Naam: _____ Datum: _____ Score: _____

DEEL 11

10 interessante VPN-feiten en inzichten uit de praktijk

Interactief werkblad en studiegids

Gebaseerd op de VPN.com-VPN-gids: **https://www.vpn.com/nl/vpn/**

Werkblad: wat is een VPN

Deel 11: 10 interessante VPN-feiten en inzichten uit de praktijk

Bekijk deze waardevolle feiten en inzichten uit de praktijk over de geschiedenis, de markt en de technologie van VPN's.

1. EERSTE VPN-PROTOCOL

PPTP (Point-to-Point Tunneling Protocol) is ontwikkeld door een groep leveranciers, waaronder Microsoft, en in juli 1999 gepubliceerd als RFC 2637 om VPN's voor toegang op afstand te ondersteunen. [6]

2. MARKTWAARDERING

De wereldwijde VPN-markt is snel gegroeid, aangedreven door de toenemende behoefte aan thuiswerken en de beveiligingseisen van bedrijven.

3. DE WIREGUARD-REVOLUTIE

WireGuard heeft een sterk gestroomlijnde codebase die is ontworpen voor efficiëntie, waardoor het gemakkelijker te controleren is op beveiligingslekken dan traditionele protocollen. [4]

4. STRIKTE AUDITSTANDAARDEN

Toonaangevende VPN-aanbieders huren externe auditors in (zoals Cure53 of PwC) voor onafhankelijke code-reviews en om te verifiëren dat ze geen gebruikersactiviteit loggen.

5. OORSPRONG VAN DE 5-EYES-ALLIANTIE

De Five Eyes-alliantie is ontstaan uit de UKUSA-overeenkomst voor signalenspionage uit 1946 tussen de VS en het VK, waarbij later Canada, Australië en Nieuw-Zeeland zich aansloten.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) onderzoekt de inhoud van pakketten en verkeerspatronen, niet alleen headers, en sommige firewalls gebruiken het om veelgebruikte VPN-protocollen te detecteren en te blokkeren.

7. ZAKELIJK GEBRUIK

Een groot percentage van de werknemers van ondernemingen wereldwijd gebruikt beveiligde VPN's om in te loggen op interne databases, waardoor het een belangrijke beveiligingsstandaard is.

8. GEDECENTRALISEERDE VPN'S

Gedecentraliseerde VPN's (dVPN's) verdelen verkeer over een netwerk van nodes die door peers worden beheerd, waardoor er minder afhankelijkheid is van één gecentraliseerde aanbieder.

9. TOR TEGENOVER VPN-ANONIMITEIT

Een VPN tunnelt verkeer via één aanbieder, terwijl Tor (The Onion Router) verkeer via drie vrijwilligersrelays stuurt (guard, middle en exit), zodat geen enkele relay beide uiteinden kent.

10. KOSTEN VAN DATALEKKEN

Het hanteren van een zero-trust-toegangsmodel met een VPN helpt organisaties intellectueel eigendom te beschermen en de financiële impact van datalekken te beperken.

Technische referenties en bronnen

Geciteerde publicaties, cryptografische specificaties en officiële documentstandaarden die in dit werkblad worden gebruikt.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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