Секция «Риски и методы воздействия на риск в условиях цифровизации»

Управление кибер-рисками в эпоху пандемии Covid-19

Научный руководитель – Орлова Любовь Николаевна

Комаричева Виктория Александровна
Студент (бакалавр)
Финансовый университет, Факультет анализа рисков и экономической безопасности имени профессора В.К. Сенчагова, Москва, Россия
E-mail: komarichevas@gmail.com

С каждым годом цифровизация охватывает все больше и больше бизнес-процессов компаний. В то же время, развитию технологий сопутствует усложнение соответствующих угроз; развиваются новые виды преступлений, к числу которых относятся кибер-преступления. Особая опасность этого вида преступлений проявляется в том, что зачастую обнаружить их можно лишь спустя время, когда неблагоприятные последствия уже наступили [1]. Поэтому для компаний все большее значение приобретает необходимость обеспечения целостности, сохранности и конфиденциальности своих данных.

В 2020 году многие компании по всему миру вынуждены были перенести часть бизнес-процессов в режим онлайн, а сотрудников - на удаленную работу. Это стало фактором значительного повышения уязвимости бизнеса перед лицом кибер-угроз. Пандемия стала своеобразным катализатором развития для компаний, которые впервые приступили к цифровой трансформации. Другие компании убедились, насколько важна цифровая трансформация для долгосрочного успеха и выживания. В любом случае, произошел необратимый сдвиг в сторону повышения уровня цифровизации во многих отраслях.

Согласно исследованиям Risk Management [2], 2020 год стал рекордным годом для кибератак на сектор здравоохранения. Согласно Tenable 2020 Threat Landscape Retrospective, в 2020 году в отрасли была зафиксирована наибольшая доля нарушений, основными причинами которых стали программы-вымогатели (46,4% случаев) и взлом электронной почты (24,6% случаев). Растущий переход к цифровым медицинским картам облегчил доступ поставщиков медицинских услуг из разных мест, но, как и все системы цифровых записей, представляет собой риск. Стремительное распространение телемедицины также создает новые риски раскрытия данных или сбоев в работе системы.

Осенью 2020 года хакером был атакован финский поставщик психотерапевтических услуг Vastaamo [2]. Злоумышленник пытался лично шантажировать тех пациентов, чьи записи были скомпрометированы, и, в итоге, получил доступ к записям компании и украл данные около 300 пациентов, пытаясь заставить центр заплатить за предотвращение дальнейшей утечки данных по 40 000 пациентам. Затем хакер изменил тактику и обратился непосредственно к пациентам, пригрозив опубликовать все документы: от персональных кодов личности до стенограмм сеансов терапии, - если они не заплатят биткойнами на несколько сотен евро.

Важно помнить, что публикация конфиденциальной информации наносит ущерб репутации и зачастую влечет за собой крупные штрафы. В сложившейся ситуации специалистам по рискам следует сосредоточить свое внимание на развитии культуры осведомленности об кибер-рисках в своих компаниях [3]. Ключевым моментом здесь может стать пересмотр привычных методов обеспечения информационной безопасности, а также обучение сотрудников, повышение их бдительности, разъяснение мер, которые необходимо предпринимать для минимизации кибер-рисков.

С учетом того, что многие сотрудники по-прежнему продолжают работать из дома, важно учитывать, с какими угрозами они могут сталкиваться при таком формате рабо-

ты. Так, например, источниками угроз могут являться разного рода виртуальные помощники или интеллектуальные колонки, а также приложения на телефонах сотрудников, способные самостоятельно переходить в режим прослушивания [4]. Посредством таких устройств злоумышленники могут отслеживать общение сотрудников, что представляет собой особый риск в случае, если сотрудники работают с конфиденциальной информацией. Коммуникационные платформы, подобные тем, которые используются для онлайн-обучения и телемедицины, представляют еще больший интерес для атак и раскрытия конфиденциальных данных. Протокол удаленного рабочего доступа для сотрудников может предоставить такой же доступ и злоумышленникам.

Какие действия можно предпринять для защиты данных компании при удаленном формате работы? Такими действиями могут стать, в частности: установка разумных ограничений для домашних «офисов»; использование корпоративной VPN (виртуальной частной сети, обеспечивающей конфиденциальность и анонимность пользователя); регулярное обновление всех рабочих устройств; обучение сотрудников распознаванию фишинговых писем; побуждение сотрудников к использованию сложных паролей на личных устройствах и т.д.

Выводы, сделанные во время пандемии, могут быть использованы в повседневных процессах компаний для постоянного повышения скорости и эффективности принятия решений. Необходимо понимать, что цифровой риск возможно превратить в цифровое преимущество. В ответ на стремительные изменения, вызванные COVID-19, появились три новые истины:

1) все больше клиентов теперь готовы регулярно взаимодействовать с цифровыми каналами;
2) цифровые аспекты, в которых было трудно ориентироваться до COVID-19, теперь упрощаются;
3) компаниями разрабатываются совершенно новые подходы для удовлетворения потребности в более быстрой работе.

Многие отделы управления рисками во время пандемии продемонстрировали свою истинную ценность для бизнеса за счет более тесного сотрудничества с группами доставки, быстрого выпуска новых продуктов, сохранения контроля за состоянием рынка. Практические шаги, которые риск-менеджеры могут предпринять для управления рисками в цифровой компании, включают, во-первых, осознание новой картины рисков (с учетом цифровых преобразований), во-вторых, выявление пробелов в навыках и знаниях сотрудников и, наконец, формирование новых способов работы. Именно эти действия будут способствовать преодолению угроз и превращению их в конкурентные преимущества.

Источники и литература

1) Маслова М. А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. No. 1. С. 31-37.
2) 2021 cyberrisk landscape: http://www.rmmagazine.com/2021/02/01/2021-cyberrisk-landscape/
3) When job functions are not cybersecure: http://www.rmmagazine.com/2021/02/01/when-job-functions-are-not-cybersecure/
4) Cybersecurity policies for remote work: http://www.rmmagazine.com/2020/10/01/cybersecurity-policies-for-remote-work/