ЦИФРОВАЯ ОБОРОНА:

СТРАТЕГИЯ БЕЗОПАСНОГО УДАЛЕННОГО ДОСТУПА

BELYAEV

ОБО МНЕ

Беляев Дмитрий Александрович

Директор по КБ в ИТ-компании

- Более 9 лет в ИБ;
- В 23 года стал ИО Начальника СИБ;
- Работал в:
  - Гос. организации;
  - Ком.Холдинге;
  - 3-х банках в т.ч из ТОП-10;
  - ИТ-интеграторе.
- Имею 2 образования (ИБ и Юриспруденция);
- Имею более 150 сертификатов/дипломов и благодарностей по тематике ИБ.
- Руководил 5-ю стартапами и командой из более 100 человек.
- Более 60 выступлений.

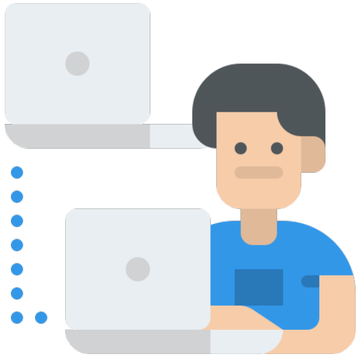
ВИДЫ УДАЛЕННОГО ДОСТУПА

1. VPN (виртуальная частная сеть): надежно соединяет удаленных пользователей с корпоративной сетью через Интернет, обеспечивая зашифрованную связь и доступ к внутренним ресурсам.

2. Протокол удаленного рабочего стола (RDP): позволяет пользователям получать удаленный доступ к компьютеру или серверу и управлять ими через сетевое подключение, часто используется для технической поддержки или доступа к офисным рабочим столам.

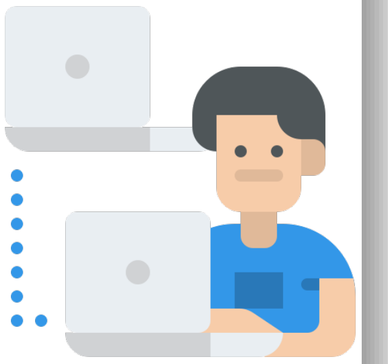
3. SSH (безопасная оболочка): обеспечивает безопасный удаленный доступ к серверам и системам, в основном используется для доступа из командной строки и передачи файлов в средах на базе Unix.
4. Citrix Virtual Apps and Desktop: предоставляет приложения и рабочие столы удаленным пользователям через централизованную инфраструктуру.

5. Программное обеспечение удаленного доступа (например, TeamViewer, AnyDesk): позволяет пользователям удаленно управлять другим компьютером для совместной работы, устранения неполадок или доступа к файлам, обычно через защищенное соединение.



6. Облачные сервисы (например, AWS, Azure): Предоставляют удаленный доступ к размещенным в облаке ресурсам и приложениям, позволяя пользователям работать из любого места, где есть подключение к Интернету.

7. Веб-доступ (например, SSL VPN): позволяет пользователям получать доступ к корпоративным ресурсам через веб-браузер, обычно используя HTTPS для шифрования и аутентификации.

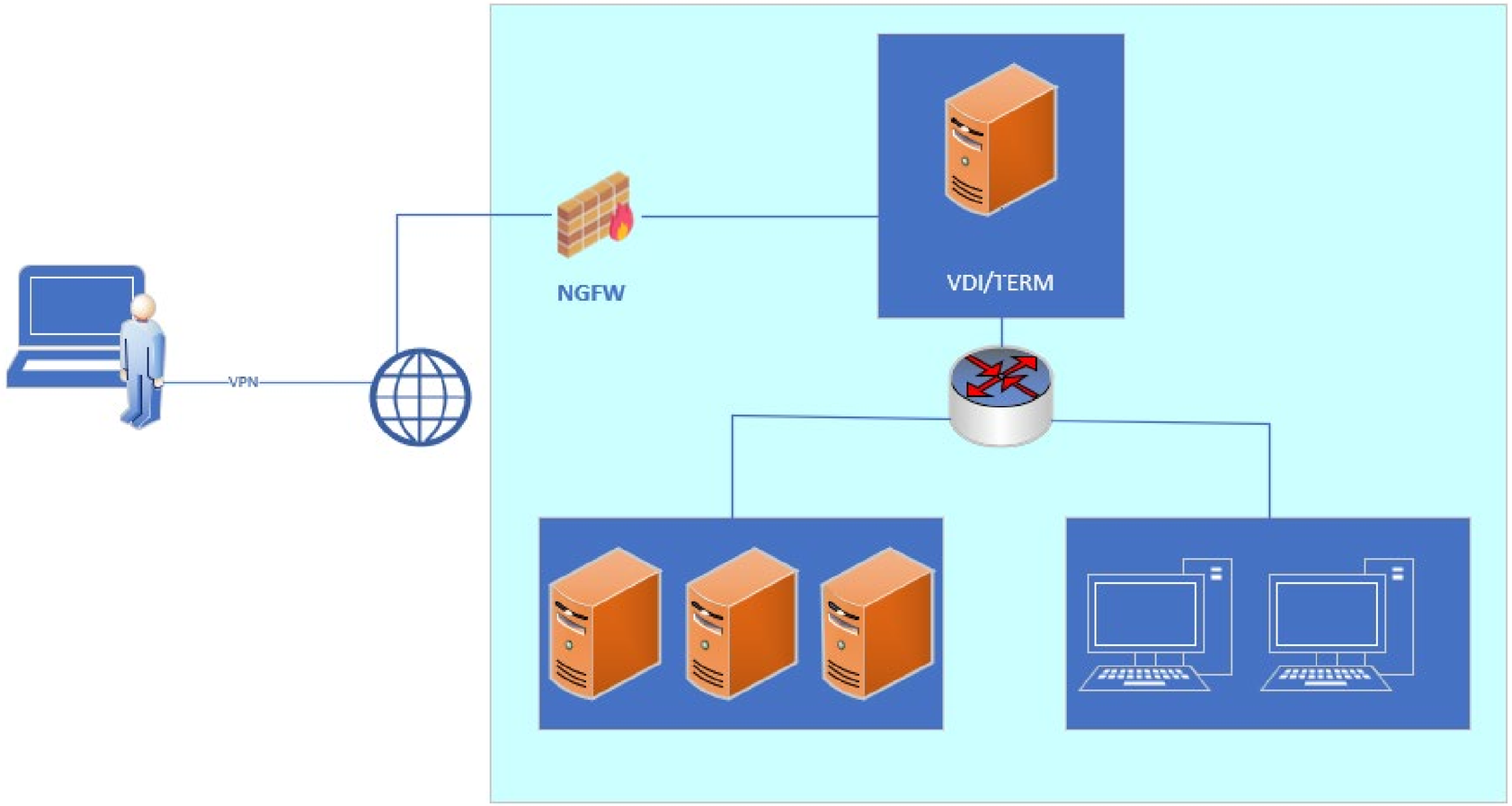


8.Серверы удаленного доступа (RAS): Обеспечивают централизованный шлюз для удаленных пользователей для подключения к корпоративной сети, управления аутентификацией, контролем доступа и шифрованием.

9. VDI (Virtual Desktop Infrastructure): Это технология, которая позволяет предоставлять виртуальные рабочие столы пользователям через удаленный доступ.

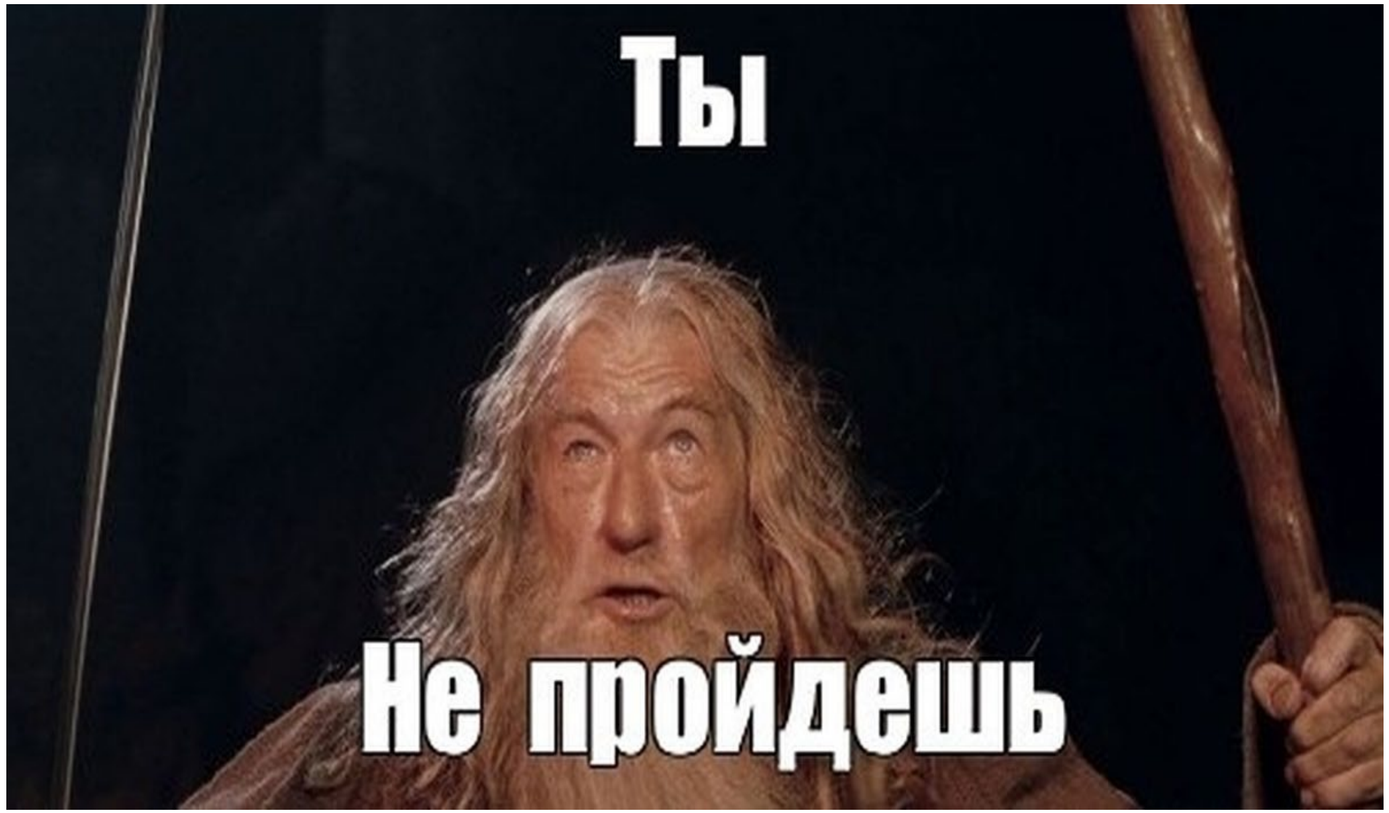
10. Jump сервер (Jump Server): Это сервер, который обеспечивает безопасный доступ к целевым системам или сетям из внешних источников. Пользователи сначала подключаются к Jump серверу, а затем с него уже осуществляют доступ к целевым системам или сетям, что помогает усилить безопасность и контроль доступа.

ПРИМЕР СХЕМЫ ПОСТРОЕНИЯ УДАЛЕННОГО ДОСТУПА



ВАЖНО

- Модель угроз
- АВЗ;
- DLP;
- PUM/PAM;
- IDS/IPS;
- EDR;
- SOC;
- САЗ;
- 2FA;
- И др. СЗИ.

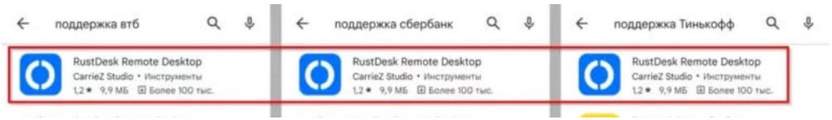


Кейсы

Мошенники воруют деньги с помощью ПО для удаленного администрирования

Мария Нефёдова , 26.09.2023 Комментарии 22639

Специалисты «Доктор Веб» предупредили, что участились случаи мошенничества с применением программ для удаленного доступа к рабочему столу. Наибольшей популярностью у злоумышленников пользуется программа RustDesk.



По словам ИБ-экспертов МТС Red, на долю атак через взлом контрагентов приходится 30% от общего числа нападений. Среди самых крупных инцидентов — атака, повлёкшая утечку данных из сетей «Ашан» и «Твой дом». Расследование показало, что партнёры сетей не обновили защитное ПО, чем и воспользовались хакеры.

Специалисты из F.A.C.C.T. сообщили, что спрос на инструменты, защищающие бизнес от атак, связанных с получением удалённого доступа, вырос на 25%. Актуальность технологий, нацеленных против вредоносных рассылок, увеличилась на 80%.

Наиболее востребованными считаются решения, которые не позволяют хакерам проникнуть в инфраструктуру компании через взлом посредников — спрос на них увеличился на 120%.

Подрядчик не успел

Что случилось: хакер опубликовал в открытом доступе данные 8 тысяч сотрудников французского ритейлера Decathlon.

Как это произошло: 7 сентября эксперты vpnMentor обнаружили в даркнете базу данных, которая содержала информацию о сотрудниках Decathlon: полные имена, номера телефонов, адреса электронной почты, страны и города проживания, токены аутентификации и фотографии.

По информации vpnMentor, хакер опубликовал данные, которые были скомпрометированы в результате утечки в 2021 году у партнера Decathlon – компании Bluenove. 9 марта 2021 года киберэксперты обнаружили, что Bluenove хранит собранные данные в неправильно настроенном облачном хранилище. О находке эксперты сообщили в Bluenove, а те закрыли доступ к данным 13 апреля. Но, как оказалось, устранить утечку без последствий компании не удалось: как минимум один злоумышленник успел получить доступ к данным сотрудников Decathlon до того, как в Bluenove закрыли доступ.

> Самый опасный яд — информационный.

Павел Валерьевич Дуров

Спасибо за внимание!