навыков безопасности и высокая стоимость сотрудников службы безопасности означают, что в большинстве организаций меньше сотрудников службы безопасности, чем им нужно. Автоматизация задач безопасности необходима для максимально эффективного использования ресурсов и обеспечения надлежащей защиты веб-ресурсов.

Это часть обширной серии руководств по безопасности приложений .

Выбор правильных решений для обеспечения безопасности веб-сайтов для бизнеса.

Современные службы защиты от DDoS-атак могут защитить веб-сайты от крупномасштабных DDoS-атак за счет масштабирования сети облачных компьютеров в соответствии с масштабом атаки. Службы защиты от DDoS - атак могут выполнять глубокую проверку пакетов входящего трафика и «очищать» или удалять неверные запросы в больших масштабах, в то же время пропуская законные запросы.

Поддержка всех типов атак — возможность защиты как от атак на сетевом уровне, так и от атак на уровне приложений с широкой поддержкой трафика приложений.

Трафик HTTP/S — возможность расшифровывать и очищать трафик SSL.

Защита вторичных активов — таких как базы данных, файловые серверы и системы CRM.

Емкость сети — проверьте, сколько Гбит/с или Тбит/с трафика поддерживает сервис; это будет примерно равно масштабу DDoS-атаки, которую он может остановить.

SLA — службы должны гарантировать время безотказной работы от трех девяток (99,9%) до пяти девяток (99,999%), указывать тип, размер и продолжительность защищаемых атак, а также указывать гарантированное время отклика.

Быстрое противодействие атакам — DDoS-атаки могут вывести из строя инфраструктуру всего за несколько секунд, а восстановление может занять несколько часов и более. Время отклика нужно измерять в секундах, а не в минутах или часах.

Постоянная защита — в идеале защита от DDoS-атак должна быть полностью незаметной для конечных пользователей. Убедитесь, что служба DDoS обладает достаточной пропускной способностью и конфигурацией для доставки содержимого веб-сайта с минимальной задержкой.

Веб-сайты и веб-приложения часто являются начальной целью для постоянных угроз повышенной сложности (APT) . APT-группы активно ищут уязвимости веб-сайтов, и если им удастся незаметно взломать веб-сайт, они начнут горизонтальное перемещение по сети, чтобы получить доступ к более конфиденциальным данным и системам.

Нет ни одного инструмента, который может защитить от APT. При выборе решения для защиты от APT рассмотрите комбинацию инструментов, которые могут защитить от многоаспектных атак.

Ключевая особенность

Обнаружение бокового перемещения — обнаружение атак, затрагивающих несколько организационных систем или пользователей, с боковым перемещением и постепенным повышением привилегий.

Двухфакторная аутентификация — для предотвращения несанкционированного доступа к системам организации.

Брандмауэр веб-приложений (WAF) — для блокировки подозрительных запросов к веб-приложениям.

Защита от бэкдор-шеллов и других уязвимостей.

Защита от DDoS — DDoS может использоваться как часть APT, чтобы отвлечь группы безопасности, в то время как злоумышленники используют другие методы для проникновения в сеть.

WAF являются краеугольным камнем проактивной безопасности веб-сайтов. Это решение безопасности, развернутое на границе сети, которое проверяет весь входящий трафик и постоянно блокирует вредоносные запросы . WAF универсальны , автоматически блокируют известные типы атак с помощью встроенных правил и позволяют развертывать собственные политики безопасности для конкретных потребностей безопасности.

Основным преимуществом WAF является то, что они могут быть развернуты без внесения изменений в базовые приложения и могут немедленно блокировать угрозы, не требуя выполнения таких действий, как исправление уязвимостей или изменение проблемного кода.

В отличие от традиционного брандмауэра, WAF может анализировать трафик приложений, различать законный и вредоносный трафик и, таким образом, обнаруживать и блокировать сложные шаблоны атак.

Ключевая особенность:

Фильтрация трафика — автоматическая блокировка трафика из подозрительных источников, топ-10 OWASP и других известных шаблонов атак.

Защита от уязвимостей — выявляйте и блокируйте трафик, связанный с известными уязвимостями программного обеспечения , не требуя сложных исправлений, автоматически обновляйте данные с помощью оперативной аналитики угроз для защиты от угроз нулевого дня.

Развертывание — легко развертывайте, не требуя каких-либо изменений в базовых системах веб-сайта. Совместимость с общедоступными облачными, гибридными и локальными средами.

Интеграция — интеграция с корпоративной SIEM , гарантирующая, что оповещения WAF можно будет легко просматривать в контексте других данных безопасности.

Сведение к минимуму ложных срабатываний — возможность настройки правил безопасности для адаптации к требованиям организации и минимального нарушения работы бизнеса. Желательно, чтобы уровень ложных срабатываний был низким в базовой конфигурации, даже без настройки.

Автоматически обновляется и обслуживается — обслуживается и поддерживается исследовательской группой безопасности на стороне поставщика, что особенно важно для угроз нулевого дня.

Литература

1. Ван Хайтао Исследование системы осведомленности об информационной безопасности на основе технологий больших данных и искусственного интеллекта, Технологии и приложения сетевой безопасности, 2018 (3): 60-63.

2. Чжэн Яньфан Исследования и практика применения искусственного интеллекта и технологий анализа в системе ситуационной осведомленности информационной безопасности Мир цифровых коммуникаций, 2018, № 160 (4): 229.
3. Чжэн Фан Информационная безопасность в эпоху искусственного интеллекта, Исследования в области информационной безопасности, 2017, 3 (11): 966-967.
4. Дэн Вэньбинь Проблемы и меры противодействия надзору за информационной безопасностью в эпоху искусственного интеллекта Информационная безопасность Китая, 2018 г., 106 (10): 106-108.

References

1. Wang Haitao Research on Information Security Situation Awareness System Based on Big Data and Artificial Intelligence Technology, Network Security Technology and Application, 2018 (3): 60-63.
2. Zheng Yanfang Research and Practice of Artificial Intelligence Application and Analysis Technology in Information Security Situational Awareness System Digital Communication World, 2018, No.160 (4):229.
3. Zheng Fang Information Security in the Age of Artificial Intelligence, Information Security Research, 2017, 3 (11): 966-967.
4. Deng Wenbing Challenges and Countermeasures for Information Security Supervision in the Age of Artificial Intelligence China Information Security, 2018, 106 (10): 106-108.

© Кобылко А.Э., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.

Для цитирования: Кобылко А.Э. БЕЗОПАСНОСТЬ ВЕБ КОНТЕНТА// Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.