29 сентября 2025

Почему малый ИТ-бизнес проигрывает в кибербезопасности

Недавно в СМИ было опубликовано исследование компании CICADA8 в котором говорится, что 55% российских компаний, выступающих IT-подрядчиками крупного российского бизнеса, имеют низкий уровень кибербезопасности. У 32% компаний в системах обнаружены «старые» критические уязвимости, а у 27% данные корпоративных учетных записей оказались в базах утечек.

При этом указываестя, что «около 60% выборки – это IT-интеграторы, 15% – компании-разработчики, а остальные – организации, представляющие разные IT- и сервисные услуги, в ходе которых контрагент получает доступ к персональным данным (ПД) клиентов или сотрудников компании-заказчика, коммерческой тайне или интеллектуальной собственности». Звучит довольно пугающе, но давайте разберемся, что стоит за этими цифрами, кого они на самом деле касаются и самое главное – что делать практикующему специалисту, который отвечает за результат.

Когда размер имеет значение

Очевидно, что на российском ИТ-рынке есть два больших, принципиально разных пласта игроков. С одной стороны – крупные интеграторы и вендоры, у которых за плечами десятки лет опыта, отлаженные по стандартам индустрии процессы и собственные, нередко сертифицированные, службы безопасности (SOC, CERT). С другой – множество небольших компаний и

подрядчиков «на выезде», которые работают с точечными проектами и нередко – в условиях крайне ограниченных бюджета и ресурсов. Несмотря на то, что крупный бизнес пользуется услугами и первой, и второй группы, именно у второй категории ИТ-компаний чаще всего и встречаются те самые уязвимости, о которых идет речь в исследовании.

Почему так происходит? Как правильно, для этого есть объективные причины:

- Ограниченные ресурсы. Небольшая компания физически не может содержать штатного CISO или специалиста, который бы занимался исключительно вопросами ИБ. Например, специалист уровня middle может обходиться компании в 150–200 тыс руб., а ведущий эксперт – от 400 до 700 тыс руб. ежемесячно.
- Инженеры, которые отвечают за инфраструктуру клиентов, попросту не успевают выстраивать и поддерживать полноценную внутреннюю защиту. Конкуренция на рынке и борьба за проекты всегда приоритетнее «гипотетических» рисков.
- Системная экономия на инструментах. Корпоративный EDR/XDR, выделенная SIEM-платформа, система двухфакторной аутентификации (2FA) для всех сотрудников, регулярный внешний аудит – это прямые и, зачастую, немаленькие расходы. Для небольшой компании совокупная годовая стоимость владения таким комплексом может начинаться от 1,5–2 млн руб. и достигает 5–7% от годовой выручки. Естественно, это кажется «роскошью», однако только до первого инцидента.
- Устоявшиеся практики, противоречащие правилам ИБ, и отсутствие регламентированных процессов. Это, пожалуй, главное. Доступы к критическим системам передаются, например, по привычке, в мессенджерах, пароли годами не меняются или используются повторно, сегментация сети отсутствует как класс. В такой среде один скомпрометированный ноутбук или аккаунт инженера может привести к

серьезному инциденту. Это создаёт идеальную среду для атак по цепочке поставок: злоумышленнику достаточно попасть в инфраструктуру подрядчика, чтобы через доверенные каналы проникнуть в сеть конечного заказчика.

Таким образом, результаты исследования – это не «приговор» всей индустрии. Это четкий и своевременный сигнал большому бизнесу: быть более вдумчивым и требовательным к выбору партнеров, поскольку уровень организации внутренней информационной безопасности у небольших игроков часто не в приоритете.

Как измерить безопасность?

Разумеется, размер ИТ-компании далеко не всегда является единственным критерием надежности с точки зрения информационной безопасности. Выявить зрелых, надежных интеграторов и подрядчиков можно с помощью вполне объективных индикаторов:

- Обязательное использование MFA/2FA для доступа ко всем критическим внутренним и клиентским системам.
- Внедрение принципа наименьших привилегий (PoLP) и строгий контроль доступа, включая регулярный ревью прав.
- Единая система централизованного логирования и мониторинга (SIEM/SOC), а не разрозненные логи на разных машинах.
- Жесткая сегментация сети, которая изолирует проекты друг от друга и не позволяет локальному инциденту парализовать всю компанию.
- Четкие, формализованные регламенты по управлению доступом, ротации паролей и обновлению ПО.
- Регулярное обучение и повышение осведомленности всех сотрудников, а не только технического персонала.

- Для заказчика это реальная гарантия того, что его подрядчик не станет тем самым слабым звеном в цепочке.

5 неудобных вопросов подрядчику

Выбрать надежного партнера не так сложно, однако это требует определенной дисциплины. Выбирать ИТ-подрядчика нужно по принципу «трех китов»: стоимость, компетенция инженеров и зрелость процессов безопасности. Например, базовая инфраструктурная задача, с учетом минимальных требований к безопасности, не будет качественно решена подрядчиком дешевле, чем за 1,5–2 млн рублей в год. Не стесняйтесь задавать прямые и даже неудобные вопросы во время тендеров и собеседований:

- «Есть ли у вас выделенная команда ИБ или привлеченный CISO?»
- «Какие инструменты защиты (EDR, SIEM, DLP) вы используете внутри?»
- «Как вы обеспечиваете безопасность удаленного доступа своих инженеров к нашим системам?»
- «Проходите ли вы регулярные независимые аудиты? Можете ли вы показать отчет?»
- «Как у вас построен процесс обновления ПО и управления уязвимостями?»

В этом смысле подход должен быть таким же, как при выборе банка или страховой компании: важна не только сиюминутная выгода, но и надёжность, репутация и зрелость на долгой дистанции.

Исследование CICADA8 поднимает важную тему, поскольку ИТ-подрядчики действительно являются ключевым вектором для целевых атак. Но важно правильно интерпретировать выводы: проблема носит не тотальный, а структурный характер и чаще всего касается сегмента малого бизнеса, у которого нет ресурсов на полноценную ИБ. Решение же для крупных заказчиков вполне очевидно и рационально: диверсифицировать риски, работая с проверенными интеграторами, для которых защита клиентов

начинается с бескомпромиссной внутренней безопасности. В конечном счете, цепочка защиты ровно настолько прочна, насколько прочно ее самое слабое звено.