ров, планы. DLP-система зафиксировала попытку скачать документы на внешний носитель, и крупной утечки удалось избежать. Однако клиент все же увидел данные, к которым доступ не должен был иметь», — вспоминает председатель совета директоров «СёрчИнформ».

Человеческая неосмотрительность и неаккуратность — главные причины бед, уверен Алексей Смирнов. «Иногда люди по ошибке или из лени могут сами отправлять всю важную секретную информацию. Например, прикрепить к письму документ, включающий в себя весь массив секретной информации, вместо того, чтобы проработать материал и выборочно отправить необходимые данные», — иллюстрирует он.

Вячеслав Медведев из компании «Доктор Веб» удивляется, что взломов и утечек происходит так мало: по его оценке, 96% компаний не имеют понятия о современных угрозах, более 80% сайтов уязвимо, все основные системные приложения имеют незакрытые прорехи. «Неквалифицированные системные администраторы, не соблюдающие базовые принципы безопасности; пользователи с административными правами, игнорирующие все правила безопасности; хакеры, действия которых принципиально не замечаются по полгода. И руководство, срезающее затраты на безопасность и обновление инфраструктуры и сокращающее квалифицированный персонал», — перечисляет он человеческие факторы.

Все проблемы в безопасности происходят из-за людей, категоричен технический директор LiveTex Сергей Ельцов. «Есть такой базовый принцип: безопасность обратно пропорциональна удобству, чем безопаснее — тем неудобнее. Поэтому важна взвешенная оценка рисков и грамотная работа с людьми. Они не любят жертвовать комфортом в работе, и если не разъяснить им причины ограничений, методика запретов будет плохо работать», — объясняет господин Ельцов.

ТРЕНИРОВКА ОСМОТРИТЕЛЬНОСТИ

Нередко причина утечки информации кроется в желании сотрудников поработать дома или в пути. Тут, по мнению Вячеслава Медведева, не обойтись без защиты личных устройств и обучения сотрудников основам компьютерной безопасности. «Есть еще один резон, по которому люди используют личные устройства: это неудобство сервисов компании, их излишняя закрытость. Например, когда чиновники различных уровней ведут служебную переписку с внешней почты — в итоге происходят громкие утечки информации. Незрелость корпоративного софта и неудобство его для сотрудников — во многом следствие низких зарплат исполнителей, создающих эти сервисы, и того, что заинтересованные лица организации не участвуют в процессе их разработки. В результате могут рождаться монстры ни для кого», — рассказывает господин Медведев.

По статистике Positive Technologies, в среднем до трети сотрудников открывают письма с вложениями, способными заразить их компьютеры, при этом для успешной атаки достаточно открытия всего одного. «Снизить риски угроз информационной безопасности позволяет обучение персонала. Компании должны регулярно проводить для сотрудников профильные семинары, курсы, тренинги и тестирования, на которых персоналу передают специализированные знания по актуальным угрозам ИБ, объясняют последовательность действий при подозрениях на атаки», — настаивает Алексей Качалин.

Большая часть ошибок совершается по незнанию или из лени, поэтому задача компании — правильно мотивировать людей, описывать ИБ-проблемы понятным языком с живыми примерами, уверен Сергей Ельцов. В его компании принято устраивать небольшие обучающие провокации для коллег: «Мы расклеиваем в офисе QR-коды, ведущие на специально созданные фишинговые ресурсы, оставляем флешки „с сюрпризом“, а затем исследуем реакцию сотрудников», — рассказывает технический директор LiveTex.

В просвещении сотрудников по вопросам информационной безопасности большую роль играет HR-отдел: обычно он берет на себя проведение тренингов и контроль прохождения всеми сотрудниками необходимой учебы. Служба безопасности привлекается только при дознании по конкретным инцидентам, а также входит в состав группы аудиторов, когда требуется осмотр рабочих мест сотрудников.

Исторически сложилось, что курировать службу безопасности в российских компаниях приходят бывшие работники силовых структур. Их бесспорным преимуществом директор регионального представительства компании Falcongaze в Санкт-Петербурге Валентин Калаша называет опыт оперативно-разыскной работы и связи. «Но для решения вопросов информационной безопасности они порой не так компетентны, как хотелось бы. К счастью, ситуация сейчас выправляется, а организации начинают все большее внимание уделять технологическим аспектам защиты конфиденциальных данных», — наблюдает эксперт.

Старший менеджер группы по оказанию услуг в области управления информационными рисками КПМГ в России и СНГ Илья Шаленков рекомендует HR-отделам и службам безопасности совместно вырабатывать подходящую для конкретной компании систему поощрений и ответственности: без нее обучающие программы просто не будут работать, поскольку у сотрудника не будет мотивации запоминать материал, который якобы не касается напрямую его рабочих процессов.

УКРЕПЛЯЮЩИЕ СРЕДСТВА

Поскольку риски ИБ не до конца понятны для бизнеса, чаще всего инвестиции в эту область начинаются после инцидента и представляют собой латание дыр, признает руководитель отдела консалтинга центра информационной безопасности компании «Инфосистемы Джет» Андрей Янкин. «В итоге системы безопасности многих компаний — как лоскутное одеяло с множеством прорех. Система ИБ в компании похожа на иммунную систему организма, которая должна непрерывно перестраиваться, чтобы давать отпор новым атакам. Поэтому технологии тут обновляются за три-пять лет более чем наполовину», — говорит господин Янкин.

Сергей Ельцов называет хорошей практикой тратить определенный процент IT-бюджета на информационную безопасность. В среднем, по его оценке, это 15–20%. Эти деньги идут на закупку и обновления средств защиты информации; на развитие специалистов службы ИБ; на проведение внешних аудитов; на тестирование на возможность проникновения зловредов.

Акцент при распределении ресурсов зависит от отрасли: ритейл вкладывается в первую очередь в защиту интернет-коммерции, производственные предприятия защищают АСУ ТП, банки — АБС и другие системы, обслуживающие платежные процессы. Государственный сектор сосредоточен на выполнении требований регуляторов.

Алексей Смирнов из Orange Business Services рекомендует раз в полгода проводить пен-тесты (penetration-test). «Постоянно появляются новые методы нападения, нужно всегда понимать, насколько ты уязвим. Стоимость такой услуги зависит от длительности и активности совершаемой атаки. Специалисту по кибербезопасности указывают мишени, уязвимость которых необходимо проверить, и он последовательно атакует их, выявляя бреши. На основании этого теста составляется отчет с рекомендациями по укреплению систем безопасности», — делится господин Смирнов.

На тот случай, если компания выдает своим сотрудникам телефоны, планшеты, ноутбуки для работы вне офиса, эксперт советует применять меры Enterprise Mobility Management — системы, которые позволяют удаленно настраивать и отслеживать соблюдение политики безопасности на мобильных устройствах.

Специалисты КПМГ призывают с осторожностью относиться к новым веяниям в области информационной безопасности. «По нашему опыту, гораздо эффективнее и дешевле начинать налаживать внутренние процессы безопасности в организации по международным стандартам, „написанным кровью“ множества компаний, чем внедрять средства, обещающие комплексную защиту от хакеров», — заключает Илья Шаленков. ■

ПЕРЕБИРАЯ ЛЕНТЫ

РЕДАКТОРЫ ПЕЧАТНЫХ НОВОСТНЫХ ИЗДАНИЙ ТЕШАТ СЕБЯ МЫСЛЬЮ, ЧТО «БУМАГА» — СТАТУСНЫЙ ПРОДУКТ, И ЛИСТАТЬ ГАЗЕТУ УТРОМ С ЧАШЕЧКОЙ КОФЕ — ЛЮБИМОЕ ЗАНЯТИЕ ГЕНДИРЕКТОРА. НА ДЕЛЕ, ДАЖЕ ЕСЛИ ЧЕЛОВЕК ВЕРЕН ТРАДИЦИОННЫМ ДЕЛОВЫМ ИЗДАНИЯМ, В ДЕНЬ У НЕГО НАЙДЕТСЯ ОТ СИЛЫ ДВАДЦАТЬ МИНУТ, ЧТОБЫ ПРОБЕЖАТЬСЯ ПО ЛИДАМ СТАТЕЙ В ИХ ЭЛЕКТРОННОЙ ВЕРСИИ, И КАРТИНУ ДНЯ ОН СОСТАВИТ ПО СООБЩЕНИЯМ НА «ПРОВОДАХ». НЕКОТОРЫЕ И ВОВСЕ ПРЕДПОЧИТАЮТ ОФИЦИАЛЬНОЙ ПРЕССЕ СОЦСЕТИ И ОТРАСЛЕВЫЕ САЙТЫ. ВЛАДА ГАСНИКОВА

Ежедневные новости руководители бизнеса узнают на сайтах «Коммерсанта», «Ведомостей», РБК, «Медузы», «Форбса», «Эксперта», «Ленты» и «Газеты.ру». Свое доверие этим ресурсам они объясняют тем, что видят качественную работу авторов и фотографов, готовность проверять источники информации, на которые ссылаются журналисты, глубину аналитики и полярность взглядов экспертов.

Новостные ленты бизнесмены в течение дня пролистывают по несколько раз, заодно отслеживая курс валют. «Электронные версии „Коммерсанта“ и „Ведомостей“ просматриваю утром по пути на работу. Как все современные деловые люди, у которых проблема со временем, выхватываю заголовки и статейные лиды, редко что-то читаю целиком», — рассказывает заместитель генерального директора страхового общества «Помощь» Ольга Родионова.

Руководитель петербургского филиала QBF Алексей Голубев затрудняется назвать ресурс, который сегодня способен дать достаточно полную и объективную картину дня, поэтому он просматривает статьи по одной теме на Investing.com, Insider.pro, Finanz.ru, сайтах Forbes, Snob, «Ведомостей» и «Коммерсанта». «Как правило, чтению материалов этих порталов я посвящаю время в пути из дома на работу и обратно. Однако от каждого из них мне регулярно приходят оповещения о важных новостях. Если я вижу что-то очень значимое для инвестиционного бизнеса, читаю материал среди рабочего дня», — говорит Алексей Голубев. ➔ 26

ИНТЕРНЕТ-СМИ