

Как выстроен процесс управления уязвимостями в российских компаниях

Мы провели анонимный опрос среди специалистов по ИБ. Цель — узнать, как организовано управление уязвимостями в компаниях в России, какие проблемы волнуют специалистов по ИБ и с какими ограничениями средств анализа защищенности они сталкиваются. Эта информация нужна нам как производителю средств класса vulnerability management, чтобы составить рекомендации для специалистов по ИБ — на что обратить внимание при построении эффективного процесса управления уязвимостями.

Опрос проводился с 21 сентября по 11 октября 2020 года. Мы разместили его на официальном сайте Positive Technologies, интернет-порталах, посвященных ИБ, в социальных сетях, тематических чатах и каналах в Телеграме. Мы получили 154 заполненных анкеты.

Ключевые результаты

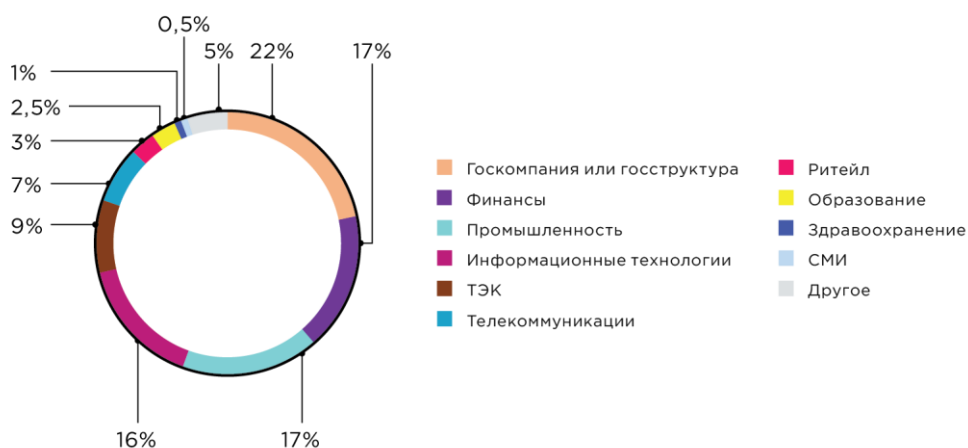
- У половины опрошенных больше всего времени уходит на то, чтобы убедить IT-отдел в необходимости установить обновления; 11% респондентов рассказали, что им приходится обосновывать устранение каждой уязвимости. Такой подход чреват тем, что при разрастании IT-инфраструктуры у специалистов просто не останется времени на обработку уязвимостей.
- 9% специалистов направляют отчет о выявленных уязвимостях напрямую IT-специалистам без предварительной фильтрации и приоритизации задач на устранение. В этом случае велика опасность, что, перерабатывая огромный список уязвимостей, IT-специалисты не дойдут до обработки действительно опасных уязвимостей.
- 11% респондентов не проверяют, устранил ли IT-отдел обнаруженные уязвимости. Это говорит о том, что у компаний отсутствует важный этап процесса vulnerability management — контроль уровня защищенности.
- Опрос показал, что не все знакомы с патч-менеджментом. Каждый десятый опрошенный ответил, что в его компании критически опасные уязвимости на важных активах не устраняются более полугода.
- Четверть респондентов не используют в своих компаниях специализированное ПО для выявления уязвимостей. Получается, специалистам по ИБ необходимо проверять каждый компонент информационной системы вручную, что долго и малоэффективно.

Профиль респондентов

Отрасль

В опросе участвовали в основном специалисты по ИБ из госсектора, кредитно-финансовых организаций, промышленных и IT-компаний.

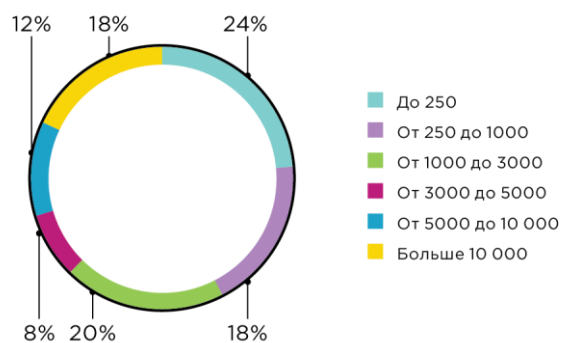
Какой сектор экономики представляет ваша организация?



Размер компании

Среди опрошиваемых были представители малого бизнеса (до 250 работников) — 24%, среднего (от 250 до 3000 сотрудников) — 38%, крупного (от 3000 сотрудников) — 38%.

Сколько сотрудников работает в вашей компании?



Как организован процесс управления уязвимостями

Трудозатраты специалистов по ИБ



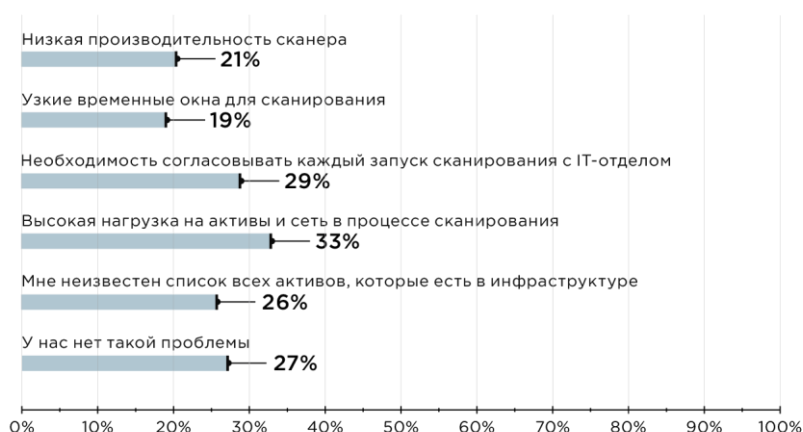
Участники опроса отметили: больше всего времени у них уходит на то, чтобы убедить IT-отдел в необходимости закрыть уязвимости (48%), и на анализ результатов сканирования (43%). Также к трудоемким задачам 31% специалистов отнесли проверку устранения уязвимостей. Указанные трудности характерны как для больших, так и для маленьких компаний. Однако прослеживается тенденция: чем больше компания, тем труднее специалистам по ИБ договориться с IT-отделом. Если для представителей малого бизнеса наиболее трудоемкий процесс — анализ результатов сканирования (50%), то для представителей среднего и крупного бизнеса это согласование установки патчей (55% и 56% соответственно).

Сканирование инфраструктуры

Для поддержки защищенности инфраструктуры важно иметь актуальные данные о составе сети (оборудовании, ПО, доступных сервисах) и об обнаруженных в ней уязвимостях. Но, как оказалось, не всегда возможно ежедневно проводить полное сканирование всей IT-инфраструктуры. Среди причин участники опроса назвали следующие: 33% респондентов жалуются на возрастающую нагрузку на сеть и на активы при сканировании; 26% ответивших неизвестен весь список активов в их инфраструктуре, что ставит под сомнение достоверность оценки защищенности; а 29% специалистов не могут регулярно сканировать IT-инфраструктуру из-за необходимости постоянно согласовывать эти работы с IT-отделом.

Представители госкомпаний (36%), финансовой отрасли (32%) и IT-сектора (42%) назвали помехой высокую нагрузку на сеть, представителей промышленности (40%) главным образом волнует необходимость согласовывать каждое сканирование с IT-отделом. Треть респондентов из финансовой сферы (32%) отметили, что у них нет проблем с регулярным сканированием инфраструктуры.

Что мешает вам регулярно сканировать полностью всю IT-инфраструктуру?



Контролировать полноту собираемых данных об инфраструктуре можно не только за счет полного сканирования. Хорошо, если это можно сделать, среди прочего, за счет выборочного сканирования IT-активов, а также за счет импорта данных об активах из внешних каталогов или из других средств защиты (данных анализа событий в SIEM-системах и анализа трафика в NTA-системах).

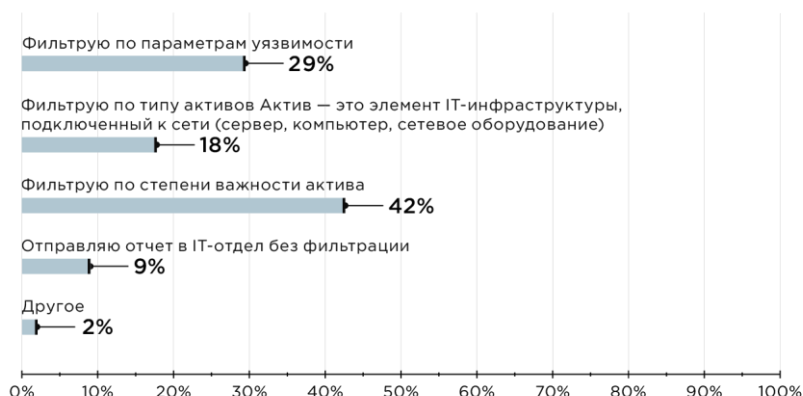
Фильтрация уязвимостей

По итогам сканирования специалисты, как правило, получают огромный список уязвимостей. На этом этапе важно определить, какие уязвимости необходимо устранить в первую очередь.

Меньше половины опрошенных специалистов по ИБ наладили процесс фильтрации выявленных уязвимостей по степени важности активов, на которых они были обнаружены. Это возможно, если при инвентаризации они также классифицировали активы по степени их влияния на работоспособность важных для бизнеса сервисов. Такой подход позволяет фокусироваться на устранении действительно опасных для бизнеса уязвимостей. Фильтрацию по степени важности активов поддерживают 63% опрошенных из госкомпаний и 42% из IT-сферы, по другим отраслям процент ниже.

Девять процентов специалистов по ИБ направляют отчет о выявленных уязвимостях напрямую IT-специалистам без предварительной фильтрации и приоритизации задач на устранение. Такой подход несет в себе много рисков: IT-отдел не будет справляться с устранением всех обнаруженных уязвимостей, поэтому есть риск пропустить наиболее опасные. Впоследствии это может привести к тому, что без контроля со стороны специалистов по ИБ сотрудники IT-отдела вовсе не будет уделять внимания вопросам безопасности.

Как вы реагируете на обнаруженные уязвимости?



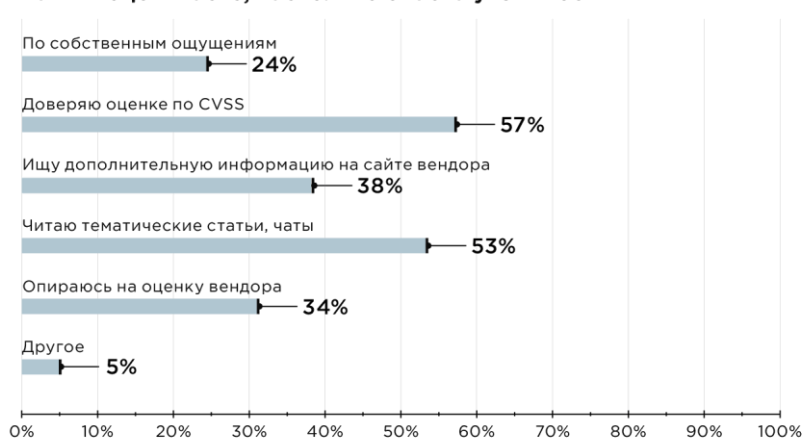
Оценка уязвимостей

Чтобы корректно оценить уровень опасности уязвимости, специалисту по ИБ недостаточно ориентироваться на собственный опыт, на тип уязвимости и на оценку по [CVSS](#). Нужно еще соотносить шкалу оценок со своей инфраструктурой и оценивать возможность эксплуатации данной уязвимости в конкретной системе.

Более половины респондентов для оценки уязвимостей пользуются системой CVSS и ищут информацию о новых уязвимостях на тематических ресурсах. Самостоятельная оценка опасности уязвимостей часто требует дополнительных ресурсов для управления уязвимостями: 43% респондентов подтвердили, что больше всего времени уходит именно на анализ результатов сканирования.

Оценке вендора доверяют 34% опрошенных. Однако несмотря на то, что в таких оценках найденные уязвимости ранжированы по степени опасности, они не дают понимания, сколько уязвимостей в сети организации нужно устранить, чтобы обеспечить достаточный уровень защищенности. Лучше, если вендор на основе своей экспертизы сможет предоставить ограниченный список самых актуальных и опасных уязвимостей, которые достаточно будет устранить, чтобы затруднить злоумышленнику проникновение в сеть.

Как вы оцениваете, насколько опасна уязвимость?



Договоренности с IT-отделом

За устранение уязвимостей (обновление версий ПО, установку патчей) и применение компенсационных мер (выключение сервисов, закрытие портов на межсетевых экранах) отвечает, как правило, IT-подразделение. Одиннадцать процентов респондентов сталкиваются с тем, что им приходится обосновывать устранение каждой уязвимости для IT-отдела. При этом 75% из тех, кто так ответил, — представители крупного бизнеса (от 1000 сотрудников). В компаниях такого размера большое количество сетевых узлов, а значит, и уязвимостей. Поэтому бюрократический процесс по заведению и обоснованию тикета на каждую уязвимость, скорее всего, съедает много времени у сотрудников отделов ИТ и ИБ.

Также 11% опрошенных не проверяют, были ли устранены выявленные уязвимости. Тем не менее 56% из них проголосовали, что опасные уязвимости на критически важных активах устраняются в их компании быстрее чем за неделю. Мы искренне надеемся, что указанные сроки соответствуют действительности, но все же советуем проверять устранение уязвимостей самостоятельно.

Больше половины респондентов проверяют устранение уязвимостей при очередном сканировании системы. Здесь важно, чтобы сканирующие системы оперировали не IP-адресами, а IT-активами. IP-адреса могут меняться от сканирования к сканированию, поэтому соотносить результаты двух отчетов будет непросто. Если приходится задавать список IP-адресов, то отчеты о сканировании

могут быть неполными (без учета новых узлов, появившихся между двумя сканированиями). Более эффективно, когда средство управления уязвимостями поддерживает обнаружение и идентификацию активов, в этом случае вы получите полные сведения об узлах и системах в инфраструктуре компании.

Зачастую в дифференциальных отчетах, применяемых для сравнения результатов нескольких сканирований, не учитываются принятые компенсационные меры. Каждый десятый из опрошенных (11%) отметил, что ему случалось забывать о принятых компенсационных мерах из-за того, что уязвимости «маячили» в отчете.

Проводить ручную проверку устранения уязвимостей эффективно, если их количество невелико. Но при расширении инфраструктуры и, соответственно, увеличении количества выявляемых уязвимостей специалисту по ИБ уже нужно автоматизировать процесс их обработки. Решать эту задачу лучше всего так: для опасных уязвимостей (в первую очередь — критически опасных уязвимостей на важных активах) необходимо создавать тикеты для IT-отдела и контролировать их выполнение в экстренном порядке. Для остальной массы уязвимостей необходимо согласовать с IT-отделом и контролировать регулярное обновление ОС и ПО. Подобный процесс поддерживают 25% респондентов.

Как вы договариваетесь с IT-отделом об устранении уязвимостей?



Скорость устранения уязвимостей

При работе с уязвимостями также важна скорость их устранения, особенно если это касается значимых активов компании. Только 39% опрошенных удается устранить критически опасные уязвимости на приоритетных для компании активах в течение первых двух дней; 9% не закрывают такие уязвимости в течение полугода.



Рассмотрим зависимость скорости устранения уязвимостей от размеров компании. В маленьких компаниях (до 250 сотрудников) критически опасные уязвимости на важных активах успевают устранять за два дня 47% респондентов и только 6% — за полгода. Критически опасные уязвимости на всех активах в основном успевают устранять за неделю (44%), а остальные уязвимости — за месяц (42%).

В средних по размеру компаниях (от 250 до 3000 сотрудников) важные активы успевают защитить за два дня 45% опрошенных — и уже 9% могут не закрывать уязвимости по полгода. Критически опасные уязвимости на обычных активах устраняют за месяц (40%), а остальные уязвимости — за полгода (38%).

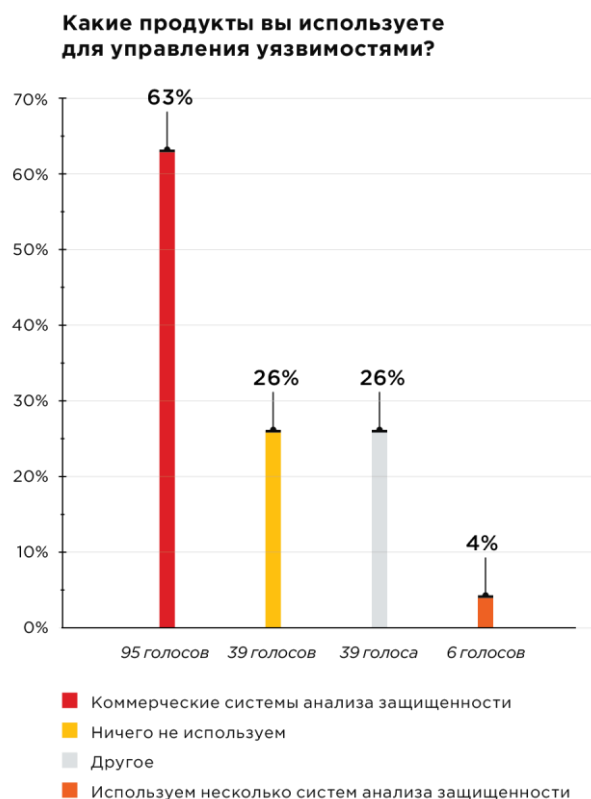
В больших компаниях (от 3000 сотрудников) критически опасные уязвимости на важных активах устраняются за неделю у 40% опрошенных и только у 26% за день-два. Уязвимости на обычных активах устраняются в основном (37%) за месяц, а менее опасные уязвимости патчат за полгода (44%) или за месяц (38%).

Опыт показывает, что компании затягивают с обновлениями, в то время как злоумышленники действуют быстро и адаптируют новейшие эксплойты для своих атак иногда [в течение суток](#).

Инструментарий специалиста по ИБ

На помощь безопаснику в борьбе с уязвимостями приходят средства анализа защищенности — специальные системы, которые в автоматизированном режиме выявляют открытые сетевые порты и доступные службы, уязвимости в ПО, а также недостатки конфигурации оборудования, серверов и средств защиты. Ими пользуются 63% опрошенных.

Многие специалисты (26%), отвечая на вопрос о продуктах, которые они используют для управления уязвимостями, назвали некоммерческие утилиты для сканирования сети. У подобных инструментов есть свои преимущества, но считаем важным подчеркнуть: они позволяют решить задачи сканирования портов и служб, но не дают информации о составе и состоянии активов, об уязвимостях ПО, приложений, баз данных, а также не выявляют ошибки конфигураций. Для полноценного процесса управления уязвимостями их будет недостаточно. Четыре процента респондентов указали, что используют сразу несколько систем анализа защищенности.



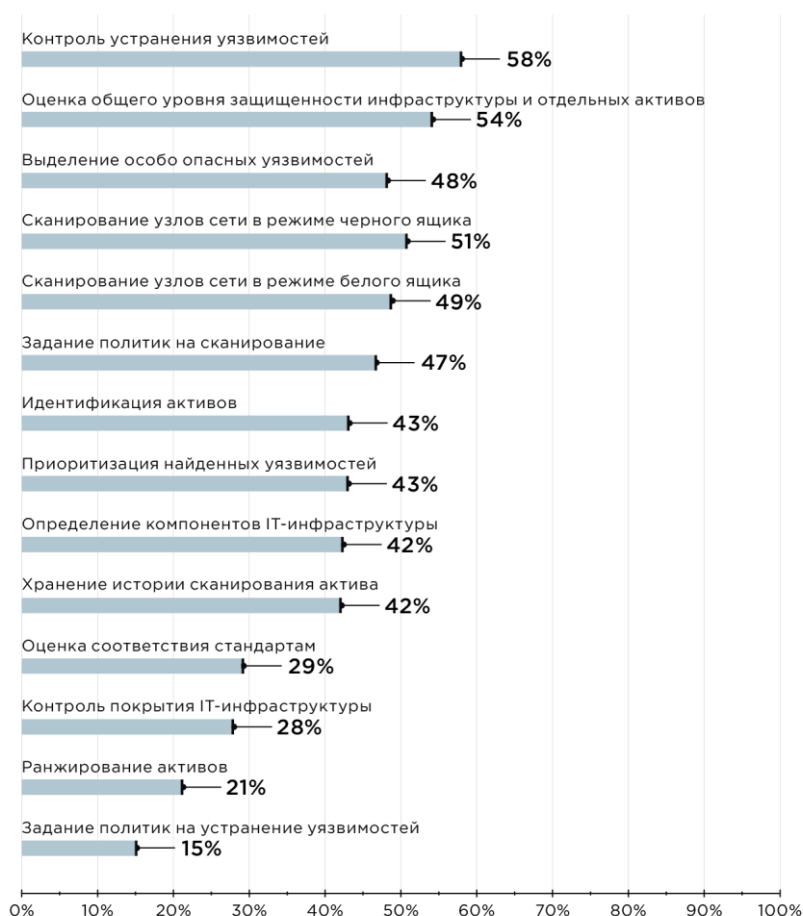
Четверть респондентов не используют специализированное ПО для выявления уязвимостей. Среди них в основном представители малого (35%) и среднего (38%) бизнеса. Получается, в таких компаниях специалистам по ИБ приходится проверять каждый компонент информационной системы вручную, что долго и малоэффективно.

Также мы попросили участников опроса отметить пять самых популярных задач, которые они выполняют с помощью систем анализа защищенности. Среди них оказались:

- контроль устранения уязвимостей (58%);
- оценка общего уровня защищенности (54%);
- сканирование узлов сети в режиме черного ящика (51%);
- сканирование узлов сети в режиме белого ящика (49%);
- выделение особо опасных уязвимостей (48%).

Все предложенные нами варианты задач оказались востребованы: как минимум каждый третий выполняет их с помощью систем анализа защищенности. Самым непопулярным вариантом оказалось задание политик на устранение уязвимостей: его выполняют только 15% респондентов.

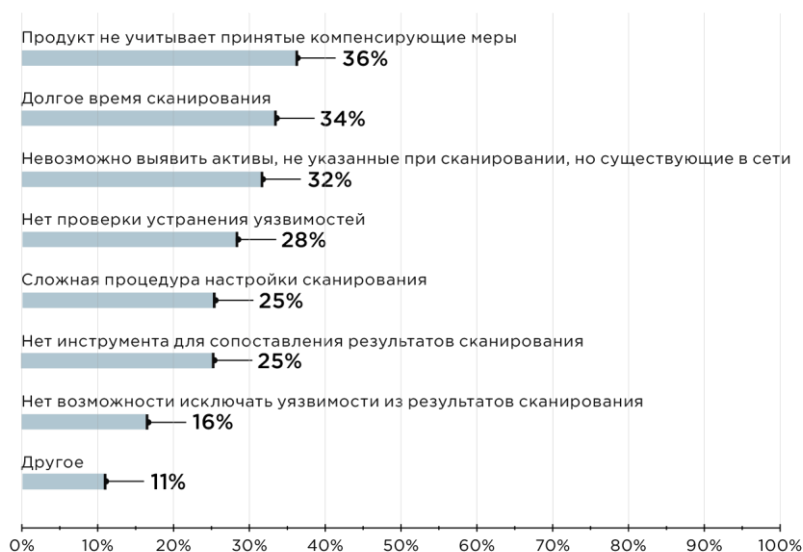
Что из перечисленного вы делаете с помощью вашего текущего инструментария?



Больше всего нам как вендору было интересно узнать, какие улучшения в системах управления уязвимостями необходимы пользователю. Более трети специалистов по ИБ (36%) хотят иметь возможность учитывать компенсирующие меры. Примерно столько же опрошенных (34%) жалуются на долгое время сканирования. По мнению 32% респондентов, в используемых продуктах для vulnerability management не хватает возможности выявлять активы, не указанные при сканировании, но существующие в сети. Двадцать восемь процентов специалистов отметили, что им поможет функция проверки устранения уязвимостей.

Остальные варианты тоже оказались востребованы.

Что вас больше всего раздражает в используемых вами продуктах для vulnerability management?



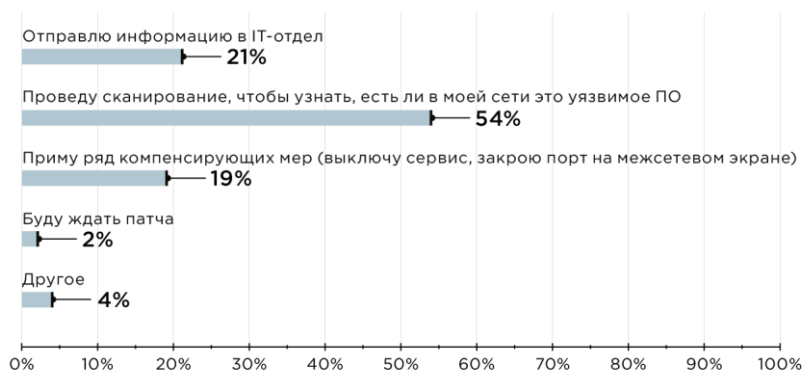
Компании до 250 сотрудников утомляют долгое время сканирования (36%) и сложная настройка (30%). Компании от 250 до 3000 сотрудников хотят учитывать компенсирующие меры (40%), а также проверять устранение уязвимостей (34%). Крупные компании от 3000 сотрудников интересует сопоставление результатов сканирования (33%) и также учет компенсирующих мер (35%).

Кроме того, респонденты жаловались на плохую приоритизацию уязвимостей и необходимость выявлять некоторые данные вручную, например дату последнего успешного сканирования актива.

Экстренная проверка

Выстроенный процесс управления уязвимостями должен быть эффективным как в штатном режиме, так и при проведении экстренной проверки. Мы предложили респондентам представить, что они будут делать в первую очередь, если узнают о новой серьезной уязвимости в ПО. Половине опрошенных понадобится провести дополнительное сканирование, чтобы узнать о существовании в сети уязвимого ПО, 19% смогут сразу принять меры по защите компании.

Представьте, что вы узнали о новой серьезной уязвимости в ПО. Что будете делать в первую очередь?



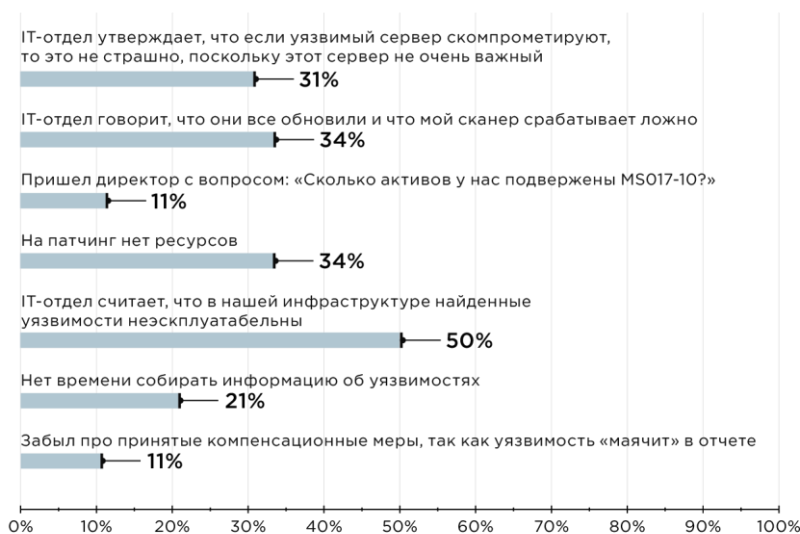
Классические сканеры решают, есть ли на узле уязвимость, непосредственно в момент сканирования. Соответственно, когда появится новая уязвимость, необходимо заново просканировать все активы. Учитывая сложный процесс согласования полноценного сканирования

во многих компаниях, оперативно узнать, опасна ли новая уязвимость для инфраструктуры, будет затруднительно. Эффективнее, если система управления уязвимостями сохраняет информацию о просканированных активах и может высчитывать применимость новой уязвимости к сети автоматически на основании прошлого сканирования.

Итоги

По итогам опроса мы пришли к выводу, что одна из самых больших проблем для специалистов по ИБ — достичь взаимопонимания с IT-отделом. В процессе управления уязвимостями больше всего времени уходит на разбор результатов сканирования и попытки убедить IT-специалистов в необходимости установить обновления (48%).

С чем из перечисленного вы сталкивались за последний год?



Половина из опрошенных сталкивалась с тем, что IT-отдел считал найденные в инфраструктуре уязвимости неэксплуатируемыми, поэтому не видел смысла тратить время на их устранение.

Также часто (больше 30% голосов) IT-специалисты прибегают к следующим аргументам:

- «На патчинг нет ресурсов»;
- «Если уязвимый сервер скомпрометируют, то это не страшно, поскольку он не очень важный»;
- «Мы все обновили, это сканер срабатывает ложно».

Вечные споры между отделами ИТ и ИБ могут сказаться на безопасности компании. Нельзя допустить, чтобы процесс управления уязвимостями в компании зависел от способности сотрудников договариваться между собой.

Чтобы взаимодействие отделов ИТ и ИБ было продуктивным, необходимо вводить правила обработки уязвимостей. Мы рекомендуем для уязвимостей среднего и низкого уровня риска вне критически важных активов фиксировать определенный срок устранения. Необходимое время компания определяет сама: каждую неделю, раз в месяц или в два — но срок нужно установить и он должен соблюдаться. Нарушение данной политики будет сигнализировать о том, что в процессе что-то пошло не так.

IT-подразделение будет регулярно устанавливать патчи или обновления ОС и ПО на основе заданных политик, не дожидаясь информации об уязвимостях от службы ИБ. Тогда специалистам по ИБ останется лишь контролировать отсутствие уязвимостей через определенное количество дней после публикации информации о них. При таких договоренностях у специалиста по ИБ появится время на ручную обработку действительно опасных уязвимостей на важных активах.

Наш опрос показал, что кроме самого выявления уязвимостей в процессе vulnerability management многое все еще вызывает трудности у специалистов по ИБ. Тысячи наших клиентов тоже сталкивались с проблемами, описанными в статье, поэтому мы решили взглянуть по-новому на управление уязвимостями. Мы запускаем новый продукт, который будет помогать выстраивать процессы в компании, охватывать всю инфраструктуру, включать регламенты по сканированию и устранению уязвимостей и контролировать общий уровень защищенности компании.

Приглашаем вас на предпоказ системы управления уязвимостями нового поколения MaxPatrol VM. Презентация пройдет в рамках глобальной конференции и кибербитвы The Standoff, 16 ноября 2020 года в 13:00. Мы расскажем, как грамотно выстроить процесс управления уязвимостями в компании и продемонстрируем отличия MaxPatrol VM от систем анализа защищенности. Чтобы присоединиться к мероприятию, необходимо [зарегистрироваться](#).