Imię i nazwisko: _____ Data: _____ Wynik: _____

CZĘŚĆ 11

10 ciekawych faktów o VPN i spostrzeżeń z praktyki

Interaktywna karta pracy i przewodnik

Na podstawie przewodnik VPN.com po VPN: **https://www.vpn.com/pl/vpn/**

Karta pracy: Czym jest VPN

Część 11: 10 ciekawych faktów o VPN i spostrzeżeń z praktyki

Przejrzyj te bardzo cenne, prawdziwe fakty i spostrzeżenia dotyczące historii, rynku i technologii VPN.

1. PIERWSZY PROTOKÓŁ VPN

PPTP (Point-to-Point Tunneling Protocol) został opracowany przez grupę dostawców, w tym Microsoft, i opublikowany jako RFC 2637 w lipcu 1999 roku, aby obsługiwać VPN do dostępu zdalnego. [6]

2. WYCENA RYNKOWA

Globalny rynek VPN szybko rośnie, napędzany rosnącymi potrzebami pracy zdalnej i wymaganiami bezpieczeństwa w przedsiębiorstwach.

3. REWOLUCJA WIREGUARD

WireGuard ma bardzo uproszczoną bazę kodu zaprojektowaną z myślą o wydajności, co ułatwia jego audyt pod kątem luk w zabezpieczeniach w porównaniu z tradycyjnymi protokołami. [4]

4. ŚCISŁE STANDARDY AUDYTU

Czołowi dostawcy VPN zatrudniają zewnętrznych audytorów (takich jak Cure53 czy PwC), aby przeprowadzali niezależne przeglądy kodu i weryfikowali, że nie rejestrują aktywności użytkowników.

5. POCHODZENIE SOJUSZU 5 EYES

Sojusz Five Eyes wyrósł z porozumienia UKUSA z 1946 r. o wywiadzie sygnałowym między USA a Wielką Brytanią, do którego później dołączyły Kanada, Australia i Nowa Zelandia.

6. GŁĘBOKA INSPEKCJA PAKIETÓW

Głęboka inspekcja pakietów (DPI) bada zawartość pakietów i wzorce ruchu, a nie tylko nagłówki, a niektóre zapory sieciowe używają jej do wykrywania i blokowania popularnych protokołów VPN.

7. UŻYTKOWANIE KORPORACYJNE

Duży odsetek pracowników przedsiębiorstw na całym świecie korzysta z bezpiecznych VPN, aby logować się do wewnętrznych baz danych, co czyni to kluczowym standardem bezpieczeństwa.

8. ZDECENTRALIZOWANE VPN-Y

Zdecentralizowane sieci VPN (dVPN) rozdzielają ruch w sieci węzłów prowadzonych przez użytkowników, zmniejszając zależność od jednego scentralizowanego dostawcy.

9. ANONIMOWOŚĆ: TOR A VPN

VPN tuneluje ruch przez jednego dostawcę, a Tor (The Onion Router) kieruje ruch przez trzy przekaźniki wolontariuszy (wejściowy, środkowy i wyjściowy), tak że żaden pojedynczy przekaźnik nie zna obu końców połączenia.

10. KOSZT NARUSZEŃ OCHRONY DANYCH

Zastosowanie modelu bezpiecznego dostępu zero trust z VPN pomaga organizacjom chronić własność intelektualną i łagodzić skutki finansowe naruszeń danych.

Źródła i odnośniki techniczne

Cytowane publikacje, specyfikacje kryptograficzne i oficjalne standardy dokumentów wykorzystane w tej karcie pracy.

PUBLIKACJE NAUKOWE I BRANŻOWE

[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