Центр научно-технической информации и библиотек – филиал ОАО «РЖД»

Дифференцированное Обеспечение Руководства

25/2020

Борьба с киберугрозами

Тенденция к полной цифровизации железнодорожной отрасли несет в себе широкие возможности и преимущества. Но чем больше эти технологии внедряются в повседневную эксплуатацию, тем более они подвержены кибератакам. Такие угрозы становятся все более серьезными, поскольку цифровые технологии получают большее распространение в критически важных для безопасности системах железных дорог.

Потенциальная возможность кибератак на железной дороге может привести к ряду последствий, включая:

- угроза безопасности работников, пассажиров или населения, что может привести к причинению вреда;
- нарушение перевозочного процесса;
- финансовые потери, в том числе выходящие за пределы железнодорожной отрасли;
- потеря коммерческой или конфиденциальной информации;
- преступное причинение ущерба;
- ущерб репутации;
- несоблюдение закона.

Несмотря на то, что крупные компании обладают большими ресурсами для подготовки к противостоянию кибератакам, они всё равно подвержены риску. В мае 2017 года, германский оператор Deutsche Bahn (DB) пострадал от вируса WannaCry, который атаковал операционные системы Windows, зашифровывал данные и требовал выкуп за биткойны. Было заражено 450 компьютеров, пострадали информационные табло, машины по продаже билетов и системы виделнаблюдения.

По словам менеджера по IT-безопасности компании DB Netz г-на Кристиана Шлехубера (Christian Schlehuber), инцидент оказал негативное воздействие на DB с точки зрения связи с общественностью из-за очень заметного характера атаки, но не привел к проникновению в защищенные системы компании благодаря быстрым действиям персонала, что снизило ущерб перевозочному процессу.

Трехуровневая модель организации сети

DB имеет трехуровневую модель организации сети. Вирус WannaCry проник только на третий уровень, так и не достигнув первого уровня, который включает критически важные для безопасности системы, такие как сигнализация. В результате привлеченного внимания средствами массовой информации к кибератаке, компания стала уделять дополнительное внимание к вопросам кибербезопасности.

Компания DB имеет несколько уровней защиты, между такими вещами, как файлы данных и сетевыми экранами (файрвол) и так далее. По словам Шлехубера, DB считает данную схему защиты систем сигнализации достаточно безопасной, так как имеются изолированные системы. Но если посмотреть на систему с точки зрения злоумышленника, самым слабым звеном является офисная IT-сеть, где доступ к ней имеют большое количество сотрудников. Исследуя уязвимости в одной из систем DB, злоумышленники смогли получить доступ к ручной версии установки программы, которая к тому же имела права администратора, что позволило получить доступ к частям сети, которые должны были быть заблокированы.

Вместо атаки на основные системы, хакеры ищут небольшие уязвимости и бреши в защите системы, которые потом можно использовать для получения более глубокого доступа в сеть. Изучается существующая сетевая инфраструктура, веб-сайты и учетные записи, потом строится система с административными привилегиями, с которой после этого они начинают противозаконную деятельность.

Но часто уязвимость защищенных систем вызвана не отсутствием процессов и мер безопасности, а не четкому следованию установленных правил. При проверке оператора за пределами Германии, пароли сервера были выписаны и находились в легкой доступности, и не смотря на то, что шкафы были заперты, ключи были оставлены внутри замков. Данная халатность не была единичным случаем. Недостаточная осведомленность о правилах безопасности является одной из самых больших проблем в железнодорожной отрасли.

Другая ошибка, которая часто упускается из виду в железнодорожной отрасли, состоит в том, что инсталляционные программы остаются установленными после завершения развертывания решений, делая их

открытыми для атак.

При развертывании нового решения, такого как система диагностики или блокировки, устанавливается удаленный доступ к нему, так как не все работники хотят каждый день выезжать на объект для его обслуживания. После установки инсталляционной программы при развертывании решения следует оценить, насколько она необходима и можно ли её удалить, потому что существует большой риск, что она будет кем-то найдена.

Несмотря на необходимость защиты от сложных атак, крайне важно обеспечить неукоснительное следование протоколу безопасности по базовым задачам. Такие риски могут включать хранение паролей в легко доступных общих файловых ресурсах, отсутствие изменения паролей по умолчанию, отсутствие обновлений и исправлений программного обеспечения, а также использование одних и тех же паролей в нескольких системах и приложениях.

Сетевая инфраструктура

Хотя процессы и программное обеспечение могут в значительной степени определять безопасность сети, базовая схема настройки сети также может сыграть важную роль в обеспечении ее безопасности.

Одна из проблем, с которой сталкиваются железнодорожные операторы, является поиск путей обмена данными между критически важными для безопасности и надежности системами и как можно большим числом сотрудников, не открывая эти системы для атаки.

Напольное оборудование в зоне отчуждения может не показаться вероятной целью для хакеров, но атаки в прошлом показали, что творческие хакеры разработали инновационные способы доступа к сетям.

Британская фирма Darktrace, специализирующаяся на кибербезопасности, выявила два отдельных случая, когда казино в США были атакованы через подключенные к интернету аквариумы. В первом случае, о котором сообщалось в 2017 году, резервуар был оснащен самой современной системой, позволяющей удаленно контролировать температуру и чистоту резервуара. Однако эта система также позволила хакерам получить доступ к остальной сети и отправить 10 ГБ информации из сети казино в Финляндию. В 2018 году, подключенный к интернету термостат в аквариуме использовался для получения доступа к сети другого казино, что позволило хакерам получить список крупных клиентов.

Существует несколько различных архитектур, которые можно встроить в сеть для получения данных с датчиков при сохранении защищенности самой сети.

Во-первых, это использование демилитаризованной зоны (DMZ), которая использует изолированную сеть, которая действует как буфер между

фронтальным веб-сайтом или сетью и внутренней защищенной сетью, передавая данные с защищенного сервера на незащищенный сервер в режиме реального времени, где к нему можно безопасно получить доступ, не ставя под угрозу безопасную сеть. Хотя это может быть полезно для систем с низким и средним уровнем безопасности, оно не всегда обеспечивает уровень, требуемый для некоторых систем с высоким уровнем безопасности.

Второй процесс аналогичен и также использует DMZ, но добавляет отдельные протоколы безопасности для передачи данных через зону. Данные собираются в защищенной сети и сохраняются или передаются в DMZ, где затем передаются на незащищенную сторону с шифрованием в обоих потоках.

Третья и наиболее безопасная система использует однонаправленные шлюзы безопасности, которые создают непроходимый физический барьер, предотвращающий все внешние атаки, проникающие через шлюз.

Промышленные системы и серверы «экспортируются» в корпоративную сеть по оптоволоконному кабелю в режиме реального времени с использованием воссоздания серверов и эмуляции устройств, которые сохраняет данные и функциональные возможности исходной сети. Поскольку устройство оснащено только оптоволоконным передатчиком на одном конце и приемником на другом конце, устройство физически не способно отправлять информацию и данные обратно в защищенную сеть, предотвращая нежелательный доступ.

Для повышения кибербезопасности европейских операторов, DB Netz и Infrabel совместно с Европейским железнодорожным агентством (ERA) и Агентством кибербезопасности Европейского союза (ENISA) работали над созданием Европейского центра обмена и анализа информации о железных дорогах (ER-ISAC). Целью работы с операторами и другими организациями, такими как DG Move, является создание безопасной и конфиденциальной платформы для обмена информацией по всему железнодорожному сектору об инцидентах, угрозах и концепциях по повышению безопасности.

Источники: railjournal.com, 28.10.2019;
материалы сайта maritimecyberalliance.com