Контрольный список для предотвращения атак программ-вымогателей

Согласно последнему отчету экспертов ИТ-индустрии из Института технологий критически важной инфраструктуры (Institute for Critical Infrastructure Technology), 2016 год стал годом программ-вымогателей. Лучшей мерой противодействия программам-вымогателям является хорошая защита. Готова ли ваша организация к отражению атак? Не тратьте время на обдумывание стратегии защиты. Приведенная ниже таблица поможет вам защититься от этих атак.

☐ 1. Организуйте резервное копирование всех своих данных

Ваше самое эффективное оружие против программ-вымогателей — это регулярное резервное копирование по расписанию. В случае атаки выключите оконечное устройство, установите нужный образ и восстановите последнюю резервную копию. Так вы предотвратите распространение программ-вымогателей на другие системы вашей сети.

Для устранения программы-вымогателя вам потребуется полностью удалить все данные с компьютера, поэтому для быстрого восстановления после атаки нужна резервная копия системы или снимок ее состояния. Чем чаще выполняется резервное копирование, тем меньше данных будет потеряно. Частота резервного копирования определяется стратегическим значением данных и объемом данных, который организация может потерять без существенных последствий. Поскольку все подключаемые устройства должны быть зашифрованы, для резервного копирования нужно использовать внешнее хранилище, немедленно отключая его по завершении этой процедуры.

☐ 2. Обновляйтесь, обновляйтесь и еще раз обновляйтесь

Проникнуть в сеть программам-вымогателям часто помогают сами сотрудники, использующие устаревшее программное обеспечение с известными уязвимостями. Такие факторы, как несогласованное установление пакетов исправлений и устаревшее ПО, ставят организацию под угрозу. Возьмите в привычку регулярно обновлять ваше ПО. ПО сторонних производителей, например Java и Flash, часто используется злоумышленниками, поэтому обновление такого ПО, несомненно, поможет предотвратить множество атак.

☐ 3. Информируйте своих пользователей об источниках атак

Обычно самое слабое звено в системе безопасности — это люди. Попавшись на уловки злоумышленников — фишинговое электронное письмо или другую схему социальной инженерии, — сотрудник может поставить вашу организацию под угрозу. Информируйте своих пользователей о сценариях атак с помощью социальной инженерии. Злоумышленники используют такую тактику, поскольку использовать доверчивость людей гораздо проще, чем искать уязвимости вашего программного обеспечения.

Вся система безопасности построена на знании о том, кому и в чем можно доверять. Научите пользователей задавать себе следующие вопросы при чтении почты:

1. Знаком ли мне отправитель?
2. Действительно необходимо открыть этот файл или перейти по этой ссылке?
3. Действительно мной был сделан заказ в этой компании?

☐ 4. Следите за безопасностью вашей сети

Защитите свою сеть, применяя многоуровневый подход. Используйте такие технологии, как межсетевой экран нового поколения (NGFW) и система предотвращения вторжений (IPS). Многоуровневая защита позволяет обеспечивать безопасность различных участков сети несколькими способами. Изолируя отдельные бреши, можно эффективно защищать вашу сеть и ваши данные.

☐ 5. Разделите сеть на сегменты доступа

Сегментация сети ограничивает объем ресурсов, к которым злоумышленник может получить доступ. При таком подходе сетевые активы, ресурсы и приложения логически объединяются в слабо взаимосвязанные области. Динамически управляя доступом к ним, можно предотвратить ситуацию, когда в результате одной атаки страдает вся сеть.

Большинство корпоративных сетей организованы «горизонтально», с небольшим числом сегментов или вообще без разделения на сегменты бизнес-подразделений, пользователей и данных, без разделения данных разных бизнес-подразделений и так далее. Благодаря сегментации можно блокировать или замедлить распространение вредоносного ПО и успешно сдерживать угрозы.

☐ 6. Постоянно контролируйте сетевую активность

Если вы не замечаете угрозу, вы не сможете защититься от нее. Сквозной мониторинг сети может представляться очень сложной задачей, но он абсолютно необходим. Возможность увидеть все, что происходит в сети и ЦОД, поможет вам выявить угрозы, прошедшие через периметр и проникшие во внутреннюю сеть.

Чтобы защитить периметр, разверните и укрепите так называемую демилитаризованную зону. ДМЗ — это физическая или логическая подсеть, которая размещает и предоставляет сервисы для вашей организации во внешнюю (обычно более крупную и менее надежную) сеть, например Интернет. Она добавляет еще один уровень безопасности для локальной сети. Она позволяет узлам внешней сети напрямую подключаться только к серверам в ДМЗ, не пропуская их ни в какие другие части вашей внутренней сети.

☐ 7. Предотвращайте проникновение на начальном уровне

Иногда ваши пользователи могут непреднамеренно перейти на опасные веб-сайты или открыть электронные сообщения с вредоносной рекламой и таким образом пропустить в вашу сеть вредоносное ПО. Начальное заражение программами-вымогателями обычно происходит через вложения электронной почты или загрузки вредоносных файлов. Постоянно блокируя вредоносные веб-сайты и массовые рассылки злоумышленников, вы сможете обезопасить свою сеть.

Рекомендуется подумать об инвестициях в утвержденную вашей организацией программу для обмена файлами как между пользователями в организации, так и с партнерами компании. Использование решения для обмена файлами и запрет пользователям обмениваться файлами по электронной почте могут практически устранить опасность фишинговых атак с использованием почтовых вложений.

☐ 8. Разверните защиту на оконечных устройствах

Развертывание антивирусного решения на оконечных устройствах — это недостаточное условие для защиты от программ-вымогателей. Концепция рабочих мест «Принеси на работу свое устройство» (BYOD) становится все более популярной, и вам необходимо найти решение для контроля над ноутбуками, мобильными устройствами и планшетами, через которые пользователи подключаются к вашей сети. Такое решение должно предоставлять две главные возможности: отслеживать все устройства в сети и запрещать доступ к опасным сайтам и загрузку подозрительных файлов.

Рекомендуется применять концепцию «минимально необходимых прав». Это значит, что учетная запись должна иметь действительно лишь те права, которые позволят пользователю выполнять служебные обязанности и ничего больше. Хотя этой концепцией зачастую пренебрегают, она может существенно обезопасить работу пользователей на оконечных устройствах и их доступ к сетевым ресурсам. Главное в ней то, что вредоносное ПО чаще всего запускается с правами, соответствующими правам текущего пользователя. Если он имеет права администратора, такие же права получает злоумышленник. Всегда используйте двухфакторную аутентификацию. Хакер может украсть пароли, но практически невозможно при этом похитить смартфон сотрудника или токен доступа.

☐ 9. Анализируйте угрозы в режиме реального времени

Чтобы заранее предупреждать угрозы, важно знать ваших врагов. Аналитика угроз заблаговременно предупреждает специалистов по безопасности о том, что их регион, отрасль и даже конкретные компании могут стать объектами атаки злоумышленников. Это позволяет им предпринять необходимые действия. Как же можно получать аналитику угроз в режиме реального времени? Для этого нужно все время быть начеку и учиться у организаций, специализирующихся на анализе угроз, таких как Talos.

В группе Talos более 250 постоянных сотрудников занимаются разработкой методов защиты от известных и новых угроз кибербезопасности. Эта группа публикует информацию по вопросам безопасности в блогах, рассылках, социальных сетях, на форумах сообщества, а также снимает обучающие видеоролики, которые помогут каждому пользователю повысить уровень своей защищенности в Интернете. Вы можете использовать результаты их работы и следить за выпускаемыми ими материалами, обновляя защиту своей организации при появлении новых угроз.

☐ 10. Скажите «Нет» программам-вымогателям

Хотя многие компании платят выкуп, чтобы вернуть контроль над своими системами, это должно быть самым последним вариантом действий. Свяжитесь с руководством и не финансируйте этих преступников, платя им выкуп.

Дополнительная информация

Дополнительные сведения о мониторинге сети и защите от программ-вымогателей в Cisco см. на веб-странице http://www.cisco.com/go/ransomware.