21 июня 2025

Атака началась: экстренный план спасения данных и репутации

К сожалению, многие компании начинают задумываться об информационной безопасности не в рамках реализации планомерной ИТ-стратегии, а только после инцидента. Вместе с Константином Юргановым, директором по стратегическому развитию MONS (входит в ГК «КОРУС Консалтинг»), рассмотрим, как оперативно реагировать на кибератаки, какие сложности могут возникнуть при устранении последствий, а также как выстроить системы защиты заранее.

ПОТЕНЦИАЛЬНЫЙ ЛАНДШАФТ УГРОЗ

Атаки на крупные компании с разветвленной структурой за последние годы стали обыденностью: согласно данным с сети сенсоров, во всех отраслях в 1 квартале 2025 года число атак в расчете на одну на организацию выросло в среднем в 3,2 раза по отношению к 4 кварталу 2024 года.

Конечно, у многих есть VPN-доступ и защищённые каналы, но если в вашей компании десятки отделов, критичные бизнес-системы, внутренние порталы, а большое количество сотрудников «внешние» или работает на удаленке, то единая точка входа может оставаться уязвимой. Тогда вы владеете настоящей

«эко-системой» с высоким уровнем сложности и рисков:

- В Active Directory — сотни, а то и тысячи учетных записей, часть из которых давно не используется.
- Пароли зачастую обновляются формально: «Password2023» становится «Password2024».
- Письма-приглашения на обновление безопасности остаются непрочитанными.
- Устаревшие процессы верификации (например, через корпоративную почту) могут быть ненадежны, если почта уже скомпрометирована.

ВОЗМОЖНОЕ РАЗВИТИЕ ИНЦИДЕНТА

Атака придет неожиданно и, вероятно, будет хорошо подготовлена. Используя уязвимость в операционной системе одного из решений, злоумышленники могут проникнуть внутрь периметра, а следующими шагами могут быть:

- Эскалация привилегий (назначение себе прав администратора),
- Запуск шифровальщика (блокировка данных с требованием выкупа),

- Скрытый сбор информации (кража конфиденциальных данных без немедленного ущерба),
- Создание «бекдоров» (для последующего возврата в систему).

Первая должная реакция — полное отключение внешнего периметра, а также изоляция сетевых сегментов. Затем необходимо начать восстановление инфраструктуры.

При этом недостаточно просто «поднять» данные из резервных копий (даже если они уцелеют). Во-первых, при восстановлении данных необходима их полная проверка: возможно вредоносное воздействие на сохраненные данные. Во-вторых, если не усилить внешнюю защиту и не устранить уязвимости – атака повторится.

Представте что первая атака отбита, инфраструктура восстановлена, периметр перекрыт, доступы пересмотрены. Однако на этом история не заканчивается — чаще всего за первой волной следуют повторные атаки. Злоумышленники могут запустить автоматизированный подбор паролей, попытаться использовать сохранённые session tokens или найти оставшиеся бэкдоры. Даже формальная смена учётных данных не гарантирует безопасности, если не устранены все векторы проникновения. В большинстве случаев атаки развиваются волнами, когда за явной угрозой следуют скрытые действия — постепенная утечка уже похищенных данных, активация «спящих» вредоносных модулей или атаки на связанные системы через общие учётные записи. Поэтому после отражения первоначального

инцидента критически важен непрерывный мониторинг и глубокий аудит всех систем.

ПРОВЕРЕННЫЕ ШАГИ ПО ПРЕДОТВРАЩЕНИЮ АТАКИ

1. Резкое усиление модели управления доступом

Внедрение обязательной многофакторной аутентификации (MFA) для всех, без исключений по роли, местоположению или типу устройства.

2. Выбор контролируемого решения

Облачные B2C-инструменты не подходят — нужна управляемая платформа с техподдержкой, логированием и возможностью тонкой интеграции. Оптимально — выбрать решение, которое обеспечивает скорость, гибкость, хорошую техподдержку и возможность интеграции с существующей инфраструктурой.

3. Построение альтернативной верификации

Если использование корпоративной почты под вопросом (например, из-за фишинга, мошенничества с подменой руководителя, подмены домена или вирусов в письмах) — можно использовать Telegram-ботов, связанных с внутренними системами, что позволит подтверждать личность пользователя без использования скомпрометированных учетных данных.

4. Плавное внедрение ИБ-решений без сбоев в бизнесе

Поэтапный переход от одиночной к обязательной многофакторной аутентификации (от 50 до 300 пользователей в неделю) позволяет не перегружать поддержку и сохранить операционную устойчивость. При этом важно не допускать ни одного исключения — независимо от должности, местоположения или типа устройства.

5. Аналитика подключения и активности

Это позволяет выявлять аномалии на ранних стадиях. На этапе внедрения ИБ-решений нужно отслеживать статистику установки и подключения, неудачные попытки входа. На этапе эксплуатации необходимо мониторить попытки подбора паролей, срок неактивности аккаунтов и т.п. Причем всю аналитику собирать с разбивкой по структуре компании с учетом данных из AD.

ЧТО МОЖНО СДЕЛАТЬ УЖЕ СЕЙЧАС

Чтобы не «залатывать дыры» в экстренном режиме, важно выстраивать систему защиты заранее. Исходя из нашего опыта внедрений и наблюдаемых стресс-сценариевможно выделить основные действия для защиты от возможных атак:

1. Экспресс-аудит ИБ

Быстрая оценка уровня зрелости защиты — за 2–3 дня выявляются уязвимости в доступе, инфраструктуре и обучении персонала.

2. Внедрение 2FA/MFA

Реализация многофакторной аутентификации под ключ, с учетом особенностей инфраструктуры, географии и типов устройств.

3. Сканирование периметра

Регулярный контроль безопасности — от ежемесячного инвентаризационного сканирования до ежедневного мониторинга уязвимостей.

4. Фишинг-тесты и обучение

Практические тренировки всех сотрудников с последующим разбором ошибок, формирование устойчивых привычек цифровой гигиены у сотрудников.

5.Пентесты и аудит приложений

Проверка безопасности веб-интерфейсов, внутренних сервисов, конфигураций и исходного кода до появления реальных угроз.

6. Комплексное внедрение решений ИБ

Подбор инструментов, их адаптация под инфраструктуру, формализация в документации и дальнейшее сопровождение — чтобы ИБ была управляемой системой. Главный вопрос не в том, произойдет ли атака, а готова ли компания к ней. И, судя по динамике роста количества инцидентов в корпоративной среде, возможность кибератаки – это только вопрос времени.