PROFESSIONAL TO PROFESSIONAL
IT'PRO

Чек-лист

Первый критичный час при ИБ-инциденте

Минуты 0–5: Обнаружение и фиксация факта

- ☐ Зафиксировать время обнаружения — часы и минуты
- ☐ Определить тип инцидента: вирусная атака, несанкционированный доступ, DDoS, утечка данных, сбой системы и др.
- ☐ Сделать скриншоты сообщений об ошибках, всплывающих окон, уведомлений
- ☐ Отметить, какие системы или сервисы затронуты по первым признакам: файловые серверы, базы данных, почтовая система, 1С или другая учетная система, рабочие станции
- ☐ Уведомить ответственного за ИБ и системного администратора по телефону или защищенному каналу связи

Минуты 6–15: Первичная изоляция и сбор данных

- ☐ Физически изолировать пораженные системы от сети — отключить сетевой кабель. При беспроводном подключении — аппаратно или программно отключить Wi-Fi.
  Питание компьютера не выключать
- ☐ Заблокировать учетные записи, которые вызывают подозрение или подтвержденно скомпрометированы
- ☐ Изолировать подозрительные файлы в отдельную папку или на внешний носитель
- ☐ Остановить подозрительные процессы и службы, предварительно зафиксировав их названия и время остановки
- ☐ Сохранить логи системы, сетевых устройств и приложений за последние 24 часа на внешний носитель
- ☐ Сделать фото/видео экрана и конфигурации оборудования, если это серверная или критическая система

Минуты 16–30: Уведомление и план действий

- ☐ Уведомить руководство при критическом или высоком уровне инцидента: генерального директора, финансового директора, если есть риск финансовых потерь, юридическую службу при подозрении на утечку данных
- ☐ Начать документирование в отдельном файле «ИБ_инцидент_ДД.ММ.ГГГГ_время.doc»: время и дата обнаружения, кто обнаружил, первые признаки, предпринятые действия
- ☐ Оценить масштабы: количество затронутых пользователей, критичные системы под угрозой, возможные потери данных
- ☐ Принять решение о привлечении внешних экспертов: форензика, антивирусная лаборатория, ИБ-подрядчик
- ☐ Подготовить краткое сообщение для сотрудников с инструкциями: что можно и чего нельзя делать

Запрещенные действия в течение первого часа

- ☐ Не перезагружать сервера и рабочие станции без указания специалиста по информационной безопасности
- ☐ Не удалять подозрительные файлы или логи
- ☐ Не менять массово пароли — сначала определить скомпрометированные учетные записи
- ☐ Не вести обсуждение инцидента в незащищенных каналах связи

Разберите свой сценарий реагирования с экспертом

Покажем, что важно сделать в первые минуты, как фиксировать инцидент и кого вовлекать в команду

Записаться на консультацию

Наши контакты

it4pro.ru sales@it4pro.ru +7 4942 39 20 41