# Trey Research Corporation

Virtuelle private Netzwerke: Eine technische Übersicht für Fabrikam, Inc.

**15. Dezember 2023**

**Virtuelle private Netzwerke (VPNs)** sind eine beliebte Netzwerksicherheitslösung, mit der der Netzwerkdatenverkehr verschlüsselt werden kann. [VPNs fungieren als sicherer Tunnel und verschlüsseln Internetdatenverkehr, was es Dritten erschwert, Aktivitäten nachzuverfolgen und Daten zu stehlen](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons).

## Vorteile der Einführung von VPNs:

* VPNs bieten eine zusätzliche Ebene für Datenschutz und Sicherheit, indem sie den Internetdatenverkehr verschlüsseln. Dies macht es Dritten schwer, Aktivitäten nachzuverfolgen und Daten zu stehlen.
* Mit VPNs können Sie verhindern, dass Sie bei der Nutzung des öffentlichen WLANs am Flughafen oder in der Bibliothek gehackt werden. Das liegt daran, dass VPNs wie ein sicherer Tunnel funktionieren und den Internetdatenverkehr verschlüsseln.
* [VPNs können verhindern, dass Ihr Internetdienstanbieter erfährt, welche Websites Sie besucht haben, da der gesamte Datenverkehr von und zu Ihrem Computer über die Server des VPNs läuft oder über Server, für deren Nutzung die VPNs bezahlen](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc)[1](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/).
* [VPNs können geografische Einschränkungen für Inhalt umgehen 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/), indem sie Ihre IP-Adresse maskieren und Ihre Internetverbindung verschlüsseln. Wenn Sie eine Verbindung mit einem VPN-Server herstellen, wird Ihr Internetdatenverkehr über den VPN-Server weitergeleitet, der Ihnen eine neue IP-Adresse zuweist. [Dadurch erscheint es so, als ob Sie von einem anderen Ort aus auf das Internet zugreifen, sodass Sie geografische Einschränkungen für Inhalte umgehen können.](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## Nachteile der Einführung von VPNs:

* Verbindungsgeschwindigkeiten können langsamer sein als Ihr ISP. [Dies liegt daran, dass VPNs Ihrem Internetdatenverkehr eine zusätzliche Verschlüsselungs- und Routingebene hinzufügen 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* Die Verwendung von VPN ist in einigen autoritären Ländern verboten. [In einigen Ländern sind VPNs verboten oder stark reguliert](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* Die Nutzung kostenloser VPNs birgt das Risiko von Werbung, Malware und Datenlecks. [Kostenlose VPNs können Nutzerdaten an Drittanbieter-Werbetreibende verkaufen oder Werbung in Webseiten einfügen](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).

## Besonderheiten bei der Installation:

* [Ein VPN richtet einen verschlüsselten Tunnel zwischen dem System ein, das den VPN-Client ausführt, und einem VPN-Server, der dann als Proxy den Datenverkehr über den Tunnel zum Rest des Unternehmensnetzwerks leitet](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/). Zu den Schritten zählen
  1. Auf dem Gerät des/der Benutzenden wird ein VPN-Client installiert, der den gesamten Datenverkehr zwischen dem Gerät und dem VPN-Server verschlüsselt.
  2. Der VPN-Server entschlüsselt den Datenverkehr und leitet ihn an das gewünschte Ziel weiter.
  3. Der Zielserver antwortet auf die Anfrage, indem er den Datenverkehr an den VPN-Server zurücksendet.
  4. Der VPN-Server verschlüsselt den Datenverkehr und sendet ihn zurück an den VPN-Client.
  5. [Der VPN-Client entschlüsselt den Datenverkehr und sendet ihn an das Gerät der Benutzerinnen und Benutzer](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922)[1](https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html).
* Führen Sie die folgenden Schritte aus, um einen VPN-Server zu installieren und zu konfigurieren:
  1. Erstellen Sie ein VPN Profil auf Ihrem Computer.
  2. Klicken Sie auf „Start“ und dann auf „Einstellungen“, um das Einstellungsmenü zu öffnen.
  3. Klicken Sie im Einstellungsmenü auf „Netzwerk und Internet“ und dann auf „VPN“.
  4. Wählen Sie VPN-Verbindung hinzufügen aus.
  5. Im Fenster zum Hinzufügen einer VPN-Verbindung sind einige Aufgaben auszuführen.
  6. [Speichern Sie die Änderungen, die Sie vorgenommen haben](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[5](https://www.techzone360.com/topics/techzone/articles/2020/09/16/446567-how-install-configure-virtual-private-network-server.htm).

## Risiken und Risikominderung:

* Angreifer sind sich der Remotearbeit als Bedrohungsvektor seit einiger Zeit bewusst. Die Remotearbeitsumgebung ist für Angreifer aus mehreren Gründen besonders attraktiv. Erstens wird die Heimnetzwerkumgebung nicht professionell verwaltet. Am kritischsten ist, dass dies bedeutet, dass viele weitere Systeme in Heimnetzwerken nicht regelmäßig gepatcht werden, und eine Reihe von ihnen in Bezug auf die Risikominderung veraltet ist. Um in einem Unternehmensnetzwerk zu bestehen, muss ein Angreifer, der ein System ausgenutzt hat, resistent gegen Erkennung und Bereinigung sein. Auch hier ist das Heimnetz für den Angreifer angenehmer; Die Bedrohungserkennung ist in der Regel kaum vorhanden, und Abhilfemaßnahmen werden eher beiläufig ergriffen, z. B. wenn ein PC neu installiert oder außer Betrieb genommen wird, weil er zu langsam läuft. Um die Remotearbeitsumgebung zu sichern, ist es wichtig, Zero Trust-Annahmen zu erweitern. [Nicht nur das Netzwerk sollte als feindlich angesehen werden, sondern alles, was nicht unter der Kontrolle des Unternehmens steht](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/).
* [Aktualisieren Sie VPNs, Netzwerkinfrastrukturgeräte und Geräte, die für den Remote-Zugriff auf Arbeitsumgebungen verwendet werden mit den neuesten Softwarepatches und Sicherheitskonfigurationen](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## Bewährte Methoden bei der Umsetzung:

Zu den bewährten Methoden für die Implementierung von VPNs in einem Unternehmensnetzwerk gehören:

* [Wählen Sie ein standardsbasiertes VPN aus, das anerkannte Standards verwendet, z. B. Internet Key Exchange/Internet Protocol Security (IKE/IPSec), die in der Regel weniger riskant und sicherer sind als Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs, die benutzerdefinierten Code verwenden, um Datenverkehr über TLS zu senden](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)[1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Verwenden Sie ein VPN mit starker Kryptografie. Überprüfen Sie, ob die Verschlüsselungsalgorithmen, Authentifizierungsalgorithmen und Protokolle, die von einem VPN verwendet werden, stark und FIP-validiert sind. [Konfigurieren Sie alle VPNs für die Verwendung der Multi-Faktor-Authentifizierung (MFA) und ersetzen Sie die kennwortbasierte Authentifizierung nach Möglichkeit durch clientbasierte Authentifizierung über digitale Zertifikate (gespeichert auf Smartcards)](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)[1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Verwalten von Softwarerisiken. Die Nutzung von VPN-Sicherheitsrisiken ist ein häufiger Angriffsvektor für Cyberkriminelle. Wählen Sie einen VPN-Anbieter mit einer guten Erfolgsbilanz beim Sicherheitslückenpatching aus und fordern Sie eine Software-Stückliste (Software Bill of Materials, SBOM) an, um zu überprüfen, ob der Drittanbieter-Code aktuell und sicher ist. Suchen Sie außerdem nach einem Produkt, das seinen Code während der Ausführung prüfen kann, um potenzielle Angriffe zu erkennen. [Überprüfen Sie nach der Bereitstellung eines VPN regelmäßig, ob Softwareupdates verfügbar sind und wenden Sie sie umgehend an](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)[1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Bereiten Sie sich auf einen Anstieg der Nutzung vor. [IT-Sicherheitspersonal sollte VPN-Einschränkungen in Vorbereitung auf die Massennutzung testen](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* Vermeiden Sie kostenlose VPNs. [Die Nutzung kostenloser VPNs birgt das Risiko von Werbung, Malware und Lecks 3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/).