Информационная безопасность при удалённой работе.

Горюнов А. А.; Чистяков Н. А.; Масленников Н. С.

Дальневосточный федеральный университет

Школа естественных наук

Кафедра информационной безопасности

Аннотация: в проделанной работе рассмотрена проблема информационной безопасности при удалённой работе. Представлены: анализ новых рисков и угроз информационной безопасности при массовой удалённой работе, обеспечение защиты информации удалённого рабочего стола, а так же Предупреждение инцидентов информационной безопасности и утечек данных при удаленной работе.

Ключевые слова: Информационная безопасность; Удалённый доступ; Конфиденциальность; Протокол RDP; DLP-системы; VPN-клиент; Информационная среда; Утечки данных.

1. Введение в проблему

Переход на удаленную работу становится все более отчетливым трендом на современном рынке труда. Особенно актуальным этот тренд стал в период коронавирусной пандемии, когда многие компании были вынуждены закрывать свои офисы. Для многих профессий и направлений деятельности удаленка дает немало преимуществ. Она позволяет поддерживать стабильную деятельность компании даже в наиболее сложных условиях, сокращать расходы на поддержание деятельности, упрощает условия работы для сотрудников. Однако при своих плюсах удаленка имеет и существенные недостатки. Одним из главных минусов является повышение уровня риска информационной безопасности. Если при работе в офисе обмен данными и взаимодействие часто проходит в сети, защищенной передовыми корпоративными средствами защиты, то при работе из дома информация передается через частные сети с гораздо более слабой защищенностью. В связи с этим особую актуальность приобретает обеспечение безопасности при удаленной работе.

2. Новые риски и угрозы безопасности при удалённой работе

Удаленная работа стала нормой для многих в связи с пандемией. Она конечно же, не нова и существует уже долгое время, но из-за неопытности сотрудников вынужденная работа удалённо усугубила многие из существующих проблем. Поскольку компании спешно переходили на новые технологические платформы для удаленной работы (и удаленного доступа к корпоративным системам) и делового взаимодействия, появились новые угрозы, вызванные неопытностью сотрудников, отсутствием должного обучения работе, а так же работой с принципиально новыми технологиями.

Риски и уязвимости распределены по двум основным направлениям:

1. Риски безопасности, связанные с сотрудниками, работающими удаленно.

2. Риски, связанные с технологиями, которые были использовались во время пандемии.

К тому же, защита персональных данных сотрудников, тоже была очень важной составляющей безопасности удалённой работы.

Работодатели стали использовать системы мониторинга.

Это может быть мониторинг нажатия клавиш, экранов и посещаемых веб-сайтов. В некоторых случаях сотрудники могут используют свои собственные технологии (смартфоны, ноутбуки) для удаленной работы, тем самым предоставляя работодателям или компаниям, доступ к огромному количеству личных данных сотрудников.

Раскрытие личной информации в результате использования технологии удаленной работы и коммуникационных технологий может стать почвой для киберпреступлений.

3. Обеспечение защиты удалённого рабочего стола

При осуществлении удаленного доступа необходимо обеспечить защиту информационных ресурсов. Обеспечение конфиденциальности и целостности информации при удаленной работе является главной задачей при таком виде работ.

Так как на сегодняшний день самой популярной операционной системой является Windows, то самым используемым сетевым протоколом удаленного подключения является протокол RDP, стандартное подключение по которому является небезопасным. Поэтому существует ряд методов, позволяющий повысить безопасность удалённых подключений по протоколу RDP:

1) *Шифрование.*
   Шифрование можно установить с помощью редактора локальной групповой политики, где необходимо настроить алгоритм шифрования.
2) *Аутентификация на уровне сети.*
   Аутентификация на уровне сети необходима для минимизации DDoS-атак. Устанавливается так же с помощью редактора локальной групповой политики.

3) *IPBan.*
4) IPBan фиксирует неудачные попыток входа в систему, их количество.
5) *VPN.*
   VPN позволяет создавать надежную и защищенную сеть на основе ненадежной.
6) *RD Gateway.*
   RD Gateway позволяет подключаться к рабочему столу через шлюз, создавая зашифрованное подключение по протоколу TLS.

4. Предупреждение инцидентов информационной безопасности при удаленной работе. Предотвращение утечек данных.

В связи с переходом на удаленную работу вопрос о защищенности информации встал остро для различных компаний и существуют различные способы и рекомендации по улучшению информационной безопасности.

- использовать передачу данных в зашифрованном виде(СКЗИ)

-использовать множество протоколов аутентификации при передачи пароля по ненадежным каналам связи

- работать с облачными сервисами с улучшенными процессами идентификации

- применять антивирусные программные продукты и сетевые экраны

- использование SIEM-систем(управление информацией и событиями безопасности) позволит отслеживать действия пользователей внутри сети

-использовать сервисы для связи сотрудников со сквозным шифрованием

Так же из-за работы в незащищенных, сетях общего пользования повысился риск утечки информации от сотрудников по различным каналам,

поэтому компании активно внедряют в свои корпоративные сети DLP-системы-системы предотвращения утечки данных. Они основываются на анализе потока данных, которые пересекают периметр информационной системы. Когда DLP-система обнаруживает конфиденциальные данные, то передача сообщения блокируется.

Основными каналами утечки информации являются:

─ съемные носители;

─ электронная почта;

─ распечатанные с компьютера документы;

─ сервисы для общения.

Обычный состав DLP-системы включает:

-центр управления и мониторинга;

-модули сетевого уровня-когда контролируется сетевой трафик в информационной системе;

-компоненты уровня хоста-когда контролируется информация на рабочих станциях.

2 способа распознавания конфиденциальной информации:

-анализ формальных признаков (хэш-значения, специальные метки и т.д.)

-анализ контента

5. Заключение

После теоретического анализа различных статей можно сделать вывод, что вопрос о защите информации и защите от утечек конфиденциальной информации как никогда актуален. На сегодняшний день существует большое количество средств и методов обеспечения защиты данных при удаленном подключении, также необходимо использовать соответствующие рекомендации отечественных регуляторов по мерам обеспечения информационной безопасности: Рекомендации Банка России; Рекомендации НКЦКИ; Рекомендации ФСТЭК России. Был выявлен ряд существенных

рисков, поэтому необходимо, чтобы организации проверяли, соответствует ли безопасность требованиям. Важно, чтобы организации при введении нового программного обеспечения переобучали сотрудников для работы с ним и, чтобы переобучение включало навыки минимизации рисков для безопасности при работе удалённо.