

ПАМЯТКА: ЧТО ТАКОЕ УЯЗВИМОСТИ И ЧЕМ ОНИ ОПАСНЫ ДЛЯ БИЗНЕСА

Что такое уязвимость?

Уязвимость — это слабое место в системе, через которое злоумышленник может нанести ущерб. Это может быть:

устаревшее программное обеспечение

открытые порты и службы

слабые пароли или их отсутствие

некорректные настройки доступа

забытые поддомен или веб-сервис, «торчащий наружу»

Почему уязвимости — это проблема?

НАРУШЕНИЕ РАБОТЫ БИЗНЕСА

Взлом CRM, сайта или почты может остановить ключевые процессы

УТЕЧКА ДАННЫХ

Часто приводит к финансовым потерям, штрафам и падению доверия клиентов

НЕВИДИМЫЕ АТАКИ

Большинство компаний узнают об уязвимости после инцидента

Где чаще всего скрываются уязвимости?

Корпоративные сервисы и программы, которые доступны из интернета (внешний периметр)

Удалённые точки входа: VPN, почта, веб-приложения

Несанкционированные изменения в ИТ-системах

Публичные «следы» компании в интернете (например, забытые поддомены)

Как бизнесу держать под контролем уязвимости?

Проводите регулярную проверку внешнего периметра

Автоматизируйте выявление уязвимостей: один раз настроили — и система работает сама.

Получайте понятные отчёты с рекомендациями, что закрыть и почему.

Обучите сотрудников: большинство атак начинаются с «не той» ссылки в письме.

Кому особенно важно?

Ритейлу —

из-за CRM, маркетинга и множества сервисов.

Финтеху —

из-за высокой чувствительности данных.

Девелоперам —

чтобы не потерять контроль над документацией и проектами.

**ДАВАЙТЕ ОБСУДИМ,
КАК ЗАЩИТИТЬ ВАШ
БИЗНЕС!**

ПРЕДЛАГАЕМ ВМЕСТЕ НАЙТИ ЛУЧШЕЕ
РЕШЕНИЕ ДЛЯ ВАШЕЙ КИБЕРБЕЗОПАСНОСТИ



ОСТАВИТЬ
ЗАЯВКУ

