Lexicon

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit en ook het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen [1].

Cybersecurity alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.

Datasecurity gaat over de bescherming gedurende de gehele lifecycle van digitale informatie tegen bedoelde of onbedoelde aanpassing, verwijdering, diefstal of openbaarmaking van data door ongeautoriseerde personen.

Cybersafety kent twee betekenissen:

1. De veiligheid en betrouwbaarheid van het geautomatiseerde systeem: dat componenten betrouwbaar werken en hun functies kunnen vervullen om, bijvoorbeeld, beschermd te zijn tegen oververhitting [2] en

2. Cybersafety is kort gezegd online veilig zijn. Cybersafety helpt je met het ontwijken van gevaren, maar helpt je ook je te beschermen tegen de gevolgen ervan. Je kunt namelijk niet alles ontwijken. Sommige aanvallen overkomen je, hoewel je aan alle gangbare beveiligingseisen voldoet [3].

Referenties

[1] Art. 1 onder k Besluit CIO-stelsel Rijksdienst 2021

[2] Fraunhofer magazine 3, 2021, p. 44: fraunhofer.de/s/ePaper/magazine/2021/03/index.html

[3] https://www.utwente.nl/nl/cyber-safety/cybersafety/