Опрос экспертов

НАШИ ЭКСПЕРТЫ

Крис Касперски

Автор многочисленных статей и ряда книг, программист

ЗАРАЗА

Руководитель службы поддержки пользователей довольно крупного ISP

Антон Карпов

IT-специалист в области информационной безопасности

Константин Гавриленко

Консультант по безопасности и по совместительству директор компании Архонт (www.arhont.com)

СПЕЦ: Как сделать корпоративную сеть безопасной?

Игорь Антонов: Для повышения безопасности сети нужно:

1. Правильно подобрать программное обеспечение для серверов. Особое внимание нужно уделить выбору софта для интернет-шлюзов, так как именно они будут подвергаться атакам в первую очередь.
2. Следить за новостями. Оперативно узнав о найденных ошибках, можно их устранить и не беспокоиться, что ими воспользуются злоумышленники.
3. Постоянно мониторить работу сервера. Просмотр лог-файлов и журналов снижает вероятность, что в вашей сети завелся большой брат.
4. Настроить систему резервирования данных. Если злоумышленник все же получит доступ к вашей сети и сможет уничтожить все данные на серверах, то у вас будут резервные копии.
5. Разграничивать права доступа пользователей. У каждого пользователя должны быть только те права, которые ему реально необходимы для работы. Лишнего быть не должно.
6. Периодически менять пароли всем пользователям. Тогда даже если пароль пользователя станет известен третьим лицам, долго они им пользоваться не смогут.
7. Деактивировать устаревшие учетные записи. Эта проблема большинства администраторов. Сотрудник уволился, а его учетная запись еще долго остается активной. В результате, он может воспользоваться ей и нанести ущерб компании.
8. Планирование стратегии восстановления работоспособности сети после взлома. Если взлом все же произошел, то нужно спланировать заранее, как быстрее всего восстановить работоспособность предприятия.
9. Нанять дополнительных администраторов. Поскольку большинство взломов совершается ночью, то не лишним будет иметь в штате «ночного администратора», который, увидев попытку взлома, сразу сможет принять необходимые меры.

Крис Касперски: Вписать «безопасность» в графу расходов и нанять лучших специалистов из имеющихся, а для подтверждения их компетентности периодически устраивать проверки в виде «тестов на проникновение», включающих в себя не только непосредственные сетевые атаки, но и социальную инженерию, попытки подкупа сотрудников и т.д. Это, конечно, не гарантирует 100% защищенности, но, по крайней мере, ликвидирует наиболее слабые места в линии обороны.

Денис Колисниченко: Чтобы сеть была безопасной, нужно еще при планировании оной делать поправку на безопасность. Имеется в виду не только выбор оборудования и программного обеспечения, но и разработка политики безопасности. Особое внимание нужно уделить человеческому фактору, четко продумать права доступа каждого пользователя. И все равно стопроцентной гарантии безопасности нет и не будет.

Константин Гавриленко: Отключить электричество! На самом деле, вопрос скорее в том, как сделать корпоративную сеть более безопасной. А это, в свою очередь, подразумевает анализ состояния безопасности на данный момент по нескольким

Денис Колисниченко

Автор книг «Linux-сервер своими руками», «Полное руководство Linux» и других

Валерия Комиссарова

Microsoft Student Partner, эксперт CNews

Антон Палагин

Директор по развитию аутсорсинговой компании Eykon (www.eykontech.com)

Игорь Антонов

Работает в крупной компании программистом и администратором БД

категориям: внутренняя, внешняя, беспроводная и политика безопасности. Нехочется повторять заезженные фразы, поэтому ограничусь советом: «Если есть возможность, обратитесь к специалистам за советом, не старайтесь сделать все сами».

Валерия Комиссарова: Для того чтобы сделать свою сеть безопасной и поддерживать ее в таком состоянии, нужно:

1. Хорошо знать свою сеть: что где находится, что требует наибольшей защиты и какого рода угрозам могут быть подвержены эти ключевые «узлы».
2. Если определены «узлы» и угроза, следующим этапом должно стать определение адекватных мер защиты.
3. Методы защиты выбраны и внедрены. Далее — ежедневный и ежечасный аудит, с максимально быстрой реакцией на возникающие проблемы и периодическим пересмотром при необходимости отдельных элементов функционирующей системы ИБ.

Антон Палагин: Как показывает ассортимент баз данных, продающихся в метро, безопасной сделать корпоративную сеть нереально. Против лома нет приема, и на каждую фишку безопасности злоумышленники всегда могут найти еще более хитроумную лазейку.

ЗАРАЗА: Это вопрос, на который легко ответит любой студент компьютерной специальности и никогда не ответит профессионал. По крайней мере сразу и бесплатно. Универсальных решений не существует, любая сеть индивидуальна и имеет собственные потребности в информационной безопасности. Кроме того, безопасность сети никогда не должна рассматриваться отдельно от информационной безопасности предприятия в целом.

СПЕЦ:
Где баланс между простотой и надежностью?

Антон Карпов: Надежность — следствие простоты. Любая система должна быть настолько простой, насколько это возможно. С повышением сложности и комплексности системы надежность неизбежно уменьшается. Это прописные истины. К сожалению, очень немногие в наши дни используют в своих системах и программных продуктах старый добрый принцип KISS — Keep It Simple, Stupid!

Крис Касперски: Чем проще система, тем меньше шансов у нее сломаться. С другой стороны, отказ предельно простой системы, как правило, фатален, а система с избыточностью способна выдержать даже значительные разрушения, сохраняя работоспособность при выходе из строя одного или нескольких узлов. В полной мере это относится и к безопасности. Если сеть разделена на несколько зон, то атаковать ее намного сложнее, чем если в системе имеется только один брандмауэр, защищающий внешний периметр. С другой стороны, всякий защитный комплекс (брандмауэр, антивирус и т.д.) сам по себе является потенциальным объектом атаки. Чем сложнее система защиты, тем сложнее убедиться, что в ней нет дыр, и тем выше вероятность проникновения хакеров сквозь охраняемый периметр. Поиск баланса — очень сложная задача, не имеющая решений «общего вида» и требующая, чтобы каждый случай рассматривался индивидуально. Популярные решения «из коробки» зарекомендовали себя не самым лучшим

Опрос экспертов

образом, а все потому, что в каждом конкретном случае они оказываются либо недостаточными, либо избыточными.

Денис Колисниченко: Обычно что просто, то и надежно. Если же анализировать, где баланс между комфортом и надежностью, получается следующее. Всем известно, что лестница гораздо надежнее лифта, но лифт более удобен и, чтобы ни говорили о надежности, о пользе для здоровья, все будут пользоваться лифтом. Но как бы ни старались сделать лифт более надежным, все равно будет вероятность его поломки. Так называемый баланс между комфортом и надежностью похож на что-то вроде аутотренинга. Мы убеждаем себя, что наша Windows XP с установленным брандмауэром и антивирусом стала безопасной и надежной. Но все мы знаем, что FreeBSD надежнее и без антивируса.

Валерия Комиссарова: Найти баланс — всегда нелегко. Необходимо понять главное: там, где началась сложность — надежность автоматически снизилась, и наоборот. Сложность и надежность/безопасность — взаимоисключающие понятия.

Антон Палагин: Видимо, это хорошо настроенный межсетевой экран и пользовательские политики безопасности внутри сети.

ЗАРАЗА: А зачем искать баланс между простотой и надежностью? Простота — это и есть надежность. Чем проще, понятней и прозрачней система защиты — тем она более надежна и менее уязвима, в ней меньше различного рода «лазеек». Именно поэтому защиту сети и защиту информационного пространства в целом никогда не следует начинать с закупки сложных устройств. Надо ее начинать с разработки простых принципов.

СПЕЦ:
Достаточно ли защиты по периметру с использованием файрволов и VPN-устройств?

Антон Карпов: Достаточно для чего? Файрволы и VPN-устройства выполняют четко ограниченные функции и не являются панацеей. Поэтому на вопрос «достаточно ли файрвола, фильтрующего пакеты на сетевом уровне, для защиты от неавторизованного трафика на третьем уровне модели OSI» я отвечу «да». На вопрос «достаточно ли его для защиты корпоративной сети» я отвечу, разумеется, «нет».

Константин Гавриленко: Все зависит от каждой конкретной сети и поставленных задач. Для домашнего компьютера, подключенного к Интернет, может быть достаточно простенького фаервола, а для большой корпоративной сети с множеством каналов подключения, подсетей с разными правами доступа и парой сотней серверов, фаервол просто необходим. Задачу безопасного соединения двух удаленных офисов можно легко решить, используя пару дешевых COXO рутеров. Обеспечение глобальной локальной сети между сотней офисов и предоставлением доступа нескольким десяткам тысяч работников потребует совершенно другого подхода к решению задачи, ВПН устроиства в которой будут играть не самую основную роль.
Фаервол, вопреки распространенному мнению, не является панацеей и решает конкретные задачи по разрешению доступа к определенным ресурсам с конкретных ИП или подсетей. На примере Email сервера, обрабатывающего входящую почту с Интернета, в правилах фаервала должен быть как минимум прописан доступ к 25 порту и запрещающий доступ ко всем остальным портам с внешнего интерфейса. Если Email сервер уязвим, то файрвол не предотвратит угрозу взлома сервера, так как злоумышленник все равно сможет послать эксплойт. А при условии неправильной конфигурации сервера, сможет использовать его функциональность для каких-то своих целей. В данном случае гораздо важнее уделить внимание на установку «заплаток» и проверку правильности конфигурации. Пожалуй, единственный случай, когда файрвол может выступить в плане обеспечения полной защиты сервера, только если он будет предотвращать прием и посылку любых пакетов с этого хоста. Проще отключить машину от сети.
Что касается ВПН-устройств, то они выполняют определенную задачу по защите трафика при транзите через Интернет и обладают расширенными функциями контроля аутентификации хостов и пользователей. Очень часто ВПН клиенты после подключения имеют права доступа в сеть наравне с локально подключенными хостами. В такой ситуации, для облегчения доступа злоумышленником в локальную сеть предприятия, имеет смысл сосредоточить усилия на поиске и взлому таких вот удаленных хостов, обычно принадлежащих удаленным сотрудникам, работающим из дома. В этом случае технология, направленная на усиление безопасности, может как раз понизить уровень защищенности.
Стоит еще раз акцентировать внимание, что в современном мире ИТ-безопасности нельзя уповать на какую-то отдельно взятую технологию. Необходимо иметь, в первую очередь, четкое представление о потребностях организации, о требованиях от сети, доступа к глобальному Интернету и предоставляемых сервисах. Только после этого можно рассматривать определенные решения и делать какой-то анализ.

Крис Касперски: Ответ отрицательный. Если мы говорим о корпоративной сети, то никакого «периметра» у нее не существует и приходится иметь дело со сложной гетерогенной структурой, практически не поддающейся централизованному управлению. В такой сети часто обнаруживаются уязвимые узлы, администраторы которых вовремя не установили заплатки или допустили другие фатальные ошибки.

Валерия Комиссарова: ИБ — не продукт, а процесс, который не может быть заранее реализован определенным набором программных и/или программных продуктов. ИБ в компании — сложный комплекс, включающий в себя множество аспектов: технических, административных (которые не менее важны) и т.д. Поэтому перечислить какие-либо продукты и сказать, что они обеспечивают «достаточный уровень защиты» — опасно.

Антон Палагин: С точки зрения соотношения цена/качество — да.

ЗАРАЗА: Файрволы и VPN'ы — это всего лишь инструментарий, посредством которого реализуется корпоративная политика безопасности. Где-то они нужны, где-

то нет, но инструментарий сам по себе никогда не бывает достаточным. Как минимум, нужны люди, которые им владеют, и четкое представление о том, что при помощи этого инструментария создается. В большинстве же случаев получается примерно так же, как если бы некий человек в костюме и галстуке дал выпускнику ПТУ токарный станок без какого-либо чертежа, плана и задания. И сказал: «Работай». А на предсказуемый вопрос «А что мне делать?» ответил: «Ты токарь, ты и разбирайся». Причем часто после того, как кому-то удалось разобраться в ситуации, выясняется, что и станок нужен не токарный, а фрезерный.

СПЕЦ: Что сейчас представляет основную угрозу сетям?

Антон Карпов: Если рассматривать исключительно техническую сторону вопроса, то с каждым годом все острее стоит вопрос безопасности пользовательских приложений. Уже никто не ломает web-серверы или почтовые серверы компаний, чтобы с помощью них получить доступ ко внутренним ресурсам компании. Замечательный и такой популярный браузер Internet Explorer перманентно имеет N (N>1) уязвимостей, которые эксплуатируются удаленно при обработке специальной web-страницы, ссылки и т.п. То же можно сказать и про MS Office. Открыл специально сформированный документ, выполнил произвольный код на своей системе, а дальше уже дело техники. Отсюда больше количество атакованных машин, отсюда большая проблема DDoS-атак на внешние и внутренние ресурсы сети. Плюс полный бардак с безопасностью внутри корпоративной сети.

Денис Колисниченко: Наибольшая опасность — утечка конфиденциальной информации, в результате которой, как можно догадаться, будут крупные финансовые потери. Как правило, утечка информации является следствием действий инсайдеров (в большинстве случаев), кражи или потери мобильных устройств (ноутбуков, КПК) и действия Spyware (значительно реже). На втором месте — действие вирусов и человеческий фактор. Причем вирус может удалить конфиденциальную информацию. И неизвестно, что хуже — утечка или потеря информации. Тут все зависит от специфики предприятия. Но в любом случае, потеря информации грозит теми же финансовыми потерями. Что касается человеческого фактора, то, прежде всего, это тот случай, когда администратор забыл сделать резервную копию... На третьем месте — отказ в обслуживании (DoS-атака или просто выход оборудования из строя). Время простоя сети обходится крупным предприятиям очень дорого. Четвертое место — это взлом сети извне. Пятое место — все остальные возможные угрозы.

Антон Палагин: Человеческий фактор.

ЗАРАЗА: Раздолбайство. Как, впрочем, и всегда.

СПЕЦ: Как бороться с «инсайдерами»?

Игорь Антонов: Для предотвращения появления инсайдеров первым делом нужно обзавестись хорошим психологом. Перед устройством на работу новый сотрудник должен пообщаться с этим психологом, и на основании этого разговора можно будет сделать вывод о том, какие цели преследует человек, устраиваясь в вашу компанию. Так 40% возможных инсайдеров можно отсеять еще до приема на работу.

Антон Карпов: Помочь может четко прописанная и развернутая система физической безопасности вкупе с системой защиты от злонамеренного воздействия инсайдера на корпоративную сеть. В последнем случае это использование принципа наименьших привилегий на рабочем месте пользователя, контроль использования на рабочем месте съемных носителей (USB-флешки, жесткие диски), контроль использования в сети неавторизованных устройств (ноутбуков, PDA, точек доступа), сегментирование сети (выделение отдельных подразделений компании в отдельные VLAN'ы), развертывание и мониторинг во внутренней сети систем обнаружения и предотвращения вторжений. Получив доступ к порту коммутатора в одной из офисных комнат и не имея никаких более привилегий в корпоративной сети (стандартная модель нарушителя в случае технического аудита безопасности внутренней ЛВС компании методом пентеста), злоумышленник в 9 случаев из 10 очень скоро будет контролировать все узлы и серверы ЛВС (а значит, и информацию, хранящейся на этих узлах).

Крис Касперски: Легче не допустить их появления. Лояльность сотрудников к компании в значительной мере зависит от отношения компании к сотрудникам. Если в них видят безликую рабочую силу, то и «рабочая сила» видит в компании только безликое сооружение из стекла и бетона, «сливая» конфиденциальную информацию при первой возможности на «сторону». Кстати, инсайдеры зачастую обнаруживаются в самых верхних эшелонах власти.

Денис Колисниченко: Если вкратце, то нужно сформировать отдел информационной безопасности, который будет работать не под управлением IT-отдела, а отдельно. Основная задача — контроль трафика и изучение отношений в коллективе. Ведь может случиться, что Иванов, у которого нет доступа к конфиденциальной информации, попросит Петрова, с которым у него дружеские отношения, скопировать ее. Кстати, подобный случай был в одном из банков, когда начальник одно из отделов попросил сотрудницу кредитного отдела предоставить ему информацию о заемщиках с целью поздравить их с Новым годом. Она выполнила просьбу, а через некоторое время инсайдер перешел в другой банк. Понятно, что произошла утечка информации. Когда же отдел безопасности начал расследовать этот случай, бывший инсайдер заявил, что сотрудница банка продала ему эту информацию уже после его увольнения…

ЗАРАЗА: Нет эффективного и универсального метода борьбы. Если в организации есть проблема инсайдеров — значит, политика информационной безопасности должна разрабатываться с учетом этого факта. **it**