ФАКТОР ДОВЕРИЯ

Роль кибербезопасности в сохранении темпа развития бизнеса

Сводный отчет

В 2018 г. количество кибератак побило рекорды предыдущих лет. Новостные ленты заполонили сообщения об инцидентах, связанных с безопасностью данных, включая крупнейшую DDoS-атаку в истории, достигшую 1,7 Тбит/с[1]. 25 мая 2018 г. в Евросоюзе вступил в силу Общий регламент по защите данных, содержащий строгие правила сбора, обработки персональных данных и управления ими. Кроме того, сети заполнены вирусами-майнерами, которые используют ресурсы компьютеров для получения криптовалюты.

Мы перешли к эпохе недоверия, в которой организации и отдельные пользователи все чаще настороженно относятся к обещанной безопасности по номинальной стоимости. Каждый раз, когда клиенты обращаются к компании, они решают, можно ли доверить ей персональные данные. Успешные кибератаки разрушают с трудом заработанное доверие между компаниями и клиентами. Последствия атак больше не являются ответственностью исключительно специалистов по безопасности, руководители компаний теперь также несут за это ответственность.

Чтобы предоставить сведения о проблемах, с которыми сталкиваются организации, пытаясь защитить свою репутацию, компания Radware ежегодно выпускает отчет Global Application & Network Security Report. Восьмой ежегодный отчет сочетает исследование Radware, реальные данные об атаках, анализ текущих тенденций и технологий, а также данные глобального исследования отрасли.

В отчете подчеркивается влияние кибербезопасности на бизнес и технологии, включая перечисленные ниже аспекты.

- Опыт, полученный в результате последних атак
- Затраты на кибератаки: как количественные, так и качественные
- Обзор картины угроз для сетей и приложений
- Сведения об уязвимостях новых технологий
- Прогнозы на 2019 год

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Вычисление соотношения затрат и рисков

Защита от кибератак требует значительных инвестиций из расходов на эксплуатацию. Компании всегда ищут способы сохранить капитал. Но сколько будет достаточно при учете риска кибератак, влияющего на защиту и бизнес?

Изучите сведения, полученные в глобальном исследовании отрасли за 2018-2019 г.

- За один год затраты, вызванные кибератаками, выросли на 52 % до 1,1 млн долларов.
- Компании, которые смоделировали общие затраты из-за кибератак, оценили их объем практически вдвое больше, чем компании, которые оценили затраты без детального моделирования.
- Две из пяти компаний сообщили об ущербе клиентам и уроне репутации из-за успешных атак.
- 93 % респондентов столкнулись с кибератаками в последние 12 месяцев, и лишь 7 % сообщили, что их это не коснулось.
- Треть компаний сталкивается с кибератаками еженедельно.
- Почти половина респондентов заявила, что кибератаки нарушили работу служб. Атаки, приводящие к полному или частичному перебою в работе, увеличились на 15 % и снижают производительность компании.
- Вымогательство денег является основным мотивом хакеров и приводит к 51 % атак.

[1] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcache-ddos-as-a-service/

Новые векторы атак

Злоумышленники применяют эффективные технологии, чтобы вызвать отказ в работе служб, такие как вспышки активности, расширение, шифрование или бот-сети интернета вещей. Часто атаки нацелены на уровень приложений, чтобы принести больше ущерба.

- Атаки на уровне приложений приводят к максимальному урону. Две трети респондентов сталкивались с подобными атаками. Одна треть считает уязвимости приложений большой угрозой в 2019 г., особенно в облачной среде. Больше половины респондентов изменяют и обновляют приложения каждый месяц, тогда как остальные делают это чаще, что повышает необходимость автоматизации системы безопасности.
- Попытки кибератак, приводящие к перебоям или повреждению служб, участились на 15 %. Каждая шестая организация сообщила, что сталкивалась с атакой мощностью 1 Тбит/с.
- Хакеры нашли новые способы для выведения из строя сетей и центров обработки данных. Количество таких атак, как HTTPS-флуд, выросло на 20 %, DNS и Burst — на 15 %, а атак ботов — на 10 %.
- Треть компаний сообщили, что столкнулись с атаками, мотивы которых неясны.

Подготовка к следующему этапу

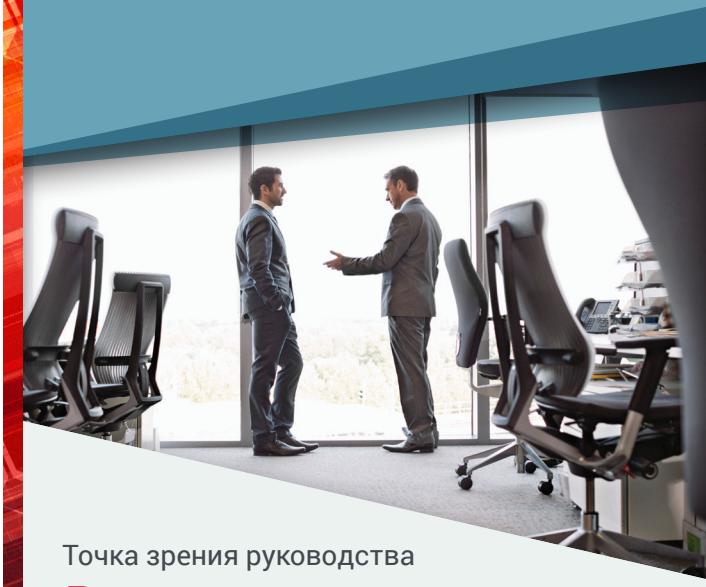
Представители компаний говорят, что понимают степень серьезности изменения картины угроз и принимают меры для защиты цифровых ресурсов, но тяжесть угрозы безопасности значительна.

- Почти половина считает, что не готова к защите от всех типов кибератак, несмотря на наличие готовых к работе решений для безопасности.
- 86 % компаний начали использовать решения на базе машинного обучения и искусственного интеллекта в течение последних 12 месяцев. Почти половина заявила, что причиной стало повышение скорости реагирования на кибератаки. Компания Radware заметила 44%-ный рост при подобном ведении бизнеса по сравнению с блокчейном.
- Компании продолжают диверсифицировать сетевые операции среди нескольких поставщиков облачных услуг. Две из пяти организаций используют гибридные решения кибербезопасности, чтобы объединить локальную и облачную защиту.
- 49 % организаций в Европе, на Ближнем Востоке и в Африке сообщили, что плохо подготовлены для внедрения Общего регламента по защите данных.

Только успех

Затраты, вызванные кибератаками, слишком высоки, чтобы не преуспеть в минимизации каждой угрозы в любое время. Доверие клиентов можно разрушить за несколько мгновений, а влияние на репутацию компании и затраты на ликвидацию ущерба для бизнеса значительны. Общий регламент по защите данных и другие государственные требования могут привести к банкротству компаний, которые им не соответствуют.

Для организаций критически важно включить кибербезопасность в долгосрочный план развития. Ответственность за защиту цифровых ресурсов должны нести не только специалисты ИТ-отдела. Планирование безопасности следует включить в новые предложения продуктов и услуг, системы защиты, планы развития и новые бизнес-инициативы. Генеральный директор и руководство компании должны задать тон и вложить средства в обеспечение благоприятной репутации среди клиентов.



Точка зрения руководства

Руководители отвечают за доверие к компании

Кибербезопасность становится очень личным вопросом для руководителей, управляющих компаниями на высшем уровне. Для создания и поддержки надежных отношений с клиентами генеральные директора должны взять на себя роль ответственного за доверие к компании. Когда годы работы над стратегией компании могут быть перечеркнуты одной кибератакой, назначение работы над стратегией безопасности директору по защите информации уже недостаточно. Слишком много поставлено на кон.

Подумайте о судьбе генеральных директоров компаний, в которых произошли масштабные утечки, таких как Equifax, Yahoo, Moller-Maersk и Anthem Healthcare. Все усилия, которые компании вложили в развитие бренда, испарились в тот момент, когда клиенты потеряли доверие в результате атаки. Генеральные директора большинства таких компаний преследовали другие интересы.

Чтобы убедиться, что кибербезопасность является неотъемлемой частью бизнес-моделей компаний, руководство должно согласовать усилия и меры по защите активов. Руководители, которые бесконтрольно делегируют работу над стратегией безопасности, значительно рискуют.

Загрузить отчет (бесплатно)

2018–2019 Global Application & Network Security Report