10 рекомендаций

по предотвращению атак с использованием программ-вымогателей

1. Осуществлять доступ к серверам по RDP только с использованием VPN.
2. Если обеспечить доступ через VPN не представляется возможным, внедрить мультифакторную аутентификацию.
3. Осуществлять блокировку учетной записи после определенного количества неудачных попыток входа за короткий промежуток времени.
4. Обеспечить сложность пароля учетной записи, использующейся для доступа по RDP, регулярно осуществлять его смену.
5. Использовать NLA (аутентификацию на сетевом уровне) для RDP-соединений.
6. Ограничить список IP-адресов, с которых могут быть инициированы внешние RDP-подключения
7. Внедрить антиспам и антифишинг фильтры.
8. Регулярно обновлять средства антивирусной защиты, а также проводить аудит журналов их работы.
9. Внедрить решение класса «sandbox» для обнаружения вредоносных программ, не детектируемых антивирусным ПО.
10. Осуществлять своевременное обновление операционных систем и прикладного программного обеспечения.

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

В большинстве случаев восстановить доступ к данным после заражения вирусом-шифровальщиком 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 инцидентов в будущем.

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.

Свяжитесь с нами для получения подробной информации: **salesteam@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**