УДК 004.89

АНАЛИЗ МЕТОДОВ ПО ОРГАНИЗАЦИИ БЕЗОПАСНОСТИ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Чумаков В.Е.

магистрант,

ИСОиП (филиал) ДГТУ,

г. Шахты, Россия

Аннотация

В статье рассмотрены способы организации минимального уровня обеспечения информационной безопасности без высоких экономических затрат. Описываются наиболее типичные виды угроз на сетевую инфраструктуру компании. Рассматриваются методы по устранения потенциальных уязвимостей, связанных с нарушением требований по обеспечению информационной безопасности в корпоративной сети.

Ключевые слова: Уязвимости, потенциальные угрозы, методы защиты, CIS Controls, комплекс инструментов для защиты.

ANALYSIS OF METHODS FOR ORGANIZING SECURITY NETWORK INFRASTRUCTURE

Chumakov V.E.

master student,

ISOiP (branch) DSTU,

Shakhty, Russia

Annotation

The article describes the ways of organizing a minimum level of information security without high economic costs. The most typical types of threats to the network infrastructure of the company are described. Methods of elimination of the potential

vulnerabilities connected with violation of requirements for ensuring information security in a corporate network are considered.
Keywords: Vulnerabilities, potential threats, methods of protection, CIS Controls, a set of tools for protection.

В настоящее время в повседневной работе сотрудник предприятия, отвечающий за информационную безопасность сталкивается с такими инцидентами, как попытки кражи интеллектуальной собственности, атаками типа отказ в обслуживании и распределенный отказ в обслуживании, нарушение конфиденциальности. Для защиты от рассмотренных инцидентов крупные компании выделяют очень большие бюджеты для обеспечения высокого уровня обеспечения информационной безопасности, но такие бюджеты не могут позволить небольшие компании или гос. учреждения, поэтому необходимо рассмотреть методы защиты для таких небольших организаций.

В первую очередь рассмотрим наиболее популярные типы угроз на небольшие компании:

Ransomware – это тип атаки, при котором разработанное и внедренное на компьютер сотрудника вредоносное программное обеспечение блокирует доступ к данным компьютера, как правило применяя специальный баннер, в результате чего баннер отображает информацию о том, что злоумышленник может открыть доступ к данным, но за внесение денежных средств на определенный счет одного из сервиса электронных платежей [1].

Потеря данных – этот тип угрозы является наиболее непредсказуемым и почти неуправляемым, так как при таком типе угрозы, важные данные могут быть утеряны по неосторожности сотрудника, из –за природных явлений или из-за несчастных случаев.

Deface – этот тип угрозы наиболее актуален для предприятия, которое имеет в составе сетевой инфраструктуры собственный веб – сервер [2]. Этот тип атаки заключается в подмене страниц веб – сайта для кражи файлов cookie, т.е. небольших фрагментов данных, передающихся в составе HTTP/HTTPS – запроса и хранящих конфиденциальные данные пользователя на стороне клиента, или же производить redirect (перенаправлять) на веб – сервер злоумышленника.

Phishing – это тип угрозы, при которой злоумышленник производит массовые рассылки пользователям предприятия от различных известных компаний и корпораций, с целью кражи таких конфиденциальных данных пользователя, как логин/пароль от учетной записи, номер/пароль/cvv/cvc кредитной карты [3].

DOS/DDOS – это наиболее трудно реализуемый метод атаки на организацию, однако этот тип атак является наиболее распространенной и заключается в том, чтобы воспользоваться одной или несколькими уязвимостями сетевой инфраструктуры и произвести отказ в обслуживании сервера или коммутирующих устройств [4].

Для защиты от перечисленных типов угроз и методов атак применяют инструменты известной компании «CIS Controls», которая разработала комплексный и хорошо зарекомендовавший себя набор методов среди специалистов, обеспечивающих информационную безопасность сетевой инфраструктуры [5]. Рассматриваемая компания предлагает поэтапное построение информационной безопасности. Рассмотрим эти этапы.

Первый этап. На этом этапе необходимо исследовать сетевую инфраструктуру и определить минимальные требования для обеспечения информационной безопасности. Для этого необходимо ответить на вопросы, которые представлены на рисунке 1.

Рис.1 – Определение минимального уровня обеспечения безопасности

Для решения поставленных вопросов необходимо соблюдать определенный перечень федерального законодательства и выполнять необходимые действия, а именно:

- № 152 –ФЗ (Закон о персональных данных);
- № 161 – ФЗ (Закон о национальной платежной системе);
- № 149 –ФЗ (Закон об информации, информационных технологиях и о защите информации);
- № 98 – ФЗ (Закон о коммерческой тайне).

Для беспроводной сети обеспечивать надежное шифрование, использовать сетевые сканеры для инвентаризации устройств, составляющих сетевую инфраструктуру, производить встроенными или сторонними средствами логирование всех происходящих событий в корпоративной сети.

Второй этап. На этом этапе необходимо обеспечить наличие минимальных требований по информационной безопасности и провести ликбез сотрудников по потенциальным инцидентам и способам реагирования на такие инциденты. Для обеспечения безопасности на этом этапе необходимо выполнить три обязательных действия, которые представлены на рисунке 2.

Рис.2 – Минимальные требования по ИБ

Дополнительными средствами является:

– Ограничение использование съемных носителей в локальной сети предприятия;

– Использование программных инструментов для выявления и закрытия уязвимостей, которые связаны с программным кодом;

– Обеспечение в многофакторной аутентификации;

– Изменение по умолчанию установленных логинов и паролей в сетевом оборудовании.

Третий этап. На этом этапе необходимо провести правильную организацию готовности к различным инцидентам, возникающим в отрасли информационной безопасности. На этом этапе необходимо выполнять как минимум три важных шага, представленных на рисунке 3.

Рис.3 – Резервное копирование

Все перечисленные методы позволяют организовать минимальный уровень обеспечения информационной безопасности сетевой инфраструктуры предприятия, однако этих методов достаточно для профилактики потенциально опасных и наиболее типичных видов угроз на предприятия с начально развитой сетевой инфраструктурой.

Библиографический список:

1 Головин А.И. Исследование программ вымогателей // Cisco Ransome Defense. [Электронный ресурс]. – Режим доступа – URL: https://www.cisco.com/c/dam/global/ru_ru/about/brochures/assets/pdfs/cisco_ransomware_defense_aag_ru.pdf (Дата обращения 19.05. 2019).

2 Обирин А.В. Замена, искажение страниц сайта // Последствия взлома сайтов. [Электронный ресурс]. – Режим доступа – URL: https://insafety.org/deface.php (Дата обращения 21.05.2019).

3 Бырдин И.В. Принципы фишинга // Обучение защиты от фишинга. [Электронный ресурс]. – Режим доступа – URL: https://www.cisco.com/c/ru_ru/products/security/email-security/what-is-phishing.html (Дата обращения 21.05.2019).

4 Ильин В.В Dos/Ddos атаки // Распределенные сетевые атаки. [Электронный ресурс]. – Режим доступа – URL: https://www.kaspersky.ru/resource-center/threats/ddos-attacks (Дата обращения 23.05.2019).

5 Tony Sager. Follow our prioritized set of actions to protect your organization and data from known cyber attack vectors // CIS Controls. [Электронный ресурс]. – Режим доступа – URL: https://www.cisecurity.org/controls/. (Дата обращения 26.05.2019).

Оригинальность 99%