ОТ БЕЗОПАСНОСТИ — К ОПТИМИЗАЦИИ

Сегодня кибербезопасность — категория уже не только репутационная и правовая, но и, безусловно, экономическая. В кризисных ситуациях, когда риски многократно возрастают, бизнес использует и внутренние, и внешние ресурсы для защиты. Но завтра задач в области кибербезопасности будет больше, считает Михаил Прибочий, управляющий директор «Лаборатории Касперского» в России, странах СНГ и Балтии.

ССТ: Как Вы оцениваете состояние кибербезопасности в период пандемии и развивающегося экономического кризиса? Какие риски и для каких сегментов экономики наиболее вероятны?

Михаил Прибочий: В эпоху кризиса и массового перехода в онлайн кибербезопасность выходит на первый план. В последние месяцы эксперты «Лаборатории Касперского» фиксируют множество фишинговых атак, связанных с пандемией, появление подозрительных ресурсов, увеличение числа мошеннических звонков, атаки на RDP (удаленные рабочие столы) и т. д. Поэтому решения для обеспечения информационной безопасности сейчас остаются очень востребованными.

В то же время понятно, что текущая ситуация сильно ударила по сегменту средних и малых бизнесов во многих отраслях, и тут ожидаемо возможно снижение затрат на ИТ. Поэтому компаниям этого сегмента сейчас мы предлагаем некоторые наши продукты бесплатно. Однако после пандемии средний и малый бизнес столкнется с новыми реалиями, связанными с переходом в онлайн и отчасти на удаленный режим работы. Поэтому необходимость защиты останется крайне актуальной. Сейчас мы смотрим на рынок информационной безопасности оптимистично.

ССТ: Есть ли различия в подходах к киберрискам за рубежом и в России, и в чем они проявляются?

М. П.: В России и других странах мы видели переход компаний от подхода, целью которого была только защита от вредоносного программного обеспечения, к необходимости сократить финансовые потери и предотвратить нарушения процессов из-за киберрисков. Безусловно, бизнес всегда стремится сокращать нецелевые расходы, однако текущий ландшафт киберугроз и ужесточение требований регуляторов заставляет компании очень ответственно подходить к информационной безопасности.

Пентест (от Penetration testing) — тестирование на проникновение. Метод тестирования уязвимостей компьютерных систем или сетей средствами моделирования атаки злоумышленника

Михаил Прибочий

Управляющий директор «Лаборатории Касперского» в России, странах СНГ и Балтии

С точки зрения оптимизации расходов мы сейчас наблюдаем тренд к использованию для обеспечения кибербезопасности внешних сервисов вместо внутренних ресурсов. Таким образом компании по всему миру существенно экономят на операционных затратах, а также могут быстро масштабировать поддержку в случае серьезного инцидента.

ССТ: К каким экономическим последствиям может привести реализация киберрисков?

М. П.: По данным нашего исследования, проведенного в 2019 году, средний ущерб от успешной атаки в России для компаний СМБ-сегмента составляет 4,3 млн руб., для крупного бизнеса — 14,3 млн руб.

825 000 000 киберугроз обнаружила «Лаборатория Касперского» с момента своего основания

11 000 000 000 кибератак обнаружила «Лаборатория Касперского» в 2019 году

342 000 новых вредоносных файлов обнаруживает «Лаборатория Касперского» каждый день

ССТ: От всех ли киберрисков спасают ваши продукты?

М. П.: Мы предлагаем комплексные решения по кибербезопасности для предприятий любого размера. Правильный подход предполагает не только защиту конечных устройств, но и образовательные программы для обычных сотрудников, а также сервисы по обнаружению и предотвращению сложных угроз. Наши эксперты консультируют, готовят отчеты о новейших угрозах и методах противодействия им, занимаются расследованием инцидентов и проводят пентесты, а также обучают сотрудников служб информационной безопасности. Однако большая работа проводится и внутри организации, где сотрудникам ИТ и ИБ необходимо грамотно оценить текущие риски и внедрить необходимые решения для их минимизации.