

End-to-end encryptie (E2EE)



Wat is het?

- End-to-end encryptie (of versleuteling) houdt in dat verzender en ontvanger hun communicatie versleuteld hebben op hun eigen apparaten en niet bij een derde.
- Doordat alleen de verzender en ontvanger de boodschap kan ontsleutelen is, is de communicatie niet in te zien door derden tijdens het versturen.
- Kernpunt is dat verzender en ontvanger elkaar vertrouwen, dus bijvoorbeeld van elkaar weten wie ze zijn.
- End-to-end encryptie geeft een hoge mate van zekerheid dat de privacy van communicatie gewaarborgd wordt.
- Het werkt alleen goed als de gebruikte apparaten (zoals smartphone) niet gehackt zijn.

Belang voor Nederland



- Het is essentieel voor het onderlinge vertrouwen van burgers en bedrijven dat zij zekerheid hebben dat hun online communicatie niet afgeluisterd of veranderd kan worden.
- Vertrouwen in de integriteit van (privé)communicatie is essentieel voor het gevoel van persoonlijke veiligheid.
- Vrijheid (van meningsuiting) vereist ook dat men zich veilig voelt om te communiceren.
- Vertrouwen dat informatie niet ingezien of veranderd kan worden door een aanval is essentieel voor zakelijk gebruik van digitale communicatie (bijvoorbeeld bij online transacties).

Gevolgen van misbruik

- Schade aan mens/omgeving
 - Bijvoorbeeld beïnvloeden/benadelen van mensen door deze om te leiden naar verkeerde informatie of kwaadaardige bestanden, onderscheppen van (vertrouwelijke) digitale communicatie.
- Verlies intellectueel eigendom
 - Bijvoorbeeld samenstelling metaal, ontwerp van een chip, ontwerp fabriek.
- Politiek/commercieel
 - Bijvoorbeeld verkenning voor sabotage, chanteren, verlies van vertrouwen, concurrentievervalsing/namaak.





Is misbruik al eens voorgekomen?

Ja, bekende voorbeelden:

- In Iran kon de overheid in privémails van o.a. Google meelezen waardoor dissidenten zijn opgepakt.
- Snowden heeft meerdere voorbeelden gegeven van aanvallen door de VS.
- Kwetsbaarheden in de implementatie van end-to-end encryptie heeft mensen in de hele wereld, waaronder Nederland, geraakt.
- Door gebruik van zwakke/verouderde versleuteling kon toch worden meegeluisterd.



Cybercrime specifieke relevante nationale wetgeving of andere richtlijnen

- Geen specifieke wetgeving. Wel indirect via bijvoorbeeld AVG en financiële wetten;



How encryption works (3 minuten)

<https://youtu.be/TlmdsUglGv4>

How does E2EE work? (4 minuten)

<https://youtu.be/lvewypxw4rw>

