Киберзащита не успевает обновляться

Издание: КоммерсантЪ, июль 2018 г.
Спикер: Иван Мелехин, директор по развитию

Несмотря на наращивание инвестиций в кибербезопасность, 70% компаний-респондентов в России считают, что решения, которые они применяют, уже устарели, говорится в исследовании VMware и Forbes Insights. Участники рынка считают, что этот показатель может быть завышен, называя оценку в 40%. В то же время квалификация злоумышленников растет еще быстрее, признают они.

75% компаний в Европе, Африке и на Ближнем Востоке не уверены в эффективности своей системы кибербезопасности, говорится в исследовании VMware и Forbes Insights (в опросе приняли участие 650 компаний региона), с которым ознакомился "Ъ". В России 75% респондентов планируют увеличить расходы на обнаружение и идентификацию атак (во всем регионе — 54%), а 37% опрошенных отмечают, что за прошлый год их компания уже приобрела новые инструменты для борьбы с потенциальными угрозами.

Почти все крупные российские компании — 96% опрошенных — планируют внедрить новые решения в сфере информационной безопасности (ИБ) в течение ближайших трех лет. Несмотря на то что компании продолжают наращивать инвестиции, 70% респондентов в России считают, что решения, которые их организация применяет для защиты систем, устарели, и только четверть (26,6%) респондентов полностью уверены в их надежности.

Ранее в компании «Информзащита» на основе данных портала zakupki.gov.ru подсчитали, что по итогам 2018 года объем госзакупок в ИБ вырос на 19,1%, до 66,7 млрд руб. В 2017 году рост составлял 34,9%. Объем контрактов госкорпораций и организаций с госучастием в этой сфере в 2018 году вырос практически во всех отраслях, кроме финансов и страхования.

Рост инвестиций в ИБ-решения есть в крупных компаниях, где цена любого инцидента значительна, в то время как малый и средний бизнес чаще выбирает максимально простое и дешевое средство для защиты, отмечает руководитель отдела технического сопровождения продуктов и сервисов ESET Russia Сергей Кузнецов. При этом иногда IT-специалисты просто не хотят внедрять новые системы безопасности, руководствуясь принципом «работает — не трогай», уверен он. Кроме того, законодательные ограничения запрещают использовать несертифицированные средства защиты информации, но поскольку сертификация — долгий процесс, далеко не всем удается применять актуальную версию защитного софта, заключает эксперт.

Доля в 70%, когда речь идет об устаревших решениях для защиты информации, скорее всего, завышена, сомневается руководитель отдела информационной безопасности Cross Technologies Алексей Даньков. По оценкам компании, речь может идти скорее о 40%. «За актуальностью средств защиты следят сами производители, которые регулярно выпускают обновления. Другое дело, что они зачастую не успевают уследить за уязвимостями, оставляя непреднамеренно лазейки злоумышленникам», — поясняет господин Даньков. При этом, по его словам, бизнес активно реагирует на финансовые потери и «довольно вяло» — на репутационные, отложенные по времени. Госструктуры же, хотя и соблюдают требования регуляторов в части обеспечения ИБ, зачастую «отстают» от мошенников, которые совершенствуют свои методы максимально оперативно, добавляет он.

В «Информзащите» также не наблюдают сильного устаревания решений в этой сфере, говорит директор по развитию компании Иван Мелехин. Однако обычной компании даже при наличии новейших инструментов защиты крайне трудно противодействовать современным киберугрозам из-за острой нехватки квалифицированного персонала, учитывая, что квалификация злоумышленников растет быстрее, констатирует эксперт.

Подробнее: https://www.kommersant.ru/doc/4032484

Компания «Информзащита»
Тел.: +7 (495) 980-2345
E-mail: pr@infosec.ru