УДК 338

СОВРЕМЕННЫЕ УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Казарян М. Т., старший преподаватель
Кузбасский государственный технический университет
имени Т. Ф. Горбачева
г. Кемерово

В современных условиях неотъемлемой частью жизни общества является выход в мировую систему Интернета. Возрастает общий поток информации, возникает потребности в новых инструментах оптимизации работы каждого экономического субъекта. Для сокращения бумажного документооборота и упрощения процедур подачи документы в государственные органы, начали функционировать системы по передачи данных по различным формам во Всемирную сеть.

На сегодняшний день разработаны различные программы по упрощению документооборота. Первоначально программные продукты предназначались для автоматизации деятельности на предприятиях непосредственно по бухгалтерскому учету и финансовой отчетности. На данный момент подобные программы способны решать задачи на всех уровнях организации по отделам, а так же отдельным операциям, позволяя аккумулировать все данные об оказываемых услугах, предоставляемых продуктах, а так же по выполняемым работам не только на предприятии, но и для лиц непосредственно участвующих в рыночных отношениях.

Для успешного функционирования организации необходимо предоставлять достоверную информацию в удобном и доступном виде для каждого сотрудника, в размере его компетенций. При использовании документации возникает сложность их хранения, поиска, а так же систематизации и сортировки, что вызывает немало проблем. Системы электронной отчетности, позволяют управлять рабочими процессами организации, а так же оперативно отправлять необходимую информацию.

При всех положительных свойствах данных систем электронной отчетности важно так же помнить и об угрозах, которые возникают при использовании данных программ.

Защита информационной безопасности является приоритетной при использовании электронных программ по финансовому и бухгалтерскому учету, представляет собой целый комплекс задач по обработке, сохранению и передаче данных от организации всем контрагентам (поставщикам и покупателям), а так же государственным органам (пенсионный фонд, налоговая инспекция, Росстат, Фонд социального страхования РФ, служба Росалкоголь регулирования). Для безопасности подобных операций требуется договор с ФНС (Федеральной налоговой службой) о сдаче бухгалтерской отчетности через интернет, а так же ключи доступа [2].

Следует так же всегда помнить о программах ransomware, созданных специально для того, чтобы получать деньги от пользователей Интернет-ресурсами путем вымогательства [3]. Если вредоносная программа попала на носитель, то возможно несколько вариантов вымогательства средств: шифрование файлов в системе, блокировка или помеха работе в системе или же блокировка и помеха в работе браузеров. Суть проста: пока злоумышленник не получит деньги - вы или ваше предприятие полностью или частично не можете осуществлять свою деятельность, в случае, если электронный документооборот неотъемлемая часть рабочего процесса, так как документы зашифровываются, или перечисленные функции становятся недоступными, не смотря на работоспособность компьютера [1].

Таким образом может быть похищена не только информация по деятельности предприятия, но и персональные данные сотрудников, которые используются для расчета заработной платы и формирования отчетности. Для безопасности, согласно Федеральному закону "О персональных данных" от 27.07.2006 N 152-ФЗ необходимо шифровать такие данные при помощи криптографической защиты.

В настоящее время в связи с увеличивающимся спросом на мониторинг и предотвращение угроз, защиту брендов, аудит экономической безопасности компьютерную криминалистику, расследование киберпреступлений и случаев мошенничества непосредственно в сети Интернет появляются компании, занимающиеся комплексным решением данных задач.

Исследование угроз, так называемый threat intelligence решает множество задач, связанных с импортом и экспортом данных об инцидентах, индикаторов угроз, а так же обеспечения конфиденциальности и целостности обмениваемых данных, хранящихся на сервере и опубликованных в сети Интернет. В качестве возможных источников индикаторов угроз для threat intelligence выделяют несколько причин, по которым возможна утечка данных: уязвимость веб-браузеров, через ботнет, уязвимость клиентов электронной почты и операционных систем, через игровые сервисы, а так же путем скачивания данных с непроверенных сайтов.

Чаще всего устройства подвержены атакам в то время как сотрудники «путешествуют по просторам» глобальной сети в первую очередь в свое свободное от работы время, а так же в поисках необходимой информации по работе, по возникающим вопросам, тем самым, подвергая систему опасности со стороны киберпреступников, которые преимущественно нацелены на счета и базы данных коммерческих организаций. Невозможно с первого взгляда понять и определить какая страница из списка результата поиска несет угрозу для системы безопасности, поэтому в таких случаях необходимо поставить ограничение к сайтам, с развлекательным контентом, чтобы сотрудники не тратили оплачиваемое рабочее время, установить нормативно-правовое обеспечение коммерческого или некоммерческого типа, позволяющие вовремя получать актуальную информацию для работы каждого отдела.

Максимальный результат позволяют достичь программы отслеживания активности сотрудника, фиксирующие, сколько времени было проведено на том или ином ресурсе, а так же в каких рабочих программах и какие процессы протекали.

В таблице 1 представлено процентное соотношение атак по типам на малый, средний и крупный бизнес.

Таблица 1 – Типы атак на малый, средний и крупный бизнес в 2015 году, %

Типы атак	средний и малый бизнес	крупные компании
программы-вымогатели	38%	15%
фишинг	36%	8%
DDoS-атаки	17%	37%
мобильные мошенничества	13%	7%
атаки с целью шпионажа	3%	14%
хищения через интернет-банкинг	1%	9%
прочие типы атак	11%	19%
затруднились ответить	3%	18%

Количество компаний, принявших участие в исследовании по ущербу экономики России от киберпреступности в 2015 году среди малого и среднего бизнеса 58 %, среди крупного бизнеса и государственных структур 42 %.

Для того чтобы в случае нападения или потери информации полностью или частично важно иметь некоторое преимущество для возмещения потерь. В первую очередь это касается резервов денежных средств, позволяющие устранить последствия вредоносных программ, наладить технологический процесс, восстановить потерянные данные или же создать новые базы. Еще один важный процесс, мероприятия по которому должны проводиться непрерывно это защита собственности и активов компании, путем анализа уязвимых мест компании, выработка способов, стратегии защиты, контроль за активами, устранение недостатков в оформлении документов, снижение привлекательности активов для конкурентов и киберпреступников. Конкурентное преимущество на рынке даст возможность при возникновении чрезвычайных ситуаций удержаться на рынке в течение определенного количества времени, тем самым позволит восстановиться компании и нарастить темпы финансовых и производственных процессов. Так же необходимо помнить о возможности инвестирования в компанию денежных средств, капитала и других источников для компании, для чего необходимо следить за привлекательностью вложения в компанию, налаживание связей с инвесторами и качеством предоставляемых товаров, работ или услуг. Для того, чтобы избежать внутренних угроз утечки информации необходимо повышать корпоративную культуру и этику на предприятии, так как в случае удовлетворенности работниками условий и оплаты труда, общей сплоченности и целеустремленности на общий результат риск передачи корпоративной информации и персональных данных работников снижается.

Важно помнить так же и о деловой репутации компании, позволяющей лояльно относиться подрядчикам и контрагентам к предприятию независимо от форс-мажорных ситуаций.

В условиях глобализации технологии защиты и инструменты по предупреждению компьютерных атак разрабатываются в ответ на создаваемые продукты, способные нанести вред деятельности организаций, тем самым нарушить работу отдельного участка, или же привести к остановке функционирования всего предприятия в целом. Для того чтобы на первых стадиях обнаружить опасность нужно проводить комплекс мероприятий для предупреждения и защиты от возникающих угроз. Прежде всего, необходимо периодически не только делать резервную копию данных с компьютера, но и проверять ее целостность, использовать лицензионный антивирус, а так же проводить проверки данных, находящихся в базе, наличие на компьютере антивируса уровня Internet Security со свежими базами перед первым запуском всех новых программ так же важно проверять их на наличие скрытых угроз, устраивая проверку антивирусом. Если при переходах по страницам в Интернет пространстве есть подозрение, что источник не проверен, то следует запускать такие программе в безопасном режиме (каждый браузер предлагает различные режимы и инструменты безопасности). Разработчики операционных систем регулярно производят обновление параметров и расширение возможностей распознавания и борьбы с вредоносными программами, которые поступают на устройства пользователей, позволяя сделать систему устойчивее.

Несмотря на опасности, таящиеся при использовании электронного документооборота популярность его не уменьшается. В России развитие данного рынка еще только набирает обороты, в отличие от более опытных зарубежных коллег. Так, с января по март 2016 года за счет хакерских атак американские компании понесли убытки в размере $209 млн. При сравнении полученной цифры с убытками годом ранее — тогда размер потерь за весь год составил в целом $206 млн.

В сентябре Datto — американская компания, оказывающая услуги по кибербезопасности — подготовила отчет, в котором оценила убытки от ransomware-вирусов (программы-вымогатели) в $75 млрд. ежегодно. Компания опросила 1 100 ИТ-специалистов и обнаружила, что 92% из них сталкивались с ransomware-атаками в прошлом году и 40% из них сталкивались с атаками не менее шести раз. В отчете сказано, что лишь в одном случае из четырех жертвы обращаются за помощью в ФБР или другие правоохранительные органы. [4]

Стоит также отметить необходимость совершенствования российской правоприменительной системы по киберпреступлениям и иным действиям, нарушающим права компаний и ведущим к финансовым потерям, связанным с Интернет-пространством. Зачастую, хакеры целенаправленно выбирают для атак компании, для которых потеря информации критична и работа без старых данных становится невозможна. Примерами подобных организаций

можно использовать медицинские центры, лаборатории, высокотехнологичные производства, государственные правоохранительные структуры, корпоративный сектор. Все угрозы можно разделить на внутренние и внешние. Внутренние характеризуются деструктивными действиями со стороны сотрудников компании как умышленные, так и случайные. К внешним же факторам относятся действия кибер-преступников, хакеров, интернет-мошенников, недобросовестных партнеров, криминальных структур. Соответственно можно выделить следующие виды угроз финансово-экономическим интересам компании: мошенничество; присвоение активов и интеллектуальной собственности; взяточничество, коррупция; подделка продукции; кража или разглашение коммерческой тайны; недобросовестная конкуренция, промышленный шпионаж; недружественное поглощение и рейдерские захваты.

Стоит отметить, что в российском законодательстве ответственность за киберпреступления и мошенничество квалифицируются лишь несколькими статьями уголовного кодекса, что говорит о небольшом опыте в данной области, но наибольшая юридическая нагрузка приходится на Уголовный Кодекс. Так, в состав главы 28 УК РФ «Преступления в сфере компьютерной информации» входит три статьи «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273), «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274). Вместе с данными статьями так же применяется статья 159 «Мошенничество», а именно 159.3 «Мошенничество с использованием платежных карт» и 159.6 «Мошенничество в сфере компьютерной информации», глава 21 «Преступления против собственности»[5].

Таким образом, можно сделать вывод о том, что защита от потери и утечки информации, персональных данных, финансово-экономических отчетностей, защита всего электронного документооборота, а так же технологий и инноваций находится в руках, прежде всего самих компаний. Руководители сами принимают решение о необходимости и степени защиты своих данных, но даже применение всех возможных инструментов не дает 100% гарантии безопасности, так как технологии в условиях глобализации постоянно развиваются как в области киберпреступности, так и в ответной разработке противодействия ей.

Список литературы:

1. Проблемы квалификации преступлений, связанных с хищением денежных средств в системах интернет-банкинга [электронный ресурс] – режим доступа: http://www.group-ib.ru/index.php/212-pressa-o-nas/zashchita-informatsii-insajd/1001-problemy-kvalifikatsii-prestuplenijsvyazannykh-s-khishcheniem-denezhnykh-sredstv-v-sistemakh-internet-bankinga%22 (дата обращения 22.07.2018)

2. Подход к формированию требований к защите информации в АСУ [электронный ресурс] – режим доступа: http://documentooborot.com/otchetnost/otchet-v-elektronnom-vide-v-nalogovuyu-sluzhbu.html (дата обращения 12.03.2019)

3. Ransomware. Вирус-вымогатель. [электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Ransomware (дата обращения 12.03.2019)

4. Без страха и упрёка [электронный ресурс] // https://vc.ru/p/ransomware

5. Преступления в сфере информационных технологий – Режим доступа: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий (дата обращения 12.03.2019)