Секция «Круглый стол для школьников «Постигая аудит»»

Управление безопасностью инфраструктур

Научный руководитель – Тарасов Иван Владимирович

Великодворская Дарья Константиновна
E-mail: tiwell24@rambler.ru

ГБОУ «Школа №556», Москва, Днепропетровская ул., 33А

Аннотация. В статье рассматриваются уязвимость в управление безопасностью информационной инфраструктуры.
Ключевые слова: безопасность, инфраструктура, образование.

Infrastructure security Management

Annotation. The article discusses vulnerability in information infrastructure security managemen
Keywords: security, infrastructure, education.

Введение

Информационные и коммуникационные технологии становятся частью современных управляющих систем во всех отраслях экономики, сферах безопасности государства, жизни людей. ФЗ187 «О безопасности критической информационной инфраструктуры РФ» ставит задачу непрерывного обеспечения безопасности критической информационной инфраструктуры и устанавливает приоритет предотвращения компьютерных атак.

Гипотеза. В современном мире безопасность информационной инфраструктуры - обязательное условие успешного существования любой компании. Количество атак увеличивается с каждым годом.

Цель. Защита конфиденциальной информации и информационной инфраструктуры образовательного предприятия от несанкционированного доступа через устройства сотрудников.

Задачи.

1) Разработать рекомендации для защиты персональной информации сотрудников образовательных организаций (ОУ).
2) Обучение сотрудников образовательной организации по использованию программ по защите инфраструктуры.

Актуальность. Если часть инфраструктуры будет скомпрометирована или выйдет из строя, под угрозой окажутся персональные данные сотрудников ОУ. Наше приложение нацелено на то, чтобы защитить инфраструктуру от атак злоумышленников, снизить вероятность технического сбоя, а также минимизировать финансовые последствия для бизнеса в случае атаки или сбоя.

Безопасность инфраструктуры

Безопасность инфраструктуры — это безопасность, обеспечиваемая для защиты инфраструктуры, особенно критически важной инфраструктуры, такой как аэропорты, автомагистрали, железнодорожный транспорт, больницы, мосты, транспортные узлы, сетевые коммуникации, средства массовой информации, электросети, плотины, электростанции, морские порты, нефтеперерабатывающие заводы, образовательные учреждения. Безопасность инфраструктуры направлена на ограничение уязвимости этих структур и систем к саботажу, терроризму и заражению. Критически важные инфраструктуры, как мы знаем, используют информационные технологии, т.к. эта возможность становится доступной.

Вторжения и сбои в одной инфраструктуре могут спровоцировать неожиданные сбои в других, что делает взаимозависимость передачи ключевой проблемой.

Есть несколько примеров, когда инцидент на одном критически важном объекте инфраструктуры влияет на другие.

Например, в 2003 году в северо-восточных районах Америки произошло отключение электроэнергии из-за ветки дерева. В 2013 году ущерб, причиненный снайперской атакой на электрическую подстанцию в Калифорнии, поставил под угрозу распределение электроэнергии по всей Силиконовой долине. Взрыв в Нэшвилле в 2020 году вызвал перебои в работе телекоммуникаций в нескольких штатах.

Что может угрожать безопасности инфраструктуры

Наиболее распространенные угрозы, которые присутствуют сегодня - это фишинг. Фишинг - самая распространённая угроза, которой подвержены как частные лица, так и организации. Главная цель фишинга - получить доступ к учётной записи сотрудника, которую злоумышленник может использовать для доступа к корпоративным ресурсам.

Рассмотрим программы-вымогатели (Рис.1). Атаки таким программа обусловлены тем, что вредоносное программное обеспечение получает доступ к данным компании и шифрует их с целью получения выкупа. Уплата выкупа не гарантирует восстановление работы системы или отсутствие утечки данных. Рис. 1 Программы-вымогатели.

Ботнет - в основном используются для организации DDoS-атак, но в последние годы автономное боты стали использовать и для скрытого майнинга криптовалют. Для этого часто используется устройства интернет вещей IoT (Рис. 2). Рис. 2. Ботнет - в основном используются для организации DDoS-атак.

Физическое вмешательство. Инфраструктура компании может быть почти неуязвимой для кибератак, но нельзя забывать и о физической защите (Рис. 3). Рис. 3. Физическое вмешательство

Речь идёт о краже или проникновении на объект и физическом вмешательстве в работу оборудования.

Как защитить инфраструктуру?

Чтобы защитить инфраструктуру, нужно знать, каким угрозам может быть подвержена система. Можно читать отчёты по анализам актуальных угроз и использовать сервисы информирования об угрозах. Кроме этого, при проектировании и поддержке инфраструктуры стоит следовать общепринятым правилам безопасности:

- удаляйте не используемое программное обеспечение и службы. Активные, но простаивающие элементы создают дополнительную угрозу безопасности инфраструктуре;
- установите правильные настройки брандмауэра. Неправильная конфигурация брандмауэра также опасна, как и его отсутствие;

- настройте регулярное резервное копирование всех систем. Это лучшая защита от программ-вымогателей;
- проводите регулярное тестирование на проникновение и сканирование безопасности. Это позволит найти уязвимые места в элементах системы;
- при разработке кода проверяйте его на соответствие требованиям безопасности. Для этого можно использовать DevSecOps, отвечает за включение требований по безопасности на всех этапах жизни разработки программного обеспечения.

Вывод. Информационная безопасность в текущем информационном поле давно перешла в разряд необходимостей. Стремительный рост технологий при этом провоцирует рост и смещение фокуса рисков информационной безопасности. В связи с этим становится сложно коррелировать все актуальные тенденции в защите информации в рамках одной инфраструктуры даже для опытного специалиста по ИБ. Тем не менее, если придерживаться основных принципов, возможно повысить уровень защищенности компании до приемлемого с умеренными вложениями.

Рекомендации. Используйте шифрование. Не храните конфиденциальные данные в незашифрованном виде. Если злоумышленники получат доступ к данным, воспользоваться ими без ключей не получится. Следите за правами доступа пользователей. Своевременно удаляйте права доступа у сотрудников, которые уволились. Установите парольные политики и строго следуйте им.

Источники и литература

1) Зегжда, Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д.П. Зегжда, Е.Б. Александрова, М.О. Калинин и др. // М.: Горячая линия - Телеком, 2019. - 640 с.: ил. ISBN 978-5-9912-0826-0.
2) Зегжда Д.П. Подход к созданию критерия устойчивого функционирования киберфизических систем / Д. П. Зегжда, Е. Ю. Павленко, Д. С. Лаврова, А. А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. - 2019. - № 2. - С. 156-163.
3) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4) Ванцева, И. О. Влияние федерального закона "о безопасности критической информационной инфраструктуры Российской Федерации" на владельцев критических информационных инфраструктур / И. О. Ванцева, Т. Ю. Зырянова, О. О. Медведева // Вестник УрФО. Безопасность в информационной сфере. - 2018. - № 1(27). - С. 71-76.
5) Калашников, А. О. Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа / А. О. Калашников, Е. А. Сакрутина // Информация и безопасность. - 2017. - Т. 20. - № 4. - С. 478-491.
6) Крундышев, В. М. Выявление киберугроз в сетях промышленного Интернета вещей на основе нейросетевых методов с использованием памяти / В. М. Крундышев // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 1. - С. 89-95.
7) https://translated.turbopages.org/proxy_u/en-ru.ru.ee41635d-633bd73c-6b2a6a7e-74722d776562/https/en.m.wikipedia.org/wiki/Infrastructure_security [Дата обращения: 15.10.2022 в 17:41].

8) https://reg-ru.turbopages.org/reg.ru/s/blog/bezopasnost-it-infrastruktury/ [Дата обращения: 16.10.2022 в 09:07].

Иллюстрации

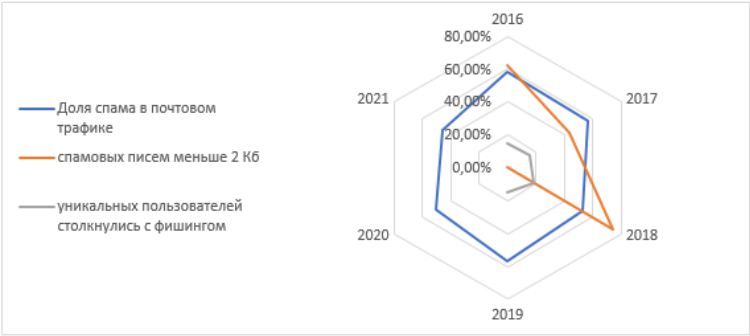

Рис. 1 Программы-вымогатели.

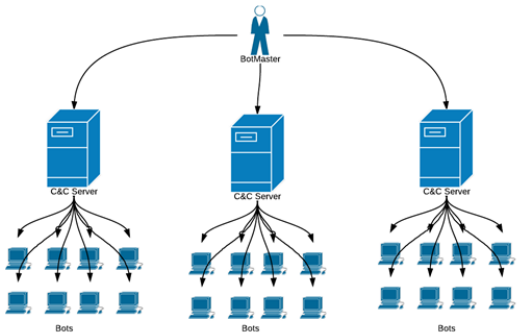

Рис. 2. Ботнет – в основном используются для организации DDoS-атак.

Рис. 3. Физическое вмешательство