Угрозы из сети

В вопросах информационной безопасности многие ритейлеры привыкли полагаться на авось и стараются максимально сэкономить деньги компании, поскольку возврат инвестиций в ИБ подсчитать практически невозможно. Однако недооценка угроз может привести к очень серьезным потерям. К примеру, конфиденциальная информация о ценовых предложениях поставщиков, условиях поставки товаров, планируемых к открытию торговых точках, попав в руки конкурентов, может значительно ослабить положение компании на рынке. В ближайшее время угрозы будут возрастать, так как в кризис теневой хакерский бизнес становится только крепче.

АВТОР: Наталья Николаева

Отчеты профильных организаций утверждают, что уровень угроз растет, а вот качество защищенности в корпоративном секторе, если сравнивать с 2011–2012 годами, наоборот, падает. Так, Positive Technologies в своем «Сборнике исследований по практической безопасности» за 2014 год заявила, что 86% исследованных ими в 2013 году корпоративных информационных систем имеют уязвимости, с помощью которых можно получить полный контроль над всеми критически важными для компании программами. Почта, ERP-система, системы управления сетевым оборудованием – все окажется в руках злоумышленника, если он знает, за какие ниточки дергать. И это еще не самое страшное! Иногда и особых знаний не требуется. По данным той же компании, если брать внутренние сети, то в «половине всех исследованных систем успешные атаки возможны со стороны любого неквалифицированного пользователя внутренней сети».

Это вроде как в теории и при тестовых проникновениях в сеть аудиторов по информационной безопасности. А что на практике? На практике то же самое. В конце ноября 2014 года хакеры успешно взломали сеть и парализовали работу ни много ни мало всемирно известной Sony Pictures Entertainment – организации солидной и с деньгами. Достоянием общественности стали внутренняя отчетность компании, сведения о сотрудниках: например, данные по зарплатам топ-менеджмента, а также такие личные данные, как номера карт социального страхования, зная которые, можно украсть у их владельцев если не все, то многое.

«Думаю, из этой истории можно сделать несколько выводов, – размышляет Сергей Хайрук, аналитик компании InfoWatch. – Во-первых, этот инцидент развенчивает миф о том, что кибератака, внутренняя или внешняя, несет в себе только угрозу репутации компании, но едва ли приведет к реальному финансовому ущербу. Как нам известно, взлом Sony Pictures Entertainment повлек за собой утечку четырех новейших фильмов, еще не вышедших в прокат. Судите сами, сколько компания потеряла на этом. Во-вторых, представители ФБР утверждают, что такая крупномасштабная операция не могла быть успешно осуществлена без помощи «крота» в самой корпорации. То есть даже в этой, казалось бы, внешней хакерской атаке был задействован бывший или действующий сотрудник Sony Pictures Entertainment, причем, по мнению ФБР, довольно высокого ранга. Это доказывает, что злонамеренные действия внутреннего сотрудника могут быть очень ощутимыми для компании, и на эти так называемые внутренние риски нельзя смотреть сквозь пальцы».

Забавный момент: СМИ опубликовали оставленную на взломанных хакерами компьютерах Sony Pictures картинку, содержащую текстовые угрозы и гиперссылки на архивы с некоторыми украденными данными. Западные масс-медиа эти ссылки прикрыли «блюром», что ничуть не помешало нашим журналистам раздобыть такую же картинку со всеми ссылками без какой-либо «занавески» и в таком виде поместить изображение в свои статьи об инциденте. Вот вам и «безопасность».

«Выводы тут самые простые, – говорит Станислав Шевченко, технический директор компании SafenSoft. – Даже такие крупные компании, которые однозначно уделяют безопасности не последнее место в своем бизнесе, подвергаются успешным атакам. В списке целей киберпреступников каждая компания может найти свое место».

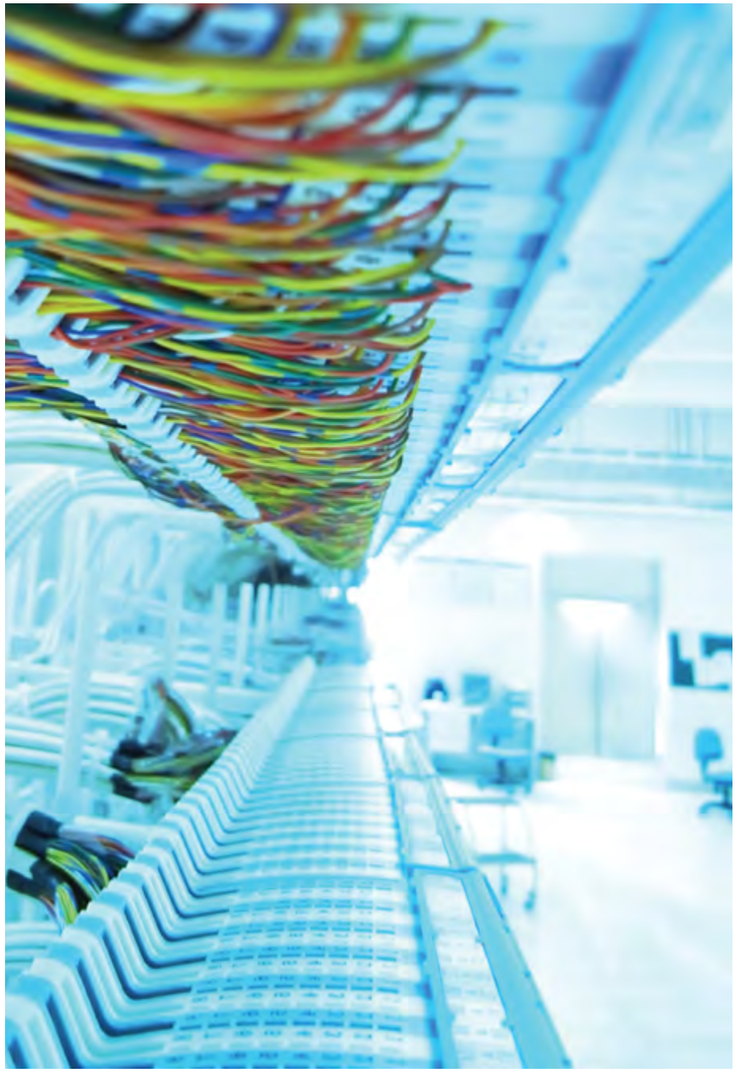
Пока писалась эта статья, пришла еще одна интересная новость, отечественного розлива: вполне добропорядочный гражданин, не чуждый мира ИТ, случайно, но с небольшой помощью соцсети «ВКонтакте» (!) получил доступ к более чем 20 000 московских камер наблюдения и сообщил об этом в Единый центр хранения данных Москвы – государственную информационную систему, которой и принадлежит это хозяйство. Ответной реакции он дождаться так и не смог, зато опубликовал информацию на крупнейшей ИТ-площадке, так что теперь любой желающий мог убедиться в том, что уязвимость присутствует, что все и проделали. После бурного обсуждения в комментариях появился наконец представитель Департамента информационных технологий города Москвы и разъяснил присутствующим, что никакой утечки информации не было, просто сервис тестируют. Однако доступ к камерам тут же прикрыли.

В БАГДАДЕ ВСЕ СПОКОЙНО...

Но вернемся к бизнесу. На первый взгляд, дела у нас обстоят не так плохо, как на Западе. Никакой русский Эдвард Сноуден (которого, кстати, в западных СМИ зовут whistle-blower – доносчик) не бежит в США с нашими секретами, особенно громких скандалов, связанных с утечками информации, не наблюдается и в отечественных корпорациях. Но если мы о чем-то не знаем, это не значит, что явления нет. «К сожалению, в России компании не обязаны раскрывать информацию об утечках, уведомлять уполномоченные органы или своих клиентов в случае компрометации их данных», – сетует Сергей Хайрук. По его словам, число

российских утечек, о которых становится известно широкой общественности, довольно небольшое, однако несколько лет подряд именно Россия прочно занимает второе место по числу утечек – сразу вслед за США.

Число «российских» утечек в 2013 году выросло на 78% к 2012 году: зарегистрировано 134 случая утечки конфиденциальной информации из российских компаний и государственных организаций. В СМИ обнародовано 109 случаев утечки персональных данных, что в 2,2 раза выше аналогичного показателя 2012 года. В результате этих утечек скомпрометировано 3,1 млн записей. На персональные данные пришелся 81% всех российских утечек. 19% утечек персональных данных пришлось на госорганы, 18% – на компании в сфере ЖКХ. Замкнули тройку «лидеров» финансово-кредитные организации с показателем 16%. Две трети утечек произошло из небольших (менее 500 ПК) организаций.



«В 2014 году мы зафиксировали более 160 «российских» утечек, – говорит Сергей Хайрук. – Чуть более 6% пришлось на ритейловые компании. В основном на салоны сотовой связи и интернет-магазины, чьи сотрудники вступали в сговор с представителями банков и в прямом смысле не отходя от кассы оформляли кредиты на чужие паспорта. Многомиллионных утечек, подобных тем, от которых пострадали Home Depot или Target, в России пока не зафиксировано. Но это не означает, что хакеры уже в ближайшее время не доберутся до информационных систем российских ритейлеров. Например, легко представить атаку на POS-терминалы отечественной торговой сети и компрометацию платежных данных миллионов клиентов. Хакеры отлично усвоили урок, поняли, что номера кредиток можно воровать не только в банках или в Интернете, но и непосредственно в магазинах, получив доступ к платежным терминалам».

«Существует мнение, что у России все очень хорошо со специалистами по ИТ-безопасности, – добавляет Станислав Шевченко. – Это так, однако наши компании далеко не впереди всей планеты с точки зрения реализованных проектов в этой области, поэтому нельзя считать, что нам не о чем беспокоиться. К тому же не следует забывать о кризисе: люди будут искать альтернативные способы заработка, в том числе незаконные. Подобных «специалистов» по взаимодействию с компьютерными

ТОП-3 угроз для ритейлера

ESET RUSSIA	TREND MICRO (ДЛЯ ОНЛАЙН-РИТЕЙЛА)	SAFENSOFT
DDoS – атаки, направленные на внешние интернет-сервисы (интернет-магазин, партнерский портал, сайт компании)	Недоступность веб-сайта компании вследствие DDOS-атак (атаки отказа в обслуживании)	Дискредитация платежной системы, внутренних транзационных механизмов
Эпидемии, связанные с программами-шифраторами. Этот тип вредоносного ПО блокирует доступ к рабочим документам зараженного компьютера, шифрует файлы большинства форматов и требует денежный выкуп за разблокировку	Недостаточная защищенность данных держателей платежных карт – незащищенные приложения и веб-сайты компаний	Информационное оповещение о том, что атака была и она была успешной
Вредоносные программы, специально разработанные для атаки на конкретную компанию (трояны, шпионское ПО и др.).	Риск взлома сайта для искажения информации (цен, наличия товаров и т.д,), кражи пользовательских данных	Необходимость в быстрых дополнительных инвестициях, чтобы закрыть варианты атак, затраты на более квалифицированный ИТ-персонал, зачастую также необходимость привлекать ИТ-консультантов и т.п.

системами в нашей стране более чем достаточно».

«Как в других отраслях, в российском ритейле есть компании с совершенно разным подходом к обеспечению информационной безопасности, – резюмирует Денис Безкоровайный, руководитель направления по работе с финансовыми организациями компании Trend Micro. – Есть как компании, которые построили процессы управления информационной безопасностью в соответствии с мировыми стандартами и лучшими практиками, так и менее зрелые с точки зрения управления ИБ».

ЧЕМ РИСКУЕМ?

С одной стороны, безопасность всегда убыточна: нужно потратить средства, а выгода неясна. Нужны ли были все те предпринятые меры или и без них бы все обошлось? Или можно было предпринять меньше: закупить половину средств по обеспечению безопасности, сократить штат специалистов? Подсчитать напрямую здесь нельзя. Отвечая на вопрос, что мешает наладить должный уровень защиты в корпоративном секторе, Станислав Шевченко заметил: «Главное препятствие здесь – наш собственный менталитет и надежда на авось. Руководство отдельных компаний думает, что их подобные проблемы не затронут, но история информационной безопасности демонстрирует, что новые угрозы затрагивают всех, просто кого-то раньше, а кого-то чуть позже».

«Случается, что владельцы компаний не хотят вкладывать средства в непонятные для них сервисы, – объясняет Антон Бугрецов, директор по работе с крупными корпоративными клиентами ESET Russia. – Они привыкли к «классическим» угрозам, имеющим некое физическое воплощение (конкуренты, криминал и так далее) и не считают опасным то, что нельзя увидеть или потрогать руками. Однако времена изменились».

Компания Leta, специализирующаяся на комплексных решениях по информационной безопасности, провела интересное исследование и составила обзор рисков для ритейла, причем для каждого отдела выделила свои проблемы. Например, в отделе закупок случится утечка информации о закупочных ценах и условиях поставки и реализации товара. В этом случае у ритейлера могут произойти снижение рентабельности точек продаж за счет оптимизации цен у конкурентов, потеря маржи при «ценовых войнах», утрата эксклюзивных условий от поставщиков. «Риски информационной безопасности в конечном счете могут влиять на экономические показатели компании, – добавляет Денис Безкоровайный. – Информация о ценовых предложениях поставщиков, условиях, планах поставки товаров, планируемые к открытию торговые точки – все это является конфиденциальной информацией, которая, попав в руки конкурентов, способна подорвать планы или изменить позиции в каких-то сегментах». Если выгоду от усиления информационной безопасности в компании посчитать сложно, то прикинуть убытки, следуя такому алгоритму, вполне реально.

Основная проблема в корпоративном секторе, как утверждает Сергей Хайрук, – это недофинансированность информационной безопасности. В большинстве компании ИБ финансируется из ИТ-бюджета. С приходом кризиса расходы на ИТ сокращают. Но информационная безопасность, в отличие от ИТ, прямо влияет на издержки компании. Крупная утечка приводит

к огромным убыткам. «К примеру, после утечки в Target только на возмещение ущерба клиентов компания потратила $150 млн, – рассказывает Сергей Хайрук. – Чем меньше компания заботится о безопасности своих данных и данных клиентов, тем больше риски. Сокращая расходы на ИБ, российский бизнес вступает на опасный путь. И есть ненулевая вероятность, что расчет на авось не сработает, и нас ждут масштабные утечки данных по всем отраслям».

По мнению Евгения Дружинина, ведущего эксперта по информационной безопасности компании «КРОК», для ритейлеров актуальны все общеизвестные угрозы, начиная от внешних сетевых атак и заканчивая внутренним несанкционированным доступом и утечками конфиденциальной информации. Кроме того, торговые организации обязаны выполнять требования ФЗ-152 «О персональных данных» и, соответственно, обеспечивать защиту персональных данных в соответствии с требованиями регулирующих органов. Таким образом, ритейлерам важно защищать периметр корпоративной среды, вовремя обновлять используемое программное обеспечение, разграничивать пользовательские права доступа к критическим бизнес-системам, обеспечивать защиту от DDoS-атак, вирусов и утечки информации, осуществлять фильтрацию трафика веб-приложений, контролировать подключения к информационным ресурсам и сетям и так далее.

«Чтобы выделить конкретные риски и угрозы, нужно рассматривать каждый отдельный случай: какие услуги предоставляет ритейлер, какую роль в его бизнесе играет Интернет, каков уровень зрелости уже выстроенной системы информационной безопасности и бизнес-процессов в целом, – рассказывает Евгений Дружинин. – В частности, для онлайн-ритейла актуальными становятся системы противодействия мошенничеству, или антифрод-системы, выявляющие подозрительные транзакции. Вообще говоря, сейчас практически все организации, у которых есть электронный канал взаимодействия с клиентом, в той или иной мере сталкиваются с мошенничеством, и каждый такой случай – это не только прямые финансовые, но и репутационные потери.

Также не стоит забывать об инсайдерских угрозах. Например, для офлайн-ритейла актуальны средства защиты от кражи денег кассирами. Подход к решению этой задачи должен быть комплексным. Так, речь может идти об интеграции POS-терминалов с системой видеонаблюдения. В этом случае сотрудники службы безопасности смогут работать с видеоархивом, промаркированным кассовыми операциями, и поиск подозрительных событий или конкретной кассовой операции по номеру чека не займет больше нескольких секунд. А видеоаналитика сама по себе позволит выявить правонарушителя в торговом зале.

И, наконец, нужно соответствовать законодательным требованиям

МЕНЯЕМ ЧУЖОЕ НА СВОЕ

Еще одна головная боль для компаний – взятый правительством курс на импортозамещение. В сфере информационной технологии это означает следующее: замещение будет происходить, но использование «сырых» продуктов отечественного производства может открыть дополнительные уязвимости корпоративных информационных систем. Как полагает Антон Бугрецов, директор по работе с крупными корпоративными клиентами ESET Russia, в первую очередь попытка импортозамещения повлияет на аппаратные решения, поскольку некоторые виды продуктов или их аналогов невозможно произвести в России: «При нынешнем положении дел стопроцентное импортозамещение – это утопия. Подобный проект в ИТ невозможно осуществить за 2–3 года, для этого необходимы многолетние разработки и значительные вложения интеллектуальных и финансовых ресурсов».

Чуть более оптимистично настроен Станислав Шевченко, технический директор компании SafenSoft: «При принятии и правильной реализации политики импортозамещения у российских компаний будет больше возможностей. Однако если посмотреть на другие стороны бизнеса, то эти возможности, наоборот, уменьшатся именно в сфере ИТ. При новых обстоятельствах, таких как импортозамещение, взрывной рост количества компаний, занимающихся ИТ-безопасностью, весьма маловероятен. В ИБ вообще очень мала вероятность возникновения новых, «скороспелых компаний». Здесь очень важна экспертиза, а молодая компания не может привлечь специалистов, которые обладали бы достаточной экспертизой для решения задач, а также неспособна реализовать продукт за короткое время. Хотя, конечно, при неограниченном количестве ресурсов этого возможно достичь, но это либо фантастика, либо речь идет о прямой поддержке на самом высоком уровне».

А вот Евгений Дружинин, ведущий эксперт по информационной безопасности компании «КРОК», полагает, что есть и положительный сценарий: «Сейчас в России разрабатываются в основном только базовые инструменты информационной безопасности, такие как антивирусы, межсетевые экраны, ряд DLP-систем, средства защиты от несанкционированного доступа и криптографической защиты. Эти продукты в большинстве своем обладают важным конкурентным преимуществом – сертификатами от регуляторов, таких как ФСТЭК и ФСБ, но зачастую проигрывают в функциональных характеристиках. Потребности российского рынка на данный момент они закрывают не более чем на 40%. Однако наличие квалифицированных кадров и подстегивающая политическая обстановка могут переломить ситуацию».

«Я считаю, что отечественные разработчики имеют возможность разработать все необходимые для защиты ритейловых сетей решения, – подводит итог Сергей Хайрук, аналитик компании InfoWatch. – И многие уже есть сейчас. Но в любом случае импортозамещение пока остается в большей степени проектом на бумаге».

в области защиты информации, например, при организации защиты персональных данных следует использовать средства, сертифицированные ФСТЭК и ФСБ России. В противном случае велик риск штрафа со стороны регуляторов».

Но есть и относительно хорошие новости: по сравнению с другими сферами бизнеса в ритейле минимален риск кражи технологий. Все дело в том, что ритейл редко обладает технологическими инновациями – красть нечего, считает Антон Бугрецов. У ритейлеров крадут другое. Прошедший год показал, что наиболее «ликвидную» информацию: реквизиты пластиковых карт и персональные данные – можно получить даже без дорогостоящих и сложных атак на защищенную инфраструктуру банков. Достаточно взломать системы компаний, которые обрабатывают большие объемы такой информации. Об этом рассказывает Сергей Хайрук: «Например, ритейлеры агрегируют персональные данные клиентов в рамках скидочных программ, а реквизиты пластиковых карт обрабатываются платежным оборудованием. Доступ к информационной системе крупного ритейлера принесет хакеру миллионы номеров пластиковых карт, записей о клиентах и в итоге деньги – десятки миллионов долларов. Естественно, столь легкий способ заработка привлечет многих. Тем более что дорога уже протоптана: по схожему сценарию в 2014 году проходили все крупные атаки на ритейловые сети».

Еще одна угроза, по мнению Сергея Хайрука, это манипуляции с программным обеспечением платежного оборудования. Известен случай, когда внутренний злоумышленник настроил программу таким образом, что с каждой покупки ему на счет перечислялась небольшая сумма. В течение двух лет ни клиенты, ни руководство торговой сети не замечало этой ошибки, а счет мошенника пополнился на солидную сумму. Очевидно, так же может действовать и внешний злоумышленник, – получив доступ к информационной системе, он может инфицировать оборудование вредоносным ПО со схожим функционалом.

Еще один пример предлагает Станислав Шевченко. По его словам, все больше крупных ритейловых операторов используют «кассы без продавца», где покупатель самостоятельно расплачивается за покупки без участия сотрудников магазина. Подобные системы можно увидеть в крупных ритейловых сетях Москвы. Как только возникает такое замещение человека, появляется возможность технически атаковать эту систему. В случае проведения злоумышленниками

успешной атаки появится общедоступная информация, что эти терминалы самообслуживания небезопасны. Клиенты будут просить обслужить их наличными деньгами, а компания будет уже не в состоянии этого сделать, что повлечет за собой дополнительные затраты и необходимость возвращаться к кассирам и наличному расчету.

КЛАССИЧЕСКИЕ ВОПРОСЫ

Пришло время классического вопроса: что делать? Мы сразу ответим: в рамках журнальной статьи исчерпывающего ответа быть не может. Для каждого вида компании, для каждого ритейлера вопросы безопасности индивидуальны. «Бизнес должен найти золотую середину в данных решениях, что сделать не всегда просто, – полагает Павел Соловьев, заместитель директора информационных технологий DPD в России. – В идеальном случае нужно соответствующее подразделение, которое будет заниматься полноценным анализом требований безопасности для разного вида данных. Сейчас ценность данного подразделения для бизнеса неочевидна, поэтому сплошь и рядом данная задача просто делегируется ИТ-департаменту, который в свою очередь ищет какое-то среднее решение с точки зрения удобства администрирования и безопасности».

Антон Бугрецов считает, что для полноценного ответа на вопрос, как обеспечить безопасность компании, необходим аудит ИТ-инфраструктуры, позволяющий выявлять потенциально уязвимые точки корпоративной сети и заблаговременно разрабатывать проекты эффективной защиты на будущее. Если же говорить в общем, то, по его мнению, для торговых компаний актуален полный спектр продуктов и услуг по информационной безопасности: обновление ПО в сети, межсетевые экраны и системы предотвращения вторжений, позволяющие контролировать подключения к информационной структуре, АПО, пресекающее действие вредоносной программы до повреждения системы. «Таким образом, мы получаем инфраструктуру, защищенную от внешних и внутренних угроз, – говорит Антон Бугрецов. – Помимо антивирусного функционала комплекс имеет дополнительные модули – системы обнаружения и предотвращения вторжений IDS и IPS».

Станислав Шевченко уверен, что первую очередь необходимо осознать, что торговое предприятие находится под угрозой так же, как и все прочие предприятия. Следующий шаг – непосредственное движение в сторону информационной защищенности, и тут уже есть как стандартные методы, так и нестандартные новые технологии.

Напомним, что уровень защищенности корпоративных систем снизился в 2013 году, при этом даже использование антивирусного ПО, улучшение алгоритмов шифрования и повышение компьютерной грамотности на предприятиях ситуацию в целом не улучшило. И ответ на второй классический вопрос – кто виноват – короткий. Как говорится в исследовании Positive Technologies, более половины (57%) исследованных корпоративных систем стали уязвимы из-за использования устаревшей операционной системы и версий обеспечения: средний возраст наиболее устаревших неустановленных обновлений составляет 32 месяца. В одной из систем была выявлена уязвимость 9-летней давности.

Что касается защищенности периметра и внутренней сети, то здесь слабость связана с использованием ненадежных паролей. Несмотря на то что даже рядовых пользователей постоянно учат не использовать словарные пароли и простые комбинации только букв или чисел, в половине систем, которые исследовали эксперты Positive Technologies, администраторы использовали недлинные цифровые пароли, причем самым распространенным был пароль 123456. Он встречался в каждой третьей системе. Выводы можно сделать самостоятельно. ◆