Новые киберусловия
для бизнеса

Кирилл КЕРЦЕНБАУМ,
менеджер по развитию бизнеса, «Лаборатория Касперского»

Киберугрозы уже давно являются тем типом рисков, который может нанести серьезный ущерб бизнесу любого размера: подпортить репутацию, привести к потере денег или критически важной информации, повлечь за собой непредвиденные траты и неприятные разбирательства с клиентами, акционерами и ведомствами, контролирующими соблюдение законодательных норм. Проблема усугубляется еще и тем, что киберугрозы далеко не статичны: они множатся с каждым днем, становятся разнообразнее и сложнее, а киберпреступники, стоящие за ними, начинают все чаще применять метод целенаправленных атак на конкретные компании. Чтобы яснее понимать ситуацию в области информационной безопасности и те последствия, к которым может привести даже единичный компьютерный инцидент, представим все в цифрах и фактах, полученных на основе данных «Лаборатории Касперского» по анализу событий 2014 г., а также взглянем на киберугрозы с позиции самих компаний. Такой подход не только даст максимально полное видение ситуации, но и позволит сделать краткосрочные прогнозы на ближайший год и понять, какие именно «рубежи» стоит защищать в первую очередь.

Киберугрозы в цифрах и фактах

В 2014 г. защитные продукты «Лаборатории Касперского», предназначенные как для корпоративных, так и для домашних пользователей, заблокировали более 6 млрд вредоносных атак на компьютеры и мобильные устройства. Любопытно, как сильно возросло количество атак на смартфоны и планшеты: в частности, было зафиксировано свыше 3,5 млн атак на платформу Mac OS X, которую часть пользователей до сих пор считают неуязвимой. Кроме того, около 1,5 млрд инцидентов пришлось на устройства с мобильной ОС Android, и за минувший год число подобных атак увеличилось в четыре раза.

Кстати, именно мобильные устройства являются сегодня отдельной «головной болью» для корпоративных ИТ-инфраструктур. Использование личных смартфонов и планшетов в рабочих целях допустимо уже в абсолютном большинстве организаций, однако надлежащее управление этими устройствами и включение их в общую систему информационной безопасности компании практикуются далеко не везде. Риску подвергаются прежде всего смартфоны и планшеты на базе Android: согласно данным «Лаборатории Касперского», на эту платформу сегодня нацелено 99% вредоносного ПО, специализирующегося на мобильных устройствах.

Основной источник киберугроз, конечно же, Интернет. За весь 2014 г. эксперты «Лаборатории Касперского» обнаружили более 123 млн уникальных вредоносных файлов, пришедших из Сети. К этому стоит добавить еще почти 2 млн «зловредов», которые попадали на устройства по локальным источникам: флешкам, съемным дискам, внутренним корпоративным сетям, файловым серверам и т. д. Чтобы понять, откуда берется такое количество угроз, и представить, с какой скоростью увеличивается их численность, достаточно сказать, что ежедневно специалисты «Лаборатории Касперского» обрабатывают 325 тыс. образцов нового (!) вредоносного ПО.

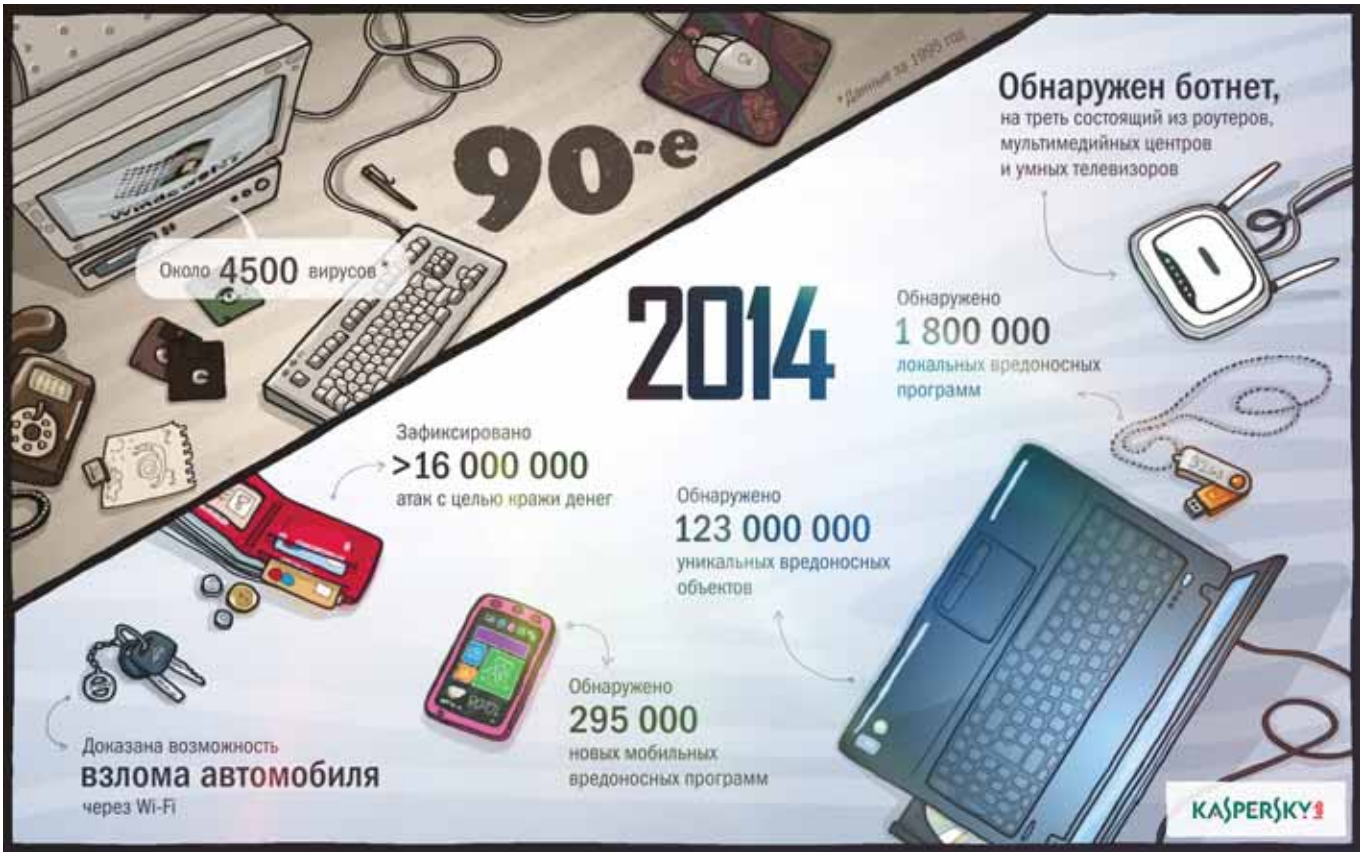
На компьютеры пользователей «зловреды» попадают чаще всего двумя способами: через уязвимости в легальном ПО и при помощи методов социальной инженерии. Разумеется, нередко встречается сочетание этих двух приемов, но злоумышленники не пренебрегают и другими уловками. Отдельная угроза для бизнеса – таргетированные атаки, которые становятся все более распространенным явлением. Но обо всем по порядку.

Уязвимости рано или поздно возникают в любом программном обеспечении. Это могут быть ошибки при разработке программы, устаревание версий

или отдельных элементов кода. Как бы то ни было, основной проблемой является не наличие уязвимости, а ее своевременное обнаружение и закрытие. К слову, в последнее время (2014 г. – яркое тому свидетельство) производители ПО начинают все активнее закрывать имеющиеся в их программах уязвимости. Однако брешей в приложениях все равно хватает, и киберпреступники используют их для проникновения в корпоративные сети. В 2014 г. 45% всех инцидентов, связанных с уязвимостями, были спровоцированы «дырами» в популярном ПО Oracle Java. Кроме того, в прошедшем году был отмечен «переломный момент» – обнаружена уязвимость в распространенном протоколе шифрования OpenSSL, получившая название Heartbleed. Эта ошибка позволяла злоумышленнику читать содержимое памяти и перехватывать личные данные в системах, использующих уязвимые версии протокола. OpenSSL широко применяется для защиты данных, передаваемых через Интернет (в том числе информации, которой пользователь обменивается с веб-страницами, электронных писем, сообщений в интернет-мессенджерах), и данных, передаваемых по каналам VPN (Virtual Private Networks), поэтому потенциальный ущерб от этой уязвимости был огромным. Не исключено, что эту уязвимость злоумышленники могли использовать как старт для новых кампаний кибершпионажа.

В отличие от уязвимостей, которые киберпреступники эксплуатируют, не затрагивая напрямую пользователей, метод социальной инженерии предполагает контактирование с потенциальной жертвой. Путем обмана, мошенничества, игры на чувствах пользователей злоумышленники вынуждают человека самостоятельно загружать вредоносный файл на компьютер или вводить нужную им информацию на фишинговых сайтах. Именно так, например, поступали киберпреступники в рамках кампании кибершпионажа Darkhotel, раскрытой «Лабораторией Касперского» в 2014 г. и затронувшей руководителей ряда известных организаций. Механика этих атак была тщательно продумана: после того как жертва заселялась в отель и подключалась к взломанной Wi-Fi-сети, указывая свою фамилию с номером комнаты, ей автоматически предлагалось скачать обновление для популярного ПО – GoogleToolbar, Adobe Flash или Windows Messenger. В реальности же это действие приводило к установке вредоносного ПО, которое и помогало киберпреступникам похищать конфиденциальные данные.

Количество организаций, ставших жертвами целенаправленных кибератак и кампаний кибершпионажа, увеличилось в 2014 г. почти в 2,5 раза. За прошедший год почти 4,5 тыс. организаций по меньшей мере в 55 странах, в том числе в России, стали целью киберпреступников. Кража



Оценка темпа роста киберугроз: 1990-е против 2010-х

данных произошла как минимум в 20 различных секторах экономики, включая государственные, телекоммуникационные, энергетические, исследовательские, индустриальные, здравоохранительные, строительные и другие компании. Киберпреступники крали пароли, файлы, геолокационную информацию, аудиоданные, делали снимки экранов и контролировали веб-камеры. Скорее всего, в некоторых случаях эти атаки имели поддержку государственных структур, другие же с большей вероятностью осуществлялись профессиональными группировками кибернаемников.

В последние годы Центр глобальных исследований и анализа угроз «Лаборатории Касперского» отслеживал деятельность более 60 преступных групп, ответственных за кибератаки, проводимые по всему миру. Их участники говорят на разных языках: русском, китайском, немецком, испанском, арабском, персидском и др.

Последствия таргетированных операций и кампаний кибершпионажа всегда крайне серьезны. Они неминуемо заканчиваются взломом и заражением корпоративной сети, нарушением бизнес-процессов, утечкой конфиденциальной информации, в частности интеллектуальной собственности. Давайте посмотрим, насколько готовы к новым угрозам российские компании.

Киберугрозы глазами самих компаний

«Лаборатория Касперского» при содействии независимой компании B2B International ежегодно проводит исследования с целью выяснить отношение ИТ-специалистов к вопросам информационной безопасности. Подобные регулярные опросы дают возможность понять, как современный бизнес воспринимает киберугрозы, как часто компании с ними сталкиваются, от каких типов атак и угроз они страдают чаще всего, какие несут потери, какие меры защиты применяют и как распределяют бюджет на ИТ.

Последнее такое исследование было проведено в 2014 г., и оно показало, что абсолютное большинство российских компаний (91%) недооценивают количество существующего на сегодняшний день вредоносного ПО. Более того, они даже не предполагают, что число «зловредов» постоянно увеличивается.

Возможно, это заблуждение и привело к тому, что в 2014 г. 98% российских компаний столкнулись с теми или иными киберинцидентами, источники которых находились, как правило, вне самих предприятий. Для сравнения: в предыдущем году таких компаний было на 3% меньше. Кроме того, в 87% организаций были зафиксированы также инциденты, обусловленные внутренними угрозами. В обоих случаях около четверти пострадавших компаний лишились важной конфиденциальной информации, а финальная сумма ущерба для крупных компаний в среднем составила 20 млн руб. за каждую успешную кибератаку, а для предприятий среднего и малого бизнеса – почти 800 тыс.

Мнение специалиста

Рустэм ХАЙРЕТДИНОВ,
CEO компании Appercut Security:

Целенаправленные атаки действительно стали самой большой головной болью служб информационной безопасности. Использование «уязвимостей нулевого дня», социальной инженерии, специально написанного зловредного программного обеспечения, отвлекающие маневры ложными атаками и сокрытие следов с помощью DDoS-атак и другие способы, требующие высокой квалификации атакующих, – реалии сегодняшнего дня. Классические системы защиты – антивирусное программное обеспечение, межсетевые экраны, системы обнаружения вторжений – уже не могут обеспечить привычного уровня защиты информационных активов. Все это накладывается на негативный кризисный, санкционный информационный фон, когда достаточно «положить» сайт крупного банка и вбросить в соцсети «банк перестал проводить платежи», чтобы спровоцировать вкладчиков снимать сбережения. Поэтому и противодействие таким угрозам должно быть комплексным, учитывающим все возможные инструменты атаки, анализ корреляций разных опасных активностей в сочетании с активным мониторингом соцсетей для быстрой и адекватной реакции на информационные вбросы.

Мир информационных технологий изменился, в кризисные времена Интернет остается самым дешевым каналом для привлечения и обслуживания клиентов, информационные технологии позволяют существенно сократить транзакционные расходы, поэтому большинству компаний еще предстоит переосмыслить свой подход к информационной безопасности в новых условиях.

Среди внешних киберугроз наибольшее опасение у бизнеса по-прежнему вызывает вредоносное ПО – этот тип угроз беспокоит 77% опрошенных ИТ-специалистов. 74% компаний озабочены проблемой спама. Около четверти респондентов признались, что они видят угрозу для бизнеса в фишинговых атаках (28%), корпоративном шпионаже (26%) и сетевых вторжениях (23%). Также компании обеспокоены распространением DDoS-атак, кражей мобильных устройств и крупного оборудования, злонамеренным вредительством. Однако лишь 10% из них считают, что сегодня стоит опасаться таргетированных атак, а между тем это одна из основных и быстро набирающих обороты угроз для бизнеса.

Из числа внутренних угроз почти половину компаний беспокоят уязвимости в ПО, и это хороший показатель, говорящий о том, что бизнес начинает осознавать опасность и пытается ее нивелировать. Кроме того, переживают компании из-за возможности случайной или намеренной утечки данных – об этом сообщили в общей сложности более половины опрошенных ИТ-специалистов. Значительную долю компаний (около 20%) волнуют утечка данных через мобильные устройства, потеря мобильных устройств сотрудниками и мошенничество работников. Любопытно, что 13% ИТ-специалистов заявили, что не переживают из-за внутренних угроз. Возможно, это объясняется тем, что в ряде компаний не принято разделять киберугрозы на внешние и внутренние. Кроме того, среди российских руководителей служб ИТ и ИБ есть такие, которые предпочитают решать все проблемы с внутренними угрозами посредством запретов. Однако если человеку что-то запрещено, это вовсе не означает, что он этого не делает. Поэтому любые политики безопасности, в том числе запрещение, требуют соответствующих инструментов контроля, которые позволят гарантировать соблюдение всех требований.

Что касается типов информации, интересующей злоумышленников прежде всего, то, как показало исследование, представления компаний и реальное положение дел существенно различаются. Сами компании больше всего боятся потерять информацию о клиентах, финансовые и операционные данные, а также интеллектуальную собственность. Немного меньше бизнес переживает за информацию по анализу деятельности конкурентов, платежную информацию, персональные данные сотрудников и данные о корпоративных счетах в банках. На деле же киберпреступники чаще всего крадут внутреннюю операционную информацию компаний (в 56% случаев), однако защищать эти данные в первую очередь считают необходимым лишь 15% компаний. Приоритет номер 2 для злоумышленников – персональные данные сотрудников: именно они крадутся в 26% киберинцидентов. А уделять повышенное внимание защите этого типа данных собираются лишь 7% компаний. Четверть инцидентов заканчивается утечкой финансовых данных – и вот здесь можно говорить о некотором соответствии ожидания и реальности, поскольку 19% компаний намерены защищать подобную информацию особенно тщательно. Любопытно, что информация о клиентах, которую компании боятся потерять больше всего, интересует злоумышленников лишь в четвертую очередь. Возможно, это объясняется тем, что в России конкурентный кибершпионаж пока не так развит, как за рубежом.

Если говорить о способах защиты от киберугроз, то наиболее

Мнение специалиста

Георгий ГАРБУЗОВ,

руководитель отдела консалтинга Центра информационной безопасности, компания «Инфосистемы Джет»:

Сегодня киберугрозы заняли далеко не последнее место в ряду других рисков уровня business critical: уже никому не нужно доказывать, что риски, связанные с ИБ, реальны и чреваты действительно серьезными потерями. Равно как и не осталось организаций, которые не знали бы о киберугрозах и не начинали бы борьбу с ними. При этом ландшафт угроз достаточно обширен (от простых вирусов, DDoS-атак и утечек до сложных APT-атак). Поэтому практически относительно любой организации можно смело утверждать, что как минимум одна из угроз точно была реализована. Одновременно с этим поток информации о новых уязвимостях и хакерских группировках столь велик и изменчив, что в нем с легкостью можно упустить нечто реально угрожающее конкретной компании.

В результате на первый план выходит необходимость грамотного построения модели угроз для каждой отдельной организации, так как даже в рамках одной отрасли они могут существенно различаться – бизнес-процессы у всех разные. Для одних компаний критично обеспечить бесперебойную работу веб-приложений, для других – не допустить даже минимальной утечки данных. Защитить можно все, но затраты на построение такой ИБ-системы, скорее всего, в разы превысят стоимость всего возможного ущерба.

ИБ-угрозы и борьба с ними стали вполне обыденным явлением, и бизнес начал просчитывать их (по аналогии с прочими рисками), сравнивая расходы на предотвращение с величиной ущерба в денежном эквиваленте. Наша практика показывает, что на первое место выходят риски прямой потери денег от внутреннего мошенничества или в результате действий внешних злоумышленников. При этом внутреннее мошенничество имеет больший приоритет, так как потери от него понятны. Что касается внешних атак, то здесь, прежде всего, необходимо говорить о защите систем, в которых обращаются деньги (или с помощью которых они зарабатываются). Самый яркий пример – это веб-приложения.

распространенной мерой обеспечения информационной безопасности в российских организациях до сих пор остается антивирусное ПО. Вместе с тем, сегодня около 40% ИТ-специалистов полагают, что компанию необходимо защищать от таргетированных атак. Более того, они прекрасно понимают, что стандартный антивирус не поможет им решить эту задачу, и настаивают на построении комплексной системы защиты, охватывающей всю ИТ-инфраструктуру предприятия. Около трети ИТ-специалистов считают необходимым всеми мерами предотвращать утечку данных и противодействовать DDoS-атакам, делающим недоступными веб-ресурсы компании. Эти цифры позволяют предположить, что компании не только начинают уделять внимание нейтрализации прямых финансовых рисков, но и стремятся избежать ущерба для своей репутации, который неизбежен в случае утечки данных или неработоспособности важных веб-ресурсов.

Однако если говорить о применяемых методах защиты, то оказывается, что сегодня 60% российских компаний концентрируют свои усилия на защите от вредоносного ПО. Более половины организаций также взяли в свои руки управление обновлениями и делают все возможное для своевременного закрытия уязвимостей в ПО. Наконец, более трети (38%) организаций применяют практику контроля приложений, т. е. ограничивают использование некритичных для бизнеса программ, избегая ряда уязвимостей.

В целом же необходимо помнить, что надежная защита от всего многообразия киберугроз базируется на трех важных составляющих: использование современного качественного защитного ПО, применение политик безопасности, регулирующих права доступа пользователей к различной информации и сервисам, обучение персонала правилам работы с конфиденциальной информацией.

Чего ждать в ближайшее время

Мы предполагаем, что в 2015 г. целевые атаки на компании будут все быстрее набирать обороты. Причем подобные вредоносные кампании будут скорее не масштабными международными операциями, спонсируемыми государствами, а локальными диверсифицированными атаками, которые будут проводиться небольшой группой хакеров в отношении конкретных организаций (не обязательно крупных). При таком подходе кампании кибершпионажа будет сложнее выявить, следовательно, число предприятий, которые могут пострадать от действий киберпреступников, вероятно, увеличится.

В зоне особого риска будут финансовые организации. Как показывают события последних месяцев, злоумышленники все больше интересуются возможностью украсть деньги напрямую у банков, платежных сервисов и других финансовых компаний. В погоне за прямой выручкой киберпреступники с большой долей вероятности будут атаковать не только интернет-сервисы банков и платежных систем, но и банкоматы, терминалы самообслуживания, системы мгновенных платежей, даже кассовые аппараты. В 2014 г. подобные прецеденты уже были: так, «Лаборатория Касперского» раскрыла операцию Tyupkin, в ходе которой злоумышленники похитили миллионы долларов из банкоматов, предварительно заразив их вредоносным ПО.

Разумеется, одну из основных опасностей для целостности корпоративной сети и сохранности конфиденциальной информации

Мнение специалиста

Алексей ФИЛАТЕНКОВ,

руководитель направления информационной безопасности, компания «Открытые технологии»:

Автор приводит очень интересное исследование, поскольку оперирует данными «Лаборатории Касперского», которая находится на переднем крае борьбы с киберугрозами. При этом автору удается избежать опасности однобокого подхода, связанного с анализом только атак со стороны хостов корпоративной сети за счет ссылок на статистику инцидентов ИБ, которая была предоставлена самими компаниями-заказчиками.

Предъявленная статистика еще раз показывает рост угроз, связанных с использованием мобильных устройств в корпоративной сети (концепция BYOD). Также по-прежнему актуальными являются и «классические» каналы проникновения вредоносного ПО в корпоративную сеть. Существенно, что во многих случаях до конца не решена проблема спама.

Очень интересными являются признания компаний, что во многих случаях единственным используемым средством защиты их сети является антивирусное ПО. При приведенной статистике роста целенаправленных или таргетированных атак наличие комплексной системы ИБ становится просто обязательным.

Вместе с тем компании весьма правильно расставляют приоритеты в защите информации и акцентируют внимание на важности сохранения информации об операционной деятельности. Правильное управление операционными рисками компании (куда входят и риски ИБ) позволяет обосновать затраты на ИБ и значительно сократить возможный ущерб.

Также можно согласиться с автором, что одной из актуальных угроз будущего станет «опасный» Интернет вещей. По крайней мере, уже сейчас нужно рассматривать указанные устройства как дополнительный канал проникновения вредоносного ПО в корпоративную сеть.

Однако в статье не упомянуты киберугрозы, связанные со все возрастающем присутствием государственных институтов в киберпространстве. В нынешнее нестабильное время следует ожидать повышения роли государства как при формировании требований к защите данных, так и в форме непосредственного участия в кибервойнах.

_ Мнение специалиста

Вячеслав МЕДВЕДЕВ,

ведущий аналитик отдела развития, ООО «Доктор Веб»:

Тема уровня угроз и уровня защиты от них, затронутая в статье, не столь однозначна, как это кажется большинству. Действительно (и это отражено в используемой в статье статистике), среднее количество вредоносных файлов, создаваемых злоумышленниками в месяц, растет год от года. Киберпреступники постоянно отслеживают популярность операционных систем и приложений и пытаются в них внедриться. Но проблема состоит в том, что данный факт привычен для потенциальных жертв и воспринимается ими так же, как и новости о катастрофах и убийствах, то есть игнорируется: «Вирус может поймать только ламер, а я знаю, что делаю».

Более того, даже если пользователь, администратор или руководство компании решают защититься (и защититься на самом деле, а не в связи с требованиями регуляторов, что происходит достаточно часто), при выборе мер и средств защиты они руководствуются неверными знаниями о возможностях средств защиты – и это тоже показывает статистика. СМИ постоянно сообщают о заражениях, но пользователи все так же полагают, что проблема защиты от вирусов – это проблема выбора между вендорами, а не смена принципов защиты. Встречи клиентов с продавцами начинаются с вопросов о наличии модного функционала, а не с того, как решить проблему безопасности компании.

Итог закономерен: количество заражений и финансовых утечек не снижается – а значит, на рынок будет приходить все больше тех, кто считает, что сольдо по праву умных должны перейти к ним.

по-прежнему будут представлять уязвимости в ПО. Обнаружение критических «дыр» в важном и широко используемом программном обеспечении (в частности, в протоколе шифрования OpenSSL) привело к тому, что ряд ключевых программ теперь проходит проверку на наличие уязвимостей. А это, в свою очередь, означает, что в 2015 г. будут обнаружены новые бреши в старых программах. Следовательно, вопросу управления обновлениями ПО следует уделить особое внимание.

Интернет вещей перестал быть идеей фантастов и все активнее проникает в повседневную жизнь, в том числе в бизнес. Корпоративные сети уже сегодня включают в себя сетевые принтеры и телевизоры Smart TV. Кроме того, многие технологические системы в современных офисных зданиях также подключены к Глобальной сети. Эти обстоятельства могут привести к тому, что киберпреступники будут использовать новые «точки входа» для проникновения в корпоративные ИТ-инфраструктуры, например сетевые принтеры. Не исключены и атаки в целях киберсаботажа и выведения из строя офисных систем жизнеобеспечения. Таким образом, компаниям придется решать вопросы по расширению периметра системы информационной безопасности и включению в него ряда новых устройств и сервисов. ■

Размах утечек информации

Согласно отчету по Индексу критичности утечек данных (Breach Level Index), опубликованному компанией Gemalto, в 2014 г. в мире зафиксировано более 1,5 тыс. утечек данных, в результате которых скомпрометировано около одного миллиарда записей. Полученные результаты свидетельствуют о том, что по сравнению с 2013 г. количество утечек данных увеличилось на 49%, а количество похищенных или скомпрометированных записей данных – на 78%. Изначально составлявшийся компанией SafeNet (приобретена Gemalto в 2014-м) Индекс критичности утечек данных (BLI) представляет собой глобальную базу данных утечек, пополняемую по мере публикации новостей об этих инцидентах. Индекс обеспечивает специалистам в области безопасности методологию и инструмент для оценки критичности того или иного взлома, позволяющий увидеть, какое место этот взлом занимает среди других инцидентов, информация о которых опубликована в открытых источниках. По данным индекса BLI, основной целью киберпреступников при осуществлении атак в 2014 г. стали персональные данные – на долю подобных атак пришлось 54% всех инцидентов, что больше, чем в любой другой категории, в том числе больше числа инцидентов с кражей финансовых данных. Кроме того, на долю утечек, преследовавших цель хищения персональных данных, пришлось около трети наиболее значимых взломов, которые были классифицированы в рамках индекса BLI как катастрофические (балл BLI в пределах от 9 до 10) и серьезные (балл от 7 до 8,9). Доля так называемых безопасных утечек, подразумевающих нарушение целостности периметра безопасности, при котором скомпрометированные данные были полностью или частично зашифрованы, увеличилась с 1 до 4%. Наряду с увеличением количества хищений персональных данных в прошлом году ужесточился и характер утечек данных: около двух третей из 50 наиболее серьезных инцидентов по критериям BLI произошли в 2014-м. Кроме того, количество утечек данных, в результате которых было скомпрометировано более 100 млн записей данных, удвоилось по сравнению с 2013 г. Чаще всего утечки происходили в розничной торговле и в секторе финансовых услуг.

www.gemalto.com