Чек-лист: защита бизнеса от шифровальщиков в условиях удаленной работы

kaspersky АКТИВИРУЙ БУДУЩЕЕ

В последнее время шифрование данных стало основной проблемой, с которой сталкивались компании. Число компаний, атакованных шифровальщиками (программами-вымогателями), возросло с 34% в 2019 году до 51,9% в 2021 году[1]. Неудивительно, что кибербезопасность становится одним из главных стратегических приоритетов для бизнеса.

В условиях удаленной работы риск стать жертвой шифровальщиков значительно увеличился. Многие организации ослабили контроль за рабочими местами или стали менее строго соблюдать обычные протоколы безопасности.

В случае атак шифровальщиков организации стремятся в кратчайшие сроки восстановить доступ к зашифрованным данным. Однако стоит помнить, что злоумышленники часто извлекают файлы из систем жертв с целью шантажа и требуют дальнейших платежей, чтобы не допустить утечки конфиденциальной информации.

По сравнению с 2020 годом в 2021 году меньше компаний развернули средства сетевой безопасности (меньше на 5%) или инструменты для мониторинга конечных пользователей (меньше на 6%)[2]. Без эффективного мониторинга и защиты рабочих мест риск стать жертвой вымогателей значительно повышается.

Рабочие места всегда были слабым звеном в корпоративной безопасности, так как атаковать их проще всего. Переход на удаленную работу вынес рабочие места за пределы периметра сети, что значительно усложнило обеспечение их безопасности.

Для защиты от масштабных атак с использованием шифровальщиков необходимо внедрить эффективную стратегию противодействия на нескольких уровнях. Так как удаленная работа становится нормой, организациям следует пересмотреть и усилить защиту рабочих мест, особенно с точки зрения обнаружения и блокирования шифровальщиков.

Это руководство вы можете использовать на практике как контрольный список, который поможет оценить уровень защиты от программ-шифровальщиков в вашей сети и определить, где защиту необходимо усилить. Вот шесть факторов, которые необходимо рассмотреть:

1. Обнаружение шифровальщиков на конечных устройствах
2. Конфигурирование рабочих мест
3. Организация резервного копирования
4. Вынесение операций из локальной среды
5. Обучение конечных пользователей
6. Планирование реагирования на инциденты безопасности

[1] «Лаборатория Касперского», «Природа инцидентов информационной безопасности», 2022. https://securelist.ru/the-nature-of-cyber-incidents/105708/

[2] Министерство Великобритании по вопросам цифровых технологий, культуры, СМИ и спорта. Опрос о нарушениях кибербезопасности, проведенный в 2021 году: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Обнаружение шифровальщиков на конечных устройствах

Крайне важно остановить атаку шифровальщика до того, как он распространится в системе. Чем быстрее вы обнаружите и заблокируете заражение, тем меньше простоев и ущерба оно вызовет.

В большинстве случаев организация может перехватить вредоносное ПО, вложенное в письма для сотрудников, еще на почтовом сервере. Однако искусный целевой фишинг может обманом заставить отдельных сотрудников загрузить исполняемые файлы из внешних источников.

Вы можете более эффективно отслеживать шифровальщики, если будете блокировать подозрительные исполняемые файлы на рабочем месте:

- Разверните надежные инструменты для защиты от вредоносного ПО, которые будут выявлять и удалять подозрительные исполняемые файлы до того, как они зашифруют конфиденциальные файлы.
- Используйте технологии EDR на базе машинного обучения, чтобы автоматически отслеживать и блокировать подозрительные действия в системе.
- Рассмотрите возможность использовать решение для управляемого обнаружения и реагирования (MDR), которое поможет нейтрализовать шифровальщиков с помощью проверенных методов и экспертных знаний.

Перечисленные инструменты помогут сдержать заражение и предотвратить распространение зловреда в других файловых хранилищах и системах.

Следует отметить, что федеральные органы и правительственные организации стали занимать более жесткую позицию в отношении того, как жертвы реагируют на атаки шифровальщиков. Так, в 2019 году в США Центр рассмотрения жалоб на интернет-преступления (IC3) ФБР призвал компании не платить выкуп[3].

«Лаборатория Касперского» разделяет этот призыв: «Ни в коем случае не платите вымогателям. Каждый выкуп – это финансовый вклад в развитие зловредов и сигнал злоумышленникам о том, что продолжать в том же духе выгодно. Кроме того, даже выполнив требования злоумышленников, вы можете ничего не получить взамен[4]».

В марте 2022 года российский Национальный координационный центр по компьютерным инцидентам (НКЦКИ) выпустил подробный перечень рекомендаций по защите от шифровальщиков для организаций. Это солидный перечень мер противодействия атакам подобного типа[5].

Последовательная реализация мер информационной безопасности означает, что рабочие места за пределами сетевого периметра защищены так же, как рабочие места внутри периметра. В данном случае – с использованием эффективных и надежных решений для защиты от вредоносного ПО и интеллектуальных EDR-инструментов, которые автоматически обнаруживают действия шифровальщиков и подобных им программ.

[3] Центр рассмотрения жалоб на интернет-преступления (IC3) ФБР. Атаки с использованием программ-шифровальщиков на организации США, повлекшие за собой значительный ущерб: https://www.ic3.gov/Media/Y2019/PSA191002

[4] «Лаборатория Касперского». Как защититься от шифровальщиков-вымогателей: 5 советов: https://www.kaspersky.ru/blog/ransomware-five-tips/31352/

[5] НКЦКИ: рекомендации для компаний по защите от компьютерных атак с использованием программ-шифровальщиков, https://safe-surf.ru/specialists/news/677142/

[6] «Лаборатория Касперского». Шифровальщики: кто, как и зачем использует их в 2021 году: https://securelist.ru/ransomware-world-in-2021/101425/

[7] Министерство Великобритании по вопросам цифровых технологий, культуры, СМИ и спорта. Опрос о нарушениях кибербезопасности, проведенный в 2021 году: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

2. Конфигурирование рабочих мест

Конфигурирование рабочих мест – еще одна мера, которая помогает избежать возможных последствий от заражения шифровальщиком. Если для работы используются устройства, выданные организацией, сделайте следующее:

- Настройте список разрешенных приложений, чтобы сотрудники могли запускать только санкционированные программы. Если установлены подходящие ограничения, сотрудники не смогут устанавливать приложения – и это снизит возможность запустить инфицированные исполняемые файлы.
- Настройте автоматическое обновление инструментов защиты рабочих мест (и остальных установленных программ), чтобы они могли блокировать новые угрозы и устранять возможные уязвимости до того, как ими воспользуются злоумышленники[6].

Специалисты по кибербезопасности рекомендуют применять обновления программного обеспечения в течение 14 дней после выхода. К сожалению, только 43% организаций следуют этому принципу[7]. Остальные упускают возможность предотвратить распространение шифровальщика, которую сравнительно легко реализовать.

Дополнительное затруднение вызывает использование для работы личных устройств (модель BYOD), так как организация может контролировать их только частично. В таком случае вам доступны несколько вариантов:

- Предложите сотрудникам установить на все личные устройства одобренные инструменты для защиты от вредоносного ПО. Обеспечив бесплатный доступ к таким программам, вы дадите сотрудникам хороший стимул для их использования. Это позволит защитить личные данные сотрудников наравне с корпоративными.

- Организуйте размещение корпоративных приложений и данных в изолированной среде (песочнице), чтобы они были отделены от личных приложений сотрудников. Песочница поможет замедлить распространение угрозы, если вредоносное ПО проникнет в устройство сотрудника через личное приложение.

Наконец, защита личных устройств предполагает компромисс и согласие использовать меры, допустимые и для компании, и для сотрудника. Если такой возможности нет, компании необходимо рассмотреть альтернативные методы доступа – или предоставить сотруднику корпоративное устройство.

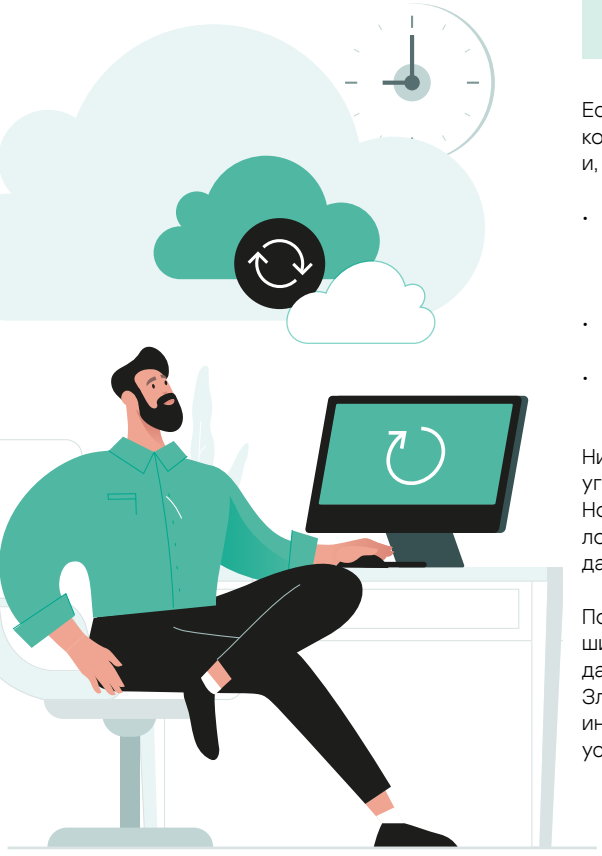
3. Организация резервного копирования

После того как файлы были зашифрованы, у вас остается два выхода: заплатить выкуп или восстановить «чистые» копии файлов из резервного хранилища. А для этого требуется надежная процедура резервного копирования данных с рабочих мест.

В идеальном варианте сотрудники не должны иметь возможность сохранять корпоративные данные на локальном устройстве. Но в реальности они, скорее всего, будут сохранять документы на локальный жесткий диск, например в папку «Загрузки» или на рабочий стол.

В процессе организации безопасной удаленной работы рассмотрите следующие вопросы:

- Насколько высока вероятность того, что корпоративные данные сохраняются в локальной среде?
- Какие данные сохраняются?
- Насколько высок риск шифрования файлов или потери доступа к ним?
- Как осуществить резервное копирование этих данных?



Если рабочее место находится за пределами периметра сети, задача резервного копирования усложнится. Как вы ее решите, зависит от технической архитектуры и, в некоторой степени, от IT-компетентности конечного пользователя. Возможные варианты:

- Синхронизация данных в выбранных папках с облачным хранилищем или другим удаленным сервисом – желательно с созданием резервных копий, которые нельзя переписать или изменить.

- Резервное копирование на локальный съемный диск.

- Использование функций, встроенных в операционную систему, для автоматизированного создания теневых копий данных и точек отката изменений.

Ни одно из этих возможных решений не является идеальным, так как изначально существует угроза создания резервной копии файлов, которые уже были заражены или зашифрованы. Но в любом случае необходимо определить способ отслеживать данные, сохраняемые локально, в частности для соблюдения нормативных требований и обязательств по защите данных.

Помните: резервное копирование данных – последняя линия обороны от атак шифровальщиков на ваши файлы. Кроме того, резервное копирование и восстановление данных не защитит вашу компанию от утечек или доксинга (раскрытия личных данных). Злоумышленники могут продолжать требовать выкуп, угрожая раскрыть конфиденциальную информацию. Единственный способ защитить закрытые данные компании – максимально усложнить злоумышленникам доступ к рабочим местам.

4. Вынесение операций из локальной среды

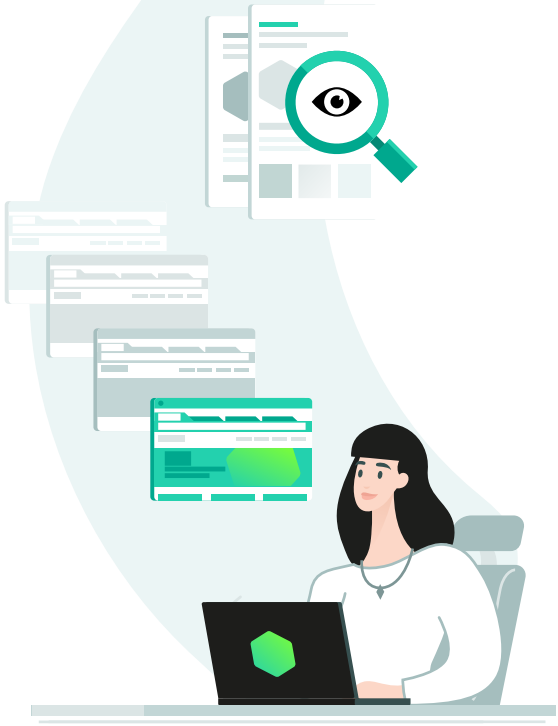
Чем больше данных и приложений находится на рабочем компьютере, тем уязвимее он становится для атак. И тем привлекательнее для злоумышленников. Поэтому, сокращая количество приложений и объемы данных, которые хранятся локально, вы снижаете потенциальный ущерб от заражения шифровальщиком.

Для удаленного выполнения приложений и минимизации объемов данных в локальных хранилищах можно использовать облачные службы. Например, электронная почта и офисные программы могут работать в облаке как веб-приложения, что позволит исключить или свести к минимуму передачу данных в локальной среде. Многие сервисы, особенно электронной почты, также обладают функциями расширенной защиты от вредоносного ПО: они проверяют, обнаруживают и блокируют подозрительные вложения до того, как пользователь их загружает.

Виртуализация – еще один один вариант вынесения нагрузок из локальной среды. Используя трансляцию рабочего стола и приложений, пользователь может войти в сеанс в корпоративном центре обработки данных или в облаке. Для конечного пользователя он будет выглядеть как сеанс рабочего стола, но данные при этом размещаются и обрабатываются в виртуализированной системе.

Сеансы подключения к удаленному рабочему столу (RDP) считаются крупнейшим вектором атаки для шифровальщиков[8]. Однако правильная конфигурация RDP позволяет создать песочницу – промежуточную среду между конечным рабочим устройством и корпоративными системами. И широкое использование RDP в корпоративных сетях свидетельствует об эффективности такого решения.

Наконец, чтобы предотвратить атаки хакеров и компрометацию подключения и сеансов RDP вредоносными программами, необходимо надлежащим образом защитить рабочее место пользователя.



Эти же преимущества RDP можно использовать и для удаленной работы, если применить следующие меры по усилению защиты рабочих мест:

- Применение политики надежных паролей, которая поможет защититься от атак путем подбора паролей.
- Развертывание многофакторной аутентификации для предотвращения перехвата сеансов.
- Использование безопасного соединения (VPN) для обмена любыми данными между рабочими местами и RDP-серверами.
- Оценка и укрепление сетевого экрана по периметру сети для предотвращения несанкционированных подключений.
- Использование EDR-инструментов для автоматического отслеживания и блокирования подозрительных действий.
- Выбор нестандартных портов для RDP-подключения с целью предотвратить возможные попытки взлома.

5. Тренинги для сотрудников

Ошибки сотрудников часто открывают двери злоумышленникам. Но в то же время они могут сыграть важную роль в защите от шифровальщиков – если знают, что нужно делать. Все сотрудники, не только удаленные, должны регулярно участвовать в тренингах, чтобы научиться распознавать потенциальные кибератаки и четко знать свои дальнейшие действия. Ежедневно по фишинговым ссылкам переходят 2% сотрудников организаций[9] – можно предположить, что примерно столько же пользователей ежедневно загружают шифровальщики.

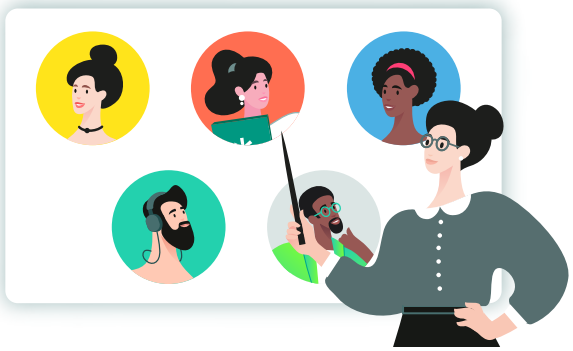
Тренинги должны быть интересными для сотрудников (не для галочки), иметь практическую направленность и проводиться регулярно, ведь киберугрозы постоянно эволюционируют. Одна-единственная презентация о том, как распознавать фишинговые письма и подозрительные исполняемые файлы, быстро устареет (и забудется).

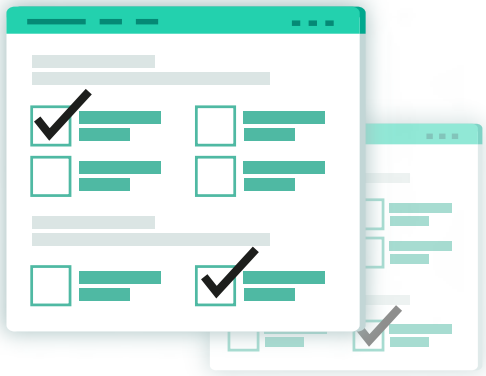
[8] Emisoft. Как защитить инфраструктуру RDP от атак с использованием программ-шифровальщиков: https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9] Verizon. Отчет Mobile Security Index об угрозах безопасности мобильных устройств в 2020 г.: https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Настройка программы обучения

Наиболее эффективные атаки с использованием шифровальщиков нацелены на людей, выполняющих в организации определенные роли. Подобным образом стоит адаптировать и тренинги по кибербезопасности. Сотрудники отделов финансов, управления персоналом, маркетинга и руководители будут подвергаться разным типам атак. Поэтому о возможных угрозах с каждым следует говорить на его «языке». Это будет полезнее для них – и для бизнеса.



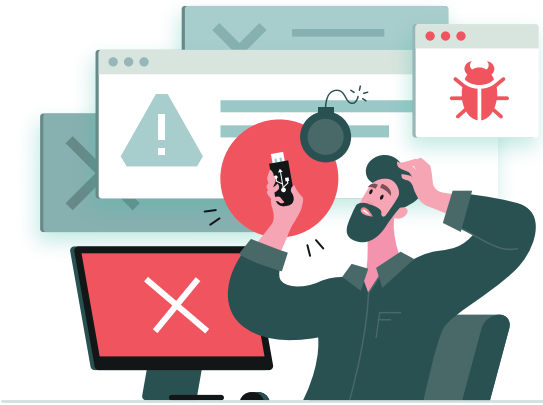


Проверка знаний

Знания немногого стоят, если не применять их на практике. Регулярная проверка знаний дает уверенность, что сотрудники смогут применить их на практике, если возникнет необходимость. Стандартизированная оценка также поможет выявить пробелы в знаниях или возможности для дальнейшего развития навыков и укрепления защиты вашего бизнеса.

Не только фишинг

Фишинг и вредоносные вложения – наиболее очевидный возможный источник заражения шифровальщиком. Однако конечным пользователям следует знать и о других угрозах. Зараженные съемные диски, вредоносные веб-сайты и перекрестное заражение между рабочими и личными приложениями тоже могут стать источниками вредоносного ПО на рабочем месте и в корпоративной сети в целом. Необходимо обучить сотрудников распознавать их.

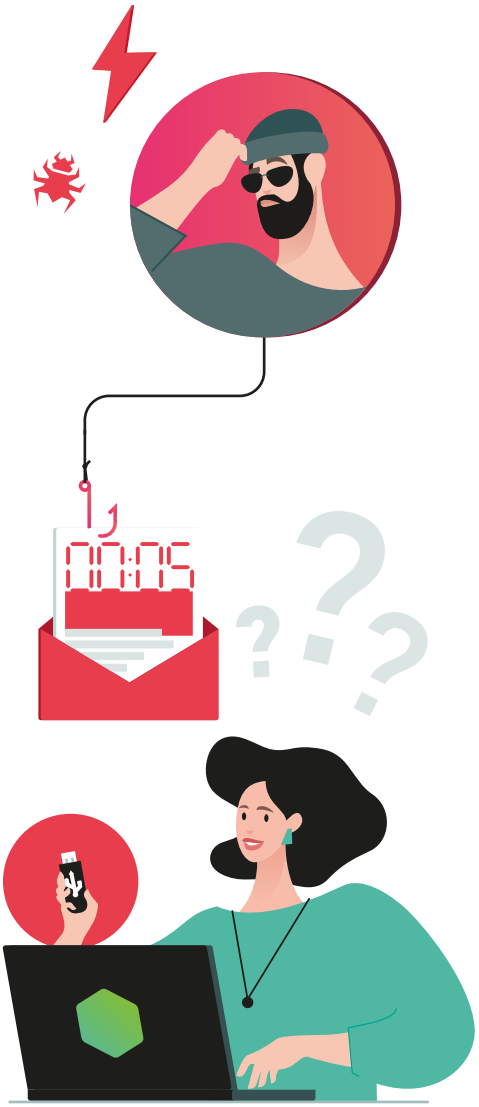


Тренинги должны быть интересными

Кибербезопасность может быть сухой, скучной темой, особенно если она не относится к основным рабочим обязанностям. Маловероятно, что ваши сотрудники будут читать (и тем более понимать) сводки Национального координационного центра по компьютерным инцидентам. Игровой формат тренингов повысит к ним интерес, особенно по мере усложнения изучаемых понятий. Постановка целей и задач, поощрение конкуренции и добавление развлекательного элемента поможет сотрудникам оставаться вовлеченными и продолжать приобретать знания и навыки.

Инвестирование в навыки сотрудников – это важный шаг к усилению защиты рабочих мест. Сведение человеческого фактора к минимуму является, возможно, самым эффективным средством предотвратить заражение шифровальщиком. Кроме того, сотрудники научатся правильно реагировать на заражение на ранних этапах, помогая предотвратить распространение шифровальщиков и снизить общий ущерб для бизнеса.

6. Налаженный процесс реагирования на инциденты безопасности



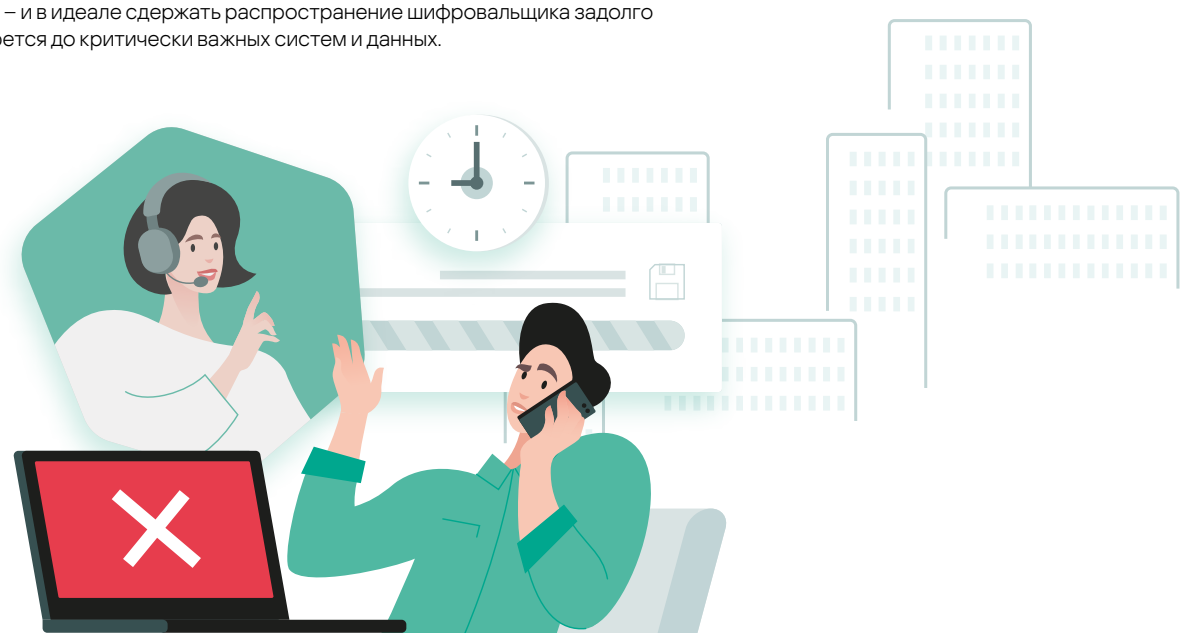
Удивительно, но 32% компаний не имеют четкого плана реагирования на инциденты безопасности, такие как атака с использованием шифровальщика[10]. Это влечет за собой неоправданно высокие риски, так как любая организация может столкнуться с вредоносным ПО в обозримом будущем.

Разрабатывая план реагирования на инциденты, компания может своевременно оценить уязвимости и принять необходимые меры по их устранению. План также поможет реагировать быстрее: когда имеешь дело с шифровальщиками, каждая секунда на счету.

Хотя каждая организация использует собственный план аварийного восстановления рабочей инфраструктуры, он обязательно должен включать следующие элементы:

- **Стратегия коммуникации.** Необходимо предоставлять нужную информацию в нужное время именно тем участникам процесса, для которых она предназначена. Также необходимо обеспечить удаленным сотрудникам возможность связаться с экспертами, которые смогут помочь им на ранних этапах заражения.
- **План действий в случае атаки.** Решите, как вы будете определять серьезность атаки и как будете реагировать.
- **Доступ к документации.** Высока вероятность того, что из-за заражения рабочего места ваши сотрудники не смогут использовать руководства или инструкции по реагированию на атаки шифровальщиков. Необходимо обеспечить доступность этой информации даже в случае отказа рабочих систем.
- **Управление действиями сотрудников.** Сразу после того, как проблема была обнаружена, вы должны назначить специалиста в помощь удаленному сотруднику. Такой специалист сможет разъяснить действия по снижению рисков и восстановлению данных, которые нужно выполнить в первую очередь, а также собрать информацию для отчета регуляторам, если необходимо.
- **Повышенная бдительность.** Если на удаленном рабочем месте обнаруживается заражение шифровальщиком, IT-специалисты организации должны сразу усилить мониторинг и формирование отчетов, чтобы оценить, насколько были скомпрометированы центральные системы. Затем, если потребуется, они смогут запустить аварийное восстановление согласно плану.

Продуманный план аварийного восстановления поможет вашему бизнесу сократить ущерб от вредоносного ПО – и в идеале сдержать распространение шифровальщика задолго до того, как он доберется до критически важных систем и данных.



[10] Министерство Великобритании по вопросам цифровых технологий, культуры, СМИ и спорта. Опрос о нарушениях кибербезопасности, проведенный в 2021 году: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Заключение

IT-руководители долгое время опасались перехода на удаленную работу – не без оснований. Однако случилось так, что удаленная работа стала нормой.

Одновременно с этим шифровальщики стали стандартным инструментом киберпреступников. Атаки происходят часто и эффективно и могут приводить к тяжелому ущербу. Переход на удаленную работу увеличивает поверхность атаки и намного повышает вероятность того, что атакам вымогателей в конечном итоге подвергнутся все организации.

Учитывая эти вводные, защита рабочих мест от шифровальщиков должна стать стратегическим приоритетом. В противном случае организация может не успеть отразить атаку шифровальщика.

В этом руководстве мы рассказали, как лучше подготовиться к атакам с использованием шифровальщиков. Вот шесть факторов, которые нужно учесть, чтобы быстро укрепить защиту рабочих мест:

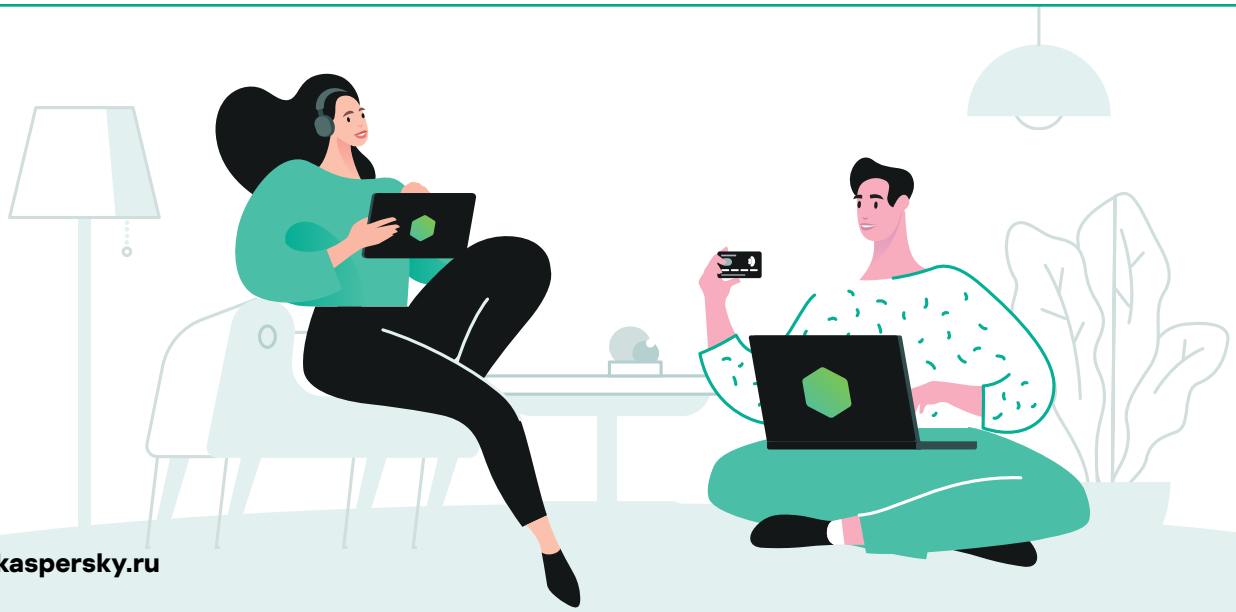
1. Обнаружение и удаление вредоносных программ
2. Конфигурирование устройств
3. Резервное копирование и восстановление данных
4. Вынесение операций из локальной среды
5. Тренинги для сотрудников
6. Налаженный процесс реагирования

Решения Kaspersky Optimum Security помогут вашей организации защититься от шифровальщиков и других современных угроз. Базовые инструменты в составе Kaspersky EDR для бизнеса Оптимальный позволяет вам быстро и точно реагировать на атаки на рабочую инфраструктуру, а тренинги Kaspersky Security Awareness сделает поведение ваших сотрудников кибербезопасным.

Подробнее см. на сайте **go.kaspersky.com/optimum**

Рекомендуем прочитать:

История года: программы-вымогатели в заголовках СМИ
Как выбрать подходящий уровень защиты рабочих мест
Руководство покупателя EDR-решения
Укрепление защиты системы для обеспечения кибербезопасности во время удаленной работы



www.kaspersky.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ