ЗАЩИТА ОТ ИНСАЙДЕРА

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ПОЯВИЛИСЬ ПРАКТИЧЕСКИ ОДНОВРЕМЕННО С ШИРОКИМ РАСПРОСТРАНЕНИЕМ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ. ОДНАКО О СЕРЬЕЗНОСТИ УГРОЗЫ УТЕЧЕК ИЛИ УТРАТЫ ИНФОРМАЦИИ В РЕЗУЛЬТАТЕ ДЕЙСТВИЙ ИНСАЙДЕРОВ СПЕЦИАЛИСТЫ СТАЛИ ВСЕРЬЕЗ ЗАДУМЫВАТЬСЯ ТОЛЬКО НЕСКОЛЬКО ЛЕТ НАЗАД. А В ПОСЛЕДНЕЕ ВРЕМЯ ЧУТЬ ЛИ НЕ ЕЖЕМЕСЯЧНО СТАНОВИТСЯ ИЗВЕСТНО О ПОЯВЛЕНИИ В ПИРАТСКОЙ ПРОДАЖЕ БАЗ ДАННЫХ С КОНФИДЕНЦИАЛЬНЫМИ ДАННЫМИ О ГРАЖДАНАХ И КОМПАНИЯХ, «УТЕКШИХ» ИЗ ГОСУЧРЕЖДЕНИЙ И БАНКОВ. АНДРЕЙ ВИНОКУРОВ

НЕОБХОДИМОЕ ВО ЗЛО Традиционным подходом к борьбе с утечками являются организационные меры и запретительные политики: отключение на компьютерах сотрудников коммуникационных портов, доступа к определенным сайтам; запрет на пользование открытыми почтовыми службами и программами мгновенного обмена сообщениями. Нередки ситуации, когда с компьютеров служащих банка вообще нет доступа во «внешний мир», за исключением корпоративной электронной почты.

Как показывает практика, такие меры не всегда работают. Во-первых, глобальные запреты могут серьезно влиять на производительность: сотрудники из-за ограничений просто не могут получить доступ к нужной им информации или он затруднен. Во-вторых, принцип «все запретить» обычно не может защитить от действий злонамеренных инсайдеров, допускающих утечку данных не по ошибке, а сознательно. Компания, полагаясь на политику общего запрета, не контролирует действия с информацией внутри охраняемого периметра, а в политике запретов всегда есть послабления, вызванные производственной необходимостью.

«Если запретить все опасное и разрешить только самое необходимое (почта, интернет), но не обеспечивать контроль и аудит, например архивирование всего почтового и веб-трафика для ретроспективного анализа инцидентов, подготовки доказательства вины и соответствия требованиям нормативных актов, то данные все равно будут утекать»,— говорит Денис Зенкин, директор по маркетингу компании InfoWatch.

Полностью предотвратить утечки невозможно никакими техническими и организационными мерами — благодаря распространению персональных цифровых устройств любые документы, к которым имеет доступ широкий круг лиц, могут покинуть пределы компании, вопреки желанию ее руководителей. Сейчас трудно встретить мобильный телефон без встроенной цифровой камеры, и, в конце концов, нелояльный сотрудник может просто сфотографировать открытый на экране ПК или лежащий на столе документ.

Однако наибольший финансовый и репутационный урон наносят компаниям утечки больших объемов данных, например баз данных клиентов с информацией о банковских картах (которые затем могут быть использованы для кражи денег с банковских счетов) или сведений о заемщиках банка, включая их персональные данные.

Совсем недавно для специалистов по ИТ-безопасности стала очевидной потребность в специализированных решениях проблемы защиты критически важных данных от инсайдеров.

Защита от непреднамеренного или умышленного распространения конфиденциальных данных за пределы организации требует комплексного подхода: определения защищаемых данных, разработки политики ИТ-безопасности, обучения сотрудников, учета всех возможных каналов утечек. При создании полномасштабной системы информационной безопасности следует учитывать не только все возможные способы совершения внутренних атак и пути утечки информации.

НИКАКАЯ ЗАЩИТА НЕ СПАСЕТ ОТ ПРЕСЛОВУТОГО ЧЕЛОВЕЧЕСКОГО ФАКТОРА

AFP/GURTERIMAGES

Технически утечка может произойти по множеству каналов: через корпоративный почтовый сервер с помощью электронной почты, через интернет-канал при использовании бесплатных почтовых систем или веб-служб для размещения файлов, посредством беспроводных подключений (Wi-Fi, Bluetooth) через принтер — при физической печати документов, а также через мобильные носители: дискеты, оптические диски или мобильные накопители.

КОРНЕВЫЕ СИСТЕМЫ Программные и аппаратные средства, предназначенные для борьбы с этими утечками, аналитики IDC нарекли ILD&P-системами (Information Leakage Detection and Prevention).

ILD&P-решения — молодой рынок. Его развитие началось несколько лет назад с небольших компаний-стартапов, получивших венчурные инвестиции. Поэтому стандарты архитектуры специализированных решений защиты от утечек и злонамеренных действий инсайдеров пока не сформировались, и каждый производитель доказывает оптимальность именно своего подхода. Многие системы, представленные на рынке, развивались из специализированного ПО — например, софта для управления коммуникационными портами ПК или систем контроля доступного в корпоративной сети веб-содержимого.

За последние несколько лет крупнейшие производители антивирусов дополнили список своих продуктов не только файрволлами и решениями для борьбы со спамом, но и продуктами ILD&P. Например, компания McAfee в конце 2006 года приобрела израильский стартап Onigma и включила разработанную им систему предотвращения утечек данных в состав своих корпоративных решений.

Другой крупнейший производитель ПО в области информационной безопасности, Symantec, самостоятельно разрабатывает Symantec Database Security, контролирующий доступ пользователей к базам данных, содержащих критически важную информацию. А компания Websense, специализирующаяся на продуктах для контроля доступа к веб-содержимому, приобрела разработчика ПО PortAuthority, получив возможность предлагать клиентам комплексное решение по защите доступа к данным. Российский производитель InfoWatch, являясь дочерней компанией производителя антивирусов «Лаборатория Касперского», интегрирует свои продукты с корпоративными решениями AVK.

Целый ряд компаний предлагает ILD&P-системы, основой которых являются специальные программные агенты, устанавливаемые на компьютеры пользователей корпоративной сети. Например, продукт Sanctuary Device Control компании SecureWave позволяет системно контролировать доступ пользователей к интерфейсам USB, LPT, FireWire, Bluetooth, Wi-Fi, IrDA, PCMCIA, COM, IDE, SATA, поддерживая централизованное управление разрешениями и ведение журналов.

Программные агенты PC Activity Monitor (Acme) компании Raytown Corp. устанавливаются на все компьютеры корпоративной сети и внедряются в операционную систему на уровне ядра, что не позволяет пользователю отключить или обойти их (следует отметить, то Microsoft заблокировала возможность модификации ядра в ОС Windows Vista). Все действия пользователя по печати, копиро-

СОВСЕМ НЕДАВНО СПЕЦИАЛИСТАМ ПО ИТ-БЕЗОПАСНОСТИ СТАЛА ОЧЕВИДНА ПОТРЕБНОСТЬ В СПЕЦИАЛИЗИРОВАННЫХ РЕШЕНИЯХ ПРОБЛЕМЫ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ДАННЫХ ОТ ИНСАЙДЕРОВ