SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed til dig

Virtuelle Private Netværk (VPN)

Oversigt

Du kan være nødt til at bruge offentlig Wi-Fi til internetadgang, når du er hjemmefra, f.eks. når du er hos din lokale restaurant eller café eller når du rejser og er på et hotel eller i en lufthavn. Men hvor sikre er disse offentlige netværk? Hvem holder øje med dig eller registrerer, hvad du laver online? Måske stoler du ikke engang på din internetudbyder hjemme hos dig selv og vil gerne være sikker på, at de ikke kan overvåge, hvad du laver online. Du kan beskytte dine onlineaktiviteter og privatliv med noget, der hedder en VPN (Virtual Private Network). En VPN er en teknologi, der opretter en privat krypteret tunnel til din onlineaktivitet, hvilket gør det meget vanskeligere for andre at se eller overvåge, hvad du laver online. Derudover hjælper en VPN med at skjule din placering, hvilket gør det meget sværere for websteder, du besøger, at bestemme, hvor du befinder dig.

Hvordan virker det?

En VPN virker ved at oprette en privat krypteret tunnel til en VPN-udbyder, som du vælger. Al din onlineaktivitet går gennem denne tunnel, og efterlader derefter din VPN-udbyderens netværk til din ønskede destination. For eksempel, hvis du er baseret i Tampa, Florida, og du forbinder til en VPN-server i München, Tyskland, vil enhver hjemmeside, du opretter forbindelse til, tro at du forbinder fra München, Tyskland. En VPN er nem at bruge. Det første skridt er at finde en VPN-udbyder, du stoler på, og derefter oprette en konto hos dem (det kræver normalt, at du køber deres service). Når du har en konto, downloader du, installerer og konfigurerer deres VPN-software. Når du har installeret og konfigureret, skal du oprette forbindelse til internettet, som du altid gør. VPN-softwaren vil oprette din krypterede tunnel og begynde at beskytte dit privatliv uden du selv bemærker noget.

Valg af VPN-udbyder

Dine onlineaktiviteter er kun lige så sikre og private som din VPN-udbyder. Sørg for at vælge en, du kan stole på. Her er nøglepunkter, når du vælger en VPN-udbyder.

Logging: Søg efter en tjeneste, der ikke logger din trafik og som fokuserer på privatlivets fred. Hvis din VPN-udbyder ikke indsamler logfiler, er det meget sværere for andre at gå tilbage og se, hvad du har lavet online.

Hvor er selskabet baseret: Forskellige VPN-udbydere er baseret i forskellige lande. Vær sikker på at du vælger en VPN-udbyder, der er baseret i et land, der har stærke privatlivslovgivning. VPN-udbydere i lande, der har meget få eller svage privatlivslovgivning, kan blive tvunget til at opgive oplysninger, de indsamler på dig.

Servere: Søg efter en VPN-tjeneste, der har serverne placeret i de lande eller byer, du har brug for. Nogle VPN-udbydere har tusindvis af servere og steder over hele kloden. Har du behov for at få dine forbindelser vist som om de kommer fra et bestemt land, skal du tjekke at din VPN-udbyder det?

Kompatibilitet: Søg efter tjenester, der fungerer på tværs af forskellige computere og mobile enheder. Du kan f.eks. bruge en Windows-bærbar computer, en tablet og en iPhone. Du vil have en VPN-tjeneste, som vil fungere på alle disse enheder.

Undgå gratis: Vær meget forsigtig med "gratis" VPN-tjenester, de skal tjene penge og holder forretningen kørende? Gratis tjenester tjener måske penge ved at indsamle og sælge dine oplysninger.

En VPN er en fantastisk måde at hjælpe med at beskytte dit privatliv på internettet. En VPN gør dog ikke noget for at sikre din computer, mobile enheder eller dine online-konti. Så selvom du bruger en VPN, skal du sørge for, at du altid følger de grundlæggende sikkerhedsforanstaltninger, dvs. sikre, at dine enheder opdateres, brug et skærmlås, og brug altid stærke, unikke adgangskoder til alle dine konti.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Phil Johnsey *(@peakreflections) arbejder med IT hos "Palm Beach County" og har erfaring inden for sikkerhed og forensics. Han er SANS certificeret i "digital forensics", "security essentials", og medlem af "OUCH community review board". Han arbejder for at gøre IT-sikkerhed mere simpelt for andre.*

Hvis du vil vide mere

Making Passwords Simple:	https://www.sans.org/u/Sd8
Securing Your Mobile Devices:	https://www.sans.org/u/Sdd
Stop Malware:	https://www.sans.org/u/Sdi