Грядут новые неприятности, а старые забудутся 1/6/25

директор отдела ИТ-консалтинга, PwC
Латвия
Dr.dat. Baiba Apine

Подробно изучив результаты проведенных в 2024 году опросов клиентов PwC о киберустойчивости предприятий (Global Digital Trust Insights Survey), можно прийти к выводу, что существенные опасения у предпринимателей вызывают вероятные издержки киберпреступлений. Они включают возможный выкуп в случае вируса-вымогателя, затраты на возобновление работы систем и потенциальные компенсации клиентам за неспособность предприятия поставить товары или оказать услуги во время ликвидации последствий кибератаки. Такие издержки могут оказаться неподъемными для малых предприятий.

Согласно докладу CERT о деятельности в 2023 году, самыми активными киберпреступниками в Латвии являются группировки хактивистов. В докладе можно найти названия тех же группировок, что принимали участие в кибератаках на Украине до официального начала войны. На Украине хактивисты довольно быстро сменили вид кибератак: по данным Национального банка Украины, уже осенью 2022 года преобладающими снова стали мошенничество и кражи. Та же тенденция наблюдается и в Латвии – при неизменно высоком уровне атак хактивистов на наших предприятиях все чаще встречаются вирусы-вымогатели и мошенники.

Чтобы не попасть в такую незавидную ситуацию, каждое предприятие должно иметь наборы двойного контроля, или мер: средства контроля управления и технологического контроля.

Касательно средств контроля управления важно, чтобы в организации были работники, отвечающие за кибербезопасность каждый в своей области. Руководитель предприятия несет личную ответственность за эффективные средства контроля кибербезопасности, при этом руководство предприятия должно понимать, является ли предприятие поставщиком существенных и важных услуг либо входит в цепочку поставок такого предприятия согласно закону «О национальной кибербезопасности», и внедрить соответствующие средства контроля, предусмотренные законом. Даже если предприятие не является субъектом данного закона, предусмотренные законом средства контроля необходимы и снизят вероятность стать жертвой киберпреступника. Руководителю по риск-менеджменту следует обеспечить, чтобы управление киберрисками не было отделено от общего управления рисками предприятия, в частности, чтобы киберриски и средства по их снижению входили в один список с геополитическими и экономическими рисками. Финансовый директор должен иметь четкое представление о необходимых вложениях в кибербезопасность, их размере и потенциальном ущербе, т. е. о том, сколько придется заплатить в случае поражения вирусом-вымогателем, нужно ли предприятию страхование от киберрисков. В свою очередь, задача юриста – обеспечить, чтобы предприятие разбиралось в законодательстве в сфере кибербезопасности и принимало меры по обеспечению нормативного соответствия. Кроме того, юрист должен заблаговременно освоить процесс документирования результата киберинцидента для нужд страхования и полиции. Руководитель предприятия по информационным технологиям (ИТ) отвечает за эффективные средства технического контроля в ИТ-инфраструктуре и системах (контроль прав доступа, тестирование программного обеспечения перед установкой, надзор за потоком сетевых данных и др.). В свою

очередь, внутренний аудитор должен удостовериться в том, что все указанные средства контроля работают и предприятие хорошо защищено от инцидентов.

На малом предприятии может не быть всех вышеупомянутых работников. В таком случае данные задачи должно выполнять руководство предприятия, при необходимости консультируясь со сторонним поставщиком услуг. Например, как минимум один раз потребуется проверка кибербезопасности, которую выполняет сторонний поставщик услуг. В идеале такие проверки нужно проводить раз в год.

Сегодняшние киберриски отличаются большей степенью вероятности и более дорогостоящими последствиями, чем прежде, – необходимо возобновить работу, возможно, заплатить вымогателю, выплачивать штрафы клиентам за неисполнение договоров о поставке товаров и услуг.
В предыдущих аналогичных опросах о кибербезопасности, например в 2018 году, в качестве наиболее существенного риска упоминалось взыскание за нарушение защиты данных физических лиц.

Несмотря на то что регулирование защиты данных физических лиц и принуждение к соблюдению условий не ослабевают, взыскания сохраняются и даже применяются, удельный вес опасений по этому поводу среди предпринимателей уменьшился в сравнении с мошенничеством и кражами в киберпространстве.