SANS SECURITY AWARENESS

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Virtuelt Privat Nettverk (VPN)

Oversikt

Når du ikke er hjemme eller på jobb vil det av og til oppstå situasjoner hvor du ser deg nødt til å bruke offentlige trådløse nettverk for å komme på nett, f.eks. på en restaurant, en kafé, på hotell, eller på en flyplass. Men hvor sikre er disse offentlige trådløsnettene? Og hvem følger med på og overvåker det du gjør over nettverket? Kanskje du ikke engang stoler på bredbåndsleverandøren du har hjemme, og vil forsikre deg om at de ikke kan overvåke deg. Du kan beskytte personvernet ditt og skjule nettaktiviteten din med noe som kalles VPN (Virtuelt Privat Nettverk). VPN er teknologi som lager en privat, kryptert tunell for nettaktiviteten din, som gjør det langt vanskeligere for enhver som ønsker å overvåke det du gjør på nett. I tillegg hjelper VPN med å skjule hvor du bruker nettet fra, som gjør det vanskeligere for nettsider å avgjøre hvor du befinner deg.

Hvordan fungerer det?

Med VPN settes det opp en privat, kryptert tunell til en VPN-leverandør du velger. All internettaktiviteten din går gjennom denne tunellen, før den går ut på nettet fra VPN-leverandørens server, og til destinasjonen (f.eks. en nettside eller en e-postserver). For eksempel, dersom du befinner deg i Gjøvik i Norge, og kobler til en VPN-leverandør i München i Tyskland, så vil enhver nettside du besøker tro at du befinner deg i München. VPN er enkelt å bruke. Det første steget er å finne en VPN-leverandør du kan stole på, og så sette opp en brukerkonto hos dem (dette innebærer som oftest at du kjøper tjenesten av dem). Når du har en brukerkonto, kan du laste ned, installere og konfigurere VPN-programvaren deres. Når installeringen og konfigurasjonen er ferdig, kan du aktivere VPN-en og gå på nett slik du alltid gjør. VPN-programvaren vil sette opp den krypterte tunellen og sikre trafikken din i bakgrunnen, uten at du trenger å tenke på det.

Valg av VPN-leverandør

Internettaktiviteten din er ikke sikrere enn VPN-leverandøren du velger, så sørg for å velge en du kan stole på. Her har du noen nøkkelpunkter for når du skal velge en VPN-leverandør:

Logging: Se etter en leverandør som ikke beholder logger, og fokuserer på personvern. Hvis VPN-leverandøren ikke loggfører aktiviteten til brukerne, er det mye vanskeligere for noen å gå tilbake i etterkant for å se hva du har gjort på nettet.

Hvor er firmaet basert: Forskjellige VPN-leverandører er basert i forskjellige land. Sørg for å velge en VPN-leverandør som er basert i et land med gode lover og regler for personvern. VPN-leverandører som er basert i land hvor personvernet ikke står sterkt, kan havne i en situasjon hvor de blir tvunget til å oppgi informasjonen de har om deg.

Servere: Se etter en VPN-leverandør som har serverne sine i de landene eller byene du har behov for. Noen VPN-leverandører har tusenvis av servere rundt om kring på hele kloden. Har du behov for at det ser ut som om trafikken din kommer fra spesifikke land, og kan VPN-leverandøren tilby servere i disse landene?

Kompatibilitet: Se etter VPN-tjenester som kan brukes på tvers av forskjellige typer datamaskiner og mobile enheter. For eksempel bruker du kanskje en laptop med Windows, et nettbrett, og en iPhone. I så fall er du nok ute etter en VPN-tjeneste som kan brukes på alle disse enhetene.

Unngå gratistjenester: Vær på vakt overfor «gratis» VPN-tjenester. Hvordan tjener de penger og holder seg gående? Gratistjenester lever ofte av å samle og videreselge informasjon om brukerne sine.

Internettaktiviteten din er ikke sikrere enn VPN-leverandøren du velger, så sørg for å velge en du kan stole på. Her har du noen nøkkelpunkter for når du skal velge en VPN-leverandør:

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Phil Johnsey *(@peakreflections) er en IT-proff ved Palm Beach County med erfaring innen sikkerhet, digital etterforskning, og revisjon. Han er SANS-sertifisert innen digital etterforskning og sikkerhetskrav, og sitter i styret for OUCH-fellesskapet. Å gjøre sikkerhet enkelt for andre er hans store lidenskap.*

Ressurser

Passord gjort enkelt:	https://www.sans.org/u/Sd8
Sikre dine mobile enheter:	https://www.sans.org/u/Sdd
Stopp skadevaren:	https://www.sans.org/u/Sdi