Большая часть кибератак в 2021 году пришлась на государственные учреждения – почти 20% преступлений. В 10% случаев жертвами кибермошенников становятся промышленные предприятия, по 8% атак направлены на медицинские и образовательные учреждения, а также финансовые организации — таковы данные исследования Страхового Дома ВСК.

В абсолютном большинстве случаев (60%) цель преступников – получение данных. Среди распространенных причин атак на бизнес также получение финансовой выгоды (21%) и хактивизм (16%) – это форма цифрового активизма, направленная не на получение личной выгоды, а на выражение той или иной общественной или политической позиции.

Чаще всего киберпреступники при осуществлении атак используют вредоносное ПО, методы социальной инженерии и эксплуатации веб-уязвимостей, а также способ отслеживания активности пользователей. Объектами кибератак в компаниях, как правило, являются компьютеры, серверы и сетевое оборудование, мобильные устройства, веб-ресурсы, банкоматы и POS-материалы, IoT.

В результате киберпреступлений российские компании несут колоссальные убытки, по некоторым оценкам они достигают нескольких трлн. рублей. Основной ущерб связан с последствиями инцидентов – хищением денежных средств со счетов, выходом из строя оборудования, а также с перерывами в хозяйственной деятельности организации. При этом, обезопасить себя от финансовых потерь компании могут при помощи страхования. Так, увеличение числа преступлений в сфере информационной безопасности обуславливает рост спроса на киберстрахование, в частности среди финансовых организаций.

«Тренд на цифровизацию большинства отраслей, безусловно, стал своеобразным «триггером» активизации кибермошенников. Причем, масштабы подобных преступлений возрастают, самый показательный пример – недавняя DDoS-атака на крупнейшую российскую IT-компанию. Киберстрахование является эффективным способом

минимизировать последствия преступлений в сфере информационной безопасности. В рамках страховой программы можно защитить как само имущество, которому нанесен ущерб – это информационные, финансовые активы и пр., так и гражданскую ответственность за последствия атаки хакеров перед третьими лицами или расходы, связанные с перерывом в хозяйственной деятельности. Мы видим, что многие российские компании проявляют интерес к киберстрахованию, на данный момент ВСК ведет переговоры с несколькими крупными игроками из разных отраслей бизнеса. Своим клиентам Страховой Дом ВСК предлагает двухступенчатую программу, которая реализовывается совместно с Angara Professional Assistance – ведущим провайдером услуг в области кибербезопасности. То есть партнеры ВСК получают одновременно и защиту информационных активов компании, и возможность компенсировать ущерб в случае атаки злоумышленников», — отметил Александр Тарновский, генеральный директор Страхового Дома ВСК.

Википедия страхования