# *Informatiebeveiliging*

**Wat is het?**

- Informatiebeveiliging is de verzameling van processen en afspraken die ervoor zorgen dat de risico's bij het werken met informatie, beheersbaar blijven.
- Een belangrijk onderdeel van informatiebeveiliging is risicomanagement. Dit proces zorgt ervoor dat de verantwoordelijkheden voor het inzichtelijk maken van risico's en het bepalen en (laten) doorvoeren van tegenmaatregelen, op de juiste plekken binnen een organisatie worden belegd.
- Informatie is, naast arbeid, kapitaal en natuur, in deze tijd een vierde productiefactor. Het beheer van informatie, en dus ook de beveiliging ervan, vraagt om die reden om aandacht en sturing vanuit directies en bestuurders.
- Hoewel informatie vandaag de dag veel met de computer wordt verwerkt, bevat informatiebeveiliging ook veel niet-technische componenten.
- Informatie is niet hetzelfde als data. Data die gecombineerd en/of geïnterpreteerd (kunnen) worden vormen informatie.

**Belang voor Nederland**

- Ook in Nederland beschikken de overheid, organisaties en burgers over vertrouwelijke en belangrijke informatie waar ze in zekere mate van afhankelijk zijn. Goede beveiliging van die informatie is bittere noodzaak.
- De Nederlandse economie speelt zich voor een belangrijk deel af in het digitale domein, waarbij de verwachting is dat dat alleen maar meer wordt. Goede informatiebeveiliging is noodzakelijk om dat deel van die economie draaiende te houden.

**Gevolgen bij misbruik**

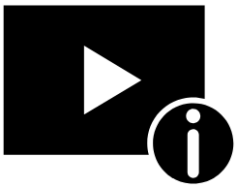
- Informatie is in veel gevallen nodig bij het fabriceren van producten of de levering van diensten. Het schaden van de beschikbaarheid of integriteit van informatie, brengt de continuïteit van de levering van producten en diensten in gevaar.
- Informatie bevat kennis en kennis is macht. Het schaden van de vertrouwelijkheid van informatie, bijvoorbeeld staatsgeheimen of bedrijfsgeheimen, brengt deze machtspositie in gevaar.

**Is misbruik al eens voorgekomen?**

- Voorbeelden van incidenten in binnen- en buitenland zijn er in overvloed. Dit zijn de vele datalekken, ransomware-incidenten, systeem-uitvallen, hacks door statelijke actoren, criminelen en script-kiddies (personen die zich misdragen op het internet) en diefstallen van concurrentiegevoelige informatie. Grote incidenten halen met enige regelmaat het nieuws. Echter vele, vaak kleinere, incidenten die niet het nieuws halen, blijven daarmee voor het grote publiek onopgemerkt.

**Cybersecurity specifieke relevante nationale wetgeving of andere richtlijnen**

- Wbni (Wet Beveiliging Netwerk- en Informatiesystemen)
- BIO (Baseline Informatiebeveiliging Overheid)
- ISO 2700x (internationale normen-serie voor informatiebeveiliging)
- NEN 7510 (informatiebeveiligingsnorm voor de zorgsector)



**Cyber Security in 7 Minutes | What is Cyber Security: How it works?**
https://www.youtube.com/watch?v=inWWhr5tnEA

netherlands by Sem Schilder from the Noun Project

Exclamation Mark by Hea Poh Lin from the Noun Project