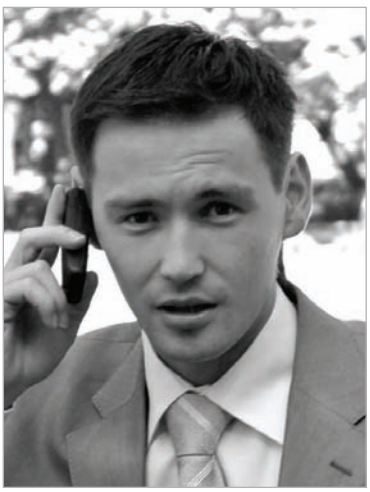
НАШИ ЭКСПЕРТЫ

Михаил Башлыков

Руководитель направления информационной безопасности компании КРОК

Руслан Рахметов



Начальник проектно-технического центра информационной безопасности компании «АйТи»

Алексей Лукацкий

Бизнес-консультант по безопасности компании Cisco

СПЕЦ:

Очень трудно, а зачастую и невозможно качественно и количественно оценить все уязвимости. С чем же в итоге бороться? Как правильно выбрать подходы к оценке рисков?

Михаил Башлыков:
Сегодня существуют различные подходы к оценке информационных рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности (ИБ), характера принимаемых во внимание угроз и эффективности потенциальных контрмер. Ключевыми моментами анализа информационных рисков являются:

— подробное документирование информационных ресурсов, причем особое внимание необходимо уделять критично важным для бизнеса приложениям;
— определение степени критичности для бизнеса нарушений штатного функционирования структурных элементов системы или безопасности хранимых и обрабатываемых данных;
— оценка потенциального ущерба в количественном или качественном эквиваленте;
— обнаружение и учет уязвимых мест;
— выявление и учет потенциальных угроз.

Вопрос анализа рисков является определяющим при построении эффективной и достаточной системы защиты. Однако не более 7% компаний используют собственные (углубленные) методики анализа рисков, которые позволяют выполнять количественный анализ и оптимизацию подсистемы ИБ. Поэтому сегодня наиболее востребованы простейшие методики анализа рисков, являющиеся частью методик базового уровня информационной безопасности. Наиболее заинтересованы в комплексных количественных методиках анализа рисков в России компании финансового профиля, для которых информационная безопасность – одна из важнейших составляющих бизнеса.

Руслан Рахметов:
Есть два подхода к анализу рисков: качественный и количественный. Каждый из них имеет свои преимущества и недостатки. Количественный анализ рисков позволяет вести оценку на языке бизнеса, т. е. делать финансовую оценку, но его применение более трудоемко и затратно. Качественный анализ рисков более дешев, но основан на использовании опыта ключевых сотрудников компании, т. е. носит субъективный характер.

СПЕЦ: Какие угрозы опаснее – внутренние или внешние? Сопоставимы ли они в принципе?

Максим Орловский

Консультант по безопасности компании «Архонт Лтд» и IT-директор компании «Аксинон Лтд»

Михаил Башлыков:
Хакерские атаки, вирусные эпидемии и спам – пожалуй, самые распространенные угрозы информационной безопасности. Среди не так часто упоминаемых рисков – действия внутренних нарушителей, халатность сотрудников, аппаратные и программные сбои, кража оборудования, финансовое мошенничество.
Согласно исследованиям компании Infowatch, разрабатывающей технологии для новой области ИБ — защиты от внутренних угроз, в последнее время растет количество информационных рисков, угроз и потерь, связанных с действиями внутренних нарушителей. Эти данные подтверждает и компания КРОК на основе проведения аудита систем информационной безопасности.
Интересно, что большинство компаний не предпринимают сегодня достаточных мер по защите от действий инсайдеров. Что, собственно, и объясняет, почему сегодня можно купить сборник баз данных и получить полную и достоверную информацию о человеке.
Самыми распространенными путями утечки информации являются электронная почта, мобильные накопители, веб-почта, форумы. Финансовые потери при утечке информации очевидны, поскольку информация сегодня – главный актив, а внутренние нарушители приносят серьезный, а зачастую непоправимый урон. Ощутимыми с финансовой точки зрения являются и другие риски, в том числе связанные со сбоями в работе корпоративной информационной системы.
Сегодня на рынке представлено много продуктов для защиты от действий инсайдеров – это многофакторные системы аутентификации и контроля доступа, системы контентной фильтрации и контроля целостности, системы мониторинга событий безопасности и многое другое.
Максимального эффекта можно достичь только при сочетании мер технических с мерами организационного характера. Например, важно не только контролировать права пользователей, блокировать действия пользователей (ICQ, USB-flash), но и прописать правила информационной безопасности, обеспечить доказуемость действий пользователей и привлекать виновных к ответственности. К тому же причиной нарушения могут стать и ошибки персонала, связанные с недостаточной подготовкой по вопросам ИБ, поэтому важно не забывать и об обучении сотрудников.

Руслан Рахметов:
Наиболее опасными считаются внутренние угрозы. Существует известная статистика: порядка 80% потерь происходит в результате реализации внутренних угроз и только оставшиеся 20% приходятся на внешние угрозы. Внутренний нарушитель всегда более опасен. Возможности для внутренних угроз создают сами компании, к примеру предоставляя избыточные полномочия по доступу к информационным ресурсам, опасаясь запретить необходимое.
Проблема в том, что, осознав необходимость защиты активов компании, управляющий персонал зачастую ограничивается корпоративной политикой и стандартом информационной безопасности, забывая о важных аспектах тактического и операционного уровня. Проще говоря, корпоративную политику и стандарт ИБ компании необходимо воплощать в жизнь, наполнять его практическим смыслом. Например, ввести ролевую модель контроля доступа к ресурсам компании и использовать административный контроль. Наиболее эффективно – периодическая смена места/должности работы сотрудника или дублирование его полномочий. В любом случае персонал всегда будет совершать сознательные или бессознательные ошибки, нарушающие политику информационной безопасности. Задача службы безопасности – управлять этим процессом.

Алексей Лукацкий:
Сопоставлять их нельзя — все зависит от бизнес-модели компании или организации. Если речь идет, например, о традиционном банке, то для него велико значение информации, которая циркулирует внутри, и на первое место встает защита от утечек информации со стороны инсайдеров. То же касается и многих госструктур. Если мы в качестве примера возьмем промышленное предприятие или компанию ТЭК, то приоритетными будут также внутренние угрозы, но не с точки зрения утечки, а с точки зрения доступности сетей, управления технологическими процессами (АСУ ТП или SCADA). А вот для брокерской площадки или интернет-банка на первое место выходит внутренняя угроза, но не с точки зрения утечки, а как проблема обеспечения непрерывности работы. Для интернет-магазина помимо проблемы доступности может быть важна защита от внешней утечки базы клиентов. Иными словами, мы видим, что для разных типов компаний и организаций могут быть различные приоритеты в угрозах. И даже на одном предприятии в зависимости от сегмента могут меняться приоритеты в области внешних и внутренних угроз.

Максим Орловский:
Внешние и внутренние угрозы линейно нельзя сопоставлять. Единственное, что их объединяет — это тот потенциальный ущерб, который они могут нанести компании. При этом масштабы ущерба могут варьироваться как для внешних уязвимостей, так и для внутренних. Другими словами, похитить базу данных с клиентами, корпоративными стандартами и пр. можно как изнутри (недобросовестный сотрудник), так и с наружи, и здесь зачастую большую роль играет случай или злой рок. Где тонко — там и рвется. И постфактум уже не важно, какой тип уязвимости стал причиной краха — внутренний или внешний.

СПЕЦ: Чем большее количество рисков

хочет предотвратить компания, тем дороже ей это обходится. Как рационально расходовать средства?

Михаил Башлыков:
Компаниис целью снижения совокупной стоимости владения ИТ-инфраструктурой и максимально быстрого периода окупаемости инвестиций в нее сокращают затраты на первых стадиях внедрения и эксплуатации информационных систем. Иногда бывает, что безопасность становится первой статьей экономии. На мой взгляд, это связано с тем, что руководство плохо информировано о возможных последствиях недостаточной защищенности ресурсов. Компании недооценивают потенциальные угрозы, а это сказывается на финансировании мер по обеспечению безопасности информационных активов. ИТ-руководителю или руководителю службы ИБ зачастую бывает действительно сложно обосновать необходимость тех или иных инвестиций в построение системы информационной безопасности. Таким образом, вовлеченность руководства в процесс управления ИБ продолжает оставаться недостаточной. Эта ситуация может продолжаться до тех пор, пока каждая компания не достигнет определенного уровня ИТ-зрелости. Совсем скоро мы придем к тому, что особое внимание будет уделяться не просто внедрению систем защиты, но и регламентированию и выстраиванию процессов безопасности. Защита информации не может осуществляться по остаточному принципу. Хотя в последние несколько лет ситуация меняется в лучшую сторону. Успешные и крупные компании создают или уже создали отдельные подразделения, разрабатывают корпоративные стандарты и постоянно поддерживают развитие средств информационной защиты.

Руслан Рахметов:
Нужно учиться правильно расставлять приоритеты. Все зависит от величины допустимого риска, вероятность которого нельзя свести к нулю. По нашему опыту количественной оценки рисков информационной безопасности, на защиту активов компании стоит тратить не менее 10% их стоимости. Но в любом случае стоимость мер защиты не должна превышать стоимость защищаемых активов.
Рассмотрим пример количественного анализа рисков, связанных с угрозой пожара. Допустим, что в результате пожара компания может потерять 1 млн. долл., но в среднем пожар случается раз в сто лет (ежегодная вероятность – 0,01). В результате, ожидаемые потери составляют 10 тыс. долл. в год. Казалось бы, логично именно эту сумму тратить ежегодно на средства защиты. Но здесь есть два нюанса. Во-первых, любой математик вам скажет, что вероятность подтверждается на достаточно продолжительных промежутках времени и без субъективных оценок не обойтись. Во-вторых, оценка стоимости активов – очень тонкий момент. Как, например, оценить имидж компании, государственную тайну и т. п? То есть нужно учитывать, что каждый случай индивидуален, и при защите трудно поддающихся оценке активов стоит исходить из стоимости компании на рынке.

Алексей Лукацкий:
Слово «рационально» тут не совсем к месту. Должна быть разработана стратегия управления рисками, в которой определяется, какие риски приоритетны и какие методы управления этими рисками мы используем — снижение, принятие, уход и т. д. После этого выписываем все наши риски и для каждого из них выписываем все контрмеры (в зависимости от методов управления рисками) — страхование, обучение персонала, организационные мероприятия, применение технических мер и т. д. Затем мы определяем (если можем и умеем) стоимость защищаемых активов и стоимость реализации и поддержания контрмер. Из списка всех контрмер выбираем те, которые дешевле стоимости защищаемых активов. Если контрмера осталась одна, то ее и реализуем. А если много, то выбираем другие критерии оценки (помимо цены) и дальше начинается классика системного анализа. В итоге опять же получаем подходящую контрмеру. Но тут есть тонкий момент. Надо учитывать, что одна и та же контрмера может защищать от нескольких рисков. И если для одного риска она оказывается дорогой, то для двух-трех-пяти рисков цена уже может быть нормальной. А вот после определения конечной стоимости всех контрмер против всех выбранных рисков мы уже окончательно оцениваем, стоит от чего-то отказаться или нет.

Максим Орловский:
Для этого в первую очередь требуется отдел IT-консалтинга или помощь сторонних экспертов, если такой отдел отсутствует. Одна из основных ошибок состоит в мониторинге и принятии решений относительно IT-безопасности теми же людьми, что и ответственными за внедрение и реализацию принятых решений. Поэтому для эффективного использования средств необходимо на первом этапе осуществить «needs, gaps and risk analysis» — общую оценку текущего состояния инфраструктуры и потенциальных рисков, в том числе с привлечением сторонних экспертов (может составить до 20% от общих средств, выделенных на поддержку безопасности). В результате этого будет составлен документ, опираясь на который руководству компании будет значительно проще выделить приоритетные направления и контролировать расходы на поддержание безопасности в рамках существующего бюджета. Разумеется, устранение 100% уязвимостей зачастую стоит больше, чем потенциальный риск, который они несут. Опираясь на экспертную оценку, можно выделить наиболее значительные недостатки в инфраструктуре безопасности и на их устранение направлять средства в первую очередь.

СПЕЦ: Как грамотно построить регулярный мониторинг, чтобы минимизировать возможные риски?

Михаил Башлыков:
Для того чтобы обеспечить полноценный контроль доступа к информационным ресурсам, необходимо решить следующие задачи: идентификацию, аутентификацию, авторизацию и регистрацию событий безопасности. Так как система управления доступом чрезмерно сложна, ее нерезультативно обеспечивать одним продуктом. Задачу идентификации пользователя эффективней решать с использованием продуктов нескольких производителей, например, следующие комплексы:
— IBM Tivoli Identity Manager и IBM Tivoli Identity Federation Manager (для web-сервисов);
— Oracle Identity Federation и Oracle Identity Manager;
— Sun Identity Manager Sun Java System Federation Manager.
Управление учетными записями важно дополнять решением по идентифика-

ции пользователей в промежуточных запросах, например запросы web-сервисов, которые идут не непосредственно от программы пользователя, а через несколько серверов приложений в многозвенной архитектуре. Для этого применяются продукты, в названии которых присутствует слово Federation. При их помощи по содержанию web-сервиса можно идентифицировать пользователя, от имени которого производится запрос, а не учетную запись, используемую сервером приложений при формировании http-запроса, который содержит XML-запрос к web-сервису.

Опыт компании КРОК показывает, что задачу аутентификации пользователей также надежнее решать с помощью продукции нескольких производителей, так как необходимо поддерживать все протоколы и схемы аутентификации, используемые в уже существующей системе, не меняя ее и не влияя на доступность функций. Например, возможен вариант с использованием следующих комплексов:

— IBM Tivoli Access Manager IBM;
— Oracle Access Manager;
— Sun Access Manager.

Решение задачи аутентификации технически сложнее, потому что поддержка всего спектра протоколов доступа и схем аутентификации просто невозможна, да и не во все системы можно встроить Plug-ins. Наш опыт показывает, что даже для систем с web-интерфейсом не удастся решить задачу централизованной аутентификации в 80% случаев. Поэтому необходимы дополнительные методы аутентификации, такие как доступ к консоли компьютера с использованием микропроцессорной карты и токена.

Решение задачи разграничения доступа на прикладном уровне связано с пониманием прикладной логики системы. Кроме того, такая система должна быть открыта для подключения внешнего механизма управления доступом, что не всегда предусматривается во всех системах. Особо хочется отметить web-сервисы. Совершенно недостаточно ограничивать доступ к web-сервису, опираясь на идентификацию клиента и сервера на уровне HTTP. Необходимо «заглянуть» внутрь XML, передаваемого в запросе к web-сервису. Именно это возможно с использованием IBM DataPower, который способен работать как XML Firewall. Это особенно необходимо при авторизации запросов от портала, доступного для внешних пользователей к внутренним web-сервисам.

Регистрация событий – также важный компонент защиты информации. Управлять доступом эффективно можно тогда, когда есть обратная связь – контроль за использованием доступа. С этой целью применяют системы сбора и анализа событий безопасности. КРОК успешно реализует проекты по внедрению TSOM. Например, в проекте по созданию системы обеспечения безопасности информации корпоративного портала ОАО РАО «ЕЭС России» специалисты компании КРОК применили комплексную систему аутентификации, которая включает и VPN, и FireWall, и WebSEAL (компонент Tivoli Access Manager), и eTouken, и RSA KEON. Система получилась комплексная и для понимания ее работы понадобилась система сбора событий информационной безопасности, таких как вход администратора, смена паролей, попытки нарушения защиты системы.

Руслан Рахметов:

Именно мониторинг является основным инструментом выявления внутренних угроз. При этом он должен быть регулярным, желательно в режиме реального времени. Грамотное построение системы мониторинга должно начинаться с экономического обоснования необходимости снижения рисков, т. е. с определения допустимого уровня риска. Если экономическая обоснованность ясна, надо построить свою методику анализа рисков, базируясь на международных стандартах. То есть определить, кто и как часто классифицирует активы компании, проводит анализ угроз и выбирает метод снижения рисков.

Для организации мониторинга и управления безопасностью предприятия в режиме реального времени следует применять комплексные решения, состоящие из организационных процедур, процессов, методик и технологий. «АйТи» имеет опыт построения таких решений, причем их можно создавать как на площадке заказчика (в этом случае «АйТи» разрабатывает программно-аппаратный комплекс, выстраивает процессы и обучает персонал заказчика), так и арендовать в нашей компании (в этом случае заказчик получает лишь результат, а персонал, процессы, оборудование и ПО находятся в «АйТи»). В результате налаженной работы центра мониторинга и управления ИБ компания получает возможность управлять рисками для принятия адекватных управленческих решений, а также контролировать и предотвращать события и инциденты безопасности. Применение таких решений обеспечивает максимальное покрытие информационных систем и инфраструктуры компании в целом, позволяет контролировать ответственность конкретных специалистов за процесс реакции на инциденты безопасности и проводить аудит информационной системы на соответствие промышленным стандартам.

Алексей Лукацкий:

Мониторинг — это техническая мера, которая, безусловно, важна, но не является самой главной и лучшей для контроля утечек информации. При сегодняшнем уровне развития технологии мониторинга не способны справиться с квалифицированным злоумышленником — достаточно просто шифровать всю передаваемую информацию. Поэтому гораздо эффективнее реализовывать меры по повышению осведомленности персонала, улучшению рабочего климата и вообще внедрять эффективную систему мотивации персонала. Это позволит не зависеть от выбранных технических мер и наличия ИТ/ИБ-специалистов. Хотя не спорю, что внедрение технических решений является более простым для службы ИБ и более выгодным для всех сторон.

Максим Орловский:

Ключевым моментом эффективного мониторинга компании служит политика безопасности, принятая на уровне внутреннего корпоративного стандарта. В этой политике, во-первых, должны быть четко определены роли персонала, связанные с поддержкой безопасности и, во-вторых, выделены ключевые критерии, регулярный и протоколируемый контроль которых необходим для выявления вновь возникающих уязвимостей. Создание такой политики является нетривиальной задачей и, зачастую, невозможно без привлечения сторонних компаний, специализирующихся на сервисах такого рода. Более того, в ряде областей существуют международные стандарты безопасности, соблюдение которых необходимо для эффективного выхода на международный уровень (в особенности это касается банковского дела), а профессионально составленная политика безопасности является необходимой не только de facto, но и de jure.

Наличие корпоративной политики в будущем ведет к значительному сокращению средств на регулярный мониторинг и аудиты, так как поддержка безопасности в отсутствии стратегии и четко определенных приоритетов связана и со значительными расходами на второстепенные вопросы, с весьма вероятными потерями от неустраненных уязвимостей, которые возможно выявить только при систематическом и регламентированном подходе. **it**