**Wat is een BIV-factor?**

**B** - Beschikbaarheid

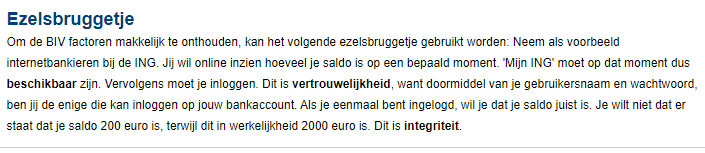
Is de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers

**I** - Integriteit

Is de mate waarin gegevens of functionaliteit juist en volledig is

**V** - Vertrouwelijkheid

De mate waarin toegang tot gegeven en functionaliteit beperkt is tot degene daartoe bevoegd zijn



**Verschil tussen kwetsbaarheid, bedreiging en risico**

**Kwetsbaarheid**

* De mate waarin een object gevoelig is voor een bedreiging
* Een bedreiging maakt misbruik van een kwetsbaarheid

**Bedreiging**

* Is een process of een gebeurtenis met een potentieel verstorende invloed op de betrouwbaarheid
* Menselijke bedreigingen:
  + Opzettelijk foutief handelen
  + Misbruik en criminaliteit
* Niet menselijke bedreigingen:
  + Invloed van buitenaf
  + Storing in de basisinfrastructuur

**Risico**

* Het gemiddelde van de verwachte schade over een gegeven tijdsperiode (wordt veroorzaakt door een verstoring van een of meerdere objecten van de informatievoorziening)
* Risico = Kans \* Impact
* Schade kan van financiële aard zijn en omvat:
  + Directe schade
  + Indirecte schade

**Wat zijn de verschillende ISM-invalshoeken?**

* Cyber security
* Productiviteit
* Toegankelijkheid voor mensen die erbij moeten kunnen
* Openheid
* Preventieve maatregelen
  + Voorkomen van probleem
* Detectieve maatregelen
  + Detecteren van probleem
* Repressieve maatregelen
  + Impact van het probleem verkleinen
* Correctieve maatregelen
  + Het voorkomen van herhaling van een bepaald probleem

**Wat zijn de juridische aspecten van informatiebeveiliging?**

Veel bedrijven moeten transparant zijn van de overheid en dit neemt problemen met zich mee voor informatiebeveiliging

**Wat is het proces van security management?**

PDCU / Deming-cyclus

**P**lan. **D**o, **C**heck, **A**ct

*Zie paragraaf 3.3 in het boek en figuur 3.2*

*blz 22-23*

The 5th domain of warfare is **cyber.**