Кибератаки: тенденции и риски

Вопрос защиты конфиденциальных и личных данных в информационном пространстве сегодня стоит как никогда остро. Любая компания, ежедневно осуществляющая обработку электронной персональной информации посредством использования портативных устройств, компьютеров, серверов, интернет-ресурсов, постоянно подвержена рискам кибератак.

Владимир Кремер
Руководитель отдела страхования финансовых рисков AIG в России

За период с середины 2014 г. по середину 2015 г. число попыток кибератак существенно возросло, но ущерб от них, нанесенный российским финансовым компаниям, снизился в 3,7 раза. Данное снижение «результативности», скорее всего, связано с массовым уходом «профессиональных» преступных групп с российского рынка на западные из-за волатильности рубля. На смену им сегодня пришли менее опытные и менее организованные киберпреступники.

Рост кибератак

Несмотря на данную положительную для России тенденцию растет не только количество самих атак, но и диапазон платформ, которые им подвергаются. С помощью вредоносного ПО для смартфонов киберпреступники способны получить доступ к электронным кошелькам и системам онлайн-банкинга, подключенным к смартфонам и планшетам. Количество существующих троянских вирусов на переносных устройствах более чем в 1,5 раза превышает количество "троянов" на персональных компьютерах. Явно обозначается тенденция увеличения количества атак на физических лиц. Если буквально несколько лет назад основная масса кибератак, способных нанести существенный материальный ущерб, происходила исключительно на корпоративном уровне, то сегодня значительно более высоким рискам подвержены простые граждане. Они – гораздо более легкая добыча для преступников, нежели крупные компании, которые тратят немалое количество денег на обеспечение безопасности собственных систем. Граждане же, к сожалению, не очень хорошо осведомлены о способах защиты и зачастую не осознают всю серьезность угрозы кибератак до тех пор, пока не увидят, что их банковский счет опустел.

Однако от кибератак страдают не только средние и крупные корпорации и физлица. Малый бизнес также подвержен такого вида преступлениям. Ввиду того, что он не может позволить себе надежной защиты от хакеров, этот сегмент, как и физические лица, становится легкой добычей даже не очень искушенных киберпреступников.

Безусловно, в такой ситуации ключевым вопросом становится поиск решений, позволяющих предотвратить хищение на ранних этапах его подготовки. К сожалению, можно отметить, что ситуация неутешительная: даже самые современные корпоративные системы защиты не лишены уязвимостей, а у абсолютного большинства компаний нет плана реагирования на случай успешной кибератаки.

Страхование киберрисков

Но до разработки систем защиты очень важно провести исследования двух типов: бизнес-исследование, показывающее, какие процессы приоритетны и должны быть максимально защищены, и обследование ИТ-систем с целью локализации наиболее важных для компании данных. После этого можно проводить анализ рисков и вероятных сценариев мошенничества, которые могут быть применимы к конкретной компании.

Кроме технических средств защиты компаниям, работающим в любой отрасли экономики, следует помнить о страховании рисков кибератак: оно способствует значительному снижению возможных финансовых потерь, выражающихся в расходах на восстановление данных и проведение расследования, а также возмещения упущенной выгоды из-за вынужденных перерывов в деятельности. Киберстрахование позволяет избежать потерь, связанных с ответственностью перед клиентами за данные, которые находятся у компании на хранении и в обработке, а также минимизировать репутационный ущерб.

Специализированные страховые продукты покрывают не только расходы на услуги сторонних ИТ-специалистов, которые проводят восстановление поврежденных данных, аудит, оперативное реагирование и расследование киберинцидентов, но и юридические расходы.

Услуга киберстрахования рисков достаточно нова на российском рынке, и компаний, предлагающих такого вида услуги, не очень много. Это построение нескольких линий обороны компании – начиная от комплексных превентивных мероприятий и активной обороны и до оплаты расходов на реагирование (ИТ-специалисты, юристы, PR). Текущий уровень киберпреступности сегодня вынуждает нас возводить укрепления вокруг данных – не пора ли удвоить оборону?

Опубликовано:
Журнал «Information Security/Информационная безопасность» #6, 2015

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

AIG