

ЕВГЕНИЙ ПАВЛЕНКО

ГОССЕКТОР И СТРАТЕГИЧЕСКИЕ КОМПАНИИ ОСТАЮТСЯ ПОД ДАВЛЕНИЕМ ИЗ-ЗА ПОЛИТИЧЕСКОГО КОНТЕКСТА И МАСШТАБА

2 → Алексей Кубарев, директор по информационной безопасности «Т1 Облако» и «Т1 Интеграция» (IT-холдинг Т1), считает, что в основе этих изменений — расширение цифрового периметра бизнеса, часто бесконтрольное со стороны ИБ, что усложняет управление им и поддержание его безопасности, исчерпание нарушителями более простых возможностей атак в связи с общем повышением уровня ИБ в российских компаниях и более активное использование ИИ нарушителями.

О том, что «точками входа» чаще всего являются сотрудники организаций, фишинг и социальная инженерия, говорит и Татьяна Белоусова, начальник отдела ИБ MONS (входит в ГК «КОРУС Консалтинг»). «Также в 2025 году возросла доля атак через цепочки поставок: как правило, большие компании защищены лучше, однако их менее крупные подрядчики имеют меньше возможностей инвестировать в ИБ. Соответственно, атаки на крупный бизнес проще проводить через мелкие компании, которые взаимодействуют с ним, обмениваются различными данными»,— утверждает она.

Небольшой поставщик с незрелыми процессами ИБ, интегрируясь в инфраструктуру крупного заказчика, становится точкой входа, превращая свою локальную уязвимость в системный риск для всего бизнеса, соглашается Валентин Богданов, генеральный директор IT-компании УЦСБ. «Этот тренд требует кардинального пересмотра подходов к оценке киберустойчивости всей экосистемы партнеров»,— заключает он.

В ЦИФРОВОЙ ОСАДЕ Злоумышленники нередко гибко сочетают две тактики: массовые автоматизированные атаки «широким фронтом» на растущие цифровые экосистемы для максимального охвата и эффективности и целенаправленные операции против конкретных организаций. «Особое внимание при этом уделяется отраслям с максимальной концентрацией критических активов: госсектор, промышленность, ТЭК, финансы, транспорт, ритейл и здравоохранение. Их привлекательность для злоумышленников определяется высокой отдачей от успешной атаки, которая измеряется в нескольких ключевых бизнес-метриках: прямой финансовый ущерб от кражи средств, операционные потери от остановки производства или услуг, репутационные риски и регуляторные издержки из-за утечек персональных данных сотен тысяч пользователей, а также целенаправленное негативное воздействие на стабильность отрасли или региона»,— подчеркивает господин Богданов.

По данным портала киберразведки (Threat Intelligence) «Лаборатории Касперского», 14 группировок, атакующих Россию, прежде всего интересуют госсектор, промышленность и телеком, поскольку сбои в работе организаций из этих сфер с высокой вероятностью вызовут большой общественный резонанс. «Однако под удар может попасть кто угодно, предприятие любого размера и профиля»,— уточняет господин Митрофанов.

Госсектор и стратегические компании остаются под давлением из-за политического контекста и масштаба последствий, добавляет госпожа Ледяева. «Атаки здесь нередко связаны с шпионажем, демонстрацией возможностей и попытками повлиять на работу важных систем»,— указывает эксперт. Кроме того, по ее словам, промышленность и транспорт часто атакуют из-за высокой зависимости от IT и технологических систем. «Короткий сбой может привести к простою, срыву поставок и прямым финансовым потерям»,— добавляет госпожа Ледяева.

Финансовый сектор, в свою очередь, интересен доступом к платежным операциям и данным клиентов. «Телеком и IT привлекают хакеров тем, что через них можно атаковать сразу множество компаний. Отдельно выделяются здравоохранение и фармацевтика. Здесь ценны персональные данные пациентов и непрерывность работы»,— делится мнением госпожа Ледяева.

В целом причины атак эксперты разделяют на финансовые и политические. «Если в первом случае цель — получить выкуп, то во втором — уничтожение инфраструктуры и нарушение значимых рабочих процессов»,— подчеркивает госпожа Белоусова.

ЗАЩИТА «ПОД КЛЮЧ» Как отмечает Алина Ледяева, в условиях, когда IT-среда постоянно меняется, лучше всего работают понятные и практичные меры. «В первую очередь это контроль доступов, так как большинство атак начинается с украденных логинов и паролей. Важно знать, кто и к каким системам имеет доступ, и вовремя убирать лишние права»,— замечает она.

Вторым пунктом является готовность к инцидентам. «Обновления, резервные копии и заранее продуманные действия на случай атаки позволяют сократить простой и избежать серьезных потерь даже при успешной атаке»,— добавляет эксперт.

Отдельного внимания требуют фишинг и социальная инженерия. По наблюдениям госпожи Белоусовой, все чаще бизнес начинает проводить киберучения как ИБ-команды, так и сотрудников организации в целом. «При этом важно не только выстроить защиту, но и проработать сценарии реагирования на возможные инциденты»,— говорит она.

Также, по словам госпожи Ледяевой, важно учитывать подрядчиков и внешние сервисы. «Интеграции расширяют контур атаки, и сбой на стороне партнера может затронуть всю компанию. Поэтому важно понимать, какие доступы есть у партнеров и как их сбой или компрометация могут повлиять на основной бизнес»,— указывает эксперт.

Ведущий эксперт по сетевым угрозам, веб-разработчик компании «Код безопасности» Константин Горбунов замечает, что современная киберзащита требует комплексного подхода, сочетающего технологии и обучение персонала. «Ключевые меры включают строгий контроль доступа (MFA, минимальные привилегии), оперативное устранение уязвимостей, защиту конечных точек с помощью EDR и сегментацию сетей. Ключевые организационные меры — обучение сотрудников против фишинга, регулярные аудиты и внедрение моделей SDL и Zero Trust»,— поясняет он.

При этом актуальные стратегии киберзащиты фокусируются на максимизации отдачи при жесткой оптимизации бюджета, подчеркивают эксперты. «Это дополняется непрерывным управлением уязвимостями и следованием базовым принципам Zero Trust. В условиях нехватки экспертизы растет спрос на аутсорсинг безопасности (MDR) как способ получить предсказуемые расходы и снизить операционные риски. Эффективность защиты проверяется через регулярные киберучения и тесты на проникновение, что напрямую сокращает время восстановления. Замыкает стратегию активное внедрение ИИ для прогнозирования угроз и автоматизации ответных действий, повышающее скорость работы SOC»,— говорит господин Богданов.

Впрочем, по мнению господина Митрофанова, базовых средств защиты уже недостаточно — актуальны продвинутые решения классов EDR и XDR для обнаружения и реагирования на сложные атаки. «Ключевую роль играет понимание ландшафта киберугроз, основанное на качественной аналитике. Речь идет о потенциальных противниках и их методах, релевантных для конкретной организации, отрасли и региона. Такие киберразведданные можно получить в публичных отчетах ИБ-вендоров и специальных сервисах, предназначенных для аналитики киберугроз»,— делится эксперт. → 5