14.07.2021 01:05

Рубрика: Экономика

В России выросло число кибератак на организации

Текст: Юлия Акиньшина

Российская газета - Столичный выпуск № 156(8507)

Число кибератак на российские организации с января по май 2021 года выросло на 69% по сравнению с аналогичным периодом прошлого года, показало исследование Check Point Research. В среднем одна компания еженедельно подвергалась 980 угрозам - это на 37% чаще, чем в среднем по миру. Наибольший рост показали банковские трояны, зимой они атаковали до 25%отечественных предприятий, в то время как в среднем по миру всего 5-10%.

Вероятность того, что пользователи столкнутся с киберугрозой, выросла во всем мире. Вероятность столкнуться с любым типом вредоносного программного обеспечения составляет 29,4%. Это примерно на 5% больше, чем в прошлом году, указано в последнем отчете Avast Global PC Risk Snapshot Report. У бизнеса вероятность столкнуться с вредоносным ПО ниже - 13,9%, но это на 24% больше, чем в прошлом году.

Одной из причин роста риска для компаний стал их переход на удаленный режим работы в пандемию, говорит управляющий партнер AVG Legal Алексей Гавришев. Связано это прежде всего с широким использованием интернета для обмена данными, в том числе составляющими коммерческую тайну, между сотрудниками организаций, а также отсутствием у них средств обеспечения безопасности информации, таких, к примеру, как файрволл. По мнению директора по стратегическому консалтингу ГК компаний "Систематика", не только пандемия повлияла на снижение безопасности компаний, но и желание сэкономить: многие просто не озадачились или проигнорировали затраты на кибербезопасность, позволив конкурентам или просто обиженным гражданам испытывать свой бизнес на прочность онлайн.

Однако на практике немалая часть инцидентов по информационной безопасности происходит и по вине сотрудников, напоминает управляющий партнер Reasons Law Firm Арам Татоян. Поэтому работодатели должны тратить деньги не только на защиту своих серверов, но и проводить тренинги для персонала по информационной безопасности.

Как отмечает ИБ-евангелист компании Avast Луис Корронс, любая компания подвергается риску стать жертвой киберпреступников, а не только крупные корпорации. Малый и средний бизнес тоже должен быть очень осторожен. Количество малых и средних организаций, сообщивших об одной атаке, продолжает расти из года в год, достигнув 47% для тех, у кого менее 50 сотрудников, и 63% для тех, у кого от 50 до 250 сотрудников, по данным Hiscox за 2019 год.

"Чаще всего подвергаются риску банки, крупные ИТ-компании и госучреждения. Для того чтобы обезопасить себя, необходимо установить на компьютере антивирусную программу, а также внимательно относиться к ссылкам в сообщениях электронной почты от кого-то, кого вы не знаете. Хакеры используют электронную почту как форму передачи вредоносных кодов. Загружайте файлы или что-либо другое только из тех источников, которым вы доверяете", - добавляет член Ассоциации юристов России Ольга Митева.

> *980 угроз в среднем получает одна компания в России еженедельно - это на 37% чаще, чем в среднем по миру*

По словам Корронса, стоит избегать общественных сетей Wi-Fi и не переходить по ссылкам в электронных письмах. Вместо этого лучше ввести URL-адрес нужного сайта в браузере. Использовать антивирус нужно на всех устройствах, как и уникальные и надежные пароли, двухфакторную (2FA) или многофакторную аутентификацию (MFA).

Бизнесу важно регулярно проводить тесты на проникновение. Это имитация кибератаки на сеть

компании для проверки слабых мест и уязвимостей, которыми гипотетически могут воспользоваться злоумышленники. Есть компании, которые нанимают этичных хакеров и предоставляют эту услугу.