ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В ТРАНСПОРТНОЙ СФЕРЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

С развитием компьютеров изменился современный мир. Теперь все управляется с помощью компьютера или с его хотя бы минимальным участием. Компьютеры отвечают за работу биржи, за работу электростанций, за движение поездов и самолетов, за работу двигателя автомашины. Компьютеры везде. Они сильно помогли нам избавиться от ошибок людей, ведь компьютер никогда не ошибается. Компьютер делает все по заранее заложенной программе. Если программа верная – то верно ведет себя и компьютер. Если хорошо отработать программу, то компьютер куда надежнее человека справится с управлением, например, атомной станцией, где одновременно надо следить за множеством параметров.

Но почему мир с глобальной компьютеризацией не стал безопаснее? Все просто: чем больше всего контролируют компьютеры, тем могущественнее становятся люди, которые могут подчинить эти компьютеры себе – хакеры.

Проблема сегодняшних руководителей заключается в том, что они мало понимают, что такое компьютерные атаки. Долгое время термин «компьютерная атака» знали только узкие специалисты, защита от вирусов была их задачей. И вдруг за последние десятилетия компьютерная грамотность стала необходима руководителям стран. Почему? Все просто – из программ студентов-любителей, вирусы стали в буквальном смысле настоящим оружием в геополитическом противостоянии стран. Теперь понимание кибер атак – обязательное знание любого руководителя по всему миру. Детали могут остаться на откуп специалистам, но только глобальное понимание этой индустрии и только оно может дать стране безопасность.

Транспортная система – одна из самых уязвимых с точки зрения киберпреступников отраслей хозяйства. Достаточно ли она защищена? Далеко нет. Существует ли угроза атак на такие системы? Безусловно!

И примеры этому есть. В 2016 году хакеры атаковали 22 аэропорта Вьетнама. Громкоговорители в аэропорту вдруг сами по себе стали выкрикивать ругательства в адрес вьетнамцев. Системы информирования вывели оскорбительные ролики про вьетнамский народ. Были похищены гигабайты личных данных пассажиров. Началась паника.

Но главный итог атак все же был не в этом. Транспортная сеть Вьетнама вдруг резко утратила привлекательность для инвестиций. Инвесторы более не верили, что аналогичные атаки не повторятся, что никто в будущем не похитит личные данные пассажиров и не опубликует их.

Представьте атаку на крупный аэропорт в нашей стране. Под ударом окажется не только страна, чей аэропорт взломали. Под атакой будет престиж транспортного узла всего региона.

Железнодорожный транспорт не исключение. Современные поезда, движущиеся на огромных скоростях также напичканы компьютерами. Очевидно, что на огромных скоростях в 300-400 км/час человек не может контролировать сотни параметров, а компьютеру это подсилу. Очевидно, вмешайся вирус в такую систему – получатся ужасные последствия.

Но тут я бы отметил совсем другую угрозу. Мало кто знает, что современные скоростные поезда, а вернее двигатели в этих поездах оснащены GSM-модемами. Зачем? Официально для передачи диагностической информации с них в штаб-квартиры производителей поездов, которые находятся не в нашей стране. Но данные с этих модемов передаются в зашифрованном виде.

Очевидно, это сделано в целях безопасности. Но в безопасности ли остаемся мы с вами? Что может еще быть в этих данных? Является ли канал однонаправленным или двунаправленным? Могут ли передаваться управляющие команды извне? Это большой вопрос.

Надо помнить, что кибератака анонимна, она дешевле чем удар военной техникой, мирное население не страдает – отключается только стратегическая инфраструктура. Одни преимущества. На самом деле кибератака – это, пожалуй, самое дешевое и эффективное средства ведение современной войны. Враг может только догадываться (а чаще всего и догадывается), кто нанес удар. Но есть ли доказательства? Почти никогда нет.

Не даром США в своей доктрине приравнивает кибердар к реальному военному удару. Почему так? Чтобы иметь право нанести ответный удар. Это означает только одно – кибератаки – это эффективное и опасное средство.

Многие руководители думают, что защититься от новых методов кибератак и киберпреступлений можно используя самые дорогие методы защиты. Это не так. Злоумышленники взяли на вооружение новые принципы атак, защитники должны поступить также – взять на вооружение принципиально новые методы защиты. Но какие? Ответ на этот вопрос не так прост. Чтобы быть готовым ко все время изменяющимся методам врага нужно быть готовым, быть гибким, нужно изменить свою парадигму.

Координация в области борьбы с кибератаками – крайне важная задача. Делая обзор ситуации в это области могу сказать точно: у нас точно не хватает координации в транспортной области.

В своем докладе, я бы хотел обратиться к задаче создания центра координации в области кибербезопасности. Задачей центра должна стать консолидация усилий для защиты транспортных объектов инфраструктуры от кибер атак.

Центр может быть реализован в форме некоммерческой ассоциации, имеющей в управлении основные функциональные единицы.

Каковы должны задачи центра? Они видятся следующими:

Во-первых, необходимо снизить консолидированные издержки на защиту от кибер атак держателей критической инфраструктуры в области транспорта за счет централизации затрат и отсутствия дублирования бюджетов. На сегодня очевидно мы не видим консолидированной связи между игроками в этой области.

На что нужны средства?
Это вторая задача центра - создать единый центр компетенций в области кибербезопасности на транспорте, включая специализированную лабораторию для исследований инцидентов. Это позволит повысить общий уровень защищенности, позволит делиться информацией.

Центр также должен способствовать развитию так называемых сертификационных лабораторий. Что это? Это лаборатория, в которой специалисты знакомятся и тестируют любое обеспечение, которое встанет на наши с вами критически участки в стране.

Любая поставка автоматизированных систем для критической инфраструктуры должна проходить только после того, как оборудование пройдет проверку в специализированных сертифицирующих лабораториях. Ключевым критерием для прохождения на особо важные объекты - будет получение открытого кода для проверок.

Такие лаборатории существенно усложнят жизнь киберпреступникам. Теперь все будет тщательно проверяться. Также сразу же появится желание крупных компаний зарабатывать на поставках в нашу страну. Мы не будем зависеть от чужой воли.

Еще одна важная задача - это координация подготовки собственных кадров по тематическим направлениям, в том числе при взаимодействии с ведушими ВУЗами страны. На сегодня мы все чувствуем острую нехватку специалистов. Но мы совсем не проводим координацию по подготовке кадров в этой области.

Центр должен выполнять работу с парламентариями страны по модернизации нормативной базы, направленной на внесение законодательных инициатив или поправок к существующим законам и подзаконным актам, регулирующими область транспортной кибербезопасности. Центр должен проводить международную координдацию в области кибербезопасности со странами ОДКБ и ЕвраЗэс, и безусловно более плотное взаимодействие со всеми странами СНГ. Проведение профильных мероприятий в рамках коммитета по безопасности РСПП/МКПП должно стать постоянным.

Ключевую же задачу Центра я оставил на последний пункт. Главной задачей центра должна стать проактивная защита транспортной инфраструктуры.

Хорошая организация всегда справится с последствиями кибератаки. Отличная организация не даст этой атаке случиться. В этом и должен заключаться наш подход к кибербезопасности. Пока большинство стран занимается вопросом защиты своих критических активов от кибератак, мы должны быть на шаг впереди всех. Мы должны понимать, что атака началась или готовится. Мы должны предугадать кто и куда нанесет удар. Как это сделать? Для этого нужно изменить наши подходы к кибербезопасности и сделать акцент на предупреждение атак. Сделать это достаточно просто. В этом и должно заключаться наше преимущество над противником.

Приведу пример. Есть замечательное понятие – honeypot. Можно представить себе этот термин также как

бочонок меда (как и переводится это выражение). Это и есть приманка. Технически это выглядит так: мы должны подготовить и расставить приманки для хакеров. Например, в Интернете должны появиться десятки имитаций аэропортов, транспортных узлов.

Соперник будет собирать информацию о наших объектах перед атакой. Атака всегда готовится заранее. Для нее нужно много информации. Противник обязательно обнаружит себя. Honeypots – это только одна из систем накапливания информации о том, что атака может случиться и кто и как и на что ее готовит. Тем не менее согласитесь, это гораздо дешевле чем объяснять прессе киберинцидент, убеждать инвесторов не уходить с нашего рынка или, скажем, восстанавливать взорвавшуюся автоматизированную котельную после того, как вирус взял верх над ее системой компьютерного управления. Мы должны быть на шаг впереди нашего врага.

Кроме техники использования Honeypots есть и другие важные методики. Если на каждом предприятии будет стоять система обнаружения аномалий: изменился траффик, кто-то стал часто интересоваться извне компьютерной архитектурой сети или что-то еще странное происходит с запросами на сервера компании – вся эта информация должна скапливаться на сервер Центра.

Все критические предприятия страны должны установить себе модули, которые будут отправлять информацию на единый центр SOC. Единая сеть, окутавшая всю страну будет эффективной и главное проактивной мерой обнаружения атак на нашу критическую инфраструктуру.

И последний пункт, но как мне видится достаточно важный. Мы должны быть готовы к активным медиа ответам на кибер атаки. Пресса должна знать, а пресс служба Центра уметь реагировать на атаку так, чтобы население видело молниеносную реакцию наших служб противодействия атакам. Для этого мы должны уделить

внимание и делать репортажи о наших службах реагирования на компьютерные инциденты заранее. Чтобы в час X пресса понимала, к кому обращаться и как освещать событие. Иначе давать интервью будут «дружелюбные» специалисты из других стран.