Как IT-аутсорсинг может помочь защитить от кибератак

Компании среднего и малого бизнеса (СМБ) всё чаще привлекают внимание хакеров. В 2019 году 43% кибератак были направлены на этот сегмент. Тенденция сохраняется и сейчас: большинство экспертов по защите данных соглашаются, что в сегменте СМБ повышен риск кибератак и инцидентов в области безопасности.

Согласно отчёту Alliant Cybersecurity, 22% компаний СМБ перешли на удалённую работу во время самоизоляции «без чёткой политики по смягчению и предотвращению киберугроз и хакерских атак». Если взглянуть на ситуацию шире, средний и малый бизнес более уязвим по сравнению с крупными корпорациями из-за ограниченного бюджета на всех направлениях, слишком сильной загруженности персонала и небольшого объёма собственной экспертизы.

ИТ-аутсорсинг способен принести серьезную выгоду компаниям СМБ, закрывая серьёзные пробелы в безопасности в рамках более широкого комплекса универсальных IT-решений. Переход к модели аутсорсинга устраняет уязвимости, высвобождает внутренние ресурсы компаний и позволяет избежать инцидентов в области кибербезопасности. Отчасти поэтому, согласно нашему новому исследованию о будущем работы, 62%

компаний со штатом примерно из 500–1000 сотрудников заявили после начала пандемии, что хотели бы инвестировать в удалённую ИТ-поддержку.

Торговые представители совершенно справедливо отмечают, что можно изменить ситуацию к лучшему и генерировать прибыль с помощью услуг ИТ-аутсорсинга. Однако не все подобные услуги и их поставщики одинаково хороши. Поэтому поговорим о том, как сервис-провайдеры могут выделиться в условиях высокой конкуренции, используя грамотный подход к кибербезопасности.

Хорошо ориентироваться в инфраструктуре заказчика

У угроз могут быть разные источники — например, кибератаки, утечки данных, ошибки персонала и личные устройства сотрудников. Уязвимым звеном может стать всё, что подключено к корпоративной сети: от компьютеров и принтеров до серверов и маршрутизаторов. Если оценить влияние инфраструктуры на бизнес и посмотреть на результаты опроса, проведённого Quocirca в 2019 году, очевидно, что на этом направлении можно добиться большего:

- 60% компаний сообщили, что сталкивались с утечкой данных, которая была связана с печатью документов;
- две трети респондентов считают процессы печати IT-риском.

Понимать специфику бизнеса и отрасли заказчика

Очевидно, что близость к клиенту и знание его отрасли крайне важны для создания хорошо проработанной с точки зрения безопасности модели IT-аутсорсинга. Однако об этих простых основах слишком часто забывают команды, которые стремятся как можно быстрее продать услугу и двигаться дальше.

Это ошибочный подход, ведь он закрывает доступ к высокодоходным отраслевым вертикалям, в которых часто встречаются уникальные требования и условия. Например, в системе здравоохранения США защита информации о пациентах имеет первостепенное значение и строго регулируется актом HIPAA (законом об ответственности и переносе данных о страховании здоровья граждан). А для государственных организаций федерального уровня в США обязательное условие сотрудничества с применением облачной инфраструктуры — сертификат FedRAMP (федеральной программы управления рисками и авторизацией). Знание уникальных особенностей отраслевой вертикали повышает шансы не просто заключить сделку, а запустить долгосрочный проект.

Если взглянуть не только на отраслевую специфику, даже простое соблюдение местных или общих норм укрепляет доверие клиентов и открывает более быстрые пути к сотрудничеству. Например, преимущество могут получить поставщики, которые учитывают требования Генерального регламента ЕС о защите персональных данных, Общих критериев оценки защищённости ИТ и калифорнийского акта SB-327, который запрещает использовать пароли по умолчанию, такие как admin.

Наконец, система кибербезопасности NIST (идентификация, защита, обнаружение, реагирование и восстановление) — инструмент, который позволяет сформировать для клиента решение в области безопасности. Мы используем именно такой подход к комплексным системам защиты данных и считаем, что его последовательное применение может быть отличным конкурентным преимуществом.

Отдавать предпочтение командной работе в области безопасности

Ни одна компания не сможет самостоятельно выпустить полный пакет инструментов безопасности — по крайней мере, такой, который соответствует заявленным требованиям. При правильном подходе эта работа должна быть командной. Вы уверены, что у поставщика, с которым вы хотите сотрудничать, хватит ресурсов для создания по-настоящему универсального решения? Разрабатывая продукцию, мы специально построили многоуровневую IT-систему, разные компоненты которой создавали отраслевые лидеры. Например, мы сотрудничаем с McAfee для интеграции белых списков встроенного ПО, а с Cisco ISE — для организации безопасного сетевого доступа. Также мы задействуем технологии управления защитой данных и инцидентами таких поставщиков, как LogRhythm, Splunk и McAfee.

Принимая решение о сотрудничестве с производителем, реселлеры и торговые посредники должны оценивать каждый элемент его систем. Как эти компоненты выглядят в сравнении с лучшими в отрасли? Соответствуют ли они отраслевым стандартам? А может быть, превосходят или даже устанавливают их? Какие преимущества они приносят с точки зрения задач клиента? Лучшие вендоры последовательно встраивают системы безопасности во все решения, которые предлагают — начиная с базового уровня.

Уделять кибербезопасности ключевое внимание на любых переговорах с заказчиком

В наше время безопасность — неотъемлемая часть продаж. Продавцы в штате торгового представителя должны уметь убедительно встраивать в разговор тему кибербезопасности начиная с первой встречи с потенциальным клиентом. Используйте готовые материалы и ресурсы, полученные напрямую от производителей, чтобы быстрее и легче научить сотрудников отдела продаж, как правильно работать с конкурентными преимуществами в области кибербезопасности.

На фоне изменения бизнес-среды во время и после пандемии IT-аутсорсинг нужен компаниям СМБ больше, чем когда-либо прежде. Комплексная интегрированная модель с удалённым мониторингом и управлением, облачными сервисами и средствами кибербезопасности освободит малый и средний бизнес от непрофильных процессов, помогая ему сосредоточиться на главном — стратегических и операционных задачах. Но именно безопасность заслуживает внимания в первую очередь, ведь всё больше представителей сегмента СМБ понимают: риски для бизнес-процессов, репутации и

конфиденциальности клиентских данных вполне реальны. А простой и недорогой способ решить эти проблемы — привлечь внешнюю экспертизу.

Джоанн Коллинз Сми,

исполнительный вице-президент, коммерческий директор

и директор по работе с СМБ и каналом Xerox

https://www.it-world.ru/it-news/it/157039.html