Ростелеком
Солар

Тренды Vulnerability Management: как компании ищут и устраняют слабые места в инфраструктуре

Содержание

Введение

Массовая цифровизация большинства бизнес-процессов значительно усложнила ИТ-инфраструктуру организаций. На их периметре появились новые цифровые активы, закрытые системы и критические серверы, хранящие конфиденциальные данные самих компаний и их клиентов. Пропустить какие-то незакрытые уязвимости в такой разрозненной инфраструктуре достаточно просто. А одна неисправленная ошибка, которую обязательно найдут злоумышленники, способна привести к финансовым и репутационным потерям, приостановке деятельности компании и штрафам со стороны регуляторов. Поэтому первый шаг в построении кибербезопасности организации – это выстраивание процесса по контролю уязвимостей (Vulnerability Management, VM).

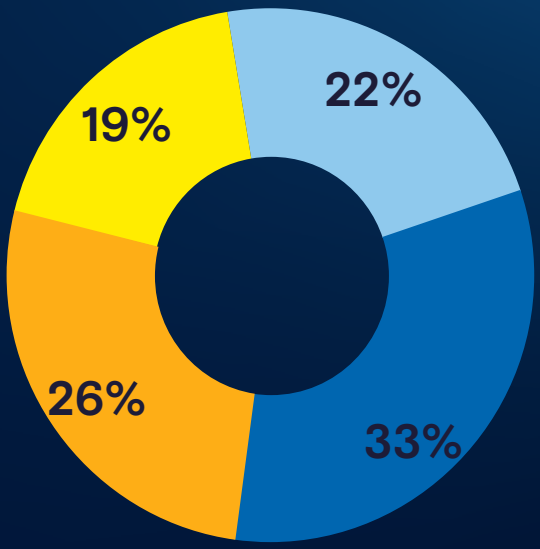
VM представляет собой процесс постоянной инвентаризации (то есть актуализации информации о всех информационных активах компании), оценки уровня защищенности сетевой инфраструктуры, разработки рекомендаций по исправлению и устранению найденных уязвимостей, а также проверки выполнения этих рекомендаций.

В данном отчете представлены результаты опроса, проведенного компанией «Ростелеком-Солар», которые показывают, как сейчас налажен процесс контроля уязвимостей в российских организациях и с какими сложностями сталкиваются специалисты при проведении сканирования и дальнейшем закрытии найденных ошибок.

Методология исследования и профиль респондентов

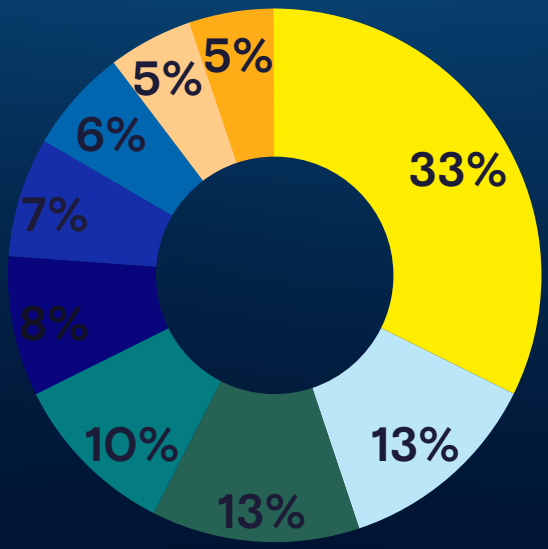
В рамках исследования были опрошены представители 200 организаций разного масштаба и профиля. Опрос проводился в апреле-июне 2021 года в онлайн-формате. Часть вопросов подразумевала возможность выбора нескольких вариантов ответа.

Масштабы организаций (по количеству хостов):



- до 250
- 1000-5000
- 250-1000
- более 5000

Профиль респондентов по отраслям:



- ИТ и телеком
- Наука и образование
- Госсектор
- ТЭК
- Здравоохранение
- Финансы
- Промышленность
- Ритейл
- Другое

При этом у большинства опрошенных (43%) в организации есть собственный полноценный ИБ-отдел. Еще 36% ответили, что защита от киберугроз находится в ведении ИТ-отдела, а 21% – что этими вопросами занимается один выделенный ИБ-специалист.

Ключевые цифры

В 70%

организаций проводится контроль уязвимостей, однако половина компаний считают налаженный у них процесс несовершенным.

> 60%

компаний сканируют инфраструктуру раз в квартал или реже. Однако этого недостаточно, так как новые уязвимости появляются чаще.

90%

респондентов уверены, что основная цель сканирования на уязвимости – это построение реальной безопасности. При этом 60% респондентов считают, что сканирование также решает задачи выполнения требований регуляторов.

45%

опрошенных считают локальную сеть самым интересным элементом для сканирования, а веб-приложения и изолированный контур находятся в фокусе внимания только у 17% респондентов. Это тревожный знак, так как за последний год веб-уязвимости стали значительно чаще использоваться хакерами для проникновения в сеть организации. Например, в 2020 году треть всех инцидентов кибербезопасности была связана именно с атаками на веб (по оценке Solar JSOC).

Как ищут уязвимости в компаниях

В данном разделе собрана информация о том, как компании проводят сканирование ИТ-периметра и с какой целью, какие источники информации об уязвимостях используют, а также какие именно элементы инфраструктуры проверяют.

Кто сканирует инфраструктуру и зачем

Сканирование уязвимостей на инфраструктуре – один из ключевых процессов построения информационной безопасности любой организации. Собирать данные о новых уязвимостях и начинать работы по их выявлению и устранению необходимо до появления эксплойта (то есть компьютерной программы, использующей уязвимости в ПО). Значимость Vulnerability Management понимает большинство респондентов: контроль уязвимостей в том или ином виде проводится в 70% организаций. Однако почти половина из них считают выстроенный процесс несовершенным. Примечательно, что такую оценку дают в основном крупные компании (более 5 тыс. хостов). При этом 41% респондентов рассказали, что проводят сканирование автоматически по расписанию, а 39% – что делают это силами только одного ИБ-специалиста. Из данных результатов следует, что эффективность процесса управления уязвимостями крайне низкая, так как:

- результаты автоматического сканирования – это большой объем технической информации, на обработку и анализ которой тратится много времени (особенно силами одного специалиста), что уже само по себе неэффективно;
- необходимы специалисты высокого уровня, чтобы корректно обработать массив информации;
- использование одного из специалистов отдела ИБ – путь, при котором на одного сотрудника, помимо множества задач безопасности, ложится также задача сканирования, на которую он не может потратить достаточно времени и зачастую выполняет ее фрагментарно или даже формально.

При очевидной неэффективности процесса абсолютное большинство респондентов (90% организаций) отмечают, что, проводя сканирование ИТ-периметра, стремятся обеспечить реальную кибербезопасность. Такое несоответствие цели и инструментов говорит о том, что в компаниях создается ощущение ложной безопасности, так как часто отсутствует финальный процесс контроля уязвимостей –их устранение. Это доказывают и расследования экспертов «Ростелеком-Солар», в результате которых выяснилось, что в большинстве инфраструктур находятся старые уязвимости, обновления для которых были выпущены несколько лет назад. А каждая десятая критическая информационная инфраструктура оказывается зараженной каким-то видом вредоносного ПО.

Помимо обеспечения реальной безопасности, Vulnerability Management – это способ выполнять требования российских регуляторов. Так считают 60% респондентов. Действительно, приказ ФСТЭК № 239 требует от субъектов КИИ проводить инвентаризацию информационных ресурсов, аудит и анализ/устранение уязвимостей, а приказ ФСТЭК № 235 требует выявлять уязвимости в значимых объектах КИИ.

Среди других целей проведения сканирования инфраструктуры респонденты назвали:

соответствие требованиям международных стандартов

проверку ресурсов сетей, операционных систем, подключенных устройств, портов

создание отчетов, в которых описываются типы уязвимостей

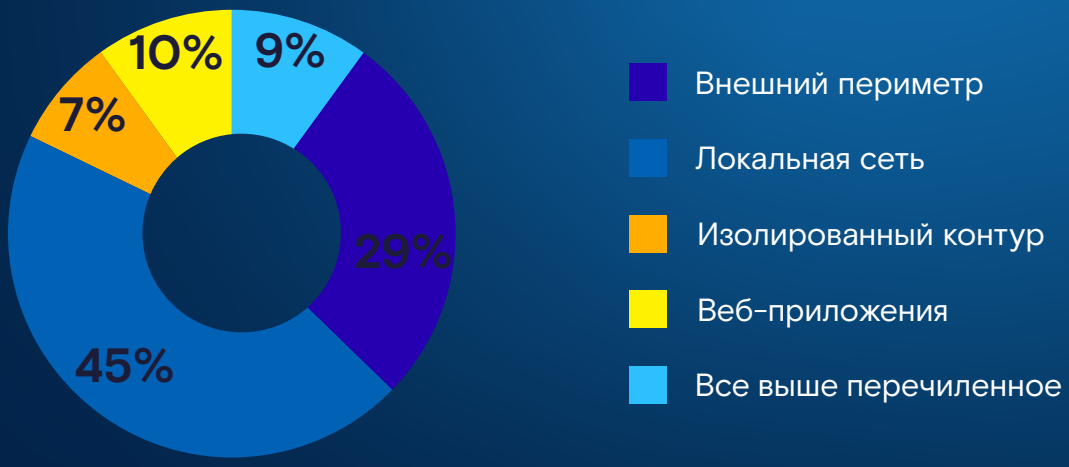
поиск различных типов уязвимостей сети и их анализ в режиме реального времени

Что сканируют

Наиболее интересным элементом инфраструктуры для сканирования большинство респондентов (45%) считают локальную сеть. Это объясняется тем, что, с одной стороны, многие компании понимают, что эксплуатация уязвимостей на внешнем периметре – это лишь первый шаг злоумышленника, а его главная цель заключается в развитии атаки внутри инфраструктуры (для кражи данных, влияния на технологические процессы и т. п.). И для развития атаки хакеры используют именно уязвимости внутренних сетевых узлов.

С другой стороны – компании, концентрируясь на внутренних уязвимостях, уделяют недостаточно внимания внешним, так как уверены, что на периметре их компании внешние злоумышленники не найдут нужного им потенциального вектора проникновения в инфраструктуру.

Какие элементы интересны для сканирования:



Второй по популярности элемент инфраструктуры для сканирования – это внешний периметр. Отметим, что именно на внешнем периметре российских организаций встречаются критические и при этом относительно старые уязвимости, некоторые из которых были обнаружены уже 10 лет назад. Среди них баг Heartbleed, который использует ошибки в криптографической библиотеке OpenSSL, уязвимость EternalBlue, через которую в 2017 году хакеры распространяли вирус-шифровальщик WannaCry, а также BlueKeep – уязвимость протокола удаленного рабочего стола RDP. Эксплуатация вышеперечисленных уязвимостей в свое время вызвала широкий резонанс в обществе, а вендоры оперативно выпустили обновления. Тем не менее эти ошибки до сих пор встречаются в компаниях разного масштаба и сфер деятельности.

Сканирование внешнего периметра стало особенно актуально в период пандемии, так как переход на удаленный режим работы и массовая цифровизация бизнес-процессов значительно ослабили ИТ-периметры:

- увеличилось количество возможных целей для атак;
- переход большого числа компаний из офлайна в онлайн происходил в спешке и потому его качество оказалось ниже существующих стандартов;
- с переходом в онлайн и переводом сотрудников на удаленный режим работы сильно возросла критичность ошибок в инфраструктуре.

За последний год более чем на 60% выросло число автоматизированных систем управления технологическими процессами (АСУ ТП), доступных из интернета. А количество хостов с уязвимым SMB-протоколом увеличилось почти в 2 раза (по данным Solar JSOC).

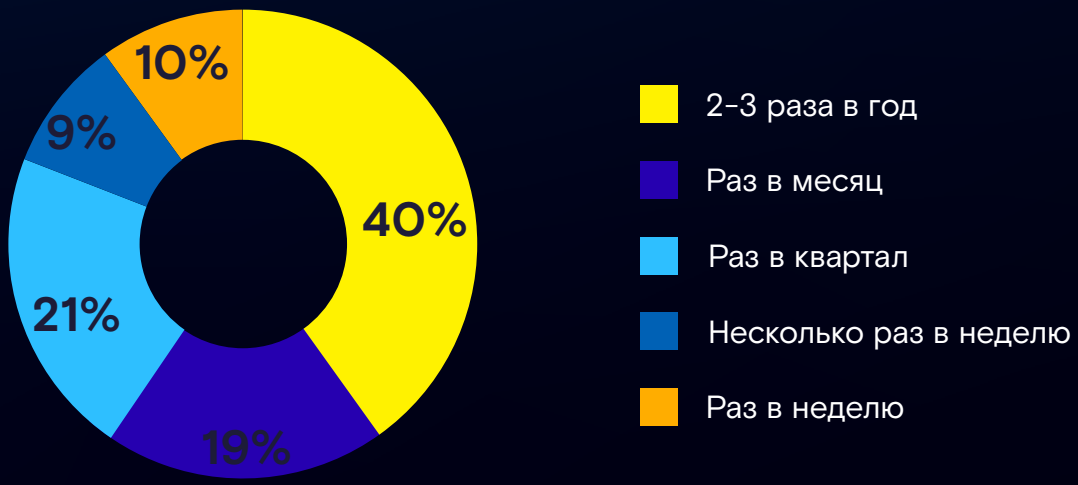
Из опроса видно, что веб-приложения и изолированный контур находятся вне фокуса внимания респондентов. Это тревожный знак, так как за последний год веб-уязвимости стали значительно чаще использоваться хакерами для проникновения в сеть организации.

По оценке Solar JSOC, 44% веб-приложений (например, корпоративные порталы, почтовые приложения) имеют некорректную настройку прав доступа, а 29% – возможности внедрения SQL-инъекций. Если говорить об изолированном контуре, то автоматические обновления ПО, которые закрывают многие уязвимости, здесь недоступны из-за отсутствия подключения к интернету. В то же время ручной или полуручной процесс установки патчей отсутствует в 90% российских организаций.

Как часто сканируют

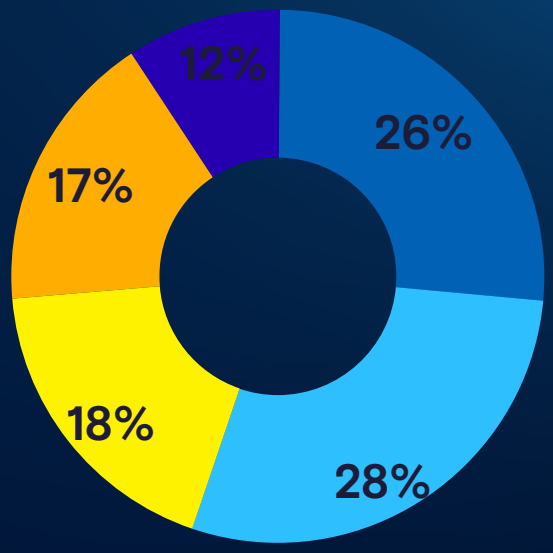
Более 60% компаний сканируют инфраструктуру раз в квартал или реже, что явно недостаточно с учетом динамики появления новых уязвимостей. Например, по данным vulners.com, за последний месяц было обнаружено 350 эксплойтов. Из них 11 получили оценку выше 7 баллов по международной системе CVSS, и их признали критически опасными. А за период с 10 по 18 августа 2021 года было обнаружено более 104 эксплойтов, из которых 6 признаны критически опасными. Поэтому сканирование необходимо проводить несколько раз в квартал в зависимости от размера, состава, критичности инфраструктуры, частоты вносимых в нее изменений, а также исходя из скорости устранения обнаруженных ранее уязвимостей.

Частота сканирования всей инфраструктуры



При этом анализ критических серверов и АРМ сотрудников проводится чаще. Это говорит о том, что компании понимают, какой удар по их бизнесу могут нанести злоумышленники, если воспользуются найденными уязвимостями. На критических серверах, например, могут храниться корпоративные базы данных и конфиденциальная бизнес-информация. Рабочие хосты также содержат много данных, которые хакеры могут использовать для развития атаки. Например, при проведении пентестов эксперты «Ростелеком-Солар» находят в обычных незащищенных файлах учетные данные от корпоративных ресурсов, а пароли от критических систем в поле «комментарий» в свойствах учетных записей.

Частота сканирования критических серверов и АРМ сотрудников:



Половина опрошенных отмечает, что в период массовых атак-пандемий решение об установке патчей принимается на уровне ИТ-администраторов, так как ситуация «прозрачна для всех». Экстренный патч-менеджмент чаще всего находится в ведении ИТ-администраторов в крупных компаниях. А в организациях среднего размера (от 250 до 5 тыс. человек) подобные решения чаще всего принимает ИТ-руководитель, но при этом сотрудники ИБ-подразделения должны аргументировать ему эту потребность. Первых лиц компании и бизнес-подразделения к принятию решения о необходимости установки патчей в период эпидемий привлекают только в крупных (более 5 тыс. человек) и мелких (менее 250 человек) организациях. В то же время есть организации, где ИТ-службы никак не реагируют на запрос об установке патчей – таких 12% среди всех опрошенных.

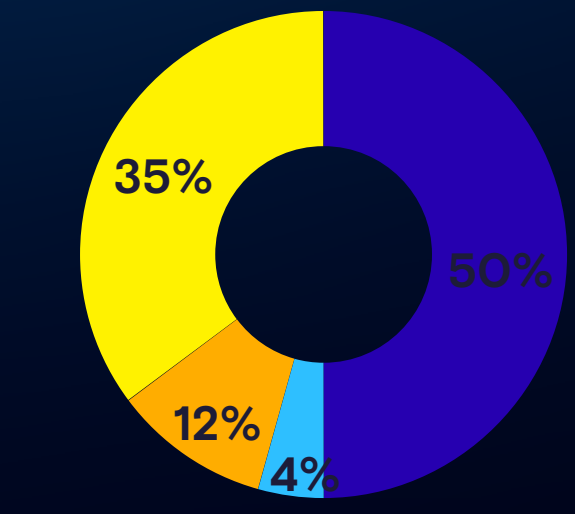
Это указывает на то, что проблема патч-менеджмента связана с несогласованностью в действиях между ИБ-службами и ИТ-администраторами и, как следствие, с некорректной приоритизацией задач. Если ИБ-подразделение не может грамотно обосновать необходимость закрытия критической уязвимости, то ИТ-отдел теряет стимул реализовать такой запрос.

Это приводит к:

- «удлинению» процесса патч-менеджмента за счет дополнительных согласований;
- откладыванию процесса патч-менеджмента в принципе.

По данным «Ростелеком-Солар», среднее время установки обновлений составляет 42 дня – что является «бонусным» временем для злоумышленников на создание эксплойта или проектирование и совершение атаки на конкретную компанию

Кто принимает решение об экстренной установке патчей



- ИТ-администраторы
- Бизнес и первые лица
- Реакции от ИТ-службы не наступает
- ИТ-руководитель

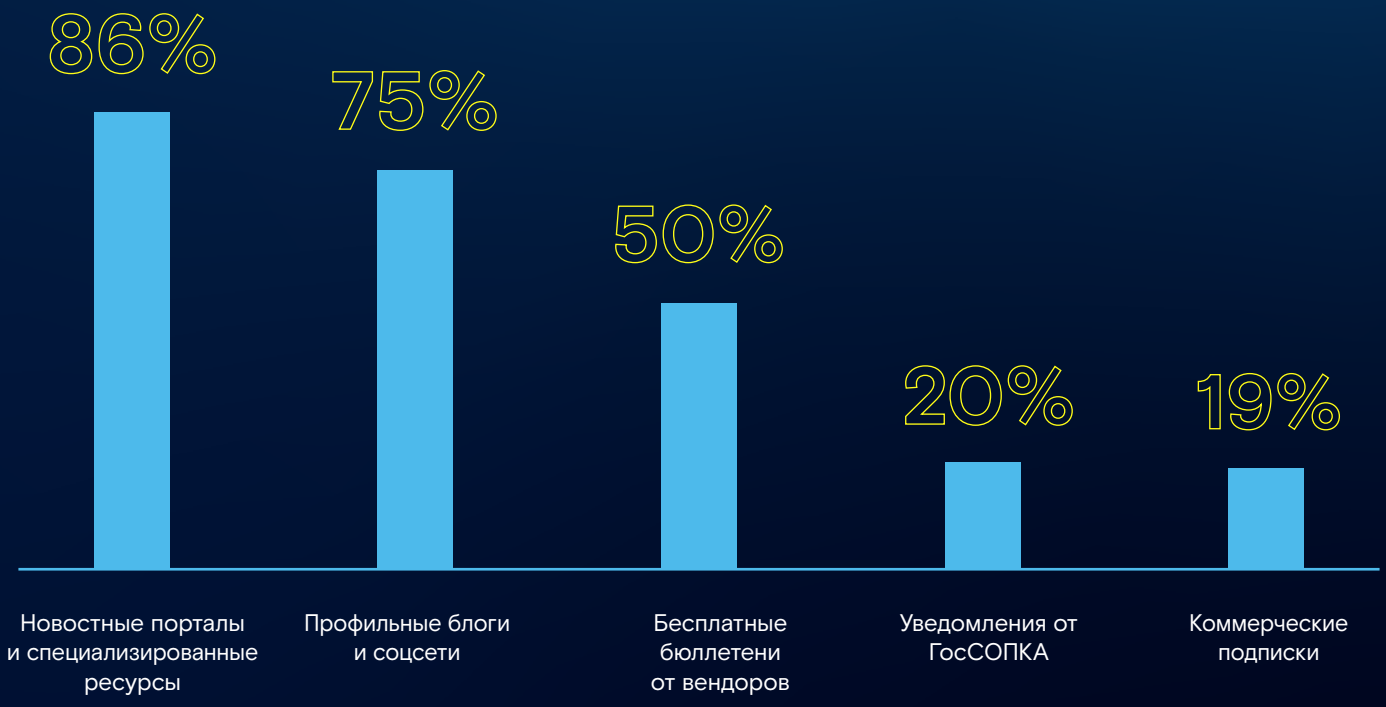
Помимо закрытия уязвимостей, процесс сканирования, в основе которого лежат современные инструменты, позволяет провести инвентаризацию цифровых активов. Современные реалии потребовали от компаний массовой цифровизации, и многие привлекли для этого внешних подрядчиков. Единая точка входа для подобных организаций в инфраструктуру заказчика обычно отсутствует, а при завершении контракта учетные записи аутсорсеров с высокими привилегиями часто не удаляются, но при этом остаются без внимания ИБ-служб. На этот случай в компании должен быть регламент управления правами доступа. Если такой регламент есть, VM поможет проконтролировать его выполнение, если его нет – обнаружить «дыры» в инфраструктуре.

Также регулярная инвентаризация требуется компаниям с разветвленной филиальной сетью, особенно если в каждом подразделении действуют собственные политики безопасности и нет единого ИБ-регламента. Это также актуально для организаций, где часто меняется ИТ-оборудование (например, в случае работы с большим количеством подрядчиков). В этих случаях из-за нерегулярности процесса VM открытые точки в инфраструктуре становятся легкой мишенью для злоумышленников.

Откуда еще получают информацию

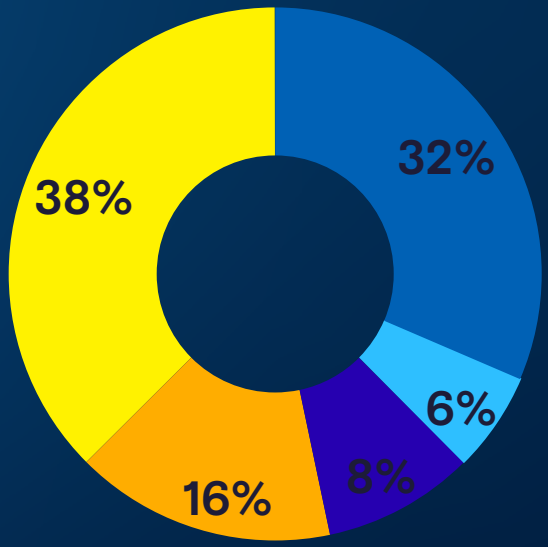
В процессе выявления уязвимостей компании не ограничиваются только сканированием инфраструктуры. В качестве источников информации о новых ИБ-угрозах респонденты чаще всего используют новостные порталы, специализированные ресурсы, профессиональные блоги и сообщества в соцсетях, а также бесплатные бюллетени от вендоров.

Способы отслеживания информации об уязвимостях



Чуть больше трети компаний уверены, что помимо сканирования инфраструктуры для поиска и закрытия уязвимостей необходимо проводить тестирования на проникновения (пентесты). При этом почти столько же респондентов уверены, что сканера для этих целей вполне достаточно. Однако сканирование и пентест не исключают, а дополняют друг друга.

Сканирование уязвимостей – это автоматизированный процесс поиска технических неисправностей и ошибок (из базы CVE), а также инвентаризация активов. Пентест же выявляет не только технические, но и логические уязвимости, показывая, как выглядит инфраструктура компании для злоумышленника, где и как он – потенциально – может проникнуть в критические системы или во внутреннюю сеть. Кроме этого, такая наглядность помогает ИБ-специалистам продемонстрировать потребность в регулярном сканировании и обосновать необходимость установки патчей.



- Пентест нужен
- Пентест не нужен
- Пентест нужен для веба
- Пентест нужен для внутренней инфраструктуры
- Пентест нужен для внешней инфраструктуры

Выводы

Как видно из исследования, текущий уровень зрелости построения ИБ-процессов во многих организациях находится в начальной стадии. Типичной картиной для них является:

- нерегулярное сканирование и как итог – пропуски слабых мест на ИТ-периметре;
- отсутствие регулярной инвентаризации, что приводит к появлению в компаниях shadow IT, то есть инфраструктуры, про которую могут даже не знать сотрудники ИТ- и ИБ-подразделений, но которая при этом может использоваться хакерами для совершения атаки;
- несогласованность между ИТ- и ИБ-службами приводит к тому, что вокруг обновления ПО и оборудования не выстроен процесс, регламенты, KPI и SLA. И следствием этого становится несвоевременное закрытие уязвимостей.

Рекомендации

Чтобы процесс закрытия уязвимостей был более эффективным, необходимо:

Не забывать, что первым этапом построения надежной киберзащиты является инвентаризация активов. Пропуск данного этапа значительно снижает эффективность последующих шагов.

Отслеживать новые уязвимости и искать информацию о них в разных источниках (от новостных порталов до вендорских рассылок).

Перейти от разового сканирования к регулярному и проводить его как минимум раз в квартал. Однако сегодня динамика появления новых уязвимостей указывает на то, что для некоторых организаций этой периодичности уже недостаточно и им требуется более частое сканирование.

Передать рутинную работу по анализу и обработке результатов сканирования на аутсорсинг, чтобы разгрузить ИБ-службу.

Ростелеком
Солар

rt.ru
rt-solar.ru

info@rt-solar.ru
+7 (499) 755-07-70

Задать вопрос или
попробовать сервис

solar@rt-solar.ru