Ведется ли сейчас в Латвии кибервойна и что нужно делать? 1/30/24

CISA, PMP, PwC Latvija Директор IT консультации
Dr.dat. Baiba Apine

Dr.dat. Baiba Apine, CISA, PMP, PwC Latvija Директор IT консультации
Фото: Gatis Dieziņš, Министерство Обороны Латвийской Республики

В средствах массовой информации активно используется понятие «кибервойна». В рамках нынешнего фестиваля Lampa я участвовала в организованной Министерством обороны дискуссии на тему «Готовы ли мы к кибервойне?». На данный момент невозможно с уверенностью провести черту между кибервойной, на которую нужно реагировать военными средствами, и той, которую следует считать атакой в толковании Уголовного закона. В Латвии мы сейчас живем в условиях кибервойны, и предприятиям нужно считаться с необходимостью пристально следить за своей кибербезопасностью.

В отчете за 2023 год компания CERT признает, что после полномасштабного вторжения России в Украину в 2022 году DDoS-атаки на Латвию, страны – участницы Европейского союза и НАТО чаще всего организуют связанные с Россией группировки – хактивисты. Их деятельность, возможно, координируется и финансируется для достижения целей внутриполитических и внешнеполитических операций влияния России. Атаки – и удачные, и неудачные – широко рекламируются как большие успехи, ведь Интернет все стерпит.

В своей повседневной работе предприятия не могут различить, кто совершил кибератаку – военный хактивист или обычный мошенник, и каждую атаку нужно расценивать как уголовное преступление.

С 2019 года до весны 2023 года я возглавляла в Украине совет Oschadbank. Это государственный банк, второй по величине в Украине, универсальный банк, обслуживающий как предприятия, так и частных лиц по всем каналам. Для банка война началась 15 февраля с кибератак невообразимой, небывалой мощи. Мы знали, что планируемой реакцией мира будут санкции, и призвали начать их разработку. Но потерпели неудачу, ведь кибервойна невидима. Ее цель – создать хаос, чтобы облегчить военные действия «на земле». Хактивисты довольно быстро сменили вид кибератак: уже осенью 2022 года, по сообщению регулятора, преобладающими снова стали мошенничество

и кражи. Когда военные действия «на земле» затягиваются, сложно финансировать высокую мощность кибервойны.

Латвийским предприятиям нужно быть готовыми непрерывно работать в условиях кибервойны. На мой взгляд, минимальный перечень действий прост:

1. централизованная архитектура информационных систем предприятий, где данные хранятся централизованно;
2. наличие резервных копий данных и программного обеспечения. Специалисты предприятия по информационным технологиям попробовали восстановить системы из резервных копий;
3. на предприятии должен быть четко определен критически важный персонал для работы в кризисной ситуации, и эти люди должны знать, что именно они вовлечены в непрерывную деятельность;
4. необходимо избавиться от разработанных и поддерживаемых в России и Беларуси программ по обработке бухгалтерской, геопространственной информации и др.

Специалисты PwC по информационным технологиям охотно рассмотрят инфраструктуру и управление информационными технологиями предприятия, чтобы выявить риски непрерывности деятельности, и разработают точный план действий по уменьшению рисков, обеспечив оптимальность инвестиций в кибербезопасность.