ПРОГРАММЫ-ВЫМОГАТЕЛИ: ПРЕДОТВРАЩЕНИЕ И ЗАЩИТА

ЗАЩИТА В РЕАЛЬНОМ ВРЕМЕНИ

Программы-вымогатели представляют все большую и большую угрозу, с тех пор как злоумышленники нашли способ монетизации вредоносных программ, парализуя работу компьютерных систем и требуя выкуп за восстановление исходного состояния. В отличие от других вредоносных программ, которым для эффективной работы часто приходится оставаться скрытыми в течение длительного времени, программы-вымогатели действуют быстро через адресный фишинг, скомпрометированные веб-сайты и поврежденные загрузки. Финансовые учреждения считаются выгодными целями и особенно уязвимы перед атаками программ-вымогателей, которые угрожают быстрому и эффективному перемещению денежных средств. Однако далеко не всегда злоумышленники сдерживают свое обещание: даже после выплаты выкупа они могут не удалить вредоносную программу и не вернуть конфиденциальную информацию.

- Инвестируйте в системы защиты от вредоносных программ, которые адаптируются к угрозам в реальном времени с помощью анализа данных.
- Оцените безопасность всех подключенных к сети устройств, на которых хранится конфиденциальная или важная информация. Подключайте все вспомогательные системы к отдельной сети.
    - Будьте осторожны при развертывании Интернета вещей и использовании смарт-устройств в рабочей среде, поскольку их системы безопасности зачастую более уязвимы, либо у них может вообще не быть систем безопасности. Кроме того, такие устройства могут использоваться как точки доступа к важным системам.
    - Подумайте о безопасности настроек при удаленной работе. Убедитесь, что инструменты безопасности работают при отсутствии сети для отслеживания всего веб-трафика.
- Стимулируйте обучение сотрудников в области фишинговых атак и необходимости защиты надежным паролем.
- Рассмотрите возможность внедрения многофакторной аутентификации в вашей организации.
- Регулярно обновляйте все системы и программное обеспечение. По возможности измените настройки и разрешите автоматическое обновление.
- Разработайте план действия в кризисных ситуациях и реагирования на инциденты для борьбы с атаками программ-вымогателей и потерей ценных данных.
- Подготовьте план внешней связи на случай атаки программ-вымогателей.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

- Инвестируйте в безопасные, регулярно обновляемые системы резервного копирования, обеспечивающие защиту ваших данных.
    - При использовании USB-накопителей или жестких дисков физически отключайте эти устройства от компьютеров, подключенных к сети, после завершения резервного копирования.
    - При использовании облачного хранилища оборудуйте сервер шифрованием высокого уровня и многофакторной аутентификацией.
- Создайте копию главной книги, предназначенную только для чтения, на случай аварийного восстановления в худших условиях.
- Разрабатывайте системы, которые выполняют автоматическое восстановление и исправление данных.
- Разработайте сценарии для оценки времени восстановления критических данных и бизнес-служб.

Оценка готовности вашей организации к атакам программ-вымогателей

При разработке плана предотвращения атак программ вымогателей и защиты от них рассмотрите следующие вопросы.

1. **Регулярно** ли в вашей организации выполняется **плановое резервное копирование**?
    - Отключены ли эти резервные копии от сети (с помощью облачного хранилища или физического отключения USB-накопителей / жестких дисков?
2. Подключены ли к сети вашей организации какие-либо **вспомогательные устройства**?
    - Могут ли они быть переподключены к другим сетям, в которых не хранится конфиденциальная информация?
3. Осознают ли в вашей организации **нормативные и правовые риски,** связанные с выплатой выкупа?
    - В каждой стране действуют свои правовые руководства, которые часто обновляются.
4. Регулярно ли в вашей организации обновляется программное обеспечение и системы? Обновления **автоматизированы**?
5. Есть ли в вашей организации **план борьбы с атаками программ-вымогателей** и предотвращения потери ценных данных?
6. Есть ли у вашей организации **полис киберстрахования**? Если есть, что покрывает план страхования при атаках программ-вымогателей?
    - Некоторые планы прямо запрещают выплату выкупа, в то время как другие покрывают такие выплаты в рамках полиса.

НОРМАТИВНО-ПРАВОВАЯ СРЕДА

- Оцените соответствующие нормативные и правовые руководства по программам-вымогателям для вашей операционной среды.
  - Изучите рекомендации для конкретной страны. Разработайте план по периодической оценке изменений в руководствах.
  - Изучите рекомендации для конкретного финансового сектора.
  - Изучите международные правовые и нормативные требования.
- Оцените риски, связанные с выплатой выкупа. В некоторых случаях выплата выкупа может нарушить действующие санкции в отношении злоумышленников.
- Поддерживайте контакт с правоохранительными органами. Организуйте способы коммуникации для быстрого обмена информацией в случае атаки.
- Оцените преимущества и недостатки полисов киберстрахования от атак программ-вымогателей.