КИБЕРБЕЗОПАСНОСТЬ ДЛЯ НЕБОЛЬШИХ ОРГАНИЗАЦИЙ

КОНТРОЛЬНЫЙ СПИСОК РЕАГИРОВАНИЯ НА ПРОГРАММЫ-ВЫМОГАТЕЛИ

ГОТОВНОСТЬ К ПРОГРАММАМ-ВЫМОГАТЕЛЯМ

☐ **При разработке плана предотвращения и защиты от программ-вымогателей периодически оценивайте следующие факторы:**

- Регулярно ли в вашей организации выполняется плановое резервное копирование?
- Подключены ли к сети вашей организации какие-либо вспомогательные устройства?
- Осознают ли в вашей организации нормативные и правовые риски, связанные с выплатой выкупа?
- Регулярно ли в вашей организации обновляются системы программного обеспечения? Эти обновления автоматизированы?
- Есть ли у вашей организации план борьбы с атаками программ-вымогателей и потерей данных?
- Есть ли у вашей системы полис киберстрахования? Если есть, что покрывает план страхования при атаках программ-вымогателей?

ЗАЩИТА В РЕАЛЬНОМ ВРЕМЕНИ

☐ **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.
- ☐ Подумайте о безопасности настроек удаленной работы. 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 программное обеспечение и системы.**

- ☐ 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 серверы 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.**

НОРМАТИВНО-ПРАВОВАЯ СРЕДА

- ☐ **Оцените соответствующие нормативные и правовые руководства по программам-вымогателям для вашей операционной среды.**
  - ☐ Изучите рекомендации для конкретной страны.
  - ☐ Изучите рекомендации для конкретного финансового сектора.
  - ☐ Изучите международные правовые и нормативные требования.
  - ☐ Разработайте план по периодической оценке изменений в руководствах.
- ☐ Оцените риски, связанные с выплатой выкупа.
- ☐ 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.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org