CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Руководство по программам-вымогателям

Как подготовиться к атаке программ-вымогателей, реагировать на нее, и восстановиться после нее

К 2021 году
«каждые 11 секунд»

новая организация станет
жертвой программ-вымогателей,
по данным исследователя рынка
Cybersecurity Ventures.[1]

Руководство по программам-вымогателям

Платить или не платить? Этот вопрос часто является первым, который задают многие организации после того, как они подверглись атаке программы-вымогателя.

К сожалению, выбор не прост. Многие организации попросту не знают, как защититься от программ-вымогателей. Это руководство предназначено для предоставления организациям (например, малым и средним предприятиям, государственным и местным органам власти) дорожной карты по защите от этой растущей угрозы.

[1] umbrella.cisco.com/blog/2019/12/17/ransomware-defense-for-dummies-2nd-edition

Все организации подвержены риску шифрования своих ценных данных (о клиентах, сотрудниках, операциях) злоумышленниками, в результате чего организация потеряет к ним доступ. Атака программы-вымогателя проводится злоумышленниками для удержания данных организации с целью получения выкупа. Злоумышленники могут получить доступ к данным организации различными способами, включая фишинг и неисправленное программное обеспечение. Патчи выпускаются компаниями-разработчиками ПО для устранения уязвимостей, которые они находят в своих программах. Многие пользователи не загружают патчи, а это означает, что уязвимости могут стать мишенью для злоумышленников.

Организация, создающая культуру киберготовности, может быть устойчива к атакам программ-вымогателей, принимая профилактические меры (например, создавая резервную копию важных данных), а также разрабатывая и тестируя план реагирования на инциденты программ-вымогателей. Организация должна обратить особое внимание на выполнение этих трех шагов: подготовка, реагирование и восстановление.

ШАГ 1

ПОДГОТОВКА

ШАГ 2

РЕАГИРОВАНИЕ

ШАГ 3

ВОССТАНОВЛЕНИЕ

Подготовка

Убедитесь, что ваша компания регулярно создает резервные копии своих данных; хранение данных в облаке — распространенный инструмент, используемый для резервного копирования. Если ваши сотрудники сохраняют важную деловую информацию на своих компьютерах, ваша организация также должна предоставить им четкие инструкции о том, как регулярно создавать резервные копии своих данных. К основным элементам защиты от программ-вымогателей относятся:

Ø Определение приоритета данных, которые наиболее важны для вашей организации, и создание их резервной копии. Убедитесь, что вы можете выполнить повторную установку из резервных копий, которые зачастую находятся в облаке, и что резервные копии часто проверяются.

Ø Раннее обнаружение. Оно важно, поэтому убедитесь, что ваши сотрудники знают, как сообщить о возможном инциденте, связанном с программами-вымогателями или необычном поведении сети.

Ø Заключение договора, если это возможно, с поставщиком, который может обеспечить поддержку реагирования в случае возникновения инцидента: заключите контракт до события, чтобы у вас был немедленный доступ к поставщику.

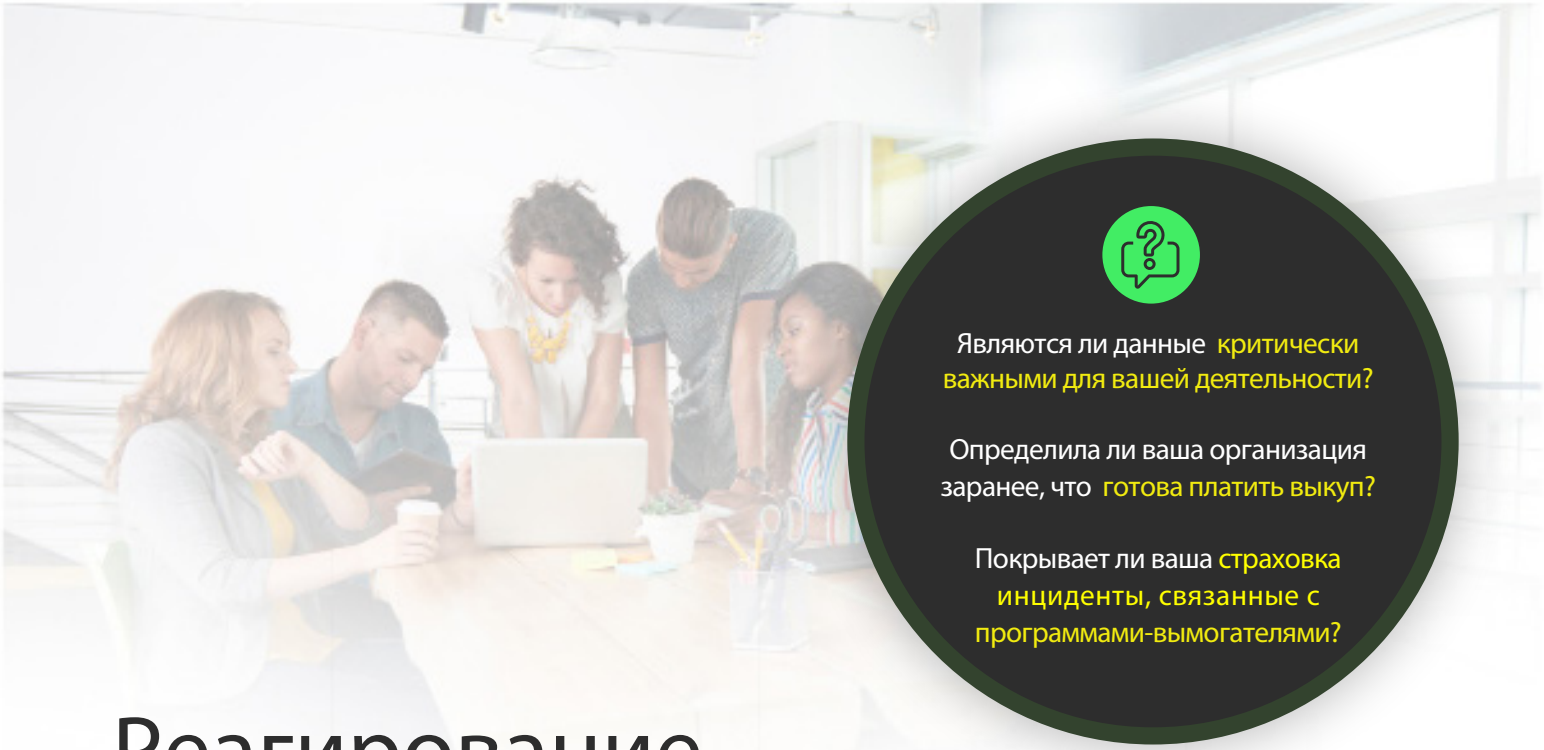
Поскольку злоумышленники часто используют фишинг для заражения системы программами-вымогателями, очень важно иметь политику в отношении фишинга. Проводите регулярные тесты на фишинг, чтобы сотрудники могли обнаружить фишинговое электронное письмо, прежде чем переходить по опасным ссылкам или вложениям, и, по возможности, использовать антифишинговую программу.

Поскольку злоумышленники часто используют фишинг для заражения системы программами-вымогателями, очень важно иметь политику фишинга. Проводите регулярные тесты на фишинг, чтобы сотрудники могли обнаружить фишинговое электронное письмо, прежде чем переходить по опасным ссылкам или вложениям, и, по возможности, использовать антифишинговую программу.

Разработайте общеорганизационную политику в отношении атак программ-вымогателей. Гораздо легче вести эти обсуждения, чем реагировать, находясь под давлением. Вопросы для рассмотрения:
Какие данные наиболее важны для вашей организации?
Покрывает ли ваша страховка программы-вымогатели?
Вы согласны заплатить выкуп? Если да, то понимаете ли вы, как использовать биткойн и другие криптовалюты?

Обсудите и примите общеорганизационную политику в отношении атак программ-вымогателей.

Гораздо легче вести эти обсуждения, чем реагировать, находясь под давлением.



Являются ли данные критически важными для вашей деятельности?

Определила ли ваша организация заранее, что готова платить выкуп?

Покрывает ли ваша страховка инциденты, связанные с программами-вымогателями?

Реагирование

Если сотрудник или организация сталкиваются с запросом о выкупе, ваша организация должна сначала оценить законность запроса о выкупе, обратившись к ИТ-менеджеру. Если это законно, то представлены два возможных сценария:

1. В вашей организации есть работающие резервные копии.
   Вам не нужно беспокоиться о программах-вымогателях.
   Вы полностью восстанавливаете свои данные и возвращаетесь к работе.

2. Захваченные данные нужны, а рабочих резервных копий нет.

   a. Проверьте, существуют ли данные где-то еще в организации (например, кэш-файлы, электронная почта). Вы могли бы соединить их вместе, чтобы заменить данные, захваченные злоумышленниками.

   б. Если вы не можете получить, доступ к данным в другом месте, задайте следующие вопросы:

   - Являются ли данные критически важными для вашей деятельности?
   - Приняла ли ваша организация заблаговременное решение о том, что она может заплатить за выкуп?
   - Покрывает ли это ваша страховка?

Реагирование

Пожар потушен, и пришло время вернуться к обычным делам. Масштабы атаки вымогателей и серьезность ее влияния на вашу повседневную деятельность будут определять, сколько времени и усилий потребуется для восстановления.

Используйте инцидент в качестве учебного опыта, чтобы подчеркнуть важность принципов кибербезопасности таких, как исправление ошибок и осведомленность о фишинге. Периодическое обновление вашего ПО последними исправлениями безопасности затруднит проникновение в вашу систему. Аналогичным образом, применение рутинного обучения фишингу сводит к минимуму человеческие ошибки и потенциальные точки входа в вашу систему. Как и в случае любого нарушения безопасности, уведомите все затронутые стороны, повторно установите идентификаторы пользователей и пароли всех скомпрометированных устройств, обновите программное обеспечение на всех устройствах и переустановите свои данные из резервных копий после нейтрализации угрозы вымогателей.

Особенно важно обновлять исправления после атаки. Если данные были восстановлены, иногда могут снова появиться уязвимости, которые были исправлены до программ-вымогателей.

Программа киберготовности включает подробные инструкции и шаблоны, которые помогут вам создать собственные политики и план реагирования на инциденты, чтобы подготовиться, отреагировать и восстановиться после атаки программы-вымогателя. Зарегистрируйтесь бесплатно на BeCyberReady.com.

Чтобы узнать о реальных примерах того, как компании и муниципалитеты реагировали на атаки программ-вымогателей, посетите раздел Новостей о киберготовности.

Программа киберготовности включает подробные инструкции и шаблоны, которые помогут вам создать собственные политики и план реагирования на инциденты, чтобы подготовиться, отреагировать и восстановиться после атаки программы-вымогателя.

Руководство по принятию решений в отношении программ-вымогателей

ПОДГОТОВКА

Классифицировали ли вы свои данные и системы по принципу приоритетности, чтобы знать, что наиболее важно для ваших бизнес-операций?

Определите, что является наиболее ценным. Перейдите на BeCyberReady.com, чтобы получить доступ к контрольному списку приоритетов.

Есть ли у вас план реагирования на инциденты, связанный с программами-вымогателями?

Разработайте план реагирования на инциденты с программами-вымогателями. Перейдите на сайт BeCyberReady.com, чтобы получить доступ к шаблону плана реагирования на инциденты.

Есть ли у вас текущая резервная копия?

Сделайте резервную копию вашей системы и всех данных.

Вы тестировали ее в прошлом месяце?

Протестируйте резервную копию, чтобы убедиться, что вы можете восстановить свои данные, особенно наиболее важные для ваших бизнес-операций.

Поздравляем. Вы готовы.

Вам лучше надеяться на то, что вы не подвергнетесь атаке программ-вымогателей. Вы ДЕЙСТВИТЕЛЬНО не готовы.

Происходит инцидент с программой-вымогателем

РЕАГИРОВАНИЕ

Изолируйте инцидент и удалите зараженные компьютеры из сети. Затем продолжайте.

Отличная работа. Переходите к этапу восстановления!

У вас есть служба ИТ-поддержки, к которой вы можете обратиться?

Можете ли вы или ваша ИТ-поддержка выполнить резервное копирование в режиме реального времени?

Являются ли захваченные данные ценными для вашего бизнеса?

Есть ли у вас киберстраховка?

Учитывает ли ваша политика случаи выкупа?

Ваши данные не подлежат восстановлению… Решайте, платить или нет.

ВОССТАНОВЛЕНИЕ

Зайдите в резервную копию в реальном времени и очистите вредоносное ПО.

Сбросьте идентификаторы пользователей и измените пароли

Сделайте чистую установку из резервной копии

Обновите свое ПО

Выполните выборочную переустановку данных

Вы снова готовы к работе!! Зарегистрируйтесь в бесплатной программе киберготовности на BeCyberReady.com чтобы предотвратить новые атаки программ-вымогателей в будущем.

CYBERREADINESSINSTITUTE.ORG

guide@cyberreadinessinstitute.org