Опасные связи

Отчеты компаний об информационной безопасности все больше напоминают приключенческие романы. Складывается ощущение, что мы с вами живем в мире, где цифровые пираты бороздят виртуальные пространства и идут на абордаж кораблей благопристойных компаний. Как заявляют профессионалы, хакеры становятся все более могущественными и изобретательными. Стоит ли бояться киберугроз торговым предприятиям? Или пристальное внимание, направленное на информационную безопасность, – это очередная маркетинговая уловка, «продажа страха»?

АВТОР: Наталья Николаева



Если посмотреть на бюллетени, выпускаемые в конце года крупными компаниями, занимающимися информационной безопасностью, то может показаться, что ритейл – не такая уж и мишень для киберпреступников. С тех недавних пор, как хакеры из хулиганистых одиночек, атакующих наши компьютеры, превратились в крупные и опасные преступные группировки, действующие по всему миру, их стала интересовать не просто крупная, а очень крупная «рыба». Сети расставляют на финансовые организации – крупнейшие банки, из которых воруют миллионы долларов, на правительственные организации, откуда черпают уже не деньги – информацию. В России под ударом энергетические комплексы. «Иногда злоумышленники в качестве цели выбирают организации, деятельность которых подрывает хакерский бизнес, – добавляет Шандор Балинт, руководитель отдела защиты прикладных задач компании Balabit. Под обстрел часто попадают исследовательские агентства и компании, разрабатывающие системы безопасности. Уверенность таких организаций в собственной неприкасаемости – вызов для преступников». Охотятся хакеры и на себе подобных. Так, в 2015 году подверглась взлому итальянская компания Hacking Team, которая сама занимается тем, что изготовляет, как написано на их сайте, «набор взломщика для госструктур» (The hacking suite for governmental interception). Хакер, который вскрыл своих «почти коллег», через год описал этот поступок на одном ресурсе, совместив описание с лекцией об информационной безопасности.

Все это крайне увлекательно, однако где тут ритейл? Эксперты предупреждают – не стоит уповать на то, что мошенники пойдут в банк, а не в магазин. «Любая сфера привлекательна для кибепреступников, если есть возможность заработать, если на данные есть спрос в даркнете, – говорит Алексей Парфентьев, ведущий аналитик компании «СерчИнформ». – Ритейл – динамичная отрасль с живыми деньгами, потому информация из этой отрасли стабильно востребована среди злоумышленников».

К этому мнению присоединяется и Евгений Акимов, руководитель отдела развития департамента информационной безопасности ГК Softline: «Списки самых громких краж электронных денег возглавляют организации реального сектора экономики: производство и ритейл как раз в силу их меньшей защищенности по сравнению с финансовыми структурами. Киберпреступники, как правило, идут по пути наименьшего сопротивления и атакуют там, где защита слабее. Неоднократно отмечалось снижение преступного интереса к наиболее защищенным организациям, прежде всего к банкам. На счетах многих компаний вполне достаточно денег, чтоб стать лакомой добычей. Для этого необязательно быть банком».

Посмотрим отчеты повнимательнее. Так, например, в бюллетене компании «Лаборатория Касперского» сообщается о серии атак в июне 2016 года, целью которых среди прочих стали и торговые организации. Руководитель и менеджеры разных компаний получали фишинговые письма с вредоносными вложениями, основным итогом которых должно было стать проникновение преступной группы Operation Ghoul в сети той или иной организации. На розничную торговлю была нацелена и деятельность еще одного нашумевшего в 2016 году многофункционального трояна – Adwind. Таким образом, как минимум в двух видах атак, вошедших в годовой отчет безопасников, ритейл фигурировал в качестве одной из жертв.

Интересен и тот факт, что чаще всего имена пострадавших компаний не называют, говоря просто об «одной крупной торговой сети» в том или ином регионе. «Открытой информации об успешных киберпреступлениях, связанных с кражей денег, не так много, – подтверждает Евгений Акимов. – В основном такие сообщения приходят из-за рубежа. Большинство жертв предпочитает об этом не распространяться, чаще всего потому, что это негативно влияет на имидж компании. Но такие преступления, конечно же, сразу замечаются внутри – денег на счету стало меньше! В противовес этому кража коммерческой тайны часто проходит незамеченной даже для самой фирмы, и никто не связывает падение продаж с кражей клиентской базы или выпуск конкурентами продукта-аналога со сливом конкурентам планов развития. Но даже если это и обнаруживают, то предпочитают сор из избы не выносить».

Хорошей иллюстрацией тут может послужить недавняя и довольно громкая история Центрального банка Бангладеш, откуда киберзлоумышленники собирались украсть почти $1 млрд. $81 млн был успешно выведен, причем сотрудники заметили пропажу далеко не сразу, а когда заметили, перемещение оставшихся $870 млн удалось предотвратить. Агентство Reuters назвало это событие одной из крупнейших банковских афер. Изюминкой происшествия стало то, что министр финансов Бангладеш узнал об инциденте только спустя месяц из газет. В результате глава Центробанка Атиур Рахман был вынужден уйти в отставку, так как он не сообщил о пропаже правительству своей страны.

ЛАКОМЫЙ КУСОК

Как видим, если о чем-то не сообщается достаточно громко, то это не значит, что явление отсутствует. Обеспечение информационной безопасности для ритейла стоит дале-

ко не на последнем месте. «В важных вопросах, а к ним, несомненно, относится вопрос информационной безопасности и защиты от кибепреступников, хорошо ориентироваться на лидеров отрасли, – полагает Алексей Парфентьев. – К примеру, недавно в интервью начальник управления информационной безопасности X5 Retail Group Алексей Овчинников рассказал, что в группе используются самые разные технологии безопасности: средства защиты данных от утечки, антифрод-система, система анализа больших данных. При этом указал, что на это направление работы не хватает собственных ресурсов и приходится привлекать поставщиков ИБ-услуг. X5 Retail Group также разработала пакет юридических документов для подрядчиков, где прописала штрафы за нарушение требований информационной безопасности. Только за месяц благодаря этому пакету документов с подрядчиков за различные ИБ-нарушения было взыскано порядка 2,5 млн руб. На мой взгляд, подобные примеры весомее мнений экспертов-теоретиков об актуальности киберугроз для ритейла».

Причина, по которой торговая сфера может стать лакомым куском для киберпреступника, заключается не только в деньгах, которые крутятся в этом бизнесе. «Уровень защиты в ритейле часто ниже, чем в том же среднем банке, – уверяет Алексей Сизов, руководитель направления противодействия мошенничеству Центра информационной безопасности компании «Инфосистемы Джет». – Ритейлу было сложнее нанести фактический ущерб, но в силу развития новых технологий карта рисков сильно расширилась, а системы безопасности в ряде случаев не поспели за контролем этих рисков. Плюс имеет значение отношение к похищаемому ресурсу. В ритейле существенной потерей является конечный товар, а на недополученную прибыль или бонусные накопления клиентов компании смотрят менее внимательно. Это не «живые» деньги, поэтому уровень защитных механизмов был невысок. За последний год достаточно компаний кардинально пересмотрели подходы к безопасности таких сегментов, и более половины из них именно по факту существенных потерь от действий злоумышленников».



НЕ ТОЛЬКО БОГАТЫЕ ПЛАЧУТ

Опасаться стоит не только крупным сетям. Даже в секторе среднего и малого бизнеса есть чем поживиться. «Едва ли хакеры перестанут интересоваться малыми и средними компаниями в качестве мишени для атаки, – уверен Никита Дуров, руководитель группы консультантов по информационной безопасности компании Check Point Software Technologies. – Во-первых, такие организации, как правило, довольно просто взломать, поскольку они редко оснащены достаточно мощными средствами безопасности. Соответственно, злоумышленники легко могут запустить в сеть компании, например, вымогательскую программу, которая заблокирует все данные, и требовать выкуп. К сожалению, в большинстве случаев руководители организаций идут на условия преступников. Во-вторых, небольшая компания может быть использована в качестве трамплина, чтобы получить доступ к данным более крупной компании-партнера или поставщика».

«Никогда нельзя быть уверенным, что какие-то компании находятся под прицелом, а какие-то нет, – соглашается с коллегой Шандор Балинт. – Чтобы разобраться в этом, нужно понять, чем киберпреступники руководствуются, выбирая себе цель. Расследуя и предупреждая кибератаки, полезно посмотреть на них через категории «расходы» и «выгода». Выбирая жертву, хакер руководствуется законами экономики и стремится получить максимум прибыли, потратив при этом минимум ресурсов. Очевидно, что крупные компании с этой точки зрения намного перспективнее. Но в то же время усилия по ловле одной «крупной рыбы» могут быть сопоставимы с атакой на десять небольших компаний, защищенных слабыми системами безопасности».

Андрей Заикин, руководитель направления информационной безопасности компании КРОК, предупреждает о том, что нападение на небольшие компании могут быть не просто опасными – фатальными: «Риски присутствуют для всех компаний, но при этом чувствительность инцидента (будь то утечка важных данных или атака на сервис) для представителей СМБ-сектора может быть гораздо выше, чем для крупной компании, вплоть до закрытия бизнеса».

ОДИНОЧКИ РЫЩУТ СТАЯМИ

Можно заключить, что уровень безопасности в сфере ИТ не связан напрямую с размером организации. Это касается как жертв, так и нападающих. Даже один киберпреступник способен причинить серьезный ущерб. «Команда хакеров может насчитывать сотни или тысячи членов по всему миру, как группа Anonymous, или состоять всего из нескольких человек, как группа, осуществившая успешные атаки Eurograbber на банки в 2012 году, – в обоих случаях воздействие на бизнес компаний, подвергшихся атаке, будет одинаково разрушительным», – рассказывает Никита Дуров.

Новые технологии, которые использует не только бизнес, но и хакеры, позволяет одному воспользоваться силой многих. Так, облака, софт как услуга (SaS), о которых так много говорилось на бизнес-конференциях последние семь лет, наконец были взяты «на карандаш» и злоумышленниками. Adwind – кроссплатформенный многофункциональный троян – распространяется по модели «вредоносное ПО как услуга». Любой желающий может оплатить услуги сервиса и получить мощности шпионского обеспечения в свое распоряжение по подписке ($25 за 15 дней или $300 в год). По данным «Лаборатории Касперского», жертвами этого сервиса за три последних года стали 443 тысячи частных лиц, коммерческих и некоммерческих компаний по всему миру.

Еще один тренд в развитии киберпреступности – это усиление деятельности так называемых «бутиков», создающих вредоносное ПО для направленных атак. Группировки, предлагающие подобные услуги, создают инструментарий, нацеленный на определенные уязвимости того или иного канала доступа в сеть определенной жертвы. И если начало заражения происходит одинаково, то дальнейшая атака развивается по сценарию, в котором учтены все особенности «реципиента». Одной из крупных групп, являющихся таким бутиком, стал Poseidon, который работает больше 15 лет, однако детальный отчет о его деятельности появился только в 2016 году. Информацию, которая добывается с помощью таких атак, группировка использует для шантажа или последующей перепродажи заинтересованным лицам.

Стоит ли ритейлу опасаться направленных атак? «Мы считаем, что в текущем году вырастет число таргетированных атак, нацеленных на конкретную компанию или человека, – подтверждает опасения Никита Дуров. – Часто такие атаки проводятся по заказу конкурентов с целью надавить или скомпрометировать компанию. Еще один распространенный сценарий – кража ценных данных. Для ритейла это могут быть клиентские базы, личные данные клиентов. Утечка такой информации может повлечь серьезные финансовые издержки и репутационные риски».

Угрозы для сферы ритейла в 2017 году
Прогноз от компании Check Point Software Technologies

В 2017 году мы ожидаем еще больший рост популярности вымогательского ПО, в частности рост атак на облачные ЦОДы с его использованием. Поскольку компании из всех секторов, в том числе и из ритейла, будут переходить в облака, злоумышленники станут искать новые способы проникновения в инфраструктуру. Поэтому необходимо учитывать все требования безопасности при переходе в облако.

В конце 2016 года активно обсуждалась тема внедрения биометрических платежей в супермаркетах. Мы ожидаем, что в 2017 году технология получит еще больший охват, соответственно, безопасности таких платежей следует обратить особое внимание. Во-первых, необходимо убедиться, что устройство для оплаты преобразовывает запись отпечатка пальца/сетчатки глаза в сложную зашифрованную систему, и организация хранит эти данные соответствующим образом. Не менее важно уделять большое внимание клиентским устройствам, при помощи которых происходит подтверждение оплаты товаров или услуг. Для злоумышленников клиентское устройство так же интересно для атаки, оно является слабым звеном в системе безопасности.

БОЛЬНЫЕ ТОЧКИ

В целом торговля подвержена тем же рискам, что и другие области бизнеса. «Ритейлу следует опасаться тех же угроз, что и остальным отраслям, в том числе программ-вымогателей, мошенничества при помощи корпоративной электронной почты, взломов бизнес-процессов, новых уязвимостей программного обеспечения», – говорит Елена Стрелкова, менеджер по маркетингу Trend Micro в России.

Но есть и специфичные для ритейла точки, которые могут попасть под удар. Одним из актуальных способов мошенничества здесь является заражение вредоносной программой POS-терминала для перехвата платежной информации покупателя. Подробнее рассказывает Андрей Заикин: «Злоумышленников интересуют данные, записанные на магнитную ленту (track1 и track2). В этих данных содержатся: имя владельца, срок окончания действия карты и иная чувствительная информация, обладая которой, можно создать клон платежной карты. По большей части такому виду атак подвержены владельцы карт без чипа – только с магнитной полосой».

По сути, конечно, эта атака не является новой, так как техническая возможность была продемонстрирована еще несколько лет назад. Но в последнее время она достаточно часто всплывала в западной прессе как нестандартная угроза. «Например, один из популярных западных ритейлеров выплатил более десяти миллионов долларов клиентам, чьи данные были украдены с помощью атаки на POS-терминалы. И это без учета репутационных издержек и трат, направленных на устранение проблемы после ее обнаружения», – рассказывает Андрей Заикин.

В качестве мер защиты от такого типа атак он рекомендует следующие действия. Во-первых, компаниям, работающим с POS-терминалами, необходимо задуматься об использовании двухфакторной аутентификации при доступе к системам, взаимодействующим с POS-терминалами, не полагаясь только на стандартную аутентификацию по логину и паролю. Также можно посоветовать использовать инструменты для анализа поведения терминалов и систем, связанных с ними, на наличие аномальных отклонений.

Во-вторых, полезным окажется и шифрование данных – независимо от того, насколько хорошо написана зловредная программа, злоумышленник ничего не сможет сделать, если данные, которые он получил, зашифрованы. Внедрение end-to-end-шифрования на всех шагах платежного процесса может существенно снизить риски компании по неправомерному использованию данных клиентов.

И, конечно, не стоит забывать и о стандартных методах противодействия зловредным программам – антивирусам и брандмауэрам. Регулярные антивирусные проверки и качественно настроенные правила межсетевого взаимодействия также понижают риск заражения зловредами.

Напоследок опишем еще одну ситуацию, характерную именно для торговой сферы, – особую уязвимость в праздничные, то есть самые «горячие» для компании дни. «Наши исследователи отмечают, что злоумышленники особенно активизируются в период распродаж и перед большими праздниками, когда офлайн- и онлайн-магазины испытывают большой прилив покупателей, – говорит Елена Стрелкова. – Киберпреступники специально готовятся к этим событиям и обновляют свои инструменты. Так, перед новогодними праздниками появилась новая версия FastPoS – вредоносного кода для POS-терминалов, похищающего данные платежных карт. Специалистам по безопасности в ритейле рекомендуется готовиться к усилению кибератак в такие периоды».

Угрозы для сферы ритейла в 2017 году
Прогноз от компании «Инфосистемы Джет»

Этот год будет годом атак на публичные сервисы ритейла, обращенные к клиентам: личные кабинеты, мобильные приложения и т.д. Предпосылки этого очень просты: в личных кабинетах содержится не только персональная информация, но и сведения о накопительных программах лояльности, которые в последние годы стали лакомым куском для кибермошенников. Современный уровень развития таких программ позволяет злоумышленнику получать существенный доход от получения доступа к накоплениям участника: это и простые бонусы ритейлеров, и бонусы транспортных компаний, и многое другое. Поисковик очень быстро выдаст вам ресурс, где свободно продают сертификаты, карты с балансом, премиальные купоны той или иной компании. Этот сегмент мошенничества уже в прошлом году перешел рубеж в миллионы рублей потерь для отдельно взятой компании, а общий объем противоправных действий оценивается более чем в сотни миллионов.

ХАКЕРОВ БОЯТЬСЯ – В ИНТЕРНЕТ НЕ ХОДИТЬ

Еще один риск для ритейла напрямую связан с мультиканальностью офлайн-площадок и стремлением завоевать онлайн: «Торговля все глубже уходит в сеть, – рассуждает Мария Воронова, ведущий эксперт по информационной безопасности группы компаний InfoWatch, – появляются интернет-магазины и мобильные приложения, возможность оплаты банковскими картами и денежными средствами с многочисленных электронных кошельков. Чего в первую очередь стоит опасаться в этом случае? Во-первых, атак типа «отказ в обслуживании»: если онлайн-магазин не представляет эксклюзивный товар, то потенциальный покупатель, наткнувшийся на неработающий пусть даже временно сервис, уйдет приобретать нужный товар или услугу на соседнюю интернет-страницу. Это прямая потеря клиентов и, соответственно, прибыли. Далее, конечно, стоит поговорить и о платежных транзакциях: подмена веб-страниц, фейковые суммы в платежах и другие получатели. Тут проблема может быть как на стороне клиента, компьютер или мобильное устройство которого заражены, так и на стороне, предоставляющей сервис по осуществлению онлайн-оплаты».



В современном Интернете даже совершенно никому не нужный и нигде не анонсированный сервис пытаются взломать в среднем через полчаса после его подключения к сети. А любой востребованный онлайн-сервис является постоянным объектом атак. «По нашему опыту установки Web Application Firewall, каждый действующий сервис интернет-магазина подвергается непрерывному сканированию на предмет уязвимостей, – обрисовывает ситуацию Игорь Гершуни, эксперт по информационной безопасности, руководитель группы инжиниринга АО «Белтел». – Любая зацепка, любая «дыра», пропущенная программистами, может быть использована для совершения мошеннических действий или для нарушения работоспособности сайта. Особенно актуальна данная угроза при внедрении новой функциональности или обновлении ПО сайта».

«Уход коммерции в Интернет спровоцировал рост числа DDoS-атак», – добавляет к сказанному коллегами Евгений Акимов. С ним соглашается Игорь Гершуни: «DoS/DDoS атаки остаются серьезной угрозой, целью которых является нарушение функциональности сайта с целью последующего шантажа или как средство нечистоплотной конкурентной борьбы. С ростом Интернета вещей есть риск существенного расширения бот-сетей, используемых для проведения такого рода атак, поэтому стоит уделить этой угрозе особое внимание».

Как только мы начинаем говорить об одних типах угроз, на ум тут же приходят другие. Казалось бы, проблемы, связанные с Интернетом вещей, ритейл затронуть не должны. Однако это не совсем так. «Естественно, нельзя игнорировать угрозы, связанные с Интернетом вещей. Поскольку все больше устройств из повседневной офисной жизни подключены к Интернету – принтеры, веб-камеры, телевизоры, в некоторых случаях даже кофемашины и холодильники, – нужно понимать, что каждое из них может стать «дверью» в сеть компании для хакеров. Соответственно, нужно внимательно контролировать настройки безопасности на каждом из таких устройств», – уверен Никита Дуров.

«Я бы отметил несколько тенденций уходящего года, – подводит итог Алексей Сизов. – Первая – это перевод атак из сегмента эпизодов в состояние ежедневной опасности. Сегодня DDos, APT стали не гипотетической угрозой, вероятность которой довольно мала для отдельной компании, а вполне ожидаемым событием в произвольный момент времени. Атаку на инфраструктуру компании можно ожидать с той же вероятностью, что и получить троян обычному пользователю на сомнительном сайте. Вторая – это атаки на особые сегменты компаний, такие как программы лояльности в ритейле (на базе личных кабинетов или

мобильных приложений), потери от которых становятся прямыми потерями для ритейлеров и серьезным ударом по репутации и лояльности клиентов».

ХАКЕРФОНЫ

Об атаках на особые сегменты компании, в частности на мобильные приложения, стоит поговорить подробнее. По словам экспертов, мобильные угрозы опять в тренде на 2017 год. Насколько сильно отразятся на ритейле киберпреступления, связанные с мобильными технологиями? Как поясняет Шандор Балинт, сетевой трафик, генерируемый мобильными устройствами, медленно, но верно обгоняет объемы, создаваемые настольными ПК и ноутбуками. Эта тенденция наблюдается и в торговле – все больше покупок совершаются через смартфоны. Работая на перспективу, ритейлеры всеми силами стараются обеспечить соответствие электронных каналов продажи требованиям пользователей, в том числе и безопасности платежей.



«Сегодня ситуация с защитой сетей компании сильно изменилась, поскольку периметра безопасности как такового уже не существует, – замечает Никита Дуров. – Сотрудники все чаще используют личные девайсы для работы в офисе или офисные для работы дома. Естественно, требуется ответственный подход к безопасности бизнес-данных, который может быть обеспечен лишь совместными усилиями работодателя и сотрудника. Все прочнее в повседневную жизнь пользователей входят современные технологии оплаты – Apple Pay и Samsung Pay. Несмотря на то что обе эти платежные системы достаточно хорошо защищены, нельзя игнорировать тот факт, что хакеры беспрестанно работают над все более усовершенствованными атаками, чтобы найти лазейку в «кошелек» пользователя. Безусловно, ритейл в этом смысле не менее подвержен рискам, чем банковский сектор».

С ним согласен Шандор Балинт. «К сожалению, в ближайшие годы мы действительно станем свидетелями роста числа мобильных угроз, – замечает он. – Вероятно, эта тенденция сохранится до тех пор, пока главной ценностью для производителей мобильных устройств будет количество выпущенных гаджетов, а не высокое качество девайсов и регулярное обновление ПО, которое бы соответствовало лучшим требованиям безопасности».

Электронная коммерция напрямую связана с крупными деньгами, на которые, как пчелы на мед, слетаются хакеры. Зачастую получить «сладкое» не так уж сложно: мобильные устройства в целом менее защищены, нежели стандартные компьютеры. По наблюдениям Шандора Балинта, это особенно актуально для раздробленного Android-рынка. Большинство производителей не обременяют себя разработкой обновлений для уже выпущенных устройств, оставляя многочисленных пользователей без возможности поддерживать свои смартфоны и планшеты в актуальном состоянии. Устройства без последних патчей безопасности – отправная точка для хакера, который с легкостью может взломать смартфон и через него получить доступ к приложениям банка или электронного магазина.

«Я бы сказал, что ритейл сегодня испытывает эффект aftershock именно от банковской индустрии, – рассуждает Алексей Сизов. – Банковский сегмент – наиболее востребованный у злоумышленников, схемы атак в нем развиваются уже десятилетия. И если раньше применить фродовую экспертизу могли лишь на другом банке, то сегодня способы и механизмы атаки на то же мобильное приложение уже может принести выгоду и в том случае, если целью является ритейл-компания. Ритейл сегодня стал не просто кассовым узлом с процессами по логистике. Это современная ИТ-компания со своими web-площадками, личными кабинетами клиентов, виртуальными средствами на счетах и online-продажами. Эти технологии максимально приближены к банковским, и именно поэтому на них направлены взоры мошенников, имеющих опыт и инструменты соответствующих атак».

«Наибольшую угрозу, по нашему опыту, представляет именно внедрение мобильных технологий для взаимодействия внутри компании, – делится опытом Алексей Парфентьев. – Сотрудник компании имеет большие привилегии и доступ к критичным данным внутри организации, нежели пользователь извне. При этом мобильные устройства, мессенджеры в частности – слабо контролируемые каналы с точки зрения информационной безопасности. Это значит, что риск утечки информации через портативные устройства сотрудников одинаково угрожает организациям любой сферы. К примеру, в середине января кредитная организация Deutsche Bank объявила о том, что запрещает сотрудникам пользоваться мессенджерами и смс-сообщениями, в том числе на личных телефонах, используемых для работы. Цель запрета – повысить уровень безопасности, ведь эти сообщения не могут быть сохранены на сервере банка. Кроме того, ранее эксперты предупредили, что пользователи WhatsApp наиболее уязвимы для перехвата переписки из-за отсутствия полной защищенности архива сообщений WhatsApp».

ПЕЧЕНЬЕ С ПРЕДСКАЗАНИЕМ

Напоследок поговорим о прогнозах. Каждый год в бюллетенях с прогнозами на следующий год нас пугают тем, что атак станет больше и ситуация с безопасностью будет тяжелее. По мнению Алексея Парфентьева, для роста атак есть три объективные причины:

1. Динамичное развитие ИТ-отрасли в целом. С увеличением количества устройств и технологий будет расти количество возможностей и вариантов для нарушения информационной безопасности компании.

2. Тяжелая экономическая ситуация стимулирует спрос на нелегальные информационные услуги и толкает на преступные действия.

3. Растущая доступность инструментов для совершения кибепреступления. По оценке экспертов «Лаборатории Касперского», вредоносное ПО для онлайн-ограбления сегодня можно приобрести меньше чем за $1000, и, чтобы им воспользоваться, преступнику не нужно быть специалистом в ИТ. На практике любой пользователь без серьезных финансовых вложений и глубоких знаний в вопросе может организовать преступный бизнес.

Ежегодные прогнозы не являются какими-то пустыми «страшилками» – с каждым годом технологический ландшафт меняется и, соответственно, меняются тактики и подходы злоумышленников, стремящихся получить максимальную выгоду в новых условиях. В 2016 году ландшафт угроз позволил киберпреступникам значительно увеличить разнообразие методов атак и видов атакуемых целей. Наступивший год выведет индустрию кибербезопасности на новые рубежи. «Мы прогнозируем появление новых методов атак на крупные корпорации, расширение тактик онлайн-вымогательства, которые будут затрагивать все большее разнообразие устройств, а также применение методов кибепропаганды для манипуляции общественным мнением», – говорит Елена Стрелкова.

«На самом деле прогнозы не всегда однозначно обещают, что атак в грядущем году будет больше, – уверяет нас Игорь Гершуни. – Если проанализировать, то можно обнаружить, что хотя общий уровень угроз и растет, но по ряду направлений опасность, наоборот, снижается. В том числе и благодаря использованию средств защиты. Идет постоянное перераспределение популярных векторов атаки, и именно предсказанием векторов и ценны эти прогнозы. Общее же ощущение увеличения уровня угроз складывается из нескольких факторов. Во-первых, растет проникновение информационных технологий в повседневную жизнь, соответственно, мы чаще сталкиваемся и со связанными с ними угрозами. Во-вторых, появляются новые технологии, и каждая новая технология открывает новые векторы атаки».

По мнению Игоря Гершуни, прогнозы ориентированы больше на разработчиков и поставщиков решений ИБ. Они необходимы, чтобы понимать, какие направления стоит развивать и куда вообще катится этот мир. Планируя же мероприятия ИБ для конкретного предприятия, в первую очередь стоит ориентироваться не на прогнозы, а на используемые сервисы, приложения и бизнес-задачи. «Вы ведь не сверяетесь со статистикой преступности по своему району, когда принимаете решение закрывать или не закрывать дверь в доме? – иронизирует он. – Интернет – это один большой «плохой район», и случиться в нем может что угодно. Соответственно, защищаться надо обязательно, а выбор конкретных средств защиты обуславливается тщательным анализом рисков и нахождением оптимального компромисса между стоимостью защиты конкретных сервисов, удобством работы пользователей и возможными потерями (финансовыми или репутационными) в случае каких-либо инцидентов ИБ». ◆