УЯЗВИМОСТЬ НА ПЕРЕПРАВЕ

ПРЕДСТАВИТЕЛИ РОССИЙСКОГО БИЗНЕСА ФИКСИРУЮТ РОСТ ЧИСЛА КИБЕРАТАК. В БОЛЬШЕЙ СТЕПЕНИ ИМ ПОДВЕРЖЕНЫ БАНКИ И ФИНАНСОВЫЕ ОРГАНИЗАЦИИ. ТАКИМ ОБРАЗОМ, ОПЕРАТИВНЫЕ МЕРЫ ПО ЗАЩИТЕ IT-ИНФРАСТРУКТУРЫ СТАЛИ ОДНИМ ИЗ КЛЮЧЕВЫХ НАПРАВЛЕНИЙ РАБОТЫ В 2022 ГОДУ, ОСОБЕННО УЧИТЫВАЯ НЕОБХОДИМОСТЬ БЫСТРОГО ПЕРЕХОДА С ЗАРУБЕЖНЫХ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОТЕЧЕСТВЕННЫЕ. АНТОНИНА ЕГОРОВА

По словам экспертов, уровень уязвимости российских компаний по-прежнему достаточно высок. Как поясняет Александр Санин, коммерческий директор компании «Аванпост», еще год назад более половины из них были легкой мишенью для хакеров. Сегодня доля уязвимых отечественных организаций стала еще выше: в процессе перехода на отечественные решения в их IT-инфраструктуре образовалось немало брешей. При этом хакеры стали атаковать ее гораздо активнее: количество атак в первом полугодии 2022 года выросло в 15 раз по сравнению с аналогичным периодом 2021-го.

В то же время российские компании стали уделять вопросам кибербезопасности больше внимания. Вместе с внедрением отечественных средств защиты они гораздо активнее интегрируют решения для защищенного удаленного доступа, например, инструменты идентификации и многофакторной аутентификации.

По словам Александра Буравцова, директора по информационной безопасности компании «МойОфис», большинство кибератак сегодня приходится на автоматизированные системы управления технологическим процессом и объекты критической информационной инфраструктуры (КИИ) — к их числу относятся, например, государственные организации, госкомпании, банки, операторы связи, объекты транспорта и здравоохранения, компании атомной, металлургической и химической промышленности, научные, оборонные, ракетно-космические предприятия. Эксперт уверен, что эскалация геополитической напряженности дает основания полагать, что в ближайшие годы количество кибератак, направленных на инфраструктуру организаций и компаний, находящихся в России, снижаться не будет.

По словам Александра Черного, архитектора IT-инфраструктуры практики «Стратегия трансформации» компании «Рексофт Консалтинг», прежде всего в контуре риска находятся системы Банка России и его подведомственных организаций, а также информационная безопасность финансовых организаций на трех технологических уровнях: инфраструктуры, прикладного программного обеспечения или приложений и технологий обработки данных.

По данным Банка России, количество кибератак на финансовые организации с февраля по апрель текущего года выросло в 22 раза по сравнению с началом текущего года. За неполный третий квартал 2022 года около 450 DDoS-атак выдержал «Сбер», а 350 отразили его дочерние компании. В совокупности это сопоставимо с общим числом кибератак на организацию за последние пять лет.

При этом, по словам Александр Киселева, доцента кафедры гражданского права юридического факультета Московского государственного областного университета, у всех банков из топ-20 в России в настоящий момент достаточно высокий уровень кибербезопасности. Это дает основание полагать, что именно банковский сектор наиболее защищен и подготовлен к киберугрозам.

Кроме финансового сектора, по словам экспертов, в зоне риска находятся госструктуры, СМИ, ритейл, телекомы и крупнейшие промышленные предприятия. По словам Евгения Качурова, эксперта по информационной безопасности компании Axenix (экс-Accenture), также наиболее уязвимы международные организации с бизнесом в РФ, в которых информационной безопасностью занималась материнская компания. Сейчас таким предприятиям нужно провести огромную работу по локализации IT-инфраструктуры и обеспечить необходимый уровень информационной безопасности — особенно в момент перехода.

ЕВГЕНИЙ ПАВЛЕНКО

БОЛЬШИНСТВО КИБЕРАТАК СЕГОДНЯ ПРИХОДИТСЯ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ И ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В АВАНГАРДЕ УГРОЗ Сегодня для бизнеса актуальны киберугрозы разного типа, например, направленные на остановку работы инфраструктуры, получение доступа к внутренним ресурсам и извлечение информации. Среди наиболее распространенных — DDoS-атаки, подразумевающие выведение из строя вычислительной техники посредством огромного количества единовременных обращений. По заявлениям «Сбера», в мае организации ежедневно приходилось отражать несколько десятков подобных атак.

«Увеличивается не только количество, но и средняя продолжительность DDoS-атак. В этом году она превысила сутки, тогда как в феврале и марте прошлого года составляла не более 12 минут. Зачастую DDoS-атаки приводили к значительному финансовому ущербу организаций — в размере более миллиона рублей»,— поясняет господин Санин.

Еще одна актуальная киберугроза — вредоносные программы. Вирусы, трояны, шпионское ПО, шифровальщики попадают в инфраструктуру предприятия через уязвимости в программном обеспечении. По словам господина Киселева, широко распространенным видом атак на компании является фишинг (от англ. fishing — «рыбалка»). Подобно рыбаку, хакер готовит приманку, способную заинтересовать пользователя. Чаще всего ею становится электронное письмо, включающее вложение с исполняемым файлом или ссылкой на таковой. Пользователь открывает файл, тем самым активизируя вредоносную программу.

«В период пандемии Россия вышла на первое место в мире по размещению фишинговых ресурсов и вредоносным рассылкам. За первые шесть месяцев 2021 года было предотвращено более 36 млн попыток перехода российских пользователей на различные фишинговые сайты, из них более 300 тыс. — попыток перехода пользователей на страницы, мимикрирующие под наиболее крупные финансовые организации»,— добавляет эксперт.

«Изучая статистику известных кибератак, можно заметить, что чаще они начинаются именно с психологического воздействия на людей. Нередки случаи проникновения вредоносных программ через корпоративную или даже личную почту и социальные сети сотрудников. Такие методы значительно проще и дешевле, чем организация кибератак в обход средств защиты информации»,— добавляет Илья Попов, доцент факультета безопасности информационных технологий ИТМО.

Сегодня российские компании устанавливают специальные программные и аппаратные средства, позволяющие решить обширный ряд задач и объединяющие много уровней защиты. По словам господина Санина, эти решения позволяют выявить целевую атаку по косвенным признакам. Например, путем фиксации отклонений в действиях сотрудников и функционировании сетевой инфраструктуры. Также организации активнее внедряют решения для защищенного удаленного доступа, включая инструменты идентификации и многофакторной аутентификации.

В целом проблему уязвимости ПО в новых реалиях нужно решать комплексно, считает господин Буравцов. Следует переходить на отечественные решения — их поддержка не будет прервана в силу изменения геополитической конъюнктуры; также они выводят на новый уровень подход к информационной безопасности. По словам экспертов, для своевременного выявления и устранения уязвимостей в коде критически важных программ необходимо регулярно проводить работы по анализу их защищенности. Стоит обратить особое внимание на устаревшие версии ПО, на открытые протоколы передачи данных и на хранение важной информации в открытом виде на серверах и рабочих станциях сотрудников. Кроме базовых мер защиты информации, следует на регулярной основе осуществлять аудит безопасности информационных систем и тестирование на проникновение со стороны. И, наконец, проводить ликбез по информационной безопасности для сотрудников.

ЛУЧШЕ, ЧЕМ В IT Как отмечает Дмитрий Москвин, доцент Института кибербезопасности и защиты информации СПбПУ, отечественный софт в сфере кибербезопасности до весны текущего года занимал более половины российского рынка. Это как раз та отрасль, в которой импортозамещение на 100% вполне возможно в ближайшие несколько лет.

Юрий Черкас, генеральный директор ООО «Мист», подтверждает, что ситуация с отечественными решениями в области кибербезопасности лучше, чем в целом в сфере IT. По словам эксперта, в первую очередь это связано с тем, что и ранее регуляторные требования предписывали в определенных случаях использовать только отечественное ПО. Эти требования послужили драйвером развития отечественных решений, а уход иностранных производителей только дополнительно подстегнул российских разработчиков.

Работа по импортозамещению в сфере IT в РФ ведется уже в течение нескольких лет. По словам юриста Марии Верховской, еще в 2016 году был установлен запрет на приобретение иностранных программ для ЭВМ и баз данных для обеспечения государственных и муниципальных нужд. Также с 1 января 2025 года вводится запрет на использование иностранных средств защиты информации органами государственной и муниципальной власти. Коммерческим организациям с государственным участием также рекомендовано обеспечить переход на российское ПО.

Как отмечает Александр Киселев, в 2018 году было принято решение о переводе всех компьютеров в военной и оборонной сфере России на ПО «Астра» и полном отказе от Microsoft. В прошлом году Минпромторг просил разработчиков ускорить адаптацию ПО под российские процессоры «Эльбрус» и «Байкал». Отмечалось, что по базовому набору ПО совместимые решения уже существуют или находятся в разработке и к 2023 году отечественные процессоры будут стоять в 70% закупаемых госорганами компьютеров.

«Переход на отечественный софт идет довольно активно, однако сделать ПО, которое сможет конкурировать и не уступать западным аналогам, в самое ближайшее время не получится, поскольку на это должны быть направлены колоссальные финансовые ресурсы, которыми мы не располагаем. В сложившихся условиях выйти на самообеспечение по производству конкурентоспособного программного обеспечения и комплектующих к компьютерному оборудованию является приоритетной, но очень непростой задачей»,— полагает господин Киселев.