Территория доверия

Согласно отчетам ведущих аналитических агентств, инциденты, связанные с утечками данных, составляют львиную долю всех нарушений информационной безопасности. Усиление рисков этой категории нарушений происходит на фоне трудностей, связанных с дефицитом бюджетов и кадровыми неурядицами.

Кто-то теряет, а кто-то находит

Аналитики отмечают, что по количеству утечек и размеру ущерба для компаний внутренние факторы чаще являются причиной инцидентов, нежели внешние.

В ежегодном отчете, спонсированном PGP Corporation, подсчитано, что потери компаний, вызванные фактом утечки информации, в 2008-м году возросли до 1,7 млн фунтов по сравнению с 1,4 млн фунтов в 2007-м. 70% всех случаев утечек информации, попавших в исследование, вызвано халатностью персонала, и только 30% составляют кражи злоумышленников. В общем количестве утечек за последний год 33% произошло по вине сторонних организаций.

Согласно исследованию InfoWatch, в новой экономической ситуации наблюдается резкое увеличение количества компаний, сталкивающихся с проблемой утечки информации. Аналитический центр InfoWatch приступил к формированию базы инцидентов в 2004 году. На сегодняшний день она содержит несколько тысяч записей, из которых 530 сделано в 2008 году, что существенно больше, чем за предыдущий год.

«Главная причина утечек в кризис — массово сокращаемые сотрудники, — считает Илья Шабанов, руководитель аналитического центра InfoWatch. — Они уносят с собой конфиденциальную информацию — в надежде, что она пригодится им на новом месте, или с целью продать ее конкурентам. В результате подобных действий инсайдеров компании несут значительные финансовые убытки, к тому же наносится серьезный ущерб репутации».

Согласно исследованию InfoWatch за 2008 год, от утечек страдают прежде всего коммерческие предприятия — 296 инцидентов (55,8%); общественные и образовательные организации — 127 (24,0%); государственные структуры — 104 (19,6%). В подавляющем числе случаев речь идет об утечке персональных данных.

При этом 45% утечек было совершено умышленно, для 42,1% инцидентов имел место факт случайной утечки. Среди ее каналов наиболее распространенными представители InfoWatch называют (в порядке убывания приоритета) ноутбуки или иные мобильные компьютеры (19,4% инцидентов), переносные носители CD, DVD, флеш-память (5,7%), сеть (кроме электронной почты, 21,1%), настольные компьютеры или серверы (7,5%), электронную почту и факс (2,3%), бумажные документы (5,3%), архивные носители (3,2%).

По данным последнего аналитического отчета компании IT Policy Compliance Group (IT PCG) «Финансирование информационной безопасности и ИТ с учетом риска» (Risk-based Performance Budgeting for Information Security and Audit in IT), выполненного на основе опроса более чем 2 600 зарубежных фирм, 68% из них недофинансируют информационную безопасность с учетом финансовых рисков и потерь. При этом риск утечки конфиденциальной информации занимает верхнюю строчку рейтинга бизнес-рисков от ИТ: 19% компаний каждый год имеет свыше 15 инцидентов потери или кражи данных, 68% работает с «нормальными» уровнями потерь, переживая в год от 3 до 15 таких случаев, а в 13% фирм подобное происходит менее трех раз в год.

Согласно исследованию, финансовые последствия этих рисков почти целиком зависят от практики управления их влиянием, применяемой ИТ-подразделением. Фирмы, не применяющие практических рекомендаций, расплачиваются за это потерей и утечкой данных, эквивалентной 9,6% годового дохода, а простои обходятся им почти в 3%.

Среди организаций с доходом в $5 млрд совокупный убыток от потери или утечки данных и простоев составил от $329 млн для фирм с наихудшей практикой до $2,25 млн для применяющих практические рекомендации (в 149 раз меньше). Помимо прямых финансовых потерь из-за утечки конфиденциальных данных, компании несут серьезные репутационные риски. При накале конкуренции отток клиентов, вызванный неприятным известием, может оказаться фатальным для бизнеса.

Что делать?

Мобильные носители информации типа флеш-накопителей чаще случайно теряют, чем злонамеренно похищают. «Принудительное шифрование мобильных носителей защитит от обоих видов утечек, — подчеркивает Илья Шабанов. — Если информация на утраченном носителе была зашифрована (а не просто «защищена паролем»), то такой случай вообще инцидентом не считается, не влечет уведомления властей и не попадает в учет».

По данным InfoWatch, в нынешней ситуации владельцы бизнеса начинают осознавать масштабы

потенциального ущерба, который могут нанести им собственные сотрудники, и ищут способы защитить свое предприятие.
— В этой связи, — говорит Илья Шабанов, — наиболее оптимальным решением на сегодняшний день является внедрение одной из существующих на рынке систем защиты информации от внутренних угроз, или DLP-систем.
Руководители компаний стараются максимально оптимизировать расходы при внедрении подобных систем. Это выражается в повышении требований к эффективности вложений за счет более гибкого подхода к данному решению, аренде оборудования совместно с партнерами, а также в использовании легкого входа и выхода из проекта и других возможностей, предлагаемых компаниями — разработчиками подобных систем.
В отчете IT PCG приводятся следующие пять рекомендаций, используемых организациями с наилучшими результатами и минимальными финансовыми потерями: привлечение высшего руководства к управлению рисками;
расстановка приоритетов, совершенствование средств контроля и автоматизация процедур по снижению рисков;
непрерывная оценка средств контроля и рисков;
применение технических средств контроля, правил и управления изменениями в ИТ-системах;
исчерпывающая отчетность.

Безопасность по закону

В России не существует единого органа, который отвечал бы за работу над стандартами в сфере ИБ. Каждая вертикаль вынуждена самостоятельно решать эти проблемы. Нормативная база на контроль и аудит средств ИБ в полной мере присутствует лишь в трех ведомствах — ФСТЭК (Гостехкомиссии), Министерстве обороны и ФСБ. В некоторой степени работа над стандартами продвинулась в банковской сфере, в авиационной и газовой отраслях.
Ответственность за утечку конфиденциальных сведений в России регулирует Закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» и нормативная база вокруг него, состоящая из постановлений правительства РФ и документов уполномоченных органов. По мнению Ильи Шабанова, в 2009 году этот закон станет основным возбудителем спокойствия со стороны российского законодательства по ИБ. Закон не только определяет само понятие «персональные данные», но и является в нашей стране правовой основой для их защиты, тем самым обеспечивая закрепленное в Конституции РФ право граждан на неприкосновенность частной жизни. «Как показывает практика, несмотря на то что закон вступил в силу еще в январе 2007 года, госструктуры и бизнес до сих пор не готовы к его исполнению», — говорит Илья Шабанов. — Всех расслабило указание на отсрочку в наступлении ответственности за неисполнение закона до 1 января 2010 года, а также мягкость возможных санкций после этого срока. Как это часто бывает, все, включая чиновников, спохватились только сейчас, когда времени осталось совсем мало. Тем не менее недавние попытки лоббирования дополнительной отсрочки в наступлении ответственности провалились, и это говорит о том, что закон все же заработает в полную силу в срок».
— Чем ближе «сакральная» дата 1 января 2010 года, тем острее для компаний, подпадающих под категорию операторов персональных данных (ПД), будет стоять вопрос приведения собственных систем, содержащих ПД, в соответствие с требованиями закона и нормативных актов, — отмечает Андрей Новиков, технический эксперт направления контент-безопасности (eSafe), компания Aladdin. — Уже сейчас закон породил невероятную информационную воронку, активизирующую проведение различных конференций, круглых столов, семинаров, порождающую острые дискуссии на страницах печати. Среди системных интеграторов набирает обороты тенденция включения в свой портфель услуг нового вида аудита — услуги по оценке соответствия требованиям Федерального закона «О персональных данных». Словом, ФЗ №152 был и остается на пике обсуждений законотворческой деятельности.
Наиболее известный из международных стандартов в банковской сфере PCI DSS (Payment Card Industry Data Security Standard) — это стандарт защиты информации в индустрии электронных платежных систем и обеспечения безопасной среды для держателей платежных пластиковых карт. Требования этого стандарта распространяются на все компании, работающие с международными платежными системами VISA и MasterCard по всему миру, включая Россию и СНГ. Этот стандарт набирает вес и является одним из немногих, где описываются реальные требования к системам ИБ, причем не только банков, но и предприятий, которые продают свои продукты и услуги с помощью карт либо предоставляют платежные шлюзы продавцам. Для операторов платежных карт этот стандарт предусматривает ежегодные аудиторские проверки, а также ежеквартальное сканирование сетей.

Работа систем DLP (Data Loss Prevention, защита от утечек конфиденциальной информации) — неважно, использует она агентов либо основана на безагентской технологии, — связана со сбором информации. «Заказчик неизбежно сталкивается с вопросом — имеет ли он право снимать эту информацию, — говорит Михаил Орешин, директор московского офиса компании «Поликом-Про». — Ведь электронная почта в соответствии с Конституцией РФ защищена от перлюстрации. И это право неотчуждаемо, кроме как по решению суда либо по желанию самих участников переписки».
За нарушение этого закона предусмотрена уголовная ответственность. И, как отмечает Орешин, заявление со словами «Прошу проверять мою

электронную почту» ничем не отличается от «Прошу унижать мою честь и достоинство с 10-00 до 18-00». С юридической точки зрения это одно и то же. Единственный вариант подстраховки при внедрении DLP — это установка автоматической системы мониторинга, которая выдает предупреждения о нарушении политик безопасности.

«Как реагировать — это уже другой вопрос, — говорит Михаил Орешин. — Если это порнография, терроризм, угроза национальным интересам государства — дело решается просто. Если же произошла утечка внутренней корпоративной информации, в этом случае сотрудника, переписка которого вызывает подозрение, можно попросить при свидетелях вскрыть письмо и показать его содержимое. Но это лишь формальность, поскольку на практике, скорее всего, сотрудники отдела безопасности уже знают содержание письма и просто стараются соблюсти порядок».

В компании TrendMicro проблему компромисса между надежной защитой и запретом на перлюстрацию решают следующим образом. «Для отделов безопасности нужно получить как можно больше собранных доказательств, что в сообщении или файле содержится конфиденциальная информация, чтобы инициировать процедуру раскрытия этой информации пользователем, — говорит Михаил Кондрашин, руководитель центра компетенции TrendMicro в России и СНГ. — В решениях Trend Micro для этих целей используется разработанная еще компанией Provilla уникальная технология снятия цифровых отпечатков. Документ, опознанный по отпечатку, не нужно перлюстрировать; скорее всего, там содержится конфиденциальная информация или фрагменты конфиденциальных документов».

Аудит для DLP

По мнению Евгения Лобачева, ведущего системного аналитика отдела ИБ компании «Открытые Технологии», важнейшей частью проекта внедрения системы DLP является аудит системы ИБ, который может существенно отличаться в зависимости от того, с какими целями он проводится. «При развертывании системы DLP основной задачей аудита является категоризация документов, информационных активов, того именно, что должна защищать система DLP, — подчеркивает Лобачев. — И только качественно выполненная категоризация позволит добиться высокой эффективности работы».

В комплексном аудите информационной безопасности предприятия Илья Шабанов выделяет нескольких частей: «Первая — это экспертный аудит, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта аудиторов, участвующих в проекте. Вторая — оценка соответствия государственным или отраслевым законам и требованиям — например, ISO 17799, руководящим документам ФСТЭК или PCI DSS. И третья — инструментальный анализ защищенности предприятия, направленный на выявление и устранение возможных уязвимостей программно-аппаратного обеспечения системы. Все эти части аудита должны содержать в себе этапы подготовки, сбора данных, анализа и подготовки рекомендаций для заказчика».

Три в одном

Большинство ведущих DLP-решений включает в себя несколько уровней контроля. Первый из них — это средства контроля трафика на уровне интернет-шлюза, которые применяются для анализа сетевого трафика (SMTP, HTTP и др.): у лучших DLP-решений их может быть около десятка. Второй — это контроль над подключением внешних устройств на уровне конечных точек (рабочие станции, файловые сервера и мобильные компьютеры). Для анализа потока данных на рабочем месте (например, при копировании информации на сменные носители) используются агенты. Некоторые решения используют агентов для анализа информации, передаваемой на принтер.

Характерно, что если еще год назад решения DLP различных производителей отличались фокусировкой либо на сетевой активности, либо на узловой, то сегодня подавляющее число игроков этого рынка используют архитектуру, предусматривающую применение как шлюзов, так и агентов, дополняя оба этих компонента шифрованием для большей надежности.

— Решение InfoWatch включает в себя контроль трафика на уровне шлюза, контроль подключений внешних устройств на уровне рабочих станций и надежное шифрование, — поясняет Илья Шабанов. — Попытки переноса в ряде конкурирующих DLP-решений анализа интернет-трафика на уровень конечных точек являются абсолютно нецелесообразным и даже вредным шагом, так как в итоге заказчик получает «второй антивирус» со всеми вытекающими последствиями в плане деградации производительности, проблем с совместимостью, надежностью и т. д. — Намного более логично производить анализ исходящего трафика на уровне шлюза незаметно для рядовых пользователей.

Девятая версия Symantec DLP, выпущенная в марте 2009 года, — это слияние двух технологий — собственного продукта Symantec и

приобретенной технологии Vontu. Продукт Symantec DLP в настоящее время состоит из трех технологических и одного управляющего модуля.

За контроль сетевого трафика отвечает модуль, включающий функциональность мониторинга и предупреждения (Network Monitor и Network Prevent). Активность на рабочих станциях отслеживает агент, объединяющий функциональность обнаружения и предотвращения (EndPoint Discover и EndPoint Prevent). Третий модуль является уникальным: он предназначен для контроля систем хранения. «Эта процедура дает ответ на вопрос — те ли данные хранятся, и находятся ли они там, где им положено, — говорит Кирилл Керценбаум, руководитель группы консультантов по безопасности компании Symantec. — В отличие от первых двух подходов, это офлайн-контроль. Он происходит по определенному графику и позволяет быть уверенными, что конфиденциальные данные не окажутся там, где им быть не положено».

Единая панель управления

Практически все ведущие зарубежные игроки рынка информационной безопасности уже приобрели фирмы, специализировавшиеся в нише DLP: McAfee поглотила компанию Onigma, Safeboot и Reconnex; Websence — PorthAuthority; Trend-Micro — Provilla; Symantec — Vontu.

На российском рынке специализированные продукты DLP собственной разработки продвигают компании InfoWatch, Leta IT-Company, «ПраймТек» и др.

Поскольку многие продукты DLP для выявления активности на хостах используют агентов, неизбежно возникает вопрос об их совместимости с такими технологиями, как мониторинг корпоративной ИТ-инфраструктуры или же комплексные системы Network Access Control, которые также основаны на консолидации информации, собираемой агентами на конечных точках.

«Вероятно, скоро у всех ведущих производителей ПО ИБ будет единый агент для обеспечения информационной безопасности на рабочем месте, объединяющий в себе функции антивируса, antispyware, HIDS, персонального МЭ, управления сменными носителями и DLP, а также поддержку NAC», — считает Евгений Лобачев.

«В настоящий момент, — отмечает Михаил Кондрашин, — наблюдается общая тенденция рынка к объединению всех средств защиты в едином модульном продукте, который позволяет заказчику самостоятельно и минимальными усилиями построить то решение, которое нужно. Кроме NAC и DLP, такое решение несомненно включает в себя антивирус, межсетевой экран и управление заплатами, возможно и некое шифрование и VPN».

После покупки Altiris, Vontu и целого ряда других компаний перед Symantec стала задача интеграции этих продуктов в собственные решения. Платформой для интеграции служит мощная конфигурационная база Altiris CMDB. На ее основе управление всеми продуктами осуществляется из единой консоли. «В девятой версии первая фаза интеграции уже сделана, — поясняет Кирилл Керценбаум. — все продукты, которые содержат агента, устанавливаемого на рабочих станциях, управляются из единой консоли». Для продукта Symantec DLP в настоящее время остается возможность управления как из консоли Altiris, так и из консоли самого Symantec DLP.

Интеграция большинства продуктов пока реализована на уровне единой консоли, но не на уровне агентов, но первый шаг уже сделан: система NAC (Network Access Control) объединена с антивирусом. «В соответствии с нашими планами для системы управления Altiris всегда будет оставаться собственный агент, — говорит Кирилл Керценбаум. — А вот антивирус и DLP-агенты должны быть объединены уже в ближайшее время. Это же касается и агента для системы резервного копирования в будущем».

Агентов DLP с агентами других подсистем безопасности уже объединила компания McAfee. «Зонтик» Total Protection for Data, обеспечивающий защиту хостов, включает в себя модули Endpoint Encryption for Devices, Files and Folders and Removable Media, Host Data Loss Prevention, Device Control, Encrypted USB, которые могут интегрироваться и комбинироваться с другими продуктами McAfee. «Приобретение компании Reconnex с решением DLP, которое сейчас называется McAfee Network DLP, дополнило арсенал средств защиты устройствами, защищающими всю парадигму DLP — данные в движении, хранении и в использовании», — говорит Рамиль Яфизов, технический консультант компании McAfee.

McAfee Data Loss Prevention обеспечивает полный контроль и видимость того, кто, как и где использует информацию. С его помощью защищаются все операции с данными — вставка, копирование, печать, изменение, передача. McAfee Endpoint Encryption предназначен для шифрования дисков, мобильных устройств, файлов, папок, содержащих чувствительную информацию. McAfee Device Control предотвращает неавторизованное использование съемных носителей информации.

Централизованное управление всеми продуктами семейства McAfee Total Protection осуществляется через единую консоль управления McAfee ePolicy Orchestrator, с единой конфигурационной базой данных. Благодаря этому обеспечивается сервис полной защиты, интегрирующий в себе антивирус, антишпион, брандмауэр, безопасность почтового сервера, контроль доступа в сеть, вместе с любым из модулей Data Protection. В составе продукта Total Protection for Data эта консоль управления поставляется бесплатно. Централизованное управление политиками на McAfee Network DLP (Reconnex DLP) осуществляется пока через собственную консоль Insight Console, но, судя по стратегии McAfee, интеграция и этого функционала не заставит себя долго ждать.

Безопасность как услуга

Согласно результатам очередного отчета Symantec об использовании предприятиями аутсорсинга услуг в области безопасности (2009 Managed Security in the Enterprise Report), 49% респондентов сообщают, что им стало труднее обеспечивать ИТ-безопасность из-за роста интенсивности угроз, нехватки квалифицированного персонала, усиления нормативных требований и недостаточных бюджетов.

Проблема выходит за рамки возможностей ИТ-подразделений, и обеспечить безопасность собственными силами все более и более сложно. Не удивительно, что многие (61%) из опрошенных, чтобы восполнить пробел, обращаются к внешним услугам по безопасности. В числе причин, называемых ИТ-менеджерами, фигурируют возможность обеспечить круглосуточное покрытие, более низкие общие затраты, доступ к высококвалифицированным специалистам по безопасности и расширенные возможности по снижению рисков для безопасности.

— Споры о том, сможет ли аутсорсинг ИТ всерьез стать альтернативой собственной службе эксплуатации ИТ или частично подменить собой ее функции, ведутся достаточно давно, — говорит Кирилл Керценбаум, руководитель группы консультантов по безопасности компании Symantec. — Сначала перенесение части задач ИТ вовне казалось приемлемым только для небольших компаний, сейчас же мы видим, что и многие крупные компании готовы к этому и идут на это. Однако вопросы ИБ всегда стояли несколько особняком, ведь доверять свою безопасность «чужим» специалистам довольно рискованно. Но в последнее время приходит понимание, что лучше профессиональная защита в виде аутсорсинга, нежели непрофессиональная собственными силами. Мировой финансовый кризис, только усугубивший ухудшающуюся ситуацию с количеством и качеством всевозможных атак, еще сильнее подталкивает компании к привлечению внешних организаций для обеспечения должного уровня сервисов ИБ.

Возможность использования модели SaaS в индустрии ИБ, и в частности в защите от утечек, у Ильи Шабанова вызывает сомнения. «Во-первых, — говорит он, — серьезные DLP-системы в принципе рассчитаны на крупные компании, которые вообще очень редко готовы пользоваться сервисами вместо покупки классического программного обеспечения. Этому есть целый ряд причин: элементарное недоверие к поставщику услуг (боязнь отдать на аутсорсинг важные для бизнеса функции), необходимость контроля ИТ-инфраструктуры, необходимость большей гибкости конфигурации, а также меньшая цена в расчете на несколько лет. Во-вторых, сама концепция DLP базируется на желании клиента контролировать работу с конфиденциальными данными и не допустить того, чтобы они покинули пределы корпоративной сети. Но это противоречит модели SaaS, когда работа с данными, наоборот, передается за пределы сети, где никто не сможет гарантировать их стопроцентной сохранности».

Аналогичной точки зрения придерживается и Михаил Кондрашин: «В настоящий момент в России основным вопросом, который обсуждается с заказчиками SaaS, является вопрос доверия провайдеру сервиса. На SaaS решаются только небольшие компании, у которых на рынке нет конкурентов, имеющих влияние на провайдера. Для компаний, всерьез рассматривающих угрозу инсайда, SaaS-решения недопустимы, так как для таких компаний первичным является недоверие к своим собственным сотрудникам. При такой постановке задачи доверять внешним контрагентам абсурдно».

Евгений Лобачев считает, что использование модели SaaS не только возможно, но уже с успехом практикуется. «По похожей схеме работает игрок рынка DLP WebSense, — поясняет он. — В данном случае, видимо, технологическое превосходство оправдывает относительно мало распространенную на нашем рынке модель продаж по подписке. Легкое внедрение, низкий процент ложных срабатываний за счет технологии цифровых отпечатков PreciseID, возможность анализа HTTPS-трафика — все эти преимущества окупают необходимость ежегодного платежа».

Мнение эксперта

Дмитрий Породин, начальник отдела систем информационной безопасности компании INLINE Technologies

Защита от утечки бизнес-информации

Технологии защиты от утечек конфиденциальной информации на сегодняшний день являются наиболее эффективным инструментом противодействия нелояльным и нерадивым сотрудникам. Большинство наиболее успешных зарубежных корпораций уже внедрили их у себя. Российские компании пока отстают. Внедрение систем DLP в отечественном бизнесе зачастую тормозит отсутствие регламентированных политик и процедур работы с конфиденциальной информацией. Дело в том, что наиболее современные и

функциональные системы DLP для определения степени конфиденциальности информации используют специальные технологии цифровых отпечатков. Эти технологии работают непосредственно с конфиденциальной информацией — каталогами, файлами различных форматов, таблицами баз данных. Таким образом, для внедрения системы DLP необходимо четко знать, какие объекты корпоративной сети содержат конфиденциальные данные. Далее необходимо определять правила работы с такими данными. Например, только сотрудники отдела по работе с партнерами могут отправлять по электронной почте данные о клиентах своим контрагентам, другие сотрудники — нет.
Далеко не все российские компании могут самостоятельно подготовиться к внедрению DLP-системы: разработать политики и процедуры работы с конфиденциальной информацией, провести обследование корпоративной сети, структурировать данные и пр. Поэтому внедрение DLP-системы целесообразно доверить профессионалам. В рамки проекта большей частью должен входить квалифицированный консалтинг, что позволит добиться максимального эффекта уже на этапе опытной эксплуатации.
Следует отметить, что DLP-система должна закрывать все возможные каналы утечки конфиденциальной информации: рабочие станции, электронную почту, принтеры, веб-доступ, системы мгновенной передачи сообщений. Объединение с другими технологиями и средствами защиты информации позволит повысить защищенность информационных ресурсов. Прежде всего, рекомендуется объединить DLP-систему с технологией контроля доступа (NAC), системами защиты от вторжений, контроля устройств и съемных носителей. Это позволит снизить риски утечки конфиденциальной информации на наиболее уязвимом звене современных корпоративных сетей — рабочих станциях пользователей. При внедрении следует также обратить внимание на процесс управления доступом к информации в целом. Особенно с учетом популярных на сегодня технологий мобильной работы и виртуализации, которые сдвигают традиционные границы корпоративной сети и привносят дополнительные риски потери критичной для бизнеса информации.

Мнение эксперта

Василий Тарасов, генеральный директор компании «ПраймТек»

Проверять — не доверять

В любой системе рано или поздно складываются ситуации, которых нельзя предусмотреть заранее. В авиации черный ящик в первую очередь нужен для того, чтобы разобрать все нештатные инциденты и сделать вывод о том, как действовать в случае наступления аналогичных событий. В информационной системе роль такого «ящика» выполняет система контроля и аудита. Это необязательная, но основная функция, ее введение чрезвычайно желательно на начальной стадии проектирования информационной системы. Иначе ИС начинает жить своей жизнью, в нее постоянно и бесконтрольно вносятся изменения, и в конце концов она становится совершенно неуправляемой.
Под контролем мы подразумеваем проверку системы на способность соответствовать ранее заданной спецификации на всех уровнях — программном, аппаратном, человеко-машинном. Причиной для «разбора полетов» становится отклонение от спецификации с точки зрения безопасности. Но даже если внешне ИС работает по заданной спецификации, и в ней отслеживаются все изменения, внутри могут оказаться закладки, вредоносные программы, которые могут нарушать и саму спецификацию, и логику работы системы.
Изначально мы строили свой продукт «Инсайдер» для обеспечения информационной безопасности с точки зрения контроля ключевых параметров, которые собирались на разных уровнях. Но на определенном этапе развития этой системы пришли к выводу, что этого недостаточно. В комплекс «Инсайдер» был введен сложный механизм аналитической обработки, позволяющий путем сравнения параметров контроля на разных уровнях сделать выводы о том, есть ли внутренний нарушитель, и кто он — программа, устройство или человек.
В архитектуру продукта было заложено три принципа независимости. Первый связан с тем, что процедуры и программы контроля должны быть разработаны независимо от основных функций ИС. Очевидно, что когда одной командой программируются основные функции ИС, и ею же параллельно создается система контроля, то могут быть допущены те же самые ошибки. Второй принцип касается процедуры сбора информации. Если информацию собирать непосредственно в ходе технологических операций работы системы — будут возникать те же самые ошибки и проблемы. Сбор информации должен быть осуществлен за рамками технологического цикла последовательности операций. Третий принцип лежит в основе эксплуатации системы информационной безопасности: ее обслуживанием должно заниматься независимое от ИТ подразделение.
Еще одно важное требование формулируется так: используемые средства контроля должны быть доверенными. Дать гарантию того, что используемые программные продукты — операционные системы, компиляторы, приложения — не хранят в себе закладок, нельзя. Но создать полностью доверенную систему контроля можно, и мы это делаем. Это компактная система, где основным элементом доверенности выступает недорогой агент, занимающийся сбором информации. Слежение за узловой и сетевой активностью позволяет выявить угрозы с различными предпосылками. Помимо активности пользователей, комплекс «Инсайдер» отслеживает все изменения программно-аппаратной конфигурации системы, в том числе в удаленном режиме. Используя такую доверенную систему контроля в недоверенной среде, организация повышает уровень

доверенности всей информационной системы в целом с точки зрения информационной безопасности. Комплекс «Инсайдер» функционирует в основных операционных средах, взаимодействует с серверными и сетевыми компонентами разных производителей, с программными приложениями различных разработчиков. Количество событий, которые он собирает и обрабатывает, велико. Благодаря тому, что в функциональности «Инсайдера» заложены не только пассивные, но и проактивные методы слежения, администратор безопасности может получить уведомления о нарушениях за некоторое время до наступления нежелательных событий. Активная защита использует запрет на применение некоторых системных ресурсов (запуск нерегламентированных программ, обращение к внешним устройствам). Для аудита этих событий и с целью дальнейшего «самообучения» системы безопасности задействуется экспертная система.

Мнение эксперта

Андрей Новиков, технический эксперт направления контент-безопасности компании Aladdin

Каналы утечки и системы противодействия утечкам

Для того чтобы понять, как строить систему защиты от утечки конфиденциальной информации, нужно представлять себе канал, по которой эта утечка может произойти. В контексте противодействия инцидентам, связанным с инсайдерской активностью и утечками данных, сводить весь арсенал средств борьбы с этими угрозами только к DLP по меньшей мере неразумно. Перекрыть все возможные каналы утечки с помощью одного продукта или технологии нереально.

Серьезную угрозу для современного бизнеса сегодня представляют каналы утечки, связанные с неконтролируемым использованием коммуникационных возможностей глобальной сети Интернет. При этом большая часть всех утечек, о которых известно на сегодняшний день, основана на халатных или неумышленных действиях персонала компаний. А значит, основная задача для обеспечения защиты бизнеса сводится к минимизации угроз, источником которых является Интернет. Эффективное противодействие веб-атакам обеспечивается только на уровне шлюза. Выбираемый продукт должен «уметь» блокировать коммуникации вредоносных приложений с их управляющими серверами, обеспечивая тотальный контроль над входящим и исходящим интернет-трафиком. Каналы передачи данных, которые вы не можете контролировать, в интересах политики информационной безопасности необходимо запретить (например, неавторизованное туннелирование в HTTP).

Решения, сочетающие в себе описанные выше возможности с технологиями выявления и блокирования всех типов современного вредоносного кода в момент попытки загрузки, позволяют достичь высокого уровня защиты информационных ресурсов от компрометации, нарушения целостности и утечки конфиденциальных данных.

Объединение технологий контентной фильтрации с решениями класса DLP позволяет добиться синергетического эффекта в построении многоуровневой системы противодействия утечкам конфиденциальной информации. Для решения таких задач недавно Aladdin и InfoWatch объявили о стратегическом сотрудничестве, в основе которого — разработка единой платформы для защиты конфиденциальных данных от утечки по внешним каналам (Интернет, электронная почта) и непосредственно с рабочих мест, то есть защита от инсайдеров. Объединение наших усилий позволит предложить рынку уникальный продукт для контроля входящего и исходящего почтового, а также веб-трафика. А главное, он сможет анализировать в том числе шифрованный трафик, передающийся по HTTPS-протоколу, что позволит перекрывать все возможные каналы утечки информации, независимо от попыток замаскировать несанкционированные действия с помощью различных инструментов преодоления систем безопасности.

Кроме того, эффективно бороться с инсайдерами невозможно без системы управления доступом пользователей к информационным ресурсам. Следовательно, для защиты конфиденциальной информации необходимо прежде всего обеспечить надежные механизмы идентификации и аутентификации. По сути, выбирая метод аутентификации при доступе к данным, вы фактически выбираете уровень защиты информационной системы. Если это пара «логин/пароль», то утечка данных — всего лишь вопрос времени. Лучшей практикой было и остается применение специализированных аппаратных устройств для аутентификации, архитектура которых базируется на микросхеме смарт-карты (USB-токены или собственно смарт-карты).

Для защиты конфиденциальной информации «классикой» является применение стойких криптографических алгоритмов шифрования, независимо от того, где эта информация хранится и обрабатывается: на ноутбуке, на рабочей станции или на сервере. Решений для шифрования данных на рынке сегодня представлено достаточно: лучшие из них объединяют технологии аппаратной аутентификации (не опционально, а в обязательном порядке) и шифрования данных.