**Security Essentials Aantekeningen**Een bedreiging gebruikt een kwetsbaarheid om schade aan te richten. De kans dat een bedreiging schade aanricht x de schade die wordt aangericht is de risicofactor.  
**De waarde die gegevens voor een organisatie hebben, hangt af van een aantal factoren**  
  
- Het procesbelang

De mate waarin bedrijfsprocessen die gebruikmaken van de betreffende gegevens van belang zijn voor de organisatie.

- De onmisbaarheid

Het belang van de betreffende gegevens voor de bedrijfsprocessen die er gebruik van maken.

- Het belang voor derden

De mate waarin derden (klanten, leveranciers of concurrenten) belang hechten aan de betreffende gegevens.

**Gegevens**

Gegevens kunnen gezien worden als de objectief weerneembare weerslag van feiten in een drager. Informatie is de betekenis die de mens aan de hand van bepaalde gevoelens of afspraken aan de gegevens toekent.  
  
Voorbeeld:   
  
Gegevens: 22122001 > Pincode? Locatienummer? ….

Informatie: 22-12-2001 > Geboortedatum!

Gegevens > Gegevensverwerking > informatie

Een informatiesysteem (**IS**) verzamelt gegevens, verwerkt deze en slaat ze op of verspreid ze, ook als het nodig is kan een informatiesysteem een correctie uitvoeren.

Invoer > Verwerking > (opslag) > Uitvoer > (correctie) > invoer  
  
**Informatievoorziening**

Als we praten over een informatievoorziening (**IV**) Dan gaat het over de IT-infrastructuur, dit bestaat uit de volgende componenten:  
  
 - Appratuur

- Basisprogrammatuur

- Besturingssystemen

- Communicatievoorzieningen

Een informatievoorziening ziet er als volgt uit:  
  
Graphical user interface

Description automatically generated

Een informatievoorziening heeft een basisstructuur:

- Elektriciteitsvoorziening

- Airconditioning

- Gebouwen en ruimten

- Kasten en meubilair

**Bedreiging, kwetsbaarheid en risico**

Een bedreiging is een proces of gebeurtenis met de potentie een verstorende invloed op een object (asset) uit te oefenen.  
  
\*Een object of asset is waar een bedrijf waarde aan hecht (procesbelang, onmisbaarheid en belang van derden).  
  
De betrouwbaarheid van een object bestaat uit 3 aspecten, deze noemen we de BIV.

- Beschikbaarheid  
Dit is de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.

- Integriteit  
Dit is de mate waarin gegevens of functionaliteit juist en volledig zijn.

- Vertrouwelijkheid

Dit is de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Hieronder zie je een schema met aspecten van betrouwbaarheid en daaraan gerelateerde bedreigingen:

Table

Description automatically generated

**Bedreigingen onderverdeeld**

Bedreigingen kunnen worden onderverdeeld in 2 groepen:

1. Menselijke bedreigingen

* Onopzettelijk foutief handelen door gebruikers: beheerders, gasten of extern personeel.
* Misbruik en criminaliteit: diefstal, inbraak, hacking, sabotage of fraude

1. Niet-menselijke bedreigingen

* Invloeden van buitenaf: aardbeving, storm, wateroverlast of brand.
* Storingen in de basisinfrastructuur: zoals uitval van elektriciteit.
* Storingen in appratuur: programmatuur of gegevensbestanden.

**Risicofactor**

Een risico is een combinatie van de kans dat een bedreiging zich manifesteert en de mogelijke schade hiervan, aldus **kans op schade x schade**. Deze formule berekend de schadeverwachting over een gegeven tijdsperiode. Dit wordt aangeduid in een Jaarlijkse Schade Verwachting (**JSV**) anders Annual Loss Expectancy (**ALE**) genoemd.

De in aanmerking te nemen schade kan al dan niet van financiële aard zijn en omvat:

* De directe schade: aan rechtstreeks getroffenen, zoals personen, apparatuur, programmatuur, gegevensverzamelingen en gebouwen.
* De Indirecte schade: (gevolgschade) zoals verstoringen van bedrijfsprocessen, het overtreden van wetten, het verlies van opdrachten en imagoschade.

**Beveiligingsmaatregelen**

Door het treffen van beveiligingsmaatregelen kan je risico’s verkleinen, beveiligingsmaatregelen zijn kostenposten. Een vermindering van de functionaliteit van een informatievoorziening moet ook worden gezien als kostenpost.

Bij het treffen van beveiligingsmaatregelen zijn er 3 klassen:

1. Risicodragend: Als een organisatie minder kosten maakt of bezuinigd op beveiligingsmaatregelen.
2. Risiconeutraal: Als een organisatie voor een middenweg kiest
3. Risicomijdend: Als een organisatie zo veel mogelijk investeert in beveiligingsmaatregelen.  
     
   **Beveiligingsmaatregelen [2]**

Beveiligingsmaatregelen zijn gebaseerd op een bepaald moment in de incidentcyclus.

**Incidentcyclus**

Bedreiging > Verstoring > Schade > Herstel > Bedreiging

Deze cyclus is in 4 stappen te onderscheiden:

1. Bedreiging, deze manifesteert zich bij een kwetsbaarheid en vormt een verstoring of een beveiligingsincident.  
     
   Een beveiligingsincident verstoord de betrouwbaarheid van een informatievoorziening.
2. Verstoring, een verstoring veroorzaakt schade.
3. Schade vraagt om herstel.
4. Na herstel beginne we weer opnieuw in de cyclus

Aan deze incidentcyclus voegen we een beveiligingscyclus toe.

**Beveiligingscyclus**

Bedreiging > Preventie > Verstoring Detectie > Respons (repressie) > Schade > Herstel Correctie > Bedreiging

Deze beveiligingsmaatregelen zijn in te delen in de volgende categorieën:

1. Preventieve maatregelen:

Preventieve maatregelen zijn maatregelen met het doel te voorkomen dat bedreigingen tot een verstoring leiden, deze laag wordt gezien als de ‘’schil’’ of ‘’de eerste laag van het vangnet’’

Er bestaan 2 subdelen van preventieve maatregelen:

* **Permanente maatregelen**

Permanente maatregelen beveiligen continu, zonder dat ze opgestart moeten worden. Bij deze maatregelen is het veelal niet zichtbaar wanneer deze effectief zijn.

* **Getriggerde maatregelen**

Getriggerde maatregelen beveiligen pas wanneer deze wordt opgestart, hiervoor moet zich een gemanifesteerde bedreiging niet automatisch worden opgemerkt door de ‘’andere’’ preventieve maatregelen. Deze trigger gaat af bij de detectieve maatregelen.

1. Detectieve maatregelen:

Detectieve maatregelen zijn maatregelen die vaststellen of een bedreiging zich manifesteert bij een daarvoor kwetsbaar object. Aan detectieve maatregelen moeten acties worden gekoppeld om iets te doen met hetgeen is gedetecteerd.

1. Responsieve maatregelen:

Responsieve (repressieve) maatregelen hebben het doel de negatieve invloed van een gedetecteerde storing te minimaliseren indien de preventieve maatregelen de verstoring niet hebben kunnen voorkomen.

Er bestaan 2 subdelen van responsieve maatregelen:

* **Proactief**

Er moeten acties worden ondernomen om een responsieve maatregel klaar te zetten voordat de maatregel geactiveerd kan worden.

* **Reactief**

De activatie van de proactieve maatregel wordt een reactieve maatregel bij activering, een voorbeeld van een reactieve maatregel is dat bij brand deze wordt geblust door het sprinkler systeem (reactief), hiervoor moeten wel de sprinkler worden klaargezet en voorbereid (proactief).

1. Correctieve maatregelen:

Correctieve maatregelen richten zich op het herstellen van de objecten die bij een incident verstoord of beschadigd zijn. Dit zijn onderhouds of beheersmaatregelen.

Text, letter

Description automatically generated

**Maatregelen opdeling**

Naast de indeling op basis van de beveiligingscyclus kunnen beveiligingsmaatregelen ook worden ingedeeld worden naar de wijze waarop ze gerealiseerd worden:

1. Organisatorische maatregelen:

Organisatorische maatregelen zijn maatregelen die betrekking hebben op de organisatie, de mensen en procedures.

Voorbeelden hiervan zijn:

- informatie beveiligingsstrategie en beleid

- functiescheidingen interne controle om fraude te voorkomen

- opleiding en voorlichting om het beveiligingsbewustzijn te verbeteren

- een portier bij de hoofdingang op de toegang te bewaken

1. Logische maatregelen:

Logische maatregelen zijn maatregelen die opgenomen zijn in de programmatuur.

Voorbeelden hiervan zijn:

- login/wachtwoord bij besturingssystemen en applicaties

- encryptie voor het verwijderen of delen van vertrouwelijke gegevens

- integriteitscontroles

- securityparameters in besturingssystemen en netwerkcomponenten

1. Fysieke maatregelen:

Fysieke maatregelen zijn maatregelen die gerealiseerd zijn met apparatuur of andere materiele middelen.

Voorbeelden hiervan zijn:

- Brandblussers

- noodstroom

- sloten tegen ongewenste toegang

Diagram

Description automatically generated with medium confidence