Столыпинский вестник

Научная статья

Original article

УДК 004

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО УДАЛЕННОГО ДОСТУПА

ORGANIZATION OF SAFE REMOTE ACCESS

Семянова Софья Игоревна, студент Ростовский государственный экономический университет (РИНХ)

Semyanova Sofya Igorevna, student, Rostov State University of Economics (RSUE)

Аннотация: В данной статье рассмотрены способы и особенности организации удаленного доступа сотрудниками. Показаны общедоступные каналы передачи данных, их плюсы и минусы. А также риски информационной безопасности, возникающие при удаленном доступе сотрудника к рабочему столу компьютера, установленного в офисе коммерческой компании.

Annotation: This article discusses the methods and features of organizing remote access by employees. Public data transmission channels, their pros and cons are shown. As well as information, security risks that arise when an employee remotely accesses the desktop of a computer installed in the office of a commercial company.

Ключевые слова: информационная безопасность, безопасный удаленный доступ, угрозы информации при удаленном доступе, виртуализация приложений.

Keywords: information security, secure remote access, information threats in remote access, application virtualization.

Во время самоизоляции согласно совместному аналитическому отчету ВЦИОМ и Social Business Group, доля россиян, работающих удаленно, увеличилась в четыре раза[1]. Но даже после сокращения заболевших дистанционная работа по-прежнему востребована, так как имеет преимущества перед работой в офисе: сотруднику не нужно проводить время в дороге, расходы на транспорт и питание снижаются. В связи с большой популярностью удаленной работы, в настоящее время, в России она регулируется на правовом уровне Федеральным законом «О внесении изменений в Трудовой кодекс Российской Федерации в части регулирования дистанционной (удаленной) работы и временного перевода работника на дистанционную (удаленную) работу по инициативе работодателя в исключительных случаях», принятым в 2020 году.

Удаленная работа — это один из способов взаимодействия с удаленными сотрудниками, ее основными видами являются:

- удаленная работа на постоянной основе;
- временная удаленная работа;
- периодическая удаленная работа;
- удаленная работа в исключительных случаях.

Несмотря на все преимущества, дистанционная работа так же имеет и недостатки. Например, сотруднику необходимо организовать доступ к определенным ресурсам организации, для этого используют один из следующих методов:

- подключение к определенному компьютеру в организации;
- использование инфраструктуры виртуального рабочего стола;

- использование виртуализации приложений.

Преимущества подключения сотрудника к определенному компьютеру в организационной сети - доступ сотрудника к компьютеру организации в командировке, низкая стоимость перехода с работы на полный рабочий день на удаленную работу, быстрое изменение штатного формата сотрудника удаленно.

Недостатком этого метода является требование отдельного компьютера для каждого сотрудника.

Инфраструктура виртуального рабочего стола (*англ*. Virtual Desktop Infrastructure, VDI) - это технология, позволяющая создавать виртуальную IT-инфраструктуру и предоставлять полноценные рабочие места на основе одного или нескольких серверов, на которых работает множество виртуальных машин[2]. То есть сотрудник подключается не к отдельному компьютеру, а к специальному серверу.

Преимущества инфраструктуры виртуальных рабочих столов - гибкое управление IT-инфраструктурой, мониторинг всех компонентов среды, технология моментальных снимков, позволяющая пользователям возвращаться к ранее сохраненному стабильному состоянию операционной системы, например, в случае заражения вредоносным программным обеспечением, простое масштабирование.

Недостатки этой инфраструктуры - высокие финансовые затраты на развертывание VDI, зависимость от сетевой инфраструктуры компании (VDI не будет демонстрировать свои преимущества при низкой пропускной способности в офисной сети), большие затраты времени на внедрение в крупных компаниях (организация VDI с 1000 рабочими местами и более может занять от нескольких месяцев до года).

Виртуализация приложений - этот метод позволяет использовать приложения, установленные на сервере, как если бы они были на рабочем компьютере сотрудника. Примером такой платформы является Microsoft Application Virtualization (App–V), разработанная Microsoft.

Преимущества использования приложений на сервере - централизованное управление приложениями, простое обновление и исправление приложений, более низкое потребление ресурсов по сравнению с виртуальной операционной системой, простой контроль использования лицензии.

Недостатком схемы является то, что любой человек, имеющий физический доступ к серверу App-V, потенциально может атаковать всю клиентскую базу. Серверы App-V должны храниться в физической защищенной серверной комнате с контролируемым доступом.

Несмотря на высокую эффективность всех вышеперечисленных методов удаленного доступа, в настоящее время, наиболее часто используется подключение одного сотрудника к одному компьютеру, расположенному в организации. Информационные угрозы есть и в данном способе. Такими являются:

- атака «человек посередине»;
- анализ сетевого трафика («перехват»);
- подмена субъекта или объекта сети (так называемый «маскарад»);
- атака «грубой силы» (англ. brute force);
- вредоносные программы;
- отказ в обслуживании (Deny of Service, DoS), или «распределенный» отказ в обслуживании (Distributed Deny of Service, DDoS);
- хакерство;
- крекинг – акт проникновения в компьютерную систему или сеть;
- уязвимости приложений (например, ошибки безопасности памяти или ошибочные проверки подлинности, которые может содержать программное обеспечение);
- человеческий фактор;
- кража устройств и носителей конфиденциальной информации[3].

В любом случае для каждой из этих угроз существуют свои методы нейтрализации. Например, чтобы защитить себя от таких угроз, как атака

«человек посередине», анализ сетевого трафика ("перехват") и взлом, необходимо использовать шифрование. Данный метод может быть реализован с помощью виртуальной частной сети. При правильном внедрении и использовании специального программного обеспечения виртуальная частная сеть может обеспечить высокое шифрование передаваемой информации.

Помимо этого, еще можно использовать VPN – технологию, которая позволяет создавать безопасное подключение пользователя к сети, организованной между разными компьютерами. В него входят несколько распространенных протоколов: туннельный протокол типа точка-точка (PPTP), протокол туннелирования уровня 2 (L2TP), специально разработанный для создания безопасных соединений Internet Protocol Security (IPSec), Secure Sockets Layer (SSL) и Transport Layer Security (TLS) (с их популярными реализациями Microsoft SSTP (SSL 3.0) и Open VPN (SSL 3.0/TLS 1.2))[4]. Каждый из этих протоколов имеет свои плюсы и минусы, которые определяют, как обрабатывать уязвимости и использовать виртуальные частные сети (например, для определения текущего общедоступного IP-адреса устройства, доступного через VPN или регулярное соединение Gap VPN и, как следствие, внезапный выход трафика в общедоступной сети). Кроме того, DNS-запросы не всегда проходят внутри виртуальной сети и обрабатываются там вашими собственными DNS-серверами. На практике при подключении не всегда используются доверенные серверы (например, Google Public DNS или Open DNS) - часто используются DNS-серверы, выводимые общедоступной сетью, ответ на которые может быть неверным. В связи с этим вместо фактического адреса запрошенного домена пользователь может получить поддельный адрес. Побочным эффектом этой проблемы является угроза анонимности, то есть злоумышленник может узнать адреса DNS-сервера пользователя и таким образом получить информацию об их интернет-провайдере и приблизительном местоположении.

Если нейтрализовать угрозу нет возможности, то можно минимизировать угрозу атак «грубой силы» с помощью следующих инструментов: сложные пароли, многофакторная аутентификация и ограничение попыток пароля. И чтобы защитить себя от вирусного программного обеспечения, необходимо использовать антивирусные программы, которые также могут нейтрализовать хакерство и крекинг. Для нейтрализации угроз используются аппаратные брандмауэры, маршрутизаторы, системное обнаружение и предотвращение вторжений, аппаратные модули доверенной загрузки и смарт-карты.

Сравнивая решения организации информационной безопасности российских производителей, выделяют оптимальными для использования – АССИСТЕНТ с версией лицензии «Корпорация + ФСТЭК» и продукты семейства «ЗАСТАВА» [5]. Выбор первого из перечисленных программных решений обоснован следующими причинами:

- программный комплекс АССИСТЕНТ поддерживает большее количество ОС;

- имеются сертификаты совместимости для различных версий Linux (в RMS совместимость с Linux еще тестируется);

- комплекс обладает встроенным сертифицированным средством защиты от несанкционированного доступа;

- в комплексе есть возможность использования сессионных паролей.

Программный комплекс АССИСТЕНТ необходимо установить, как на устройство сотрудника, с которого он будет подключаться, так и на удаленный компьютер. Также необходима установка серверной части данного ПО.

Выбор продуктов семейства «ЗАСТАВА» обосновывается наличием сертификата совместимости с ранее выбранным комплексом АССИСТЕНТ. Решение необходимо установить на устройства сотрудника и на VPN-сервер[6].

Список использованной литературы:

1. Абашев А., Жедрин И., Акулов В. Глобальные тенденции рынка информационной безопасности // Information Security/ Информационная безопасность. 2015. № 5. С. 16–17.
2. Пиджикян Д.С., Шарыпова Т.Н. Система защиты персональных данных Российской Федерации. В сборнике: Наука и технологии: актуальные вопросы, достижения и инновации. сборник научных трудов по материалам XXVI Международной научно-практической конференции. Анапа, 2021. С. 14-18.

a. Шарыпова Т.Н, Селиванов С.А. Анализ угроз информационной безопасности и способы ее защиты.2021 №1-1. С. 242-245

3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) [Электронный ресурс].
4. Шарыпова Т.Н., Зархатаев Д.К. Система защиты персональных данных с точки зрения противодействия угрозам информационной безопасности в Российской Федерации. 2022. С. 47-48..
5. Новые виды удаленной работы по ТК РФ // Web-сайт «Кадровое дело». URL: https://www.kdelo.ru/art/386028-vidy-udalennoy-raboty-po-tk-rf-21-m1 (дата обращения: 03.05.2021).
6. Разумовская Е. А. Некоторые проблемы безопасности России в сфере информационных технологий // МИФИ: Безопасность информационных технологий. 2015. № 4. С. 91–96.

List of used literature:

1. Abashev A., Zhedrin I., Akulov V. Global trends in the information security market // Information Security / Information security. 2015. No. 5. P. 16–17.
2. Pidzhikyan D.S., Sharypova T.N. Personal data protection system of the Russian Federation. In the collection: Science and technology: topical issues, achievements and innovations. collection of scientific papers based on the materials of the XXVI International Scientific and Practical Conference.

Anapa, 2021, pp. 14-18.

3. Sharypova T.N., Selivanov S.A. Analysis of threats to information security and ways to protect it. 2021 No. 1-1. pp. 242-245
4. Doctrine of information security of the Russian Federation (approved by the President of the Russian Federation on 09.09.2000 No. Pr-1895) [Electronic resource].
5. Sharypova T.N., Zarhataev D.K. Personal data protection system in terms of countering information security threats in the Russian Federation. 2022, pp. 47-48.
6. New types of remote work according to the Labor Code of the Russian Federation // Web-site "Kadrovoe delo". URL: https://www.kdelo.ru/art/386028-vidy-udalennoy-raboty-po-tk-rf-21-m1 (date of access: 05/03/2021).
7. Razumovskaya E. A. Some problems of Russian security in the field of information technology // MEPhI: Security of information technologies. 2015. No. 4. P. 91–96.

Для цитирования: Семянова С. И. В.ОРГАНИЗАЦИЯ БЕЗОПАСНОГО УДАЛЕННОГО ДОСТУПА//Научный сетевой журнал «Столыпинский вестник», №6/2022