Trey Research Corporation

Virtuelle private Netzwerke: Ein technischer Überblick für Fabrikam, Inc.

15. Dezember 2023

Virtuelle private Netzwerke (VPNs) sind eine beliebte Netzwerksicherheitslösung, die zur Verschlüsselung des Netzwerkdatenverkehrs beitragen kann. VPNs fungieren als sicherer Tunnel und verschlüsseln den Datenverkehr im Internet, so dass es für Dritte schwierig ist, Aktivitäten nachzuverfolgen und Daten zu stehlen[1].

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 VPNs bezahlen [1].
- VPNs können geografische Beschränkungen für Inhalte [2] umgehen, indem sie Ihre IP-Adresse verschleiern und Ihre Internetverbindung verschlüsseln. Wenn Sie sich mit einem VPN-Server verbinden, wird Ihr Internetdatenverkehr über den VPN-Server weitergeleitet, der Ihnen eine neue IP-Adresse zuweist. Dadurch wird der Eindruck erweckt, dass Sie von einem anderen Ort aus auf das Internet zugreifen, wodurch Sie geografische Beschränkungen für Inhalte umgehen können

Nachteile der Einführung von VPNs:

- Die Verbindungsgeschwindigkeit kann langsamer sein als die Ihres Internetserviceanbieters. Das liegt daran, dass VPNs Ihren Internetverkehr zusätzlich verschlüsseln und weiterleiten [2].
- Die Nutzung von VPNs ist in einigen autoritären Ländern verboten. In einigen Ländern sind VPNs verboten oder stark reguliert [2].
- Die Nutzung kostenloser VPNs birgt das Risiko von Werbung, Malware und Datenlecks. Kostenlose VPNs können Nutzerdaten an Drittanbieter verkaufen oder Werbung in Webseiten einbauen [2].

Besonderheiten bei der Installation:

- Ein VPN baut einen verschlüsselten Tunnel zwischen dem System, auf dem der VPN-Client läuft, und einem VPN-Server auf, der dann den Datenverkehr durch den Tunnel an das übrige Unternehmensnetzwerk weiterleitet [4].
  Dies umfasst folgende Schritte:

  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 des/der Benutzenden [1].

- 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 „PN-Verbindung hinzufügen“ aus.
  5. Im Fenster zum Hinzufügen einer VPN-Verbindung sind einige Aufgaben auszuführen.
  6. Speichern Sie die Änderungen, die Sie vorgenommen haben [5].

Risiken und Risikominderung:

- Angreifer sind sich seit einiger Zeit bewusst, dass Fernarbeit ein Bedrohungsvektor sein kann. Die Remote-Arbeitsumgebung ist für Angreifer aus mehreren Gründen besonders attraktiv. Erstens wird die Heimnetzwerkumgebung nicht professionell verwaltet. Vor allem aber bedeutet dies, dass viel mehr Systeme in Heimnetzwerken nicht regelmäßig gepatcht werden und viele von ihnen im Hinblick auf die Minderung von Sicherheitsrisiken veraltet sind. Um in einem Unternehmensnetzwerk bestehen zu können, muss ein Angreifer, der ein System ausgenutzt hat, der Entdeckung entgehen und sich der Abhilfe widersetzen. Auch hier kommt das Heimnetzwerk Angreifern entgegen; Bedrohungen werden in der Regel kaum erkannt, und Abhilfemaßnahmen erfolgen eher zufällig, etwa wenn ein PC neu installiert oder ausgemustert wird, weil er langsam läuft. Für die Sicherheit der Remote-Arbeitsumgebung ist es unerlässlich, die Zero-Trust-Annahmen weiter auszudehnen. Nicht nur das Netzwerk sollte als feindlich betrachtet werden, sondern alles, was sich nicht unter der Kontrolle des Unternehmens befindet [4].
- Aktualisieren Sie VPNs, Netzwerkinfrastrukturgeräte und Geräten, die für den Fernzugriff auf Arbeitsumgebungen verwendet werden, mit den neuesten Software-Patches und Sicherheitskonfigurationen [6].

Bewährte Methoden bei der Umsetzung:

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

- Auswahl eines standardbasierten VPN, das anerkannte Standards verwendet, wie z. B. Internet Key Exchange/Internet Protocol Security (IKE/IPSec), die im Allgemeinen weniger riskant und sicherer sind als Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs, die benutzerdefinierten Code verwenden, um Daten über TLS zu senden [12].
- Verwendung eines VPN mit starker Kryptographie. Überprüfung, ob die von einem VPN verwendeten Verschlüsselungsalgorithmen, Authentifizierungsalgorithmen und Protokolle stark und FIP-validiert sind. Konfigurieren aller VPNs so, dass sie eine Multi-Faktor-Authentifizierung (MFA) verwenden, und Ersetzen der passwortbasierten Authentifizierung nach Möglichkeit durch eine Clientauthentifizierung über digitale Zertifikate (auf Smartcards gespeichert) [12].
- Verwalten von Softwareschwachstellen. Die Ausnutzung von VPN-Schwachstellen ist ein gängiger Angriffsvektor für Cyberkriminelle. Wählen Sie einen VPN-Anbieter mit einer guten Erfolgsbilanz beim Patchen

von Sicherheitslücken und fordern Sie eine Software Bill of Materials (SBOM) an, um zu überprüfen, ob der Drittanbietercode aktuell und sicher ist. Achten Sie außerdem auf ein Produkt, das seinen Code bei der Ausführung validieren kann, um potenzielle Eindringlinge zu erkennen. Prüfen Sie nach der Einrichtung eines VPN regelmäßig, ob Softwareupdates verfügbar sind, und wenden Sie diese umgehend an [12].

- Vorbereitung einen starken Anstieg der Nutzung. IT-Sicherheitspersonal sollte VPN-Beschränkungen in Vorbereitung auf den Masseneinsatz testen [2].
- Vermeidung kostenloser VPNs. Die Nutzung kostenloser VPNs birgt das Risiko von Werbung, Malware und Datenlecks. [3].