Научная статья
Original article
УДК 004.424

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ И API (WAAP)

WEB APP AND API PROTECTION (WAAP)

Гнутова Ольга Викторовна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), ol.gnutova@mail.ru

Мотуз Николай Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), motuz0nik@yandex.ru

Gnutova Olga Viktorovna bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), ol.gnutova@mail.ru

Motuz Nikolay Sergeevich bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), motuz0nik@yandex.ru

Аннотация: Веб-приложения - это программы, к которым пользователи могут получить доступ через веб-браузер, и они являются важным компонентом присутствия многих организаций в Интернете. Веб-приложение может также включать интерфейсы прикладного программирования (API), которые обеспечивают программный доступ к возможностям приложения.

Abstract: Web applications are programs that users can access through a web browser and are an essential component of many organizations' Internet presence. A

web application can also include application programming interfaces (APIs) that provide programmatic access to the capabilities of an application.

Ключевые слова: Блокировка на основе портов, HTTP-трафик, проверка зашифрованного трафика, защита от ботов, защита систем

Keywords: Port-based blocking, HTTP traffic, encrypted traffic inspection, protection from bots, system protection

Адам Хилс и Джереми Д'Хоинн из Gartner придумали название «Защита веб-приложений и API» (WAAP) для обозначения облачных сервисов, созданных для защиты уязвимых API-интерфейсов и веб-приложений.

Облачные сервисы WAAP предоставляют различные модули безопасности, основанные на автоматически масштабируемой многопользовательской облачной инфраструктуре. Основные функции Cloud WAAP - это защита от ботов, WAF, защита API и защита от DDoS. Для каждого модуля возможна разная степень защиты. Облачные сервисы WAAP часто предоставляются с дополнительными сервисными компонентами, которые могут улучшить производительность веб-приложений.

Почему важен WAAP?

Веб-приложения и API-интерфейсы доступны через общедоступный Интернет и обеспечивают доступ к конфиденциальным данным, что делает их основной целью для злоумышленников . Традиционные решения безопасности не могут эффективно защитить эти приложения, поэтому WAAP является обязательным.

Вот несколько причин, по которым традиционные решения не могут эффективно защитить веб-приложения:

- **Обнаружение атак на основе сигнатур неэффективно** - угрозы для веб-приложений постоянно меняются. Попытка защититься от них с помощью решений для обнаружения на основе сигнатур - это не масштабируемая стратегия. Решения WAAP предлагают непрерывное

самообучение, что помогает организациям опережать развивающуюся среду угроз безопасности приложений.

- **Блокировка на основе портов не работает** - традиционные брандмауэры фильтруют трафик в соответствии с используемыми протоколами и портами. Однако атаки на веб-приложения и веб-API используют те же веб-порты и протоколы, что и пользователи, например HTTP (S), что делает невозможным фильтрацию только вредоносного трафика с помощью этого метода. Необходим более подробный уровень проверки, чтобы отличить потенциальные атаки от легитимного трафика.
- **Может быть задействован HTTP-трафик - могут быть задействованы** веб-приложения, и киберпреступники используют эту сложность для сокрытия вредоносного контента. Уровень проверки безопасности, предлагаемый традиционной системой обнаружения и предотвращения вторжений (IDS / IPS), недостаточен для изоляции и защиты от угроз для веб-приложений.
- **Необходима проверка зашифрованного трафика - сегодня** более половины всего веб-трафика использует шифрование TLS , что обеспечивает конфиденциальность, но затрудняет обнаружение вредоносных программ и другого вредоносного содержимого. Решения WAAP могут проверять соединения TLS, позволяя им выявлять конфиденциальные данные и вредоносный контент, скрывающийся в зашифрованном трафике.

Почему традиционных WAF уже недостаточно

По оценкам аналитиков Gartner, продажи физических устройств WAF снижаются, поскольку у большинства поставщиков наблюдается низкий или выраженный однозначным числом рост или спад. Есть определенные ожидания, когда поставщики WAF работают над улучшением своих облачных сервисов WAF, предлагая их в соответствии с требованиями WAAP.

Упадок устройств WAF в основном связан с развитием корпоративных веб-приложений:

- **Современные приложения часто меняются** - внедрение гибких методов разработки и DevOps означает, что современные веб-приложения и API-интерфейсы постоянно **меняются** . Брандмауэры веб-приложений (WAF), требующие ручной настройки и создания пользовательских правил, плохо приспособлены к быстро меняющимся приложениям.
- **Облачный хостинг стал популярной архитектурой** - ведущие поставщики решений предлагают решения для обеспечения безопасности облачных приложений. Это также дает большие преимущества, включая минимизацию потенциальных узких мест или задержек, особенно когда веб-приложения обслуживают клиентов из разных областей.
- **Отсутствует позитивная модель безопасности** - технология WAF **не** дала гарантии автоматического создания разрешенных списков для URL-адресов и параметров, основанных на автоматическом изучении трафика приложений. На самом деле они требуют сложной ручной настройки и настройки.
- **В последнее время** в **WAF наблюдаются минимальные инновации** - быстрый рост веб-стандартов (HTTP 2.0 , более широкое использование полезной нагрузки JSON) монополизировал планы разработчиков по разработке, оставляя мало места для разработки новых функций безопасности.
- **Стратегия с** несколькими облаками - каждый поставщик облачных услуг предлагает разные функции и использует разную архитектуру. Организациям, работающим в нескольких облаках, необходимо создать сложную матрицу возможностей для разных поставщиков, чтобы обеспечить эффективный контроль безопасности. Защита среды выполнения на основе облачных агентов и услуги WAAP больше подходят для многооблачной среды.

Служба защиты веб-приложений и API: основные возможности

Комплексные службы защиты веб-приложений и API-интерфейсов защищают ваши веб-приложения и API-интерфейсы от широкого спектра атак. Служба WAAP должна эффективно проверять запросы, прежде чем они достигнут конечной точки API или приложения.

Основные возможности широкой службы WAAP включают:

- **Брандмауэр веб-приложений нового поколения (WAF следующего поколения)** - защищает и отслеживает веб-приложения от широкого спектра атак в точке их развертывания - на уровне приложений. WAF следующего поколения отличается от традиционного WAF тем, что он использует поведенческий анализ и искусственный интеллект (AI) для блокировки атак, не полагаясь исключительно на известные шаблоны атак и правила безопасности, установленные вручную.
- **Самозащита приложения** во время выполнения **(RASP)** - встроенная в домен времени выполнения приложения, это обеспечивает защиту от атак в реальном времени для API-интерфейсов и веб-приложений.
- **Защита** от **вредоносных ботов** - изолирует и останавливает атаки подозрительных ботов , позволяя безопасному трафику ботов достигать приложения.
- **Распределенная защита** от **отказа в обслуживании (DDoS) - защита** от DDoS-атак, направленных на приложения, API-интерфейсы и микросервисы, на уровне приложений и сети. Возможность масштабирования для защиты от массовых атак.
- **Расширенное ограничение скорости** - защита от злонамеренных действий на уровне приложения, которые отрицательно влияют на производительность веб-сайта и API.
- **Защита микросервисов и API-интерфейсов** - обеспечивает безопасность внутри микросервисов, приложений или бессерверных функций для создания микропериметра с учетом контекста и данных вокруг всех отдельных служб.

- **Защита** от **захвата учетной записи - защита** от киберпреступников, использующих скомпрометированные учетные данные из дампов данных и списков паролей. Обнаруживает несанкционированный доступ к учетным записям клиентов через API-интерфейсы аутентификации или процесс аутентификации приложения, ориентированный на клиента.



Рекомендации по оценке облачной службы WAAP

Вот несколько способов оценить, подходит ли решение WAAP для вашей организации.

Нормативные и культурные ограничения

Страх перед юридическими проблемами может вызвать не только эффективные регулятивные ограничения, но и спровоцировать сопротивление организации. Это может помешать внедрению облачных сервисов безопасности, включая облачные сервисы WAAP.

Некоторые из ключевых проблем включают:

- Разрешение стороннему облачному решению расшифровывать TLS-соединения, работать с секретными ключами приложений и регистрировать конфиденциальные данные клиентов, которые могут зависеть от условий хранения данных.

- Адаптация бюджетов к SLA и модели ценообразования поставщика.
- Интеграция облачного решения WAAP в текущий рабочий процесс реагирования на инциденты, который, как правило, основан на инструменте управления информацией и событиями безопасности (SIEM).

Зрелость решения

Многие сервисы Cloud WAAP не имеют некоторых характеристик устройства WAF - защиты URL-адресов и форм, подписи файлов cookie и токенов подделки межсайтовых запросов (CSRF). Это замедляет внедрение в организациях, уже использующих этот метод и ищущих поэтапный подход к своей стратегии безопасности облачных приложений.

Техническая Архитектура

Сервисы WAAP, созданные с нуля, а не основанные на установленных решениях WAF, как правило, упускают возможность интеграции с экосистемой предприятия, включая тестирование безопасности приложений (AST) и SIEM. Они также могут обеспечивать ограниченное хранение журналов и параметры конфигурации. Консоли мониторинга сервиса Cloud WAAP могут не предлагать запись в журналы в реальном времени.

Литература

1. Война в киберпространстве: уроки и выводы для России [Электронный ресурс] // Круглый стол в редакции «Независимого военного обозревателя». - Режим доступа : http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. Госучреждения Германии страдают от хакерских атак [Электронный ресурс]. - Режим доступа : http://www.dw.de/ госучреждения-германии-страдают-от-хакерских-атак/a-16691699.
3. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. - 2010. - № 5. - С. 19-37.

4. Кибервойна: вымысел или реальность [Электронный ресурс] // Журнал Безопасность. - Режим доступа : http://www. securityinfowatch. ru/view.php? section=news&item= 121.
5. Кибернетическая безопасность и свобода информации [Электронный ресурс]. - Режим доступа : http://mediakritika.by/ article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.

References

1. War in cyberspace: lessons and conclusions for Russia [Electronic resource] // Round table edited by the Independent Military Observer. - Access mode: http://nvo.ng.ru/concepts/2013-12-13/l_war.html.
2. State institutions in Germany suffer from hacker attacks [Electronic resource]. - Mode of access : http://www.dw.de/ governmental-institutions-of-germany-suffer-from-hacker-attacks/a-16691699.
3. Dubov D. Approach to molding the thesaurus in the field of cybersecurity / D. Dubov // Political management. - 2010. - No. 5. - S. 19-37.
4. Cyberwar: fiction or reality [Electronic resource] // Journal of Security. - Access mode : http://www. security info watch. en/view.php? section=news&item=121.
5. Cybernetic security and freedom of information [Electronic resource]. - Access mode: http://mediakritika.by/article/kiberneticheskaya-bezopasnost-i-svoboda-informacii.

© Гнутова О.В., Мотуз Н.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Гнутова О.В., Мотуз Н.С. ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ И API (WAAP) // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.