ГОЛОВОТЯПСТВО СО ВЗЛО

ОЛЬГА КРАСИЛЬНИКОВА

Россия — страна с хорошо развитым рынком хакерских услуг, причем чаще «черных», нежели «белых». Стоимость взлома корпоративного сервера здесь начинается с $800. А беспечность многих российских компаний в вопросах информационной безопасности создает кибервзломщикам прекрасные условия для работы.

Согласно данным исследования «Информационная безопасность бизнеса», проведенного «Лабораторией Касперского» и B2B International в 2015 году, 95% организаций сталкивались с внешними киберугрозами в той или иной форме, при этом около половины из них теряли важную информацию или деньги.

Подлинный масштаб проблемы со стороны часто не виден, поскольку пострадавшие компании предпочитают по возможности не афишировать свои потери и слабость ИТ-систем. Но сведения о крупных потерях, понесенных бизнесом в результате действий киберпреступников, время от времени все-таки попадают в информационное поле. «В 2014 году, например, в результате целенаправленной атаки злоумышленников на платежную систему Qiwi было похищено 88 млн рублей», — говорит Алексей Коняев, старший консультант по противодействию мошенничеству компании «SAS Россия/СНГ». Относительно недавняя история — потеря казанским Энергобанком 234 млн рублей в ходе торгов на валютном рынке. 27 февраля этого года Центробанк РФ зафиксировал целую серию «странных» крупных сделок, совершенных Энергобанком, которые в течение нескольких минут привели к колебанию курса рубля почти на 15%. Регулятор даже заподозрил в этом либо сознательное манипулирование рынком, либо ошибку трейдеров банка. Впоследствии выяснилось, что в ИТ-систему банка удаленно проникли неустановленные лица и совершили от его имени неправомерные сделки по покупке и продаже валюты на бирже.

Ведущий аналитик отдела развития компании «Доктор Веб» Вячеслав Медведев сравнивает хакера с человеком-невидимкой, попавшим в чужую кварти-

ЮМ

ру: «Злоумышленник, проникший в корпоративную систему, может многое: перевести деньги со счета компании, зашифровать данные и потребовать выкуп, провести с компьютеров компании DDoS-атаку[1], заблокировать общение с партнерами и отправить им от вашего имени «заманчивое предложение», записывать ход совещаний. По сути, он получает все полномочия гендиректора, являясь при этом самозванцем».

ОБЛАКА ИЛИ ТУЧИ?

Бизнес все чаще использует облачные сервисы и предоставляет сотрудникам удаленный доступ в корпоративную сеть. Однако новые технологии несут не только новые возможности, но и угрозы. Мы начинаем так от них зависеть, что стоит киберзлоумышленникам вывести из строя, например, CRM-систему, как компанию разбивает настоящий операционный паралич: рушится взаимодействие не только между филиалами, но и отделами, которые трудятся бок о бок, теряется связь с клиентами, а удаленные сотрудники оказываются

1 *DDoS — аббревиатура от англ. distributed denial of service — «распределенный отказ в обслуживании». Суть такой атаки состоит в том, что сеть зараженных хакерами компьютеров (ботнет) начинает формировать такое число запросов на сервер-цель, что его функционирование в нормальном режиме становится невозможным. В результате пользователи интернет-ресурса не могут получить к нему доступ или доступ сильно затрудняется.*

БИЗНЕС И КИБЕРУГРОЗЫ В 2015 ГОДУ

95% компаний столкнулись с внешними угрозами, и около половины из них вследствие этого потеряли информацию или деньги.

23% заявили, что уже становились жертвами целевых атак.

37% потеряли конфиденциальную информацию благодаря незнанию сотрудниками правил ИТ-безопасности.

24% столкнулись с обнародованием конфиденциальной информации после хакерских атак.

55% считают самой большой угрозой вирусы-шифровальщики, вымогающие деньги.

76% хотя бы минимально позаботились о защите информации.

59% боятся в случае хакерской атаки потерять доступ к критически важной для бизнеса информации, 50% опасаются репутационного ущерба, а 34% — потери важных деловых контактов и бизнес-возможностей.

66% обращаются в случае хакерских атак к сторонним специалистам по информационной безопасности.

44% считают, что риски информационной безопасности в виртуальной среде ниже, чем в физической.

33% вообще не использует антивирусных продуктов в виртуальных средах.

Источники: «Лаборатория Касперского», B2B International

полностью изолированными. Показательным стал случай, произошедший в феврале 2016 года в США, в Голливудском пресвитерианском медицинском центре. Хакеры заразили компьютеры учреждения вирусом-шифровальщиком, из-за которого использовать CRM-систему стало невозможно, и потребовали выкуп в размере 40 биткойнов (примерно $17 тыс. по тогдашнему курсу). Все делопроизводство сразу же встало, медперсоналу пришлось вести записи с помощью ручки и бумаги, часть пациентов распределили по другим клиникам. Тогда не помогли ни ФБР, ни приглашенные эксперты по информационной безопасности; медцентру пришлось выплатить хакерам запрашиваемую сумму, чтобы система была разблокирована.

Оборотная сторона каждой новой технологии — новая потенциальная уязвимость системы безопасности. «Все чаще компании отказываются от собственных серверных мощностей и переносят свои информационные системы в ЦОДы и облачные сервисы, — отмечает Сергей Сошников, руководитель ИТ-отдела компании «Актив». — Одновременно растет потребность бизнеса в мобильности сотрудников и ведении разбросанных по всему миру контрагентов. Все это сильно влияет на информационную безопасность. Сегодня кибератаки чреваты для компании не просто материальным ущербом — они могут полностью уничтожить ее бизнес».

Помимо требования выкупа, хакеры используют множество других способов «монетизации» своих навыков. Например, стремятся получить доступ к компьютеру, где установлена программа «Клиент — Банк», чтобы взять под контроль управление счетами компании. «Затем они легко проводят мошенническую платежную операцию, похожую на настоящую, после чего форматируют систему, чтобы уничтожить все улики», — говорит Сергей Сошников.

Иногда целью хакеров становится информация: клиентские базы, данные по сделкам, техническая, юридическая или бухгалтерская документация. Ее перепродажа конкурентам может принести немалые барыши. А обнародование — нанести репутационный вред фирме-жертве.

Бизнес со значительной онлайн-составляющей особенно уязвим для DDoS-атак, от которых «падают» официальные сайты и коммуникационные сервисы компании и перестают работать личные кабинеты клиентов. Это приводит к замедлению работы веб-ресурса и ухудшению клиентского обслуживания, а также к незапланированным тратам на восстановление системы и репутации в глазах пользователей. Потери среднего и крупного бизнеса от одной DDoS-атаки, согласно исследованию «Лаборатории Касперского», обычно составляют от $50 до $440 тыс. Эксперты рынка информационной безопасности обычно включают Россию в Топ-5 стран мира по распространенности DDoS-атак.

Еще большей трагедией для онлайн-бизнеса может обернуться взлом корпоративного сайта с высокой посещаемостью — интернет-магазина или развлекательного ресурса. Злоумышленники таким образом получают доступ к персональной информации клиентов портала — номерам паспортов, банковским реквизитам, адресам регистрации, телефонам. «Взлом сайта позволяет также заразить компьютеры его посетителей вредоносными программами и достать потом номера кредиток, пароли для доступа в интернет, почту и платежную систему, — объясняет Дмитрий Канаев (Caravan). — Результатом становится хищение денег у пользователей сайта и создание ботнетов для организации последующих DDoS-атак, спам-рассылок и прочего. Для владельца портала огласка такой утечки данных часто означает либо серьезные финансовые траты, либо прекращение коммерческой деятельности».

Один из недооцениваемых предпринимателями рисков — простой ресурса. Чаще всего компании бросают все силы на защиту денег и конфиденциальной информации, а на такие угрозы смотрят сквозь пальцы — и зря.

— Совсем недавно у меня были переговоры с клиентом, который довольно спокойно относился к безопасности своих данных, так как они имеют малую ценность на рынке, — рассказывает Владимир Княжицкий, генеральный директор ГК «Фаст Лейн» в России. — При этом он совершенно не учитывал того, что цена часа простоя в его бизнесе огромна. А ведь перед хакером часто ставят задачу элементарно приостановить на некоторое время работу компании и тем самым нанести ущерб.

ЛЮДИ И ПРОГРАММЫ

Инструментов информационной безопасности очень много. К ним относятся программные продукты, инструкции по безопасной работе в интернете, распределение прав доступа и многое другое. Поэтому начинать выстраивать систему защиты в компании необходимо с оценки угроз. «В первую очередь стоит точно определить для себя, какие риски более критичны, — советует Дмитрий Мананников, директор по безопасности SPSR Express. — Нужно понимать, что защитить всё и ото всех невозможно. Следовательно, важно на начальном этапе расставить приоритеты. И уже исходя из этого определять те меры, которыми вы будете защищать свои системы».

Надежным помощником в этом деле может стать система управления информационными рисками. Ее функции заключаются в оценке потенциальных угроз. «Существуют различные автоматизированные средства анализа и управления рисками, — сообщает Сергей Барбашев, эксперт по информационной безопасности Русской школы управления. — Например, такие как CRAMM, RiskWatch, Operational Risk Builder, Risk Advisor, COBRA, а также российская разработка ГРИФ 2006 из состава Digital Security Office 2006».

После определения потенциальных угроз и расстановки приоритетов проектируется система защиты. К базовому уровню защиты корпоративной информационной системы относятся антивирусные

программы, антиспам для электронной почты и межсетевой экран (Firewall), к продвинутым — системы прозрачного шифрования, системы обнаружения вторжений (IDS/IDP), системы противодействия утечкам (DLP), системы защиты от целенаправленных атак (antiAPT). Если компания ведет бизнес через интернет (электронная коммерция, торговые площадки), то необходимо использовать специальное программное обеспечение или облачные сервисы для защиты веб-приложения от хакерских и DDoS-атак. Для крупных компаний практической необходимостью становятся центры управления безопасностью (SOC), построенные на системах мониторинга событий информационной безопасности (SIEM). Существуют также системы противодействия мошенничеству (antifraud), отслеживающие подозрительные транзакции в крупных информационных системах, и много других специфических систем информационной безопасности для решения точечных или нишевых задач, объясняет Рустэм Хайретдинов, руководитель проекта Appercut и заместитель генерального директора ГК InfoWatch.

Однако, при всем разнообразии технических инструментов защиты, невозможно построить эффективную систему информационной безопасности без участия сотрудников компании. Персонал своими действиями может как помочь уберечь секретную информацию, так и осознанно или неосознанно открыть к ней доступ злоумышленникам. Надеяться на программы — это все равно что поставить железную дверь в квартиру и дать ключ от нее соседке, которая при первой же возможности выдаст этот ключ цыганке, проводит аналогию Вячеслав Медведев («Доктор Веб»).

ХАКИНГ НА ДОВЕРИИ

Самое слабое звено любой системы безопасности — все-таки люди. Поэтому хакеры-виртуозы, атакующие корпоративные системы безопасности, обычно не чистые «технари»: они, помимо прочего, прекрасно владеют психологией и навыками социального инжиниринга. Не зря многие приемы, позволяющие несанкционированно получить доступ к корпоративным секретам, называют «социальным хакингом».

Персоналу необходимо объяснять, как работать с секретной информацией, и проводить специальные тренинги. Злоумышленник, обладающий необходимой подготовкой, может выудить важную информацию даже по телефону. Не менее серьезную угрозу несут также фишинговые страницы и рассылки. Преступники копируют стиль и манеру изложения известного фирме-жертве учреждения — например, партнера или банка. Не заподозривший подвоха сотрудник может скачать вложение с вирусом или отправить конфиденциальные данные третьим лицам. Российские хакеры отмечают, что 80% взломов происходят при вольном или невольном содействии жертвы. Чаще всего последней посылаются письма с опасными вложениями или ссылками.

Очень важно объяснить персоналу «технику безопасности» при работе в Сети. Например, донести до сотрудника, отвечающего за осуществление платежных транзакций, что серфинг интернета с компьютера, где хранятся ключи для программы «Клиент — Банк», может окончиться весьма плачевно. Несет риск выход в интернет через смартфон — особенно когда сотрудники пользуются личным гаджетом для подключения к корпоративным веб-ресурсам.

— С развитием виртуализации корпоративных ресурсов увеличивается также количество взломов публичных «облаков», — говорит Дмитрий Канаев из Caravan. — По данным организации по защите

Самое слабое звено любой системы безопасности — все-таки люди. Поэтому хакеры-виртуозы, атакующие корпоративные системы безопасности, обычно не чистые «технари»: они, помимо прочего, прекрасно владеют психологией и навыками социального инжиниринга

облачных технологий Alert Logic, ежегодный темп роста таких преступлений в мире — около 45%. Как правило, этому способствует размытый периметр безопасности у компаний, недостаток их знаний об облачной среде. Так, утечка данных из облачного приложения нередко связана с использованием сотрудниками собственных смартфонов для просмотра конфиденциальных корпоративных документов. Смартфон автоматически сохраняет копии файлов, доступ к которым может легко получить хакер, заразивший тот или иной сайт вирусом. Для этого владельцу смартфона достаточно будет только посетить этот сайт.

Многие эксперты полагают, что сохранить корпоративные секреты можно также с помощью «запугивания» сотрудников материальной ответственностью в случае разглашения важных данных. «В каждом трудовом договоре с каждым сотрудником должны быть прописаны условия об обязанности обеспечить сохранность вверяемой конфиденциальной информации, — считает Владимир Берлизов, начальник юридического отдела компании CTI. — Либо следует подписывать с работниками соглашение о неразглашении конфиденциальной информации. Не стоит рассчитывать на штрафы: такой меры дисциплинарной ответственности не существует. Самое большее, на что можно рассчитывать (если удастся должным образом определить размер причиненных

убытков), — это взыскать убытки в порядке, предусмотренном Трудовым кодексом».

При этом подписывать соглашение необходимо как с работающими в штате, так и вне его. Впрочем, как отмечает Владимир Берлизов, лучшая защита от утечки информации через сотрудников, — это максимальное ограничение их доступа к секретным данным. Одна из крупных угроз информационной безопасности связана с наличием у работников избыточных полномочий в корпоративных системах, которые не используются ими для выполнения своих непосредственных должностных обязанностей. Такое может произойти при получении повышения или переходе на службу в другой департамент.

За контроль над полномочиями сотрудников в информационных системах компании, как правило, отвечает служба информационной безопасности. Если и сотрудников много, и информационных систем, то выполнять функцию контроля и аудита прав доступа в ручном режиме проблематично. На этот случай, объясняет генеральный директор компании 1IDM Роман Федосеев, на рынке имеются специальные системы класса IdM (Identity Management), которые позволяют грамотно организовать процесс управления правами пользователей на основе ролевых моделей. По мнению Федосеева, благодаря использованию в компаниях IdM-систем сводится к минимуму человеческий фактор, а оценка и контроль прав доступа производятся автоматически, что, в свою очередь, приводит к снижению рисков разглашения секретных данных со стороны сотрудников компании.

ДРУЖЕСТВЕННЫЙ ХАК

Чтобы организовать эффективную систему информационной безопасности в компании, можно пойти от обратного — попросить стороннего специалиста взломать корпоративную систему и тем самым обнаружить «дыры». Таких специалистов называют «пентестерами»[2]. «На рынке работают компании, которые специализируются на проведении пентестов, — говорит Рустэм Хайретдинов из ГК InfoWatch. — Они проводят аудит информационной безопасности системы, исследуя ее и указывая на все найденные бреши в защите». Разумеется, привлечение пентестеров целесообразно лишь в том случае, когда корпоративная система информационной безопасности уже хорошо налажена и требуется провести ее испытания в «боевом» режиме.

«Когда все очевидные пути взлома уже перекрыты, хакер может дать ценный взгляд со стороны, предоставить совершенно неожиданную перспективу, увидеть специфический угол атаки, о котором никогда бы не подумали люди, мыслящие как «защитники баррикад», — поясняет Дмитрий Кузнецов, представитель компании «Параллакс».

Хакеры, постоянно практикующие взлом компьютерных программ, нередко привлекаются к проверке корпоративных систем ИБ за вознаграждение. Однако не все эксперты считают подобный вид обнаружения уязвимостей безопасным. «Тут стоит задаться вопросом: а насколько вы доверяете этому специалисту и какова вероятность того, что он действительно сообщит обо всех выявленных уязвимостях, а не использует в дальнейшем некоторые из них в своих корыстных целях?» — говорит Игорь Корчагин, руководитель группы обеспечения безопасности информации компании «ИВК». По мнению эксперта, наиболее оптимальное решение — это привлечение специализированных организаций, оказывающих услуги по оценке безопасности компьютерных систем. В рамках такой практики заказчик услуги может себя обезопасить, заранее зафиксировав ответственность аудитора, в том числе за разглашение конфиденциальной информации или сведений о выявленных уязвимостях.

Не обязательно шагать в ногу с технологическим прогрессом, чтобы обеспечить информационную безопасность своей компании. Иногда полезно, напротив, отстать.

Интересным кейсом в сфере защиты информации стало использование устаревших технологий в Министерстве обороны США. В военном учреждении до сих пор используются компьютеры 1970-х годов IBM Series/1 и 8-дюймовые дискеты для управления ядерным арсеналом. Подобные «артефакты» очень сложно взломать. Во-первых, компьютеры минобороны США изолированы от внешних сетей — и для проникновения в систему необходимо получить физический доступ к «железу». Во-вторых, злоумышленнику придется иметь дело с устаревшими программами, написанными на языках программирования COBOL и Fortran[3], с которыми современному хакеру непросто разобраться. Таким образом, «отсталость» компьютерной системы американского Министерства обороны сама по себе становится отличной защитой от взлома.

В арсенале хакеров — огромное количество мошеннических схем: они могут завладеть ценной информацией, украсть со счетов компании деньги, зашифровать данные и требовать выкуп и многое другое. Хакерские атаки могут стоить компаниям миллионов долларов, ценной информации и способны серьезно навредить репутации, подчеркивает Винс Стеклер, главный исполнительный директор Avast Software. Позиция «У моей фирмы нет секретных данных, представляющих ценность» не сможет уберечь от хакерских атак. А последствия могут быть самыми плачевными. Важно правильно оценивать риски и защищать свою компанию от посягательств злоумышленников. БЖ

2 *Пентест — сокр. от англ. penetration test — тест на проникновение в компьютерную систему для оценки уровня ее безопасности и поиска уязвимости, моделирование атаки злоумышленников.*

3 *Старейшие языки программирования, созданные в конце 1950-х годов.*