HC 13, 8-01-2019, IT-beveiliging

Tegenwoordig wordt IT-beveiliging information security genoemd. Het gaat veel meer om het beschermen van gegevens. Des te meer toegang er is tot bepaalde gegevens, des te makkelijker de informatie gestolen kan worden.

IT-beveiliging kun je optimaliseren, maar niet garanderen. Er zijn drie functies van IT-beveiliging:

- Vertrouwelijkheid
- Integriteit
- Beschikbaarheid

Beschikbaarheid
Beschikbaarheid houdt in dat gegevens op het juiste moment voorhanden zijn. Er zijn momenteel steeds meer DDoS-aanvallen. Jacobs: 'De nadruk in de ICT-wereld ligt meer op functionaliteit dan op de beveiliging.' Zijn conclusie: 'Wanneer je zelf besluit je tegen cruciale operaties naar het wilde westen van het internet te verplaatsen, moet je natuurlijk wel zorgen dat je eigen pistolen groot genoeg zijn!'

Integriteit en vertrouwelijkheid
Encryptie is het versleutelen van gegevens.
Symmetrische versleuteling: versleuteling en ontsleuteling kan met dezelfde sleutel.
Door **multi-factor** kun je ervoor zorgen dat je account niet gehackt wordt. Dit bestaat uit iets wat je kent (wachtwoord), iets wat je bent (iris, duimafdruk) en iets wat je hebt (sms-bericht). Gezichtsherkenning blijkt niet heel veilig te zijn. Iemand anders met jouw pasfoto kan dan in sommige gevallen ook toegang krijgen tot jouw telefoon.
Een **pentestovereenkomst** is een overeenkomst tussen bedrijven en hackers om hun beveiligingssysteem te laten testen. Dit is niet wederrechtelijk, omdat het in opdracht is van het bedrijf. Hacken vanuit eigen beweging is wel wederrechtelijk en dus strafbaar.
Wanneer ergens een datalek ontstaat moet dit gemeld worden door de instelling (art 33 AVG). De functie hiervan is het beschermen van de belangen en gegevens van de personen wie het datalek betreffen.
Berichten kunnen ook beveiligd worden; dit kan door het gebruik van **end-to-end encryptie. Asymmetrische encryptie** maakt gebruik van twee sleutels die bij elkaar horen, een publieke en een private sleutel. De publieke sleutel is openbaar en de private sleutel is geheim en houdt de gebruiker voor zichzelf. Door de private sleutel te gebruiken kan het bericht ontsleuteld worden. Deze wijze wordt ook wel private-key encryptie genoemd. Deze manier wordt vaak op het internet gebruikt door mensen die elkaar niet kennen, maar wel berichten naar elkaar willen versturen. Bij asymmetrische encryptie wordt vaak gebruik gemaakt van een 'trusted third party'. Door deze partij wordt de identiteit van de gebruikers geverifieerd en deze partij maakt ook de private sleutels en geeft deze aan de gebruikers.