Продолжая использовать программное обеспечение, созданное и поддерживаемое в России или Беларуси, руководители предприятий должны осознавать риски

CISA, PMP, директор в сфере услуг по ИТ-консалтингу, PwC Латвия
Dr.dat. Baiba Apine

По данным опроса Global Digital Trust Insights, проведенного PwC в 2023 году, более 70% из 3522 опрошенных руководителей предпринимательской деятельности и информационных технологий заявили, что с 2020 года добились существенных улучшений в сфере кибербезопасности. Руководители действовали правильно: проведена переоценка киберрисков, переработана документация по безопасности, улучшена защита от вирусов-вымогателей, укреплено представление пользователей об информационной безопасности. Однако 2022 и 2023 годы войны изменили характер киберпреступлений. Если в 2021 году мало кто жаловался на атаки по политическим и идеологическим мотивам, то с начала войны в 2022 году удельный вес таких атак стал существенным. Активность киберпреступников, которые используют свои знания, руководствуясь политическими или идеологическими мотивами, неизменно высока и сопоставима с активностью вирусов-вымогателей и других коммерчески мотивированных преступников.

Руководители предприятий в Латвии часто делают свои компании легкой целью для злоумышленников, продолжая использовать программное обеспечение, разработанное и поддерживаемое в России. К примеру, в начале января в латвийских СМИ появилось сообщение, что камеры видеонаблюдения с российским программным обеспечением TRASSIR повсеместно используются на Украине, а также их можно приобрести на популярных в Латвии торговых интернет-площадках. Но это лишь небольшая часть. Еще есть бухгалтерия 1С, системы геопространственной информации и многое другое. Оправданий достаточно: поставщик не внесен в санкционный список, замена дорого обойдется, выбранное российское решение в два раза дешевле европейских аналогов, работникам проще работать с пользовательским интерфейсом на русском языке.

Руководители предприятий несут ответственность за соответствие законодательству и безопасность обработки информации, находящейся во владении компании. Например, за то, чтобы не использовать программное обеспечение поставщиков, внесенных в список санкций против России и Беларуси, поскольку с ними невозможно рассчитаться. Это хорошее начало, однако в контексте использования программного обеспечения этого недостаточно. Перерегистрация поставщика за пределами России или Беларуси мало что меняет по существу, поскольку команды разработчиков по-прежнему физически находятся в диктаторских государствах, где на них может оказываться воздействие с целью завладеть нашими данными или встроить вредоносное программное обеспечение в решения, поставляемые в Латвию. В ходе повседневного тестирования корпоративные ИТ-специалисты не способны выявить такие «дыры».

Каждый руководитель предприятия как рачительный хозяин обязан идентифицировать все используемое компанией российское и белорусское программное обеспечение и целенаправленно

избавиться от него, не дожидаясь включения конкретного поставщика в санкционный список. Безопасная обработка информации в первую очередь является ответственностью руководителя предприятия. В конце текущего года планируется принять закон «О национальной кибербезопасности», который недвусмысленно предписывает, что руководитель предприятия обязан осознавать киберриски и нести ответственность за кибербезопасность. Целенаправленную нетерпимость к российскому программному обеспечению руководителям предприятий следует внедрить уже сейчас, поскольку замена программного обеспечения требует времени. К примеру, Национальный банк Украины установил нетерпимость к российскому и белорусскому программному обеспечению. Несмотря на то что очищение от него началось еще в 2014 году после вторжения России в Крым, такое программное обеспечение все еще можно найти.