Кибератаки в коммунальной и производственных отраслях могут причинить материальный ущерб, а также вызвать перерывы в производстве, в случае если промышленные системы управления неверно ориентированы. Результаты Четвертой промышленной революции (Industry 4.0) сократят частоту материальных потерь, но общий потенциал убытков вырастет. Для отраслей с высоким уровнем дигитализации нематериальные активы становятся гораздо важнее и требуют нового подхода к риск-менеджменту и страховым стратегиям.

Три коммунальных компании на Украине, Национальный департамент электроснабжения Израиля и атомная электростанция в Германии подверглись кибератакам несколько месяцев назад. Что касается транспортного, а также промышленного сектора, энергетических и телекоммуникационных компаний, то поскольку все эти предприятия все больше зависят от автоматики, робототехники, цифровых сетей и взаимозависимых устройств, они все больше и больше становятся уязвимыми в части кибератак. В отличие от утечки данных, кибератаки, направленные на критически важные элементы инфраструктуры и производителей, скорее всего, затронут промышленные системы управления (ПСУ), чтобы манипулировать или остановить производство. Текущий номер журнала Global Risk Dialogue, который издается подразделением Allianz Global Corporate & Specialty (AGCS) и посвящен рискам в корпоративном страховании, фокусируется на том, как снизить растущую угрозу кибератак в ЖКХ, сетях и умных производствах.

Особенно беспокоит недостаточная защищенность ПСУ, которые применяются для мониторинга и контроля процессов в промышленных и производственных секторах. Например, в прошлом году в США было зарегистрировано 295 киберинцидентов в промышленных системах управления. «Кибератака на ПСУ может привести к материальному ущербу, такому как пожар или взрыв, а также к перерыву в производстве (BI), – комментирует Найджел Пирсон, директор по глобальной безопасности AGCS. – Ряд ПСУ, которые до сих пор используются коммунальными и производственными компаниями, были спроектированы в то время, когда проблема кибербезопасности еще не стала приоритетной».

Кроме того, ПСУ угрожают технические неисправности и ошибки оператора, которые происходят чаще и могут быть более существенными с точки зрения последствий, но они не отражаются в отчетах по кибербезопасности.

Возможности и риски умных производств

В то время как работа ПСУ может вызвать проблемы в коммунальном секторе, аналогичный материальный ущерб и перерывы в производстве по причине кибератак случаются и в производственном секторе. Так называемые умные предприятия эры Четвертой промышленной революции (Industry 4.0) большей частью основываются на автоматизации, робототехнике и взаимосвязанных цепочках поставок. С точки зрения страховщика все это приводит к новым рискам и одновременно открывает новые возможности. «Продолжительный мониторинг и стабильная работа автоматизированных производственных линий немного сократят частоту потерь и увеличат срок эксплуатации оборудования, – объясняет Михаэль Брух, глава подразделения по изучению новых тенденций AGCS. – Цепочки поставок будут лучше отслеживаться, процесс поставок станет более предсказуемым и прозрачным благодаря улучшенным опциям мониторинга, и сократится ущерб от производственного брака или истечения срока годности».

Однако взаимосвязанность цепочек поставок и производственных процессов увеличат киберугрозы, особенно поскольку бреши в системе безопасности, присущие встроенным программным кодам, сложно выявить. «Общая потенциальная возможность потерь значительно растет, при этом растет возможность получения все более сложных убытков, – поясняет Брух. – Если робот подвергнется атаке хакеров или пострадает от технической ошибки, производственная линия может остановиться на часы или месяцы, и принесет убыток в размере десятков миллионов долларов в день. Если алгоритм неверный, и ИТ-системы выходят из строя, глобальная цепочка поставок может резко прерваться, и убытки могут распространиться на целые регионы и отрасли.

В то же самое время новые технологии поднимают вопросы при возникновении ответственности. Например, равные требования могут быть предъявлены как к разработчикам, так и к поставщикам программного обеспечения по предотвращению технических неисправностей, в случае наступления ущерба.

Как эффективно предотвращать и минимизировать растущие киберриски в промышленном секторе? «Поскольку такого понятия как 100-процентная безопасность не существует, то, чтобы успешно бороться с киберрисками, необходима стратегия управления серьезными кибер- и ИТ-рисками, учитывающая различные корпоративные функции, – комментирует Йенс Крикхан, эксперт по страхованию киберрисков AGCS в

ЦВЕ. – Высокие стандарты по ИТ-безопасности сетей, программного обеспечения и мобильных устройств, проведение тренингов по информированию персонала, постоянная оптимизация процессов и жесткое управление правами доступа и руководства должны идти параллельно. Для управления остаточными рисками страхование киберрисков становится для многих компаний основным фактором в управлении ИТ-рисками».

Совершенствование существующих риск-сервисов

В будущем дигитализация преобразует природу корпоративных активов от в основном материальных до все более неосязаемых. Ценность бренда и репутация, а также интеллектуальная собственность, технологическое ноу-хау, сеть цепочек поставок станут более важными активами. Брух добавляет: «Покрытие для завода все чаще будет требовать включения защиты от перерывов в производстве в результате наступления киберрисков, репутационных и специфических рисков, приводящих к нематериальному ущербу. Совершенствование существующих и разработка новых риск-сервисов в отличие от традиционных – это ключевое направление как для страховщиков, так и для бизнеса, чтобы они совместно готовились к следующей промышленной революции».

Для снижения рисков цепочек поставок в цифровую эру предоставить решение по рискам означает нечто большее, чем просто страховой полис. Это целый набор услуг, включая анализ рисков, бенчмаркинг и советы по снижению рисков, которые могут помочь в анализе качества и устойчивости систем. «Мы можем предоставить оценку конкретной компании для локаций поставщиков и сравнить ее со стандартами, принятыми в данной индустрии, – объясняет Фолькер Мюнх, эксперт по андеррайтингу в страховании имущества AGCS, – чем больше у нас информации, тем лучше мы можем моделировать и управлять рисками и предлагать более высокие лимиты страхового покрытия».

Источник: Википедия страхования , 17.06.16