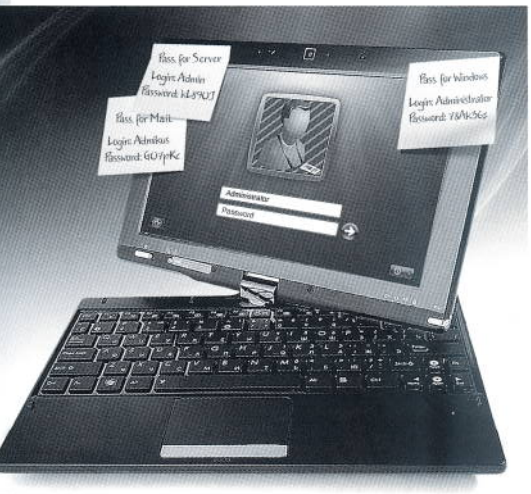
Мнимая безопасность

А. Комаров, *начальник отдела маркетинга Компания SafeLine*

Человек так устроен, что собственные субъективные ощущения склонен воспринимать порой как объективную данность. В области информационной безопасности такие ситуации возникают вряд ли реже, чем в любой другой.



Скажем, придумал человек длинный пароль и использует его на протяжении нескольких лет подряд на всех сервисах, где только ни регистрируется. Каждый из его аккаунтов на сайтах сам по себе находится в достаточной степени безопасности, а вот в целом ситуация далеко не безопасная. Достаточно компрометации всего одного сайта (а кто знает, как в конкретном сетевом сервисе реализована работа с паролями пользователей – быть может, они все лежат в открытом виде?) – и под угрозой оказывается абсолютно все, что защищено этим паролем.

Другой пример: системный администратор поставил межсетевой экран, долго возился с его настройками (предположим, ему досталось не современное UTM-устройство, настраиваемое через web-интерфейс «двумя кликами», а самый обычный широко распространенный межсетевой экран), редактировал конфигурацию, подбирал нужные параметры и выставлял правила, а сменить пароль администратора по умолчанию забыл. Казалось бы, система под надежной защитой, а на практике это не так, ведь этот пароль любой злоумышленник проверит первым или вторым после «qwerty».

Можно привести множество таких примеров из самых разных областей информационной безопасности, поэтому проблема, очевидно, актуальна и, что называется, «стоит остро».

Действительно надежная защита должна быть комплексной, многокомпонентной и учитывать все нюансы как реальной сетевой инфраструктуры, так и особенностей процессов внутри конкретной организации. При всей очевидности этого утверждения поражает, как часто на практике про данное правило забывают, ограничиваясь поверхностным рассмотрением проблем и моделированием угроз лишь на самом общем приближенном уровне.

Особое внимание хотелось бы обратить на процесс внедрения систем предотвращения утечек (DLP – Data Loss Prevention), стремительно набирающих популярность в последнее время. Принцип работы таких систем достаточно прост: определить данные, которые нельзя отправлять за пределы компании и пресекать/фиксировать действия пользователей, нарушающие этот запрет.

Вендоры совершенствуют свои продукты, встраивают поддержку новых языков (русский, украинский, албанский), реализуют механизмы контроля новых каналов утечек (Skype, социальные сети, торренты) и расширяют функционал своих систем. Интеграторы рапортуют об успешных проектах и новых крупных внедрениях.

Конечно, на рынке есть ограниченное количество действительно серьезных игроков, профессионально подходящих к контролю утечек и качественно реализующих проекты на высоком уровне. К сожалению, для большинства организаций (небольших, муниципальных и т. п.), услуги этих профессионалов стоят дорого, хотя, безусловно, они того стоят.

Вместе с тем, на рынок широким потоком хлынули, с позволения сказать, недоDLP, выросшие из систем контроля подключения внешних устройств или вообще клавиатурных шпионов (кейлоггеров). Проблема практической неэффективности большинства из них заключается в том, что в вопросах борьбы с инсайдерами никоим образом нельзя обойтись чисто техническими мерами. В конце концов, у сотрудника, имеющего легальный доступ к конфиденциальному документу и инструментам для его редактирования, есть неограниченное количество способов его модификации: перестановка и замена символов, примешивание дополнительных символов или,

наоборот, удаление их части без потери смысла и т. д. Все эти методы можно комбинировать (а ведь были приведены только самые примитивные), и как бы ни старались разработчики, неконтролируемый вариант все равно можно подобрать.

Производители антиспама много лет решают схожую проблему, вот только задача злоумышленника в этом случае – не отправить сообщение вовне, а наоборот, преодолеть рубеж защиты и оказаться в почтовом ящике пользователя. Практически любой человек, глядя на письмо, легко распознает в нем спам, а вот «машина» качественно это делать до сих пор так и не научилась.

С другой стороны, даже просто проверить все возможные комбинации модификаций в режиме реального времени нереально. Включение полного анализа существенно увеличит нагрузку на систему мониторинга и внесет временные задержки в коммуникации, допустимые до определенного предела, например, для электронной почты, но невозможные в тех же службах мгновенного обмена сообщений.

Рекламные материалы таких разработчиков уверяют клиентов в полной и комплексной защите от любых утечек по любым каналам, рождая то самое чувство мнимой безопасности. Определенно, что-то таким механическим способом выявить можно, но для настоящей борьбы со злонамеренными сотрудниками необходимо работать, прежде всего, с живыми людьми. Регулярное повышение осведомленности, четкое осознание сотрудниками политик безопасности, понятные регламенты и инструкции, мониторинг атмосферы в коллективе – вот примеры человеко-ориентированных подходов к борьбе с инсайдерами.

Не стоит забывать: зачастую работодатель даже не может четко сформулировать, чего конкретно он опасается. Да, существуют некоторые общие фильтры: «поиск работы», «нарушения закона» и т. д., но нет фильтра «я знаю что-то о коллеге и вымогаю у него деньги» или «я использую рабочую информацию для целей собственного бизнеса», вернее, их можно попытаться создать, но не факт, что они сработают, уж слишком разными могут оказаться ситуации.

На практике даже реально работающие DLP-системы нередко используются просто для слежки за конкретным сотрудником. Он может вызвать подозрение теми или иными действиями или просто находиться в зоне риска в силу своего статуса (испытательный срок, повышение в должности его коллеги, а не его самого и т. д.). Возникает естественное желание присмотреться к такому сотруднику поближе, но сделать это может только человек, никакими алгоритмами и анализами выявить угрозу для компании не представляется возможным, по крайней мере, до того момента, когда он начнет действовать.

С учетом всего вышеизложенного весьма сомнительной представляется целесообразность для средних и небольших организаций внедрять системы DLP. Автоматический поиск, который настраивать, очевидно, должны профессионалы, чьи услуги не могут стоить дешево, хорош в случае большого числа сотрудников и наличия достаточной статистики их поведения: в компании из пяти человек аномальным будет поведение всех сотрудников.

На рынке существуют решения, очень близкие к DLP, но не позиционирующие себя таковыми. Речь идет о системах мониторинга действий пользователей в корпоративной сети (UAM – User Activity Monitoring). Разумная ценовая политика, простота внедрения (все работает уже из коробки) и использования (интерфейс понятен и не требует специального обучения) делает такие решения выгодным вложением инвестиций для компаний, где нет тысяч сотрудников.

Современные системы мониторинга далеко ушли от простого просмотра рабочего стола в реальном времени или записи всех нажатых клавиш. Фильтры по типам событий, именам файлов и окон, приложениям и т. п. позволяют гибко настраивать систему и быстро просматривать только действительно важную информацию о действиях сотрудников.

Развитая система отчетности, аналитика и построение диаграмм и графиков тоже помогают в выявлении злоумышленников на самых ранних стадиях, полностью оправдывая извечную мудрость: профилактика – лучшее лечение.

Многие UAM-системы позволяют наблюдать за сотрудником в режиме реального времени, строить комплексные отчеты о времени работы и используемых приложениях по отдельным пользователям либо по их группам. Такие отчеты позволяют оценить общую эффективность работы сотрудников, например, выявить «трудоголиков» и «лентяев», часто опаздывающих «сов» или любителей разложить пасьянс. Полезен и функционал выявления аномалий в поведении сотрудников: возросший трафик, нестандартное время работы и т. д.

В итоге человеческий фактор выходит на первое место, потому что именно хороший руководитель может понять, что творится в его коллективе, кто из его сотрудников способен стать (или уже стал) инсайдером. Ведь DLP-системы борются уже со следствием, а не с причиной. Вместе с тем, хорошо известно, что профилактика необходима не только в случаях, когда речь идет о здоровье.

Вполне достаточно обратить внимание на поведение сотрудника, который вызывает подозрение. Причем для этой цели DLP-системы, фиксирующие только факт (или попытку) осуществления утечки, приспособлены мало, а вот системы мониторинга действий пользователей в корпоративной сети, предназначенные для фиксации того, чем занимается пользователь, подходят как нельзя лучше.

Безагентские варианты таких систем анализируют лишь сетевой трафик или используются исключительно для мониторинга, не пытаясь ничего блокировать. Однако для осуществления полного контроля на рабочие места устанавливаются (чаще – скрытно) агенты, дополнительно отслеживающие файловые операции, нажатия клавиш и пр. Причем они могут вмешиваться в действия пользователя и запрещать те из них, которые не соответствуют корпоративным политикам. ■