ЗАЩИТНЫЙ РЕФЛЕКС

КИБЕРПРЕСТУПЛЕНИЯ ЕЖЕГОДНО ОБХОДЯТСЯ МИРОВОЙ ЭКОНОМИКЕ В МИЛЛИАРДЫ ДОЛЛАРОВ. РАСХОДЫ НА ИНФОРМАЦИОННУЮ ЗАЩИТУ СТАНОВЯТСЯ СЕРЬЕЗНОЙ СТАТЬЕЙ БЮДЖЕТОВ НЕ ТОЛЬКО ЧАСТНЫХ КОМПАНИЙ, НО И ГОСУДАРСТВА. МАРИЯ ПОПОВА

К 2020 году киберпреступность будет обходиться мировой экономике более чем в $1 трлн, прогнозируют в международной исследовательской компании IDC. Количество атак растет, говорит старший менеджер отдела услуг в области управления ИТ и ИТ-рисками Ernst & Young (EY) Андрей Абашев.

Масштабы и сложность киберпреступлений сегодня настолько высоки, что 40% из почти 2 тыс. опрошенных PwC руководителей компаний считают их самой серьезной угрозой для бизнеса. По словам руководителя практики анализа и контроля рисков PwC в России Тима Клау, инвесторы связывают с дестабилизирующим влиянием новых технологий риски, которые в ближайшие 12 месяцев будут препятствовать росту доходов компаний.

В России, по данным аналитического центра НАФИ, в 2017 году 46% малых предприятий и 62% крупных сталкивались с кибератаками. 22% всех организаций понесли реальные финансовые потери, размер которых в НАФИ оценивают в 116 млрд руб.

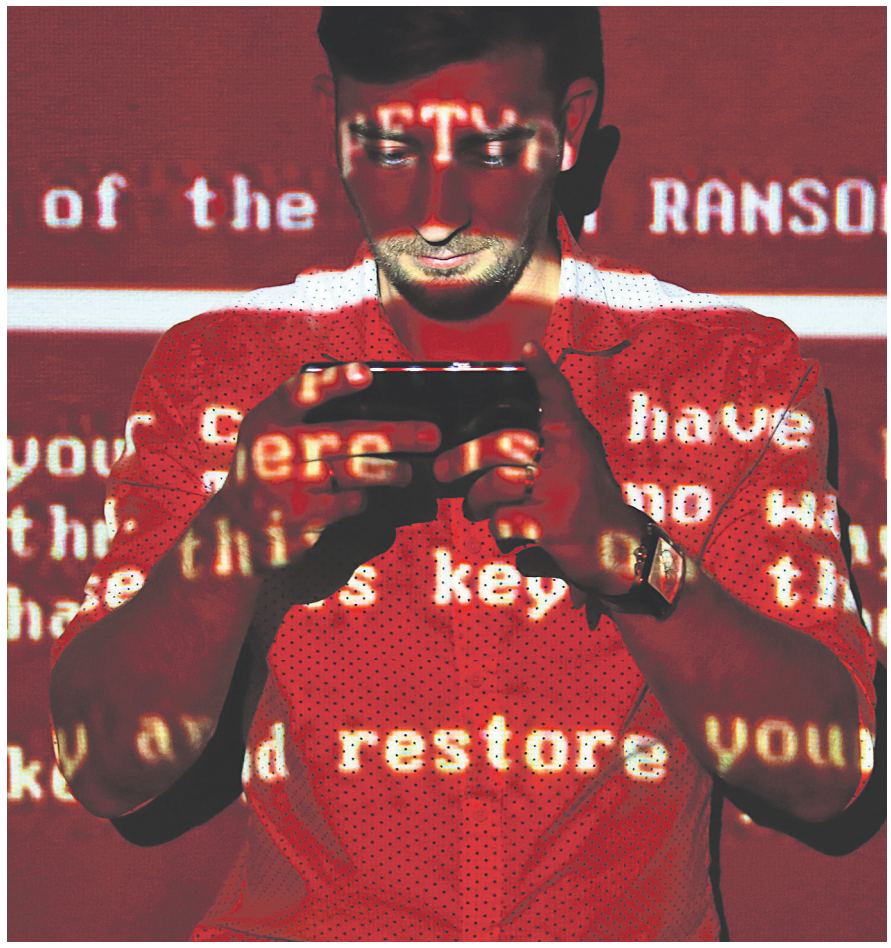

ФОТО: АЛЕКСАНДР РЮМИН/ТАСС

ОХОТА НА ДАННЫЕ

«Стремительный рост использования новых технологий в рамках реализации стратегий по цифровизации компаний повышает уровень рисков, в том числе связанных с кибербезопасностью», — считает Андрей Абашев. Целевые атаки стали менее предсказуемы, а противостоять им становится все дороже.

Ключевым товаром для киберпреступников остаются данные. Их можно зашифровать в целях получения выкупа (ransomware — вредоносный софт, действующий как шифровальщик-«вымогатель»), можно продать, можно использовать для проведения недобросовестных транзакций и т.д. По мере распространения интернета вещей (Internet of Things, IoT) появляются также программы-«вымогатели», блокирующие «умные» устройства, требуя выкуп за восстановление доступа к ним. Заражение подключенных устройств в целом набирает обороты — в 2017 году только ботнет Hajime смог охватить 300 тыс. таких объектов (данные «Лаборатории Касперского»).

Вымогательство, мошенничество с использованием корпоративной почты, а также трояны остаются наиболее популярными методами работы киберпреступников, по оценке полицейской службы Евросоюза Europol. В 2017 году «вымогатели» WannaCry и Petya серьезно затронули как бизнес, так и частных пользователей. В частности, была парализована работа датской судоходной компании Maersk, нанесен ущерб индийским портам, российским нефтяным компаниям (включая «Роснефть», «Башнефть», «Татнефть») и ряду промышленных предприятий (Mars, Nivea, Mondelez, ММК). Объем ущерба превысил, по разным оценкам, $1 млрд. Потери только Maersk составили от $200 млн до $300 млн, а FedEx/TNT сообщал об упущенном доходе в размере $300 млн.

64% респондентов EY отмечают рост количества таких угроз, как фишинг и вредоносное программное обеспечение. В то же время 77% участников опроса видят наиболее вероятный источник киберугрозы в собственных сотрудниках.

Ландшафт рисков быстро меняется, и в 2018 году самой распространенной угрозой могут стать веб-майнеры для добычи криптовалюты. Специалисты израильской Check Point Software Technologies уже отмечают рост количества атак криптомайнеров, а также атак на IoT-устройства и облачных угроз.

КОМПРОМЕТАЦИЯ И УТЕЧКИ

В соответствии со всемирным Индексом критичности утечек данных (Breach Level Index) каждый день компрометируется минимум 10 млн записей. В конце 2017 года стало известно о публикации данных 57 млн пользователей и водителей такси Uber. Примерно тогда же утечка из бюро кредитных историй Equifax затронула более 145 млн американцев. Facebook допустил утечку данных 50 млн пользователей, по поводу чего основателю сети пришлось давать объяснения в конгрессе США.

В целом за 2017 год объем утечек критически важной конфиденциальной информации вырос в четыре раза, подсчитали в InfoWatch. По данным СМИ и других открытых источников, был зафиксирован 2131 такой случай — на 37% больше, чем в 2016 году. Объем скомпрометированной в результате информации, в том числе номеров полисов социального страхования, реквизитов пластиковых карт и других важных сведений, вырос с 3,1 млрд до 13,3 млрд записей. Подавляющая часть утечек была связана с кражей персональных данных (64,8%) и финансовой информации (21,1%). Самые большие объемы данных «потеряли» высокотехнологичные компании (32%), ретейл (27%) и государственные организации (23%).

ПОВСЕМЕСТНЫЕ УГРОЗЫ

Уязвимость становится повсеместной. По всему миру компании отстают от современных кибератак на десять лет и как минимум на два «технологических» поколения, показало исследование израильской Check Point. Кибератаки Gen V (атаки «пятого поколения» — на мобильные устройства, облачные ресурсы и сети) становятся все более частыми, но 97% компаний не обладают решениями, способными им противостоять. Необходимый темп модернизации сдерживают финансовые ограничения. 71% компаний, опрошенных EY, отмечают необходимость увеличения бюджета на кибербезопасность до 50%.

В общемировом масштабе рост кибератак в первую очередь касается компаний из отраслей экономики, обладающих значимым объемом капитала, — это банковский сектор, телеком, тяжелая промышленность, нефтегаз, где темпы роста цифровизации особенно высоки, а последствия возможной реализации киберугроз могут оказаться катастрофическими.

Компании из таких отраслей зачастую являются субъектами, определяющими критическую инфраструктуру страны своего присутствия, что повышает их привлекательность для злоумышленников, говорит Андрей Абашев. Объектами критической информационной инфраструктуры, в частности, считаются системы в оборонной промышленности, энергетике, связи, сфере транспорта, финансов и других отраслях.

По данным «Лаборатории Касперского», за последний год каждая вторая промышленная компания в мире пережила до пяти киберинцидентов, которые затронули критически важную инфраструктуру или автоматизированные системы управления технологическими процессами (АСУ ТП). Стоимость устранения последствий одного такого инцидента для крупного бизнеса оценивается «Лабораторией Касперского» в среднем в $456 тыс. при условии его оперативного выявления. Если же процесс займет более недели, то стоимость вырастет более чем вдвое.

В 2017 году участились атаки на банкоматы, отмечают в Positive Technologies, — киберпреступники научились контролировать их удаленно. В целом около 30% всех хакерских нападений в России приходится на банки, 26% — на госорганы, 17% — на СМИ, оценивают в Российской ассоциации электронных коммуникаций (РАЭК).

Новая зона риска — «умные» города, где жизненно важные системы обеспечивают подключенные к сети устройства: светофоры, дороги, счетчики коммунальных услуг и пр. Атаки на них могут полностью парализовать работу и жизнь города, считают в международной Positive Technologies.

ЭКОНОМИКА ЗАЩИТЫ

К 2020 году компании будут тратить до 60% корпоративных бюджетов на информационную безопасность — быстрое выявление и реагирование на кибератаки, прогнозируют в американской Gartner. В 2016 году этот показатель составлял не более 30%.

Поддержка информационной безопасности становится существенной расходной частью бюджета государств. Расходы США, например, на кибербезопасность в 2017 году выросли на $5 млрд и составили $19 млрд.

Цифровые преобразования в России делают защиту информационных систем, данных граждан и предпринимателей одним из основных приоритетов. На эти цели в федеральном бюджете предусмотрено 22 млрд руб., а также внебюджетное финансирование — 11,7 млрд руб. Кроме того, с 2018 года причинение вреда критической информационной инфраструктуре стало уголовным преступлением — согласно статье 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру РФ» за создание или распространение вредоносного ПО может последовать наказание — пять лет принудительных работ с ограничением свободы на срок до двух лет либо штраф в размере 0,5–1 млн руб. и лишение свободы на срок от двух до пяти лет.