Jméno: _____ **Datum:** _____ **Body:** _____

ČÁST 11

10 zajímavých faktů o VPN a poznatků z praxe

Interaktivní pracovní list a studijní příručka

Podle průvodce VPN od VPN.com: **https://www.vpn.com/cs/vpn/**

Pracovní list Co je VPN

Část 11: 10 zajímavých faktů o VPN a poznatků z praxe

Projděte si tato velmi cenná fakta a poznatky z praxe o historii, trhu a technologii VPN.

1. PRVNÍ VPN PROTOKOL

PPTP (Point-to-Point Tunneling Protocol) byl vyvinut skupinou dodavatelů včetně Microsoftu a publikován jako RFC 2637 v červenci 1999 pro podporu VPN se vzdáleným přístupem. [6]

2. TRŽNÍ OCENĚNÍ

Globální trh s VPN zažil rychlý růst, tažený rostoucími požadavky práce na dálku a poptávkou po podnikové bezpečnosti.

3. REVOLUCE WIREGUARD

WireGuard má vysoce zjednodušenou kódovou základnu navrženou pro efektivitu, takže se snáze audituje na bezpečnostní zranitelnosti než tradiční protokoly. [4]

4. PŘÍSNÉ AUDITNÍ STANDARDY

Přední poskytovatelé VPN najímají externí auditory (jako Cure53 nebo PwC) k nezávislým revizím kódu a ověření, že nelogují žádnou aktivitu uživatelů.

5. POČÁTKY ALIANCE 5 OČÍ

Aliance Five Eyes vyrostla z dohody UKUSA o signálovém zpravodajství z roku 1946 mezi USA a Spojeným královstvím, k níž se později připojily Kanada, Austrálie a Nový Zéland.

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Hloubková inspekce paketů (DPI) zkoumá obsah paketů a vzorce provozu, nejen hlavičky, a některé firewally ji používají k detekci a blokování běžných VPN protokolů.

7. FIREMNÍ VYUŽITÍ

Velké procento zaměstnanců podniků po celém světě používá zabezpečené VPN k přihlašování do interních databází, což z nich činí klíčový bezpečnostní standard.

8. DECENTRALIZOVANÉ VPN

Decentralizované VPN (dVPN) rozdělují provoz přes síť uzlů provozovaných jednotlivci, čímž snižují závislost na jediném centralizovaném poskytovateli.

9. ANONYMITA TOR VS. VPN

VPN tuneluje provoz přes jediného poskytovatele, zatímco Tor (The Onion Router) posílá provoz přes tři dobrovolnická relé (vstupní, prostřední a výstupní), takže žádné jednotlivé relé nezná oba konce.

10. NÁKLADY NA ÚNIKY DAT

Zavedení modelu zabezpečeného přístupu zero-trust s VPN pomáhá organizacím chránit duševní vlastnictví a zmírnit finanční dopad úniků dat.

Technické reference a zdroje

Citované publikace, kryptografické specifikace a oficiální dokumentační standardy použité v celém tomto pracovním listu.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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