10 рекомендаций

по предотвращению атак с использованием программ-вымогателей

1. Обезопасьте используемые средства удаленного доступа. Используйте мультифакторную аутентификацию или, как минимум, сложные и регулярно сменяемые пароли.
2. Незамедлительно устраняйте уязвимости в публично доступных приложениях, особенно те, которые могут позволить атакующим преодолеть внешний периметр.
3. Внедрите комплексную защиту электронной почты, которая позволит обнаруживать и блокировать самые сложные угрозы. **Подробнее >**
4. Контролируйте работу подрядчиков в вашей сети. Удаленный доступ с их стороны должен быть строго регламентирован.
5. Убедитесь, что учетные записи имеют минимальные привилегии в системах. В случае компрометации это затруднит атакующим продвижение по сети.
6. Незамедлительно устраняйте уязвимости на узлах внутренней сети, которые могут позволить атакующим повысить привилегии или продвинуться по сети.
7. Осуществляйте мониторинг использования инструментов двойного назначения, которые могут помочь атакующим провести сетевую разведку, получить аутентификационные данные и пр.
8. Ограничьте доступ к облачным хранилищам. Это может затруднить атакующим выгрузку данных из корпоративной сети.
9. Используйте отдельные учетные записи с мультифакторной аутентификацией для доступа к серверам, содержащим резервные копии. Кроме этого, убедитесь, что у вас также есть оффлайн-копии.
10. Внедрите современное средство мониторинга и блокирования угроз, которое позволяет локализовать и нейтрализовать атаку на любом этапе ее жизненного цикла. **Подробнее >**

Правильное реагирование на атаки с использованием программ-шифровальщиков имеет критическое значение

!

В 97% атак с применением программ-вымогателей восстановить доступ к данным без программы-декриптора невозможно. При этом, торопиться платить выкуп злоумышленникам не рекомендуется.

По итогам реагирования эксперты Group-IB подробно описывают инцидент в отчете и готовят свод рекомендаций по улучшению безопасности инфраструктуры, что позволит свести к минимуму возможность возникновения подобных

Профессиональное реагирование на атаки позволяет:

- Минимизировать ущерб;
- Установить начальную точку компрометации, выявить цепочку заражения, чтобы локализовать инцидент и не допустить его повторения;
- Собрать информацию, необходимую для составления списка индикаторов компрометации;
- Собрать доказательную базу, а также требуемые для проведения расследования сведения;
- Получить рекомендации по улучшению безопасности инфраструктуры и персонала.

Для поддержки вашего бизнеса команда Group-IB предлагает подписку на услугу оперативного удалённого реагирования в случае инцидентов информационной безопасности.

Group-IB Incident Response Retainer
Свяжитесь с нами для получения подробной информации:
lab@group-ib.ru

Подверглись кибератаке?

24/7 **реагирование на инциденты**

Сообщите об инциденте:

— Звонок по номеру **+7 (495) 984-33-64**
— Отправка запроса на email: **response@cert-gib.com**
— Заполнение **формы об инциденте**