Veilig E-mailen

Wat is het?

- Om een e-mail te kunnen versturen, wordt meestal eerst een gebruikersnaam en wachtwoord ingevoerd.
- Een wachtwoord beschermt de email niet ‘onderweg’ tussen verzender en ontvanger, daar moeten een aantal andere maatregelen voor worden getroffen, waardoor ‘veilige e-mail’ ontstaat.
- Wanneer het transport van de e-mail gebeurt met slechte of zelfs zonder versleuteling, is het alsof je een brief verstuurd zonder envelop, iedereen kan de inhoud lezen of er zelfs iets aan veranderen. Het transport van veilige e-mail geschiedt versleuteld, waardoor alleen de bedoelde ontvanger van de e-mail deze kan openen.
- Ook valt van veilige e-mail vast te stellen dat de afzender écht is wie diegene zegt te zijn en niet vervalst is door een kwaadwillende. Daarnaast kan er bij veilige e-mail vanuit worden gegaan dat de inhoud van de e-mail onderweg niet is veranderd.

Belang voor Nederland

- E-mail is een van de meest gebruikte communicatiemiddelen, maar wordt van oudsher helaas vaak op een onveilige manier gebruikt.
- Door gebruik te maken van veilige e-mail kunnen persoonsgegevens, paspoortscans, CV’s en documenten die gevoelige informatie bevatten op veilige wijze uitgewisseld worden.
- Hoe meer veilige e-mail gebruikt wordt, hoe makkelijker spam en phishing e-mails te onderscheiden zijn van echte e-mails wat reputatieschade en hoge kosten kan voorkomen.
- Het gebruik van veilige e-mail is essentieel om het vertrouwen in email te behouden.

Gevolgen bij misbruik

- Kwaadwillenden kunnen e-mailberichten versturen waarvan niet goed vast te stellen is of ze afkomstig zijn van een rechtmatige organisatie of persoon, zogenoemde CEO-fraude.
    - Op die manier kunnen nepberichten verstuurd worden (‘phishing’) om anderen schade te berokkenen met reputatieschade en hoge kosten tot gevolg.
    - Op die manier kan reputatieschade toegebracht worden aan een organisatie door uit hun naam vreemde berichten te e-mailen.
- Kwaadwillende met toegang tot de e-mailcommunicatie kunnen e-mailberichten meelezen, veranderen en zo toegang tot vertrouwelijke stukken of communicatie krijgen.

Is misbruik al eens voorgekomen?

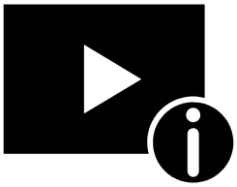
- Ja, zeer vaak dagelijks, zowel nationaal als internationaal.
  - In 2011 werd een e-mailserver van de Australische overheid overgenomen door een andere natie. Gedurende meer dan een jaar kon er met mails van ambtenaren meegelezen worden.
  - Gelekte e-mailberichten verzonden door Amerikaanse topambtenaren zijn herhaaldelijk in het nieuws gekomen, met heftige gevolgen.
  - In 2020 kon in Finland door een hack meegelezen worden met de e-mails van diverse topambtenaren.
  - In 2021 waren meer dan 1200 servers binnen Nederland geïnfecteerd waardoor er meegelezen kon worden met de e-mails die verstuurd werden.

Cybersecurity specifieke relevante nationale wetgeving of andere richtlijnen

- De maatregelen, voortvloeiend uit de Algemene Verordening Gegevensbescherming, beschermen in beperkte mate tegen spam.
- Diverse online beschikbare technische richtlijnen voor verschillende e-mailservers.
- Een aantal internationale technische standaarden om e-mail te versleutelen en te verifiëren of de afzender werkelijk degene is die hij zegt te zijn, zijn PGP, SMIME, SPF, DKIM, DMARK, STARTTLS en DANE.

E-mail en E-mail security in het kort uitgelegd (23 minuten)
https://www.youtube.com/watch?v=tZJoMjEsf4E

Hoe werkt geautomatiseerde E-mail verificatie (4 minuten)
https://www.youtube.com/watch?v=OsdXGiPLnLw



https://www.internet.nl
Tool waar je o.a. kunt testen of jouw of jouw website, e-mail en internetverbinding moderne, betrouwbare internetstandaarden gebruikt en hoe deze te verbeteren.

NCSC over phishing
https://www.ncsc.nl/onderwerpen/phishing