НАШИ ЭКСПЕРТЫ

Андрей Владимиров

Глава по безопасности и соучредитель компании Arhont Ltd (www.arhont.com)

Алексей Лукацкий

Бизнес-консультант по безопасности компании Cisco Systems (www.cisco.com)

Михаил Башлыков

Руководитель направления информационной безопасности компании КРОК (www.croc.ru)

СПЕЦ:

Кто-то полагает, что для создания системы сетевой безопасности достаточно один раз грамотно установить и настроить программное и аппаратное обеспечение. Другие эксперты считают, что обеспечение безопасности сети — это непрерывный циклический процесс. А что вы думаете об этом?

Андрей Владимиров: Первая точка зрения исходит от производителей соответствующего программного и аппаратного обеспечения. Оно и понятно: им нужно повысить продажи своего продукта во что бы то ни стало и «под любым соусом». Однако далеко не всегда то, что выгодно вендору, в той же степени выгодно его клиентам.

Вторая точка зрения более характерна для независимых консультантов по безопасности и ближе к истине. По крайней мере, она принимает во внимание большее количество факторов, которые могут повлиять на информационную безопасность компании и ее сетей. Такие факторы включают в себя социальную инженерию, физическое проникновение, латеральные каналы утечки информации («болтун — находка для шпиона», а потерянный ноутбук или выброшенный в мусорный бак винчестер с восстанавливаемыми конфиденциальными данными могут оказаться хуже любого болтуна), обучение пользователей и системных администраторов, их ответственность и лояльность, юридические и финансовые аспекты ИТ безопасности, эффективную организацию расследования инцидентов и т. п.

Да и одномоментно установить и настроить технические средства безопасности на все случаи жизни тоже никак не получится — современные корпоративные сети динамичны, подчиняются ситуационным требованиям бизнеса, часто растут в размерах, инкорпорируют в себя новые технологии. Кроме того, подходы, методы и средства взлома не стоят на месте, и то, что считалось абсолютно безопасным вчера, сегодня может стать крупным фактором риска. У нас бывали случаи, когда сеть, бывшая высокозащищенной

при проведении аудита безопасности, оценивалась как слабозащищенная при аналогичной проверке через полгода.
Все вышесказанное, безусловно, ни в коем случае не уменьшает важности тщательно выбранных мощных технических средств защиты, их правильной настройки и отладки. Это как с армией: в идеале она должна быть вооружена по последнему слову техники с регулярными ее проверками и переоснащением. Однако помимо вооружения и умения им пользоваться должны быть еще организация, устав, дисциплина и различные меры ее поддержания, эффективное взаимодействие между частями, тактические и стратегические планы и наработки для различных штатных и критических ситуаций, своевременное снабжение и т. д.

Алексей Лукацкий: Тех, кто считает, что можно обойтись железом и софтом, экспертами назвать сложно. Достаточно только вспомнить, что обновление антивирусных решений и систем обнаружения атак надо производить постоянно, и сразу все встанет на свои места. Мы поймем, что поставить программное и аппаратное обеспечение и забыть про него — невозможно. Но и это не конец. Средства защиты надо правильно внедрить, правильно настроить и правильно эксплуатировать. Когда мы выбираем машину, мы не останавливаемся на ее покупке, которой предшествует мучительный процесс выбора. Мы регулярно проходим техосмотр, покупаем запчасти, посещаем мойку и, наконец, просто занимаемся вождением. Также и с безопасностью. К сожалению, немногие понимают это. Отсюда и все наши проблемы с защитой.
Однако и процессным подходом не стоит излишне увлекаться. Сегодня многие говорят о стандарте управления информационной безопасностью ISO 27001, который весь построен на понятии «процесс». Однако процесс процессом, но не стоит забывать ради чего занимаются безопасностью. Не ради процесса, а ради результата, который должен быть ориентирован на потребности бизнеса.

Михаил Башлыков: Мы живем в такое время, когда все технологии развиваются достаточно быстро. И нельзя забывать, что также эффективно и быстро развиваются различные хакерские программы и решения, предназначенные для нарушения сетевой безопасности. Если на ранних этапах развития сетевых (информационных) технологий было достаточно отдельных программно-аппаратных платформ для борьбы со злоумышленниками, сетевыми угрозами, атаками и вирусами, то теперь этого мало. Создание надежной системы защиты корпоративных сетей невозможно без комплексного решения, которое бы включало в себя такие компоненты, как межсетевые экраны, системы обнаружения и предотвращения вторжений, ПО сетевого оборудования со встроенным функционалом сетевой безопасности, системы управления сетевой безопасностью, системы анализа, мониторинга сетевой безопасности и прочие компоненты. Но для организации системы информационной безопасности помимо обязательного внедрения комплексного решения надо выстроить систему управления информационной безопасностью, которая бы определяла требования к информационной безопасности с точки зрения процессного подхода, т. е. включала в себя создание, внедрение, мониторинг изменений параметров и политики информационной безопасности.
Для обеспечения сетевой безопасности мало просто настроить корректно сетевое оборудование и полный функционал, обеспечивающий сетевую безопасность. Так как это комплексная задача, то необходимо непрерывно следить за уровнем безопасности в сети, проводить анализ и мониторинг систем защиты и постоянно делать перенастройку оборудования, чтобы гибко адаптироваться к реальным условиям работы. В связи с появлением новых типов сетевых атак, угроз и вирусов приходится регулярно устанавливать обновления на сетевое оборудование. Сетевая инфраструктура — это живая система, для обеспечения безопасности которой требуется точно такое же комплексное «живое» решение. Поэтому задача обеспечения сетевой безопасности является постоянным процессом, для которого можно определить следующие состояния: разработка системы сетевой безопасности -> внедрение и настройка -> эксплуатация -> мониторинг и анализ текущего состояния сетевой безопасности -> тестирование уровня сетевой безопасности –> разработка новых решений по модернизации системы безопасности и далее по циклу.

СПЕЦ:
Безусловно, наибольшая эффективность системы сетевой безопасности достигается в том случае, если ее проектирование осуществляется одновременно с проектированием самой сетевой инфраструктуры. Но как быть, если уже имеется конкретная сетевая инфраструктура?

Андрей Владимиров: В первую очередь необходимо выжать все возможное из функциональности уже имеющейся инфраструктуры. По нашему опыту, огромное количество опций безопасности развернутых сетевых устройств просто не используется по причине незнания о них. Особенно это относится к коммутаторам и защите протоколов канального уровня. Можно оптимизировать логическую архитектуру безопасности сети, не меняя физической, например увеличить число VLAN'ов и перераспределить узлы на них, помня о возможных атаках по пересечению VLAN'ов (VLAN hopping) и принимая меры по их предотвращению. Изменить логическую сегментацию сети в сторону усиления разграничения доступа и потоков данных можно и посредством перенастройки протоколов маршрутизации, скажем, увеличив число зон маршрутизации OSPF и введя дополнительные списки доступа для этого протокола. Многие маршрутизаторы и межсетевые экраны способны поддерживать базовые IDS/IPS-функции, которые очень часто не используются. Безусловно, такая функциональность не так полноценна в сравнении со специализированными IDS/IPS-сенсорами и станциями управления, но все же лучше, чем ничего.
Повысить количество доступных настроек безопасности можно путем обновления версий операционных систем сетевых устройств. Проверьте, существуют ли версии ОС с дополнительными полезными функциями безопасности, которые потянет установленное у вас аппаратное обеспечение. В случае недостатка оперативной или постоянной памяти для поддержания таких систем их всегда можно докупить. Кроме того, часто имеется возможность добавить модуль безопас-

ности там, где нельзя установить отдельное специализированное устройство. Большинство современных промышленных коммутаторов и маршрутизаторов могут быть оснащены дополнительными модулями для скоростной фильтрации трафика, обнаружения и предотвращения вторжений, построения эффективных виртуальных частных сетей.
Рано или поздно сетевую инфраструктуру все равно придется менять — уже с учетом необходимости построения системы ее безопасности. Но в совокупности с другими мерами защиты использование по максимуму того, что под рукой, позволит продержаться до капитальной смены инфраструктуры с гораздо меньшими потерями.

Алексей Лукацкий: В настоящее время этот тезис уже не столь актуален, как раньше. По крайней мере для ряда сетевых вендоров это именно так. Все дело в том, что сегодня у смотрящих вперед производителей сетевое оборудование зачастую уже обладает большим набором защитных функций. Они есть, и их нельзя исключить из оборудования, даже если ими никто не пользуется на начальном этапе. Со временем, когда приходит понимание важности вопросов безопасности, эти функции активируются и они начинают бороться с угрозами и аномалиями.
Но если сеть строится на оборудовании производителей, которые не считают безопасность неотъемлемым свойством сети, то проблема, конечно, возникнет, и эффективность системы защиты будет не такой, какой хотелось бы. Разумеется, можно навесить на сеть программное и аппаратное обеспечение и получить очень высокую эффективность системы безопасности. Однако достигнуто это будет более высокой ценой, чем в случае с интегрированным подходом.
И конечно, надо понимать, что ситуации, когда мы имеем дело с еще не существующей сетью и защитой, сегодня не так уж и часты. Как правило, сеть и система безопасности в том или ином виде уже построены, и перед нами скорее стоит задача не построить все с нуля, а модернизировать тот или иной участок инфраструктуры.

Михаил Башлыков: В этом случае нужно провести обследование сетевой инфраструктуры заказчика на предмет проверки уровня ее системы сетевой безопасности и полный аудит сетевой безопасности. После этого предложить решение по модернизации текущей сетевой инфраструктуры и внедрению системы сетевой безопасности. Все это можно выполнить поэтапно, не нарушая текущий рабочий ритм. Можно начать с обновления ПО на настоящем сетевом оборудовании и внедрения новых систем защиты сети, затем наращивать уровень сетевой безопасности. Такое решение практикуется у большинства наших заказчиков. Изначально они проводят только модернизацию сетевой инфраструктуры, но потом начинают постепенно внедрять другие подсистемы. В частности, систему сетевой безопасности. К примеру, компания КРОК реализовала масштабные проекты по созданию систем мониторинга событий и оценки уровня информационной безопасности в ОСАО «Ингосстрах», ОАО «Уралсвязьинформ» и ОАО «РЖД».

СПЕЦ:

При построении системы обеспечения сетевой безопасности какие программно-аппаратные средства имеет смысл использовать, учитывая необходимую эффективность и функциональность?

Андрей Владимиров: Для большинства компаний и организаций современный межсетевой экран, СПАМ-фильтр и антивирус (желательно как централизованный, так и установленный на всех серверах и рабочих станциях) — это абсолютный минимум. Система журналирования должна быть централизованной, хранение и резервное копирование учетных записей необходимо защитить от любых изменений. Мы также рекомендуем использовать утилиты для борьбы со шпионскими программами (spyware) на рабочих станциях сотрудников. Остальное уже будет зависеть от структуры, функций и задач сети, а также требований и политики безопасности ее владельцев.
Компания, серьезно относящаяся к информационной безопасности, никогда не будет сводить меры защиты исключительно к периметру ее сетей, а также оставлять и периметр, и его «подбрюшье» без постоянного присмотра. Внутренние сегменты сети будут разделены межсетевыми экранами, на каждом сегменте и на всех выходах из корпоративной сети установлены IDS/IPS сенсоры. На критических серверах и даже рабочих станциях имеет смысл поставить локальные программные IPS и даже использовать ролевой доступ (RBAC).
Отдельный и сложный вопрос — предотвращение несанкционированного использования мобильных носителей памяти (обычно USB-флэшек) и подключения беспроводных устройств, включая устройства Bluetooth. Существуют технические решения, позволяющие централизованно обнаруживать и автоматически блокировать подключение несанкционированных устройств к USB- и сериальным портам, но эти решения недешевы. Что же касается беспроводной безопасности, ряд крупных корпораций, с которыми приходилось работать, не имеют беспроводных сетей и полностью запрещают их использование. Но при этом у них развернута беспроводная IDS — чтобы было неповадно нарушать запрет.
Остается перечислить специфические средства, которые, однако, получают все более широкое распространение:
– VPN-концентраторы/клиенты + двухфакторная система аутентификации для удаленных отделов и работников. В настоящее время системы двухфакторной аутентификации, использующие мобильные телефоны и SMS-сервис, начали появляться на рынке и даже теснить более традиционные токены, вследствие удобства использования и администрирования таких систем;
– межсетевые экраны 7-го уровня (application layer firewalls) для защиты корпоративных сайтов с динамическим содержанием и критическими для бизнеса веб-приложениями;
– анти-DDoS шлюзы, используемые в случаях, когда доступность сетевых ресурсов является критической (сетевые аукционы, онлайновые казино, правительственные сайты).

Алексей Лукацкий: Есть заезженная, но по-прежнему верная фраза о необходимости анализа рисков, по результатам которого составляется «дорожная карта» угроз и других проблемных мест. И только потом выбираются конкретные типы средств защиты, способные предотвратить идентифицированные риски. Может оказаться так, что нам достаточно будет антивируса и системы предотвращения атак, а функции межсетевого экрана можно будет возложить на маршрутизатор. А в другом случае этого джентльменского набора будет явно мало и нам придется потратиться на систему отражения DDoS-атак, межсетевой экран прикладного уровня, систему контроля поведения пользователей, систему защиты компьютеров пользователей и т. п.

щиты компьютеров пользователей и т. п.

Михаил Башлыков: В наше время использование отдельного программно-аппаратного решения не позволит построить эффективную систему безопасности. Сегодня требуется комплексное решение. А также требуются грамотные специалисты, способные корректно настраивать оборудование, анализировать, проводить мониторинг уровня защиты и разумную модернизацию системы сетевой безопасности.

СПЕЦ:

Такие угрозы, как кража конфиденциальной информации сотрудниками, несанкционированные действия администраторов или использование рабочего времени в личных целях предотвратить одними техническими средствами практически невозможно. Как бороться с ними?

Андрей Владимиров: Кое-что технически сделать все же можно: тщательное фильтрование трафика, используя списки запрещенных к посещению ресурсов и приложений, четкое разграничение привилегий доступа к информации, сопряженное с ее криптографической защитой, отлаженная система мониторинга сети и (физически) серверных помещений, системы защищенного документооборота, исключающие фальсификацию документов и т. д. Но на первом месте, безусловно, должна стоять грамотная политика обеспечения информационной безопасности, подписанная перед тем, как приступить к своим рабочим обязанностям, всеми сотрудниками и контрактором компании без исключения. И разумеется, требуются отлаженные механизмы административного контроля за беспрекословным соблюдением этой политики, с показательными порками злостных нарушителей, вплоть до увольнения и заведения уголовных дел. Только помните, что усердно пользуясь кнутом, не следует забывать и о пряниках.

Алексей Лукацкий: Что касается использования рабочего времени в личных целях, то проблема существует, но во многом она раздута производителями средств борьбы с этой «напастью». Детальный анализ может показать, что стоимость борьбы с этой проблемой оказывается гораздо выше, чем ущерб от нее. **it**