АРГУМЕНТЫ В ЗАЩИТУ

РОССИЙСКИЙ РЫНОК РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ СЕГОДНЯ РАСТЕТ ВМЕСТЕ С ЕЖЕГОДНЫМ КОЛИЧЕСТВОМ КИБЕРАТАК. ПРИ ЭТОМ, ПО СЛОВАМ ЭКСПЕРТОВ, ОТЕЧЕСТВЕННЫЕ РАЗРАБОТЧИКИ СТАРАЮТСЯ АКТИВНО ОСВАИВАТЬ НОВЫЕ ДЛЯ СЕБЯ НИШИ, ОПУСТЕВШИЕ ПОСЛЕ УХОДА С РЫНКА ИНОСТРАННЫХ КОМПАНИЙ.

АНТОНИНА ЕГОРОВА

По данным исследования «СёрчИнформ», в 2023 году увеличение числа внешних атак отметили 35% российских организаций. Что касается инцидентов, связанных с разглашением конфиденциальных данных, то в среднем с ними сталкивались 66% компаний. Основным виновником утечек из года в год остается сотрудник, который совершает нарушения по личной инициативе или содействуя внешнему злоумышленнику.

По словам Дмитрия Хомутова, директора компании Ideco, в российской экономике особенно уязвимы отрасли, связанные с финансовыми услугами и информационными технологиями. «Сфера банковского сектора является приоритетной целью для киберпреступников из-за обилия информации, которая хранится в этих организациях. Более 70% всех взломов имеют денежную мотивацию, в результате чего компании тратят до $18,3 млн в год на покрытие одной кибератаки. В настоящее время свыше 80% банковских приложений подвергались взломам злоумышленников. Однако простой атаки на существующую разработку хакерам уже мало — они создают фейковые приложения, с помощью которых вымогают личные данные пользователей»,— поясняет он.

Михаил Сергеев, ведущий инженер CorpSoft24, среди наиболее подверженных кибератакам сфер выделяет финансовый сектор, критически важную инфраструктуру (например, объекты энергетики), так как нарушение ее работы может иметь серьезные последствия. А также телекоммуникации и IT-компании в этой отрасли управляют большими потоками данных и часто становятся мишенями для атак с целью кражи данных или DDoS-атак.



ЕВГЕНИЙ ПАВЛЕНКО

БИЗНЕС ПРИЗНАЕТ ДАЛЕКО НЕ ВСЕ УТЕЧКИ ДАННЫХ, ТАК ЧТО ЗА СЧЕТ СКРЫТЫХ УТЕЧЕК МАСШТАБ ПРОБЛЕМЫ МОЖЕТ БЫТЬ ЕЩЕ БОЛЬШЕ

ИНСТРУМЕНТЫ По словам экспертов, как правило, инциденты случаются там, где сложная организационно и технически цифровая система, или там, где защита пока недофинансирована. «Чаще всего компании сталкиваются с DDoS-атаками, действиями вредоносного ПО и социальной инженерией. При этом процент успешных и серьезных киберинцидентов относительно небольшой, в большинстве случаев это именно попытки несанкционного вмешательства в работу предприятий»,— считает Игорь Душа, директор портфеля решений НОТА КУПОЛ.

По словам Андрея Арсентьева, руководителя направления аналитики и спецпроектов экспертно-аналитического центра ГК InfoWatch, наиболее опасный комплекс рисков информационной безопасности (ИБ) связан с кибератаками на информационную инфраструктуру организации. Одно из самых серьезных последствий кибератак — это потеря конфиденциальных данных. Соответственно, чем более привлекательной для хакеров информацией обладает компания, тем более высок уровень киберрисков.

«Исследуя утечки данных за 2023 год, аналитики экспертно-аналитического центра ГК InfoWatch пришли к выводу, что в России больше всего их произошло в торговых компаниях, госорганах, а также в сфере IT и телекоммуникаций. В общей сложности на эти отрасли пришлось более половины всех утечек информации. При этом отмечу, что бизнес признает далеко не все утечки, так что за счет скрытых утечек масштаб проблемы может быть еще больше. Минимизировать их можно только путем постоянного контроля угроз, что предполагает, в частности, составление матрицы рисков, методичное выстраивание систем кибербезопасности и поддержку этих систем в состоянии, актуальном текущему спектру угроз»,— заключает эксперт.

По словам господина Хомутова, для защиты периметра от киберугроз компании обеспечивают регулярное обновление программного обеспечения и установку антивирусных программ. «Однако не каждый антивирус дает 100% защиты: большая часть продуктов не может обеспечить даже 90% уровня безопасности. По этой причине необходимо прибегать к более серьезным мерам. Например, применение межсетевых экранов (NGFW) снижает риск ошибок на 80% и значительно увеличивает производительность системы организации. С их помощью можно создать комплексную защиту до 98%»,— поясняет он.

Кроме того, предприятия проводят обучение сотрудников по правилам безопасности информации и проверяют уровень доступа к конфиденциальным данным. Для усиления защиты используют многофакторную аутентификацию, технологии шифрования и мониторинга сетевой активности для обнаружения аномалий. Также популярными мерами являются регулярное проведение аудита безопасности и резервное копирование для предотвращения потери конфиденциальной информации в случае атаки.

«Крупные компании имеют в штате квалифицированных специалистов, которые обеспечивают поддержку собственной инфраструктуры и ее безопасность. Часто они используют специализированные вендорские средства защиты, объединенные в целые экосистемы. Однако стоит понимать, что сопровождение таких средств связано с серьезными финансовыми вложениями. Те организации, для которых информационные технологии не являются основным бизнесом, с целью экономии все чаще предпочитают пользоваться услугами партнеров, в частности, облачных провайдеров»,— отмечает Денис Полянский, директор по клиентской безопасности компании Selectel.

По словам Алексея Парфентьева, руководителя отдела аналитики «СёрчИнформ», в 2023 году 40% российских компаний увеличили бюджеты на информационную безопасность, в 2022-м этот показатель составил 28%. На увеличение бюджетов, в том числе, повлияли регуляторы, которые планируют усилить законодательство в области защиты персональных данных. Организации, увеличившие бюджет на ИБ, чаще всего направляли средства на продление лицензионных ключей на защитные решения (73%), закупку нового оборудования и ПО (70%), импортозамещение зарубежных решений (52%). Срез по отраслям показывает, что в 2023 году активнее всего бюджеты на безопасность выделяли в энергетической отрасли, также наращивают бюджеты финансовые организации, логистические и транспортные компании.

В целом меры, которые используются, зависят от отрасли и уровня зрелости компаний с точки зрения информационной безопасности. «Где-то и выбора особенно нет — регулятор четко формулирует, что надо делать и в какой последовательности. Молодые владельцы цифровых систем действуют по принципу „сначала закроем периметр, потом будем разбираться с тем, что внутри“. Зрелые идут от сквозной защиты важных процессов „там, где риски выше, защита больше“»,— отмечает Рустэм Хайретдинов, заместитель генерального директора группы компаний «Гарда».

Ключевая задача в направлении информационной безопасности для российских компаний — выполнение указа 166 до 1 января 2025 года, то есть импортозамещение иностранных решений на значимых объектах критической инфраструктуры. «В процессе импортозамещения большую роль играет государственная поддержка, которая позволяет развивать отечественные решения, в том числе и для продвижения на зарубежных рынках. Например, есть ряд успешных кейсов с компаниями и продуктами, которые поддерживает РФРIT, они нашли своего потребителя на российском рынке и рынках дружественных стран»,— заключает он.

РЫНОЧНЫЙ ПРОГНОЗ Как отмечает Александр Чёрный, архитектор IT-инфраструктуры практики «Стратегия трансформации» «Рексофт Консалтинга», по итогам 2023 года один из крупнейших разработчиков решений информационной безопасности — Positive Technologies — отчитался об увеличении чистой прибыли на 59%. Еще один крупный разработчик средств информационной безопасности — ООО «Юзергейт» — отчитался о росте чистой прибыли на 2164,1%. «Поскольку количество кибератак растет ежегодно, а возвращение иностранных производителей ПО в сфере ИБ в ближайшей перспективе не просматривается, можно ожидать дальнейший рост рынка ПО ИБ в 2024 и следующих годах»,— поясняет он.

«Рынок продолжает расти на импортозамещении — этот год последний, когда еще можно успеть выполнить указ президента по импортозамещению, поэтому ждем рекордных показателей. Страшно загадывать, но видно, что рост будет больше 30%. Затем рынок стабилизируется и рост ИБ снова будет привязан к росту IT: чем больше объектов для защиты, тем больше самой защиты. Постепенно на базе пользовательского опыта будет происходить замена продуктов, приобретенных на волне ажиотажного импортозамещения на продукты, лучше подходящие заказчикам по соотношение функциональности и цены. Это не даст рынку роста, но могут смениться лидеры в некоторых нишах»,— считает господин Хайретдинов.

Александр Быков, руководитель направления сервисов защиты облачного провайдера «НУБЕС», полагает, что на российском рынке разработки средств защиты сейчас преобладают две тенденции. Во-первых, крупные отечественные ИБ-разработчики активно дополняют линейку своих продуктов теми классами решений, которые до ухода предлагали на рынке иностранные вендоры, и занимают таким образом образовавшуюся нишу. Например, межсетевыми экранами следующего поколения (NGFW). Вторая тенденция, способствующая росту рынка,— появление, адаптация и активное внедрение российских нишевых, отраслевых решений в области ИБ.

По словам Виктора Гулевича, директора центра компетенций по информационной безопасности компании «Т1 Интеграция», довольно сложно давать оценку рынка конкретного города. Однако стоит отметить, что государство поддерживает создание во многих городах специализированных IT-кластеров, компании в области информационной безопасности проводят специальные мероприятия для развития отрасли, а учебные учреждения трансформируют учебные программы согласно запросам текущих реалий.

Так, по мнению экспертов, особенности развития рынка разработки кибербезопасного ПО в Санкт-Петербурге связаны с высоким уровнем технологического развития города и наличием крупных IT-стартапов. В городе более 30% новых разработок посвящено сфере информационных технологий. Местные специалисты активно участвуют в создании инновационных решений в области кибербезопасности, что способствует развитию индустрии в целом. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Guide «Цифровая экономика»)

Владимир Желонкин — генеральный директор АО «Коммерсантъ», главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Мария Кузнецова — выпускающий редактор
Марина Шевченко — корректор
Мария Громова — верстка
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб, д.10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ». Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит. Распространяется бесплатно. 16+

Фото на обложке: Евгений Павленко