ежемесячный журнал деловое совершенство #8 2009

Business Excellence

Дмитрий Гришин

генеральный директор Mail.Ru

Главное — не упустить время!

ISSN 1813-9485

Алексей Миняйло

Top secret

Всего двадцать лет назад методы защиты информации отличались от современных примерно так же, как первый IBM PC от мощных персональных компьютеров последней модели. И это закономерно: развитие техники привело к тому, что почти вся информация была переведена в электронный вид. А защитить ее теми же способами, что и бумажные папки, попросту невозможно. Если к «спецхрану» достаточно было приставить милиционера, то как быть в случае обеспечения контроля над содержимым сотен и даже тысяч компьютеров, входящих в локальную сеть предприятия? О мыслимых и немыслимых способах защиты от всевозможных нарушителей информационной безопасности специально для читателей Business Excellence рассказывает Наталья Касперская, председатель совета директоров «Лаборатории Касперского» и генеральный директор компании InfoWatch.

Невидимая война

Долгое время считалось, что основная угроза для информации компаний — это хакеры, пытающиеся получить доступ к базам данных и другой ценной информации. Но постепенно и предприниматели, и разработчики программного обеспечения пришли к осознанию того, что самый опасный канал утечек — внутренний. То есть неосторожные или злонамеренные действия сотрудников компании. Например, знаменитый хакер Кевин Митник предпочитал не тратить недели на вычисление кодов доступа, а порыться в помойке возле главного офиса своей жертвы: настолько часто важнейшие пароли просто выбрасывали в мусорное ведро. И тот же Митник, устроившись оператором ЭВМ в компанию Great American Merchandising, украл у компании данные о банковских счетах тысяч людей.

— Для многих предприятий внутренняя информационная безопасность сегодня выходит на первый план просто потому, что защита от внешних угроз (хакерских атак и вирусов) уже обеспечена на 99%, — говорит Наталья Касперская. — А защита от внутренних информационных рисков по-прежнему либо полностью отсутствует, либо находится на очень низком уровне. Ведь решений, которые обеспечивали бы конфиденциальность данных внутри компании, до недавнего времени просто не было на рынке. «Лаборатория Касперского» стала первой в России компанией, выпустившей программу защиты от утечек, — а это произошло лишь в 2002 году. В 2001-м мы разрабатывали программу защиты от спама Kaspersky Anti-Spam и подумали: если умеем фильтровать информацию, которая приходит в компанию, то почему бы не фильтровать исходящие данные? И уже в 2002 году мы написали пилотную версию, а первый коммерческий продукт вышел в начале 2003 года.

К этому времени проект стал достаточно крупным, и в декабре 2003 года «Лаборатория Касперского» основала ЗАО «Инфовотч». Большинство продуктов InfoWatch ориентированы на крупные предприятия, но про малый и средний бизнес в компании тоже не забывают. В 2009 году была выпущена программа по обеспечению информационной безопасности на малых и средних предприятиях, рассчитанная на 50—500 рабочих станций. Помимо программ предотвращения утечек, в InfoWatch разрабатывают и другие системы защиты данных, например, криптографические програм-

INFOWATCH

InfoWatch

Инновационная компания, разрабатывающая технологии для новой области информационной безопасности — защиты от внутренних угроз. В сферу компетенции компании входит минимизация риска утечки, уничтожения данных, саботажа, промышленного шпионажа и других неправомерных и неосторожных действий сотрудников в отношении корпоративной информации. InfoWatch была основана в ноябре 2003 года и является дочерней компанией «Лаборатории Касперского».

мы, защищающие данные на мобильных устройствах в случае их утери или кражи.

За семью печатями

— Пока что украсть информацию изнутри гораздо проще, чем извне, — говорит Наталья Касперская. — Но это ненадолго, — улыбается она. — Например, один из наших клиентов поймал шпиона сразу же после установки Traffic Monitor[1]. Этот человек регулярно скачивал секретные данные и продавал их на сторону.

В первую очередь обеспечить безопасность данных стараются компании, обладающие секретной или конфиденциальной информацией: данными о клиентах, ноу-хау или персональными данными. Соответственно наибольший интерес к программам защиты от внутренних угроз проявляют банки, нефтяные компании, юридические компании и медицинские учреждения.

Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных» обязывает все компании, обладающие персональными данными граждан, обеспечить защиту этих данных от «неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий».

— Мы предотвращаем кражу или потерю информации, перекрывая основные каналы утечек. Большинство утечек случайные: секретарь отправил конфиденциальный документ на неверный адрес электронной почты; сотрудник распечатал секретную информацию и не забрал ее из лотка принтера, а уборщица выбросила эти листы в урну; потерялся диск с базой данных. Ущерб от таких случайностей может исчисляться миллиардами долларов. Но гораздо опаснее преднамеренная кража информации сотрудником компании. Хотя и здесь можно поставить надежные барьеры — например, заблокировать доступ к конфи-

[1] Флагманский продукт компании.

денциальной информации, ее печать, копирование на цифровые носители или пересылку через интернет.

Программы по защите от внутренних угроз фильтруют информацию с помощью нескольких технологий. Первая и самая важная — это лингвистический анализ. Он ищет в документах определенные слова или группы слов, которые содержатся в конфиденциальных документах. Вторая технология — это так называемый копирайтный анализ. Суть его заключается в том, что с конфиденциального документа снимается цифровой «слепок», по которому можно отследить использование этого документа или его части. И третья технология — это детектор объектов, который на основе ряда характеристик помечает определенные типы документов как секретные. Например, если в документе содержится массив данных в виде «12 цифр, фамилия, дата», то программа определяет этот документ как базу данных по кредитным картам и перекрывает доступ к этому файлу всем, кто не обладает необходимыми полномочиями.

Без качества — никуда

За пять с половиной лет своего существования компания стала абсолютным лидером российского рынка в своей области. По данным за 2008 год, доля ЗАО «Инфовотч» составила 70% от общего объема рынка решений в области защиты от внутренних угроз. Выручка компании за 2008 год составила около 5 млн долларов. В числе клиентов такие компании, как «Вымпелком», «ВТБ», «РусГидро», Федеральная таможенная служба и другие. Помимо этого, программные продукты InfoWatch успешно вышли на рынки европейских стран.
И немецкая версия Traffic Monitor — единственная в мире программа, умеющая анализировать немецкую морфологию.

Наталья Касперская

Родилась 5 февраля 1966 года.

В 1989 г. окончила Московский институт электронного машиностроения (МИЭМ) по специальности «Прикладная математика».

В 1994 году пришла на работу в НТЦ «Ками», где возглавила антивирусный проект AVP. В 1997-м стала одним из основателей и генеральным директором «Лаборатории Касперского». Летом 2007 года была избрана на пост председателя совета директоров «Лаборатории Касперского». В октябре 2007 года Наталья Касперская стала генеральным директором компании InfoWatch — разработчика систем защиты конфиденциальной информации от внутренних угроз.
В 2008 году заняла 4-е место в рейтинге влиятельных деловых женщин России, а также получила награду «Предприниматель года в области ИТ» от компании Enrst&Young.

Свободно владеет английским и немецким языками. Имеет степень бакалавра бизнеса Открытого университета Великобритании. Увлекается игрой на гитаре, горнолыжным спортом, туризмом, чтением профессиональной литературы, любит путешествовать в компании друзей и детей.

Все это произошло не вдруг. Но выводить стартовые проекты в лидеры Наталье Касперской не впервой. Двенадцать лет назад она встала во главе только что созданной «Лаборатории Касперского» и была ее бессменным руководителем до 2007 года. За это время антивирусные продукты лаборатории завоевали рынки всего мира. В InfoWatch уверены, что то же самое произойдет и у них. Но на вопрос о причинах успеха Наталья отвечает очень скромно: все лавры отдает команде.

— Я стараюсь собрать вокруг себя людей, которые лучше и умнее меня. Чего-то добиться можно, только опираясь на сильную команду. Хорошая команда — это самоходный аппарат: только бензин вовремя заливай, а все остальное люди сделают сами. В нашей стране очень распространен авторитарный стиль руководства, когда начальник говорит: «Я четко знаю, что нужно делать. Я вам поставлю задачи, выполняйте». А я очень редко ставлю перед подчиненными какие-то задачи. Я могу только сказать цель, например выйти на европейский рынок. А список задач человек составляет уже сам, и мы его обсуждаем вместе. Иначе невозможно, ведь у нас интеллектуальный бизнес, и каждый сотрудник должен чувствовать, что он важен и способен горы свернуть.

Но даже с сильной командой единомышленников трудно свернуть горы, не уделяя внимания качеству. Поэтому в InfoWatch организована строгая система контроля качества.

— А как же? Без качества — никуда, — говорит Наталья Касперская. — У нас есть строгие критерии по качеству выпускаемого продукта, и если продукт им не соответствует, он отправляется на доработку. Для нас важно соблюдение высокого уровня качества и в обслуживании клиентов. Сейчас кризис, и некоторые клиенты перестали оплачивать техническую поддержку. Мы продолжаем их обслуживать, ведь, несмотря на кризис, это наши клиенты, и мы несем за них ответственность.

TOP-5 самых громких утечек

1. Август 2007 года. Сотрудник ядерной лаборатории в Лос-Аламосе (США) украл сверхсекретную информацию и переслал ее по электронной почте. Утечка классифицирована как серьезная угроза ядерной безопасности США.
2. Июль 2007 года. Инспектор по контролю качества компании Boeing скачал на флэшку 300 тыс. секретных документов с целью продажи. По приблизительным подсчетам, потери компании составили 15 млрд долларов.
3. Ноябрь 2007 года. В Великобритании утеряны два диска государственного управления по налогам и таможенным пошлинам с конфиденциальными данными о 25 млн человек. Последствия инцидента оцениваются в 3 млрд долларов.
4. Август 2008 года. Хакеры украли персональные данные и номера кредитных карточек 8 млн человек, взломав базу данных компании Best Western Hotel group. Убытки компании оцениваются в 2 млрд 147 млн долларов.
5. Ноябрь 2007 года. Два сотрудника Doosan Heavy Industries and Construction продали компании STX Heavy Industries информацию, представлявшую коммерческую тайну и оценивающуюся в 1,8 млрд долларов. С помощью этой информации STX выиграла четыре тендера на общую сумму в 2,2 млрд долларов.