ADVIESKAART

DIGITALE REISVEILIGHEID

Zomer 2023

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Op (zaken)reis? Afhankelijk van de bestemming en de situatie daar, liggen er verschillende digitale dreigingen op de loer. Houd je daarom aan de volgende reisadviezen:

1 > GEBRUIK EEN VPN

Op reis ontkom je er vaak niet aan om onveilige netwerken te gebruiken. Een VPN stuurt al je dataverkeer door een apart beveiligde, versleutelde 'tunnel' naar het internet. Zo voorkom je lokale informatiediefstal, zelfs als je verbindt via een onveilig netwerk.

2 > GEBRUIK BEVEILIGDE GEGEVENSDRAGERS

USB-sticks, externe harde schijven, laptops en mobiele telefoons zijn aantrekkelijk voor kwaadwillenden. Er is weinig tijd nodig om ze ongemerkt uit te lezen, bijvoorbeeld tijdens een douane-inspectie of in een hotelkamer. Versleutel daarom de dataopslag van alle apparatuur en sla gevoelige gegevens enkel op versleutelde, externe gegevensdragers op.

3 > HOUD JE APPARATUUR IN HET OOG

Laat apparatuur nooit onbeheerd achter en verzegel de gevoeligste apparatuur met stickers of een druppel nagellak langs de randen van behuizingen zodat je fysieke toegang door een onbekende kunt herkennen. Dat helpt voorkomen dat men data steelt of malware installeert.

4 > GEBRUIK UNIEKE, STERKE WACHTWOORDEN

In onvertrouwde omgevingen bestaat een aanzienlijk risico op fysiek of digitaal 'meekijken' om wachtwoorden te achterhalen. Gebruik daarom een uniek, sterk wachtwoord voor elk online account en sla deze wachtwoorden op in een password manager.

5 > GEBRUIK BEVEILIGDE CHAT-APPS VOOR COMMUNICATIE

In hoogrisicolanden* kun je ervan uitgaan dat men telefoongesprekken afluistert en sms'jes meeleest. Daarom is het een goede gewoonte om te communiceren via versleutelde chat-apps voor telefoongesprekken en voor het sturen van berichten.
Deze beveiligde apps bieden 'end-to-end encryption'.

6 > MAAK EEN BACK-UP

Voorkom dat bestanden verloren gaan. Maak voor vertrek een back-up op een externe harde schijf of in de cloud. Bewaar een back-up bij voorkeur altijd op twee plaatsen: in huis en buitenshuis.

7 > ZORG VOOR ANTIVIRUSSOFTWARE

Dit geldt ook voor iPhones en iPads, al denken veel gebruikers dat deze standaard goed beveiligd zijn.

8 > VERGRENDEL JE MOBIELE APPARATEN

Bijvoorbeeld door middel van een pincode, wachtwoord, biometrisch, etc.

*Hoogrisicolanden: landen in gewapend confl ict (bijv. Oekraïne) of landen met een streng oppressief of autoritair regime (bijv. China)

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant
Secura
A BUREAU VERITAS COMPANY