ЧТО НЕ ТАК С ПЕРИМЕТРОМ

ПРАКТИЧЕСКИЕ НЕДОСТАТКИ БЕЗОПАСНОСТИ ВНЕШНЕГО ПЕРИМЕТРА В 2024 ГОДУ

Давид ОРДЯН
генеральный директор ООО «МЕТАСКАН»

Владимир СОЛОВЬЁВ
руководитель направления внедрения средств защиты АО «ДиалогНаука»

На сегодняшний день в России не существует публично распространённых стандартов и практик обеспечения информационной безопасности внешнего периметра. При этом проникновение через внешний периметр остаётся одним из наиболее простых и часто используемых способов проникновения в корпоративную инфраструктуру организаций. В этой статье мы рассмотрим общие подходы, а также активно используемые злоумышленниками векторы атак, которые всё ещё игнорируются большинством СЗИ.

ТИПОВОЙ СОСТАВ ВНЕШНЕГО ПЕРИМЕТРА. ВЕКТОРЫ АТАКИ

Чем больше организация, тем больше изменений в её периметре происходит каждый день. Это могут быть релизы прикладного или системного ПО, обновление прошивок оборудования, новые открытые порты или целые новые VM.

Самым простым вектором атаки являются сервисы, опубликованные в интернете по ошибке, — базы данных, самописные административные панели, сервисы 1С, хранилища документов.

Многие современные веб-приложения используют технологии, которые не были популярны или не существовали ещё 5 лет назад. Один из самых типичных и при этом слабозащищённых векторов атаки — уязвимые API. Лучшей практикой тут будет загрузка API-спецификации в сканер уязвимостей. Наличие API-спецификации делает процесс поиска уязвимостей надёжнее, чем классический обход сайта пауком, ведь система поиска уязвимостей заранее знает о существовании каждого URL-адреса и каждого параметра в приложении.

Краеугольным камнем безопасности периметра является уверенность в том, что назначение каждого сервиса на внешнем периметре известно отделу ИБ и каждый опубликованный сервис прошёл процедуру приёмки.

При исследовании зарубежных рынков мы общались с отделами ИБ Google и Amazon, и даже у таких гигантов есть проблема с тем, чтобы ответить на вопросы: «Что нам принадлежит?» и «Где границы нашего периметра?» (Возьмите на заметку, если планируете исследовать эти периметры.)

Наиболее простые сканеры уязвимостей попросят вас загрузить в них список проверяемых доменов или IP-адресов. Более продвинутые решения умеют проводить автоматизированную разведку всего интернета и собирать данные с помощью брутфорса dns, скрапинга поисковых систем, интеграции с Censys/Shodan, собирать данные о сертификатах из системы certificate transparency или других сторонних источников. Но все эти способы ограничены своей реализацией, и технически невозможно обнаружить доменное имя, созданное из случайного набора символов и не имеющее выписанных сертификатов или сетевых баннеров. Единственным гарантированным источником данных на вход вашей сканирующей системе может служить конфигурационный файл вашего DNS-сервера, который требуется не только выгрузить с сервера, но ещё и сопоставить его с действительностью, «как это есть» на самом деле, и только потом уже импортировать в сканирующую систему. В этом случае может помочь автоматизация процесса обновления списка реальных доменов и IP-адресов организации на стороне сканирующей системы с помощью интеграции системы по API с существующими СЗИ. Данный подход используется в решениях класса ASM (Attack Surface Management) — управление поверхностью атаки внешнего периметра. Metascan — отечественный ASM, позволяющий автоматизировать процесс поиска новых активов организации и поиска уязвимостей на них.

СКОРОСТЬ РАБОТЫ

Современные злоумышленники далеко ушли от необходимости кропотливого ручного сканирования каждого внешнего сервиса и узла. В мире киберпреступности активно применяются атакующие пайплайны,

в которых на вход подаются данные из Censys/Shodan или других глобальных сканеров, а далее происходит моментальная эксплуатация конкретного сервиса с конкретным эксплойтом. В этом случае нет возможности заблокировать злоумышленника за сканирование периметра или неудачные попытки атаки. Противостоять этому может только раннее обнаружение уязвимостей. И задача современного специалиста ИБ — обеспечить себе максимум времени на устранение обнаруженной уязвимости.

К 2024 году парадигма еженедельных/ежемесячных сканов является скорее опасной, чем полезной, так как создаёт ложное чувство защищённости: уязвимости появляются намного чаще и быстрее. При этом большинство зарубежных вендоров переходят на концепцию Continuous Vulnerability Scanning, в которой сканирование каждого домена или IP-адреса происходит несколько раз в день.

Metascan имеет обширную распределённую сеть глобальных сканеров по всей сети Интернет, что позволяет иметь полную и актуальную информацию по всем активам внешнего периметра в кратчайшие сроки.

ПОЛНОТА И КАЧЕСТВО

Многие решения по поиску уязвимостей хороши, но имеют узкую направленность. Nessus — отличный сканер для системных сервисов, но он практически беспомощен в поиске веб-уязвимостей. Acunetix — отличное решение для поиска веб-уязвимостей, но в нём отсутствуют даже механизмы сканирования портов. Помимо этого, у нас есть сетевое оборудование, сервера с интерфейсами IPMI и ILO, CMS Bitrix и 1С, IP-камеры и системы их управления, проприетарные решения от отечественных вендоров, использующих собственные протоколы, которые не определяются популярными сканерами портов, но при этом имеют учётные записи со стандартными паролями и др.

Metascan имеет более 30 модулей и движков проверок, которые могут быть запущены в любое время с необходимой частотой запуска. Модули можно кастомизировать и добавлять собственные. В качестве языка разработки модулей используется Python.

METASCAN — ОБЛАЧНЫЙ L3-L7-СКАНЕР УЯЗВИМОСТЕЙ С ЭКСПЕРТНЫМ СОПРОВОЖДЕНИЕМ

Metascan позволяет решать следующие проблемы ИБ:

- большое количество ложных срабатываний;
- низкая скорость работы сканеров уязвимостей;
- отдел ИБ перегружен текучкой и не знает, как работать с найденными уязвимостями;
- узкая специализация сканеров периметра.

И если вы не можете ответить хотя бы на один следующий вопрос, мы рекомендуем вам задуматься об использовании решения Metascan:

- Вам известны все доменные имена и IP-адреса вашей организации?
- Вам известно назначение каждого сетевого порта и то, с каким бизнес-сервисом этот порт связан?
- Поиск уязвимостей происходит на ежедневной основе или чаще?
- Используются ли движки сканирования, умеющие находить уязвимости в отечественном ПО (Bitrix, 1С Предприятие, R7 Office, системы видеонаблюдения, СКУД и др.)?

Для веб-приложений используются ли движки, поддерживающие сканирования на основе API, умеющие искать уязвимости в websocket и других современных протоколах?

Решение Metascan не привязано к человеческому фактору и может сканировать активы периметра постоянно, способно отслеживать изменения защищённости периметра 24 часа 7 дней в неделю, обнаруживать уязвимости сетевого оборудования и системных сервисов, а также проводить инвентаризацию активов компании.