УДК: 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ КОРПОРАТИВНЫХ СЕТЕЙ

Панин Д. Н.

к.физ.-мат.н., доцент,

Поволжский государственный университет телекоммуникаций и информатики,

Самара, Россия

Козлов З. С.

студент,

Поволжский государственный университет телекоммуникаций и информатики,

Самара, Россия

Аннотация. В наше время информация является ценным ресурсов не только для физических лиц, но и для юридических. В статье рассматривается актуальная проблема на нынешний момент – это информационная безопасность в корпоративных сетях. В научной работе описываются профиль угроз конфиденциальности информации, способы борьбы со взломом со стороны злоумышленников, а также инструменты для обхода антивирусного программного обеспечения. Цель была достигнута и были рассмотрены методы противодействия угрозам и схема их появления.

Ключевые слова: корпоративные сети, безопасность информации, информация, злоумышленник, антивирус.

INFORMATION SECURITY OF CORPORATE NETWORKS

Panin D. N.

PhD, Associate Professor,

Povolzhky State University of Telecommunications and Informatics,

Samara, Russia

Kozlov Z. S.

Student,

Povolzhky State University of Telecommunications and Informatics,

Samara, Russia

Annotation. Nowadays, information is a valuable resource not only for individuals, but also for legal entities. The article deals with the current problem of information security in corporate networks. The research paper describes the profile of threats to the confidentiality of information, ways to combat hacking by hackers, as well as tools for circumventing antivirus software. The goal was achieved and methods of countering threats and the scheme of their appearance were considered.

Keywords: corporate networks, information security, information, attacker, antivirus.

Введение

Мы живем в двадцать первом веке и информационные технологии играют большую роль в нашей жизни. С появлением информационных технологий возникла потребность обеспечивать секретность и целостность информации, так как злоумышленники создают и развивают угрозы несанкционированного доступа к конфиденциальной информации для собственной выгоды [1-6]. Каждый год информационные технологии существенно прибавляют в своем

развитии, поэтому возникают новые способы воздействия на информацию [7]. Организации необходимо защищать информацию для того, чтобы прогрессировать. Но и в средствах защиты можно найти уязвимость [8]. В статье рассматриваются корпоративные сети. На них наиболее часто совершаются атаки со стороны злоумышленников. Через данные сети проходят потоки информации. Остановка данного потока нейтрализует деятельность организации, что приводит в возникновении множества серьезных проблем. Нарушение конфиденциальности корпоративной информации приводит к серьезным материальным убыткам, репутационным потерям и может поставить под угрозу существование организации, поэтому ее защита становится одной из важных функций жизнеобеспечения и развития организации.

Цель исследования

Необходимо проанализировать основные угрозы информационной безопасности корпоративных сетей и причины их возникновения. Так же рассмотреть методы защиты конфиденциальности информации в организации.

Методы исследования

Работа проводилась с использованием методов исследования: сравнения и анализа.

Основная часть

1. Схема угроз корпоративной сети.

Схема (*Рис.1*) информирует нас об актуальных угрозах для корпоративной сети. Целью угроз является нарушение работоспособности защитных механизмов и нарушение конфиденциальности, целостности и доступности информации. Схема (*Рис.1*) содержит списки угроз, их источники и уязвимости сети. Существуют два типа нарушителей: внутренний и внешний.

Внутренний нарушитель — это пользователь или администратор сети. Внешним является сотрудник организации. Внутренний нарушитель производит атаки на ресурсы информационной системы: программные средства, средства разграничения доступа, сервера. Внутренний злоумышленник производит атакующие действия на вычислительные системы и коммуникационные технологии. Источниками нарушения информационной безопасности в организации можно назвать:

1) Сотрудники, обладающие доступом к передачам данных и системам хранения.

2) Пользователи информационной системы.

3) Нарушение полномочий администраторов системы.

4) Сотрудники, обладающие доступом к информационной системе для поддержания ее работоспособности.

5) Сбои аппаратного и программного обеспечения.

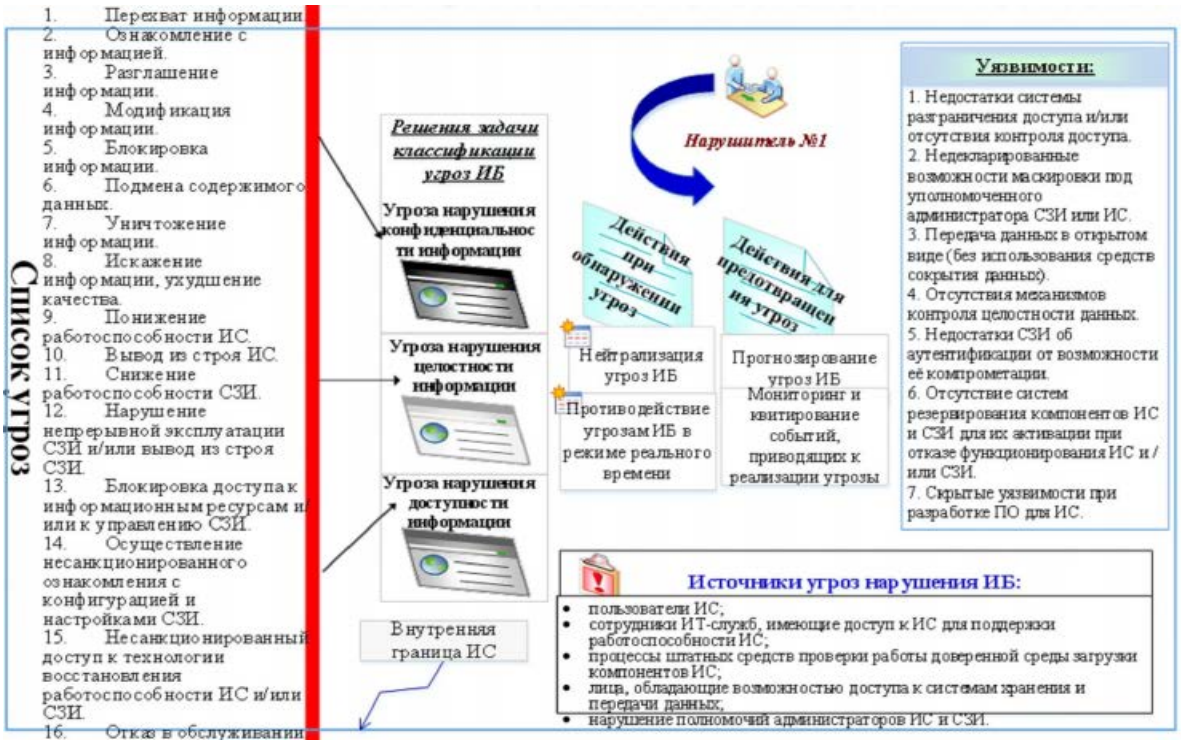

Рис.1-Схема профиля угроз информационной безопасности корпоративной информационной системы [1].

2. Несколько способов защиты информации в организации

Для обеспечения целостности информации корпоративных сетей необходимо использовать все доступные программно-аппаратные средства.

2.1. Система предотвращения вторжений

Система самостоятельно находит и блокирует атаки из сети. Она состоит из систем IPS. Сетевые IPS отслеживают входящие и исходящие пакеты данных, то есть контролируют трафик компьютерной сети и блокируют подозрительные на атаку потоки данных. IPS для отдельных компьютеров следят за подозрительной активностью на персональном компьютере. IPS для беспроводных сетей обладают задачей обнаружения спуфинг mac-адресов. Мас-спуфинг заключается в том, что злоумышленник изменяет mac-адрес маршрутизатора или коммутатора для обхода доступа к серверам. Наконец анализатор поведения сети способен анализировать трафик сети и идентифицировать Dos и DDos атаки.

2.2. Система обнаружения вторжений (СОВ)

Программное или аппаратное средство для выявления фактов неавторизованного доступа в сеть. Сетевая система обнаружения вторжений автоматически мониторит трафик с концентратора. Так же существует СОВ, которая ведет наблюдение за HTTP и HTTPS протоколами. HTTPS является расширением протокола HTTP с шифрованными транспортными механизмами SSL и TLS. СОВ основанная на прикладных протоколах проверяет данные протоколы. Узловая СОВ располагается на хосте и отслеживает вторжения, используя анализ журналов приложений и системные вызовы. Гибридная СОВ комбинирует данные с хостов с сетевой информацией для представления о безопасности сети.

Denuvo

Данная технология позволяет защищать данные от несанкционированного доступа. Denuvo Software Solutions официально не объявили каким образом работает их программное обеспечение Denuvo Anti-Tamper. Однако существуют предположения что технология шифрует и расшифровывает любые данные на носителе так, что возникают большие трудности при взломе [2]. Так же утверждают, что Denuvo состоит из 64-битной шифровальной машины, которая требует уникальные криптографические ключи для каждого оборудования.

3. Антивирусное программное обеспечение и способы его обхода.

Антивирус — это программа, обладающая возможностью сканировать несколько файлы на носителе, сравнивая их с известной базой данных [3]. Он собирает исходный размер файла и сравнивает его с файлом в данный момент, чтобы проверить, что файл не увеличился в размере. Антивирус способен сканировать загрузочный сектор носителя, чтобы определить заражен он или нет. Но существуют инструменты для уклонения от антивируса. Они используются для того, чтобы вредоносный исполняемый PE-файл не был обнаружен антивирусным ПО. Данные инструменты, как правило, служат для нахождения слабых мест в антивирусах.

3.1. AntiVirus Evasion Tool (AVET)

Shellcode binder (связка шелл кода) необходима для изменения закодированной нагрузки перед выполнением. Полезная нагрузка также должна быть закодирована, чтобы сделать ее невидимой для антивируса.

3.2. peCloak.py

Данный инструмент является скриптом python, который совершает автоматизированный процесс сокрытия от антивируса вредоносного файла [8]. Для того, чтобы избежать обнаружения применяется кодирование с

использованием базовых функций add, sun, xor и динамического построения порядка кодирования. По умолчанию скрипт кодирует весь раздел PE, содержащий исполняемый код. При эвристическом обходе используются инструкции NOPS, ADD/SUB, PUSH/POP, INC/DEC, которые выбираются случайным образом для конечного числа итераций, чтобы обмануть антивирус. Этот скрипт кодирует разделы PE-файла, затем вставляет кодовую ячейку, соответствующую функцию декодера.

Результаты

Были рассмотрены источники возникновения угроз информационной безопасности и уязвимости корпоративной сети, а также предложены методы защиты информации.

Заключение

Были выявлены угрозы, которые несли опасность нарушения работы корпоративных сетей и потере конфиденциальных данных.

Цель была достигнута и были рассмотрены методы противодействия угрозам. Например, система предотвращения вторжений. Необходимо, чтобы информация была доступна тем, кто вовлечен в работу организации и пользуется ее услугами, и недоступна для злоумышленников, недобросовестных конкурентов.

Библиографический список:

1. Бабенко А.А., Козунова С.С. Модель профиля угроз информационной безопасности корпоративной информационной системы // NBI-технологии. 2018. №1. – С. 6-11.
2. Табилова А.З., Коннов А.Л. Анализ проблем информационной безопасности в корпоративных сетях // Вестник науки и образования.

2019. №17 (71). – С. 10-13.

3. Евсеев С. Разработка методологии построения системы защиты информации в системе корпоративных исследований и образования в условиях автономии вуза // Восточно-Европейский журнал передовых технологий. - 2019. - №. 3 (9). - С. 49-63.
4. Панин Д.Н., Бобков Е.О., Балашова Е.А. Анализ кибератак на критическую информационную инфраструктуру с IOT- технологиями // Автономия личности.2020. №2 (22). С. 55-64.
5. Панин Д.Н., Филиппова Д.Н., Пирогов Д.С., Афонин А.М. Облачная безопасность - рекомендации по снижению угроз // Информатизация и связь. - 2020. - №2. - С. 73-76.
6. Бобков Е.О., Балашова Е.А., Панин Д.Н. Обеспечение информационной безопасности критической информационной инфраструктуры с IOT-технологиями // В сборнике: Экономика и общество: перспективы развития. Сборник материалов IV Всероссийской научно-практической конференции. Киров, 2020. С. 221-225.
7. Омельченко М.В., Плотникова К.А., Дяглев С.П. К вопросу о защите корпоративных локальных сетей // Инновационная наука. 2020. №2. – С. 31-33.
8. Калогранис С. Уклонение от антивирусных программ: оценка средств AV Evasion: дис. - Университет Пирея, 2018. – С. 1-30.

Оригинальность 87%