Name: _____ Datum: _____ Punkte: _____

TEIL 11

10 interessante VPN-Fakten und Einblicke aus der Praxis

Interaktives Arbeitsblatt und Lernhilfe

Basierend auf VPN-Leitfaden von VPN.com öffnen: **https://www.vpn.com/de/vpn/**

Arbeitsblatt „Was ist ein VPN?“

Teil 11: 10 interessante VPN-Fakten und Einblicke aus der Praxis

Lernen Sie diese besonders wertvollen, realen Fakten und Erkenntnisse zur Geschichte, zum Markt und zur Technologie von VPNs kennen.

1. ERSTES VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol) wurde von einer Herstellergruppe unter Beteiligung von Microsoft entwickelt und im Juli 1999 als RFC 2637 veröffentlicht, um VPNs für den Fernzugriff zu unterstützen. [6]

2. MARKTBEWERTUNG

Der weltweite VPN-Markt ist rasant gewachsen, angetrieben durch steigende Anforderungen an Remote-Arbeit und die Sicherheitsbedürfnisse von Unternehmen.

3. WIREGUARD-REVOLUTION

WireGuard hat eine stark verschlankte, auf Effizienz ausgelegte Codebasis, die sich leichter auf Sicherheitslücken prüfen lässt als herkömmliche Protokolle. [4]

4. STRENGE PRÜFSTANDARDS

Führende VPN-Anbieter beauftragen externe Prüfer (wie Cure53 oder PwC) mit unabhängigen Code-Reviews, um zu bestätigen, dass sie keine Nutzeraktivitäten protokollieren.

5. URSPRÜNGE DER 5-EYES-ALLIANZ

Die Five-Eyes-Allianz ging aus dem UKUSA-Abkommen von 1946 zur Fernmeldeaufklärung zwischen den USA und Großbritannien hervor; später kamen Kanada, Australien und Neuseeland hinzu.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) untersucht Paketinhalte und Verkehrsmuster, nicht nur Header, und einige Firewalls nutzen sie, um gängige VPN-Protokolle zu erkennen und zu blockieren.

7. NUTZUNG IN UNTERNEHMEN

Ein großer Teil der Beschäftigten in Unternehmen weltweit nutzt sichere VPNs, um sich bei internen Datenbanken anzumelden, was VPNs zu einem wichtigen Sicherheitsstandard macht.

8. DEZENTRALE VPNS

Dezentrale VPNs (dVPNs) verteilen den Datenverkehr über ein Netzwerk von Knoten, die von Teilnehmern betrieben werden, und verringern so die Abhängigkeit von einem einzigen zentralen Anbieter.

9. ANONYMITÄT: TOR VS. VPN

Ein VPN leitet den Datenverkehr durch einen einzigen Anbieter, während Tor (The Onion Router) ihn über drei freiwillig betriebene Relays (Guard, Middle und Exit) schickt, sodass kein einzelnes Relay beide Enden kennt.

10. KOSTEN VON DATENPANNEN

Ein Zero-Trust-Modell für den sicheren Zugriff mit VPN hilft Organisationen, geistiges Eigentum zu schützen und die finanziellen Folgen von Datenpannen abzumildern.

Technische Referenzen und Quellen

Zitierte Veröffentlichungen, kryptografische Spezifikationen und offizielle Dokumentstandards, die in diesem Arbeitsblatt verwendet werden.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637