Как найти слабые места сетевой инфраструктуры и почему это важно

Незакрытые уязвимости, "дыры" и ошибки на узлах сетевой инфраструктуры компании дают злоумышленникам немало возможностей. Одна неисправленная ошибка способна привести к финансовым и репутационным потерям, приостановке деятельности компании и штрафам со стороны регуляторов.

По данным центра мониторинга и реагирования на кибератаки Solar JSOC компании "Ростелеком", в 90% успешных атак на веб-приложения (будь то интернет-магазины, сайты-сервисы или корпоративные порталы) киберпреступники используют уязвимости. Еще больше ошибок скрывают внутренние ресурсы организации, количество инцидентов с которыми, по данным экспертов компании, составляет более 45% от общего числа атак.

Чаще всего злоумышленники используют уязвимости массовых программных продуктов, протоколов операционных систем (Windows и проч.), прикладного ПО (например, MS Office), веб-серверов Nginx или Apache (на них развернуто подавляющее большинство ресурсов), протоколов SMB, SSH, RDP (они нужны для удаленного доступа к устройствам, например, при дистанционной работе). Многие из них затрагивают миллионы устройств, а построенные на них атаки принимают по-настоящему глобальный характер. Так произошло, например, с уязвимостью SMB-протокола, эксплуатация которой привела к распространению печально известных вирусов WannaCry и NotPetya в 2017 году. И, хотя с тех пор прошло уже три года, в одной только России эта уязвимость остается незакрытой на более чем 266 тыс. серверов (в мире - более чем на 1,7 млн). При этом ежегодно киберпреступники находят новые "прорехи" в инфраструктуре: за последние два года мировая база данных уязвимостей CVE (Common vulnerabilities and exposures) пополнилась более чем 24 тыс. новых уязвимостей.

Как найти уязвимости?

Для поиска слабых мест в инфраструктуре существует два основных подхода: сканирование на уязвимости и пентест (тестирование на проникновение). Эти два процесса отличаются фокусом работ. Задача пентестера состоит в эмуляции, то есть воспроизведении действий злоумышленника, попытке проникнуть в систему и закрепиться в ней. А цель сканирования на уязвимости – оценка не "вглубь", а "вширь". Специалиста по тестированию на проникновение интересуют самые слабые звенья цепи, специалиста по сканированию на уязвимости - абсолютно все.

Но для обоих типов исследований требуются значительные затраты на закупку средств сканирования и прочего оборудования, а также на квалифицированный персонал, который с этим оборудованием сможет работать. Кроме того, для многих компаний обеспечение ИБ – это вложения в непрофильную деятельность, которые не факт, что отобьются (например, если злоумышленники так и не обратят внимания на вашу компанию). С другой стороны, игнорировать проблемы с безопасностью нельзя, ведь успешная атака (если она все-таки произойдет) гарантированно станет серьезным ударом для компании.

На помощь бизнесу приходят сервис-провайдеры, которые могут предоставить клиенту профессиональную команду, способную проверить его инфраструктуру, проведя пентест или сканирование на уязвимости.

Какой подход к поиску уязвимостей лучше выбрать, зависит от зрелости компании в области ИБ. Идеальный вариант – комплексный. Первоначальную, а также поддерживающую оценку уровня защищённости лучше проводить в рамках процесса контроля уязвимостей, а вот проверять на прочность свою инфраструктуру и навыки специалистов - с помощью пентеста (делать это "редко, но метко").

Так с 2019-го года "Ростелеком" предлагает сервис контроля уязвимостей (Vulnerability Management, VM) на базе облака Qualys, который подойдёт как для компаний, впервые озаботившихся вопросами сетевой безопасности, так и для клиентов, уже осознающих важность данного процесса.

Что такое сервис контроля уязвимостей?

С помощью сервиса контроля уязвимостей заказчики могут сканировать как внешний периметр организации, так и внутреннюю сеть: веб-приложения, серверы, сетевые устройства, рабочие места (в том числе удалённых сотрудников – с помощью агентских модулей). Само сканирование может быть как разовым (оно подойдёт для небольших компаний и точечных задач), так и периодическим (этот вариант гарантированно повысит уровень защищённости организации). Сервис-провайдер также может провести предварительную инвентаризацию активов заказчика, а по результатам сканирования проверить возможность эксплуатации наиболее критичных уязвимостей и подготовить

отчёт с рекомендациями по их устранению, собранной статистикой и общей оценкой защищённости.

На рынке существуют различные сканеры уязвимости. "Ростелеком" предлагает сервис на базе решения компании Qualys, причем облако, в котором обрабатывается информация, расположено на территории России. Так что клиент может не переживать, что конфиденциальная информация передается за границу.

Какие сегменты инфраструктуры необходимо просканировать – зависит от текущих задач заказчика. Практически всегда есть смысл сканировать веб-приложения – будь то корпоративный портал, внешний сайт, веб-система для клиентов или подрядчиков организации. Без должной защиты любой из этих узлов может быть взломан злоумышленниками – по статистике Solar JSOC, треть всех внешних атак приходится именно на веб-приложения.

Если компания беспокоится о защите своих серверов и ПК сотрудников, то стоит исследовать внутреннюю сеть. Если же локальная сеть надежно защищена и ключевая задача – выстроить крепкий внешний периметр, то его и нужно проверить. В целом, как показывает практика последних лет, соотношение внешних и внутренних инцидентов информационной безопасности составляет примерно 58% и 42% соответственно.

Внешний периметр организации сканируется непосредственно из облака. Внутренняя сеть анализируется с помощью локальных сканеров – специальных виртуальных машин, развертываемых в инфраструктуре заказчика. Они позволяют оптимизировать нагрузку при сканировании и упростить его организацию.

Альтернативой локальному сканеру являются уже упомянутые агенты, которые можно развернуть на сетевых узлах для непрерывного получения информации о них (в таком случае собираться будут сведения не только об ОС, открытых портах и сервисах, но и данные об установленном ПО, запущенных процессах и т.п.). Чем больше информации удастся собрать в ходе сканирования, тем более точными и полными будут сведения об уровне защищённости инфраструктуры.

Для тех клиентов, кто обладает ресурсами в области ИБ, работал с сетевыми сканерами ранее и просто хочет удобный инструмент, сервис может быть предоставлен в режиме самообслуживания, а также в промежуточном формате, когда заказчик может в любой момент провести сканирование самостоятельно, а все регламентные работы выполнят уже специалисты "Ростелекома".

Кроме непосредственного поиска уязвимостей, сервис VM поможет проверить инфраструктуру заказчика на соответствие политикам ИБ, будь то требования PCI DSS (этому стандарту безопасности должны соответствовать все поставщики товаров и услуг, принимающих в качестве средства оплаты платежные карты), рекомендации Центра интернет-безопасности CIS, лучшие практики Solar JSOC или внутренние требования самой компании.

Можно ли без этого обойтись?

По своей сути, VM - это своеобразный техосмотр, в котором вместо автомобиля исследуются сайты, локальная сеть или внешний периметр организации. Сканер не сможет выявить 100% уязвимостей, но найдет те, которые, скорее всего, будут применять злоумышленники, если захотят атаковать вашу организацию. В информационной безопасности отлично работает закон Парето: "20% усилий дают 80% результата". Достаточно хотя бы немного поднять уровень кибербезопасности, чтобы отсечь 80% или даже больше из реально угрожающих бизнесу атак. В ином случае со временем хакеры и конкуренты доберутся и до вас. И тогда останется лишь надеяться, что у компании хватит прочности, чтобы перенести потери.