2 Begrippenkader

LEERDOELEN:

- Kennis over en inzicht in informatiebeveiliging gericht op het beschermen van informatiesystemen (in de meest ruime zin van het woord) en de gegevens daarin.
- Kennis over en inzicht in de relevante begrippen met betrekking tot informatiebeveiliging.

2.1 Gegevens, informatie en informatievoorziening

Het werken met *gegevens* speelt een cruciale rol in elke organisatie. Voor veel organisaties is het verwerken van gegevens zelfs het belangrijkste proces. Voorbeelden van gegevens zijn:

- personeelsgegevens;
- klantgegevens;
- leveranciersgegevens;
- contractgegevens;
- ordergegevens;
- financiële gegevens;
- marktgegevens;
- plannen en procedures;
- productiedocumenten;
- correspondentie;
- processturingsgegevens;
- archieven.

De *waarde* die de gegevens voor een organisatie hebben, hangt af van een aantal factoren:

- Het *procesbelang*: de mate waarin bedrijfsprocessen, die gebruikmaken van die gegevens, die van belang zijn voor de organisatie.
- De *onmisbaarheid* voor de bedrijfsprocessen: het belang van die gegevens voor de bedrijfsprocessen die er gebruik van maken.
- De *herstelbaarheid*: de mate waarin ontbrekende, incomplete of onjuiste gegevens gereproduceerd of hersteld kunnen worden.
- Het *belang voor derden*: de mate waarin derden (klanten, leveranciers of concurrenten) belang hechten aan de gegevens.

Het belang van gegevens ligt erin dat de bedrijfsprocessen die er gebruik van maken niet verstoord mogen worden. Daarnaast kunnen gegevens een zeker belang vertegenwoordigen voor anderen. Een voorbeeld hiervan zijn persoonsgegevens: deze

gegevens zijn voor organisaties van steeds groter belang voor de uitvoering van de bedrijfsprocessen, maar ze zijn in het kader van de privacy ook van belang voor degene wiens gegevens het betreft. Daarnaast kan het belang van gegevens ook liggen in het concurrentievoordeel dat ermee behaald kan worden ten opzichte van andere organisaties die in dezelfde markt opereren, of het concurrentienadeel dat het verlies van de betreffende gegevens op zou leveren. Een maat hiervoor is de prijs die een derde bereid is voor deze gegevens te betalen.

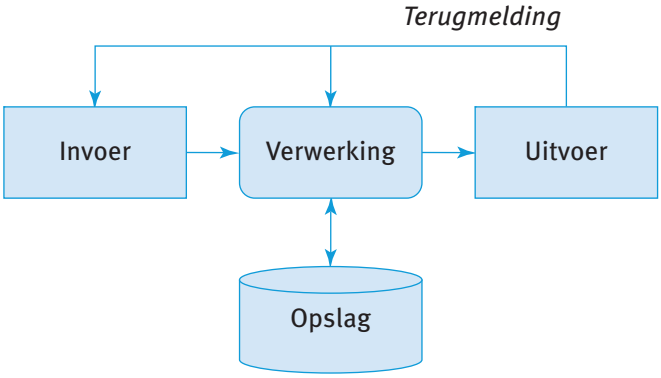
De begrippen gegevens en informatie worden vaak door elkaar gebruikt. Tussen de twee begrippen bestaat echter een duidelijk onderscheid. *Gegevens* kunnen gezien worden als de objectief waarneembare weerslag van feiten in een drager. *Informatie* daarentegen is de betekenis die de mens aan de hand van bepaalde gevoelens of afspraken aan gegevens toekent, of de kennistoename als gevolg van het ontvangen en verwerken van bepaalde gegevens. Hierdoor is informatie subjectief. Vanuit bepaalde gegevens kan, afhankelijk van degene die de gegevens bewerkt of interpreteert, verschillende informatie ontstaan. Zo kan de bekendmaking van een nieuwe kwetsbaarheid in Windows voor een hacker tot andere informatie leiden dan voor een informatiebeveiliger. De hacker interpreteert de kwetsbaarheid bijvoorbeeld als een uitdaging voor het bedenken van een nieuwe aanval, terwijl de informatiebeveiliger dezelfde kwetsbaarheid interpreteert als een noodzaak voor het ontwikkelen van een nieuwe tegenmaatregel. Daarnaast kan de waarde van gegevens in de tijd variëren, zelfs voor een en dezelfde persoon. Denk bijvoorbeeld aan een persbericht over een bedrijfsovername door een beursgenoteerde onderneming. De mate waarin gegevens over deze overname voor iemand op de beurs interessant zijn, is vóór het uitkomen van het persbericht anders dan ná het uitkomen ervan.

De relatie tussen gegevens en informatie is vergelijkbaar met de relatie tussen een grondstof en een eindproduct. Gegevens kunnen verwerkt worden tot informatie. Daarbij is het mogelijk om gebruik te maken van een informatiesysteem. Het informatiesysteem kan gegevens die voor een ontvanger niet direct nuttig zijn, verwerken tot gegevens die voor de ontvanger een zinvolle betekenis hebben en daarmee voor de ontvanger informatie zijn (zie figuur 2.1).

FIGUUR 2.1 De relatie tussen gegevens en informatie.

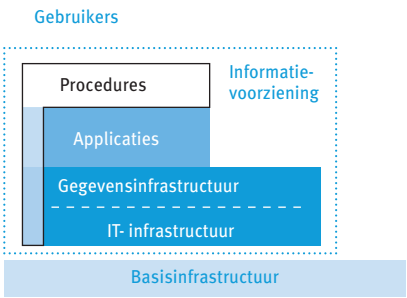
Een bijzonder voorbeeld van gegevens zijn *big data*: grote verzamelingen gegevens waarvan het vooraf niet duidelijk is wat de gebruiker eruit kan destilleren. Door bepaalde bewerkingen op de gegevens uit te voeren, kunnen interessante verbanden en structuren in de gegevens worden ontdekt die voor de gebruiker informatie vormen.

Een *informatiesysteem* (IS) is in de ruime zin van het woord een samenhangende gegevensverwerkende functionaliteit die gegevens verzamelt (invoer), manipuleert (verwerking), opslaat en verspreidt (uitvoer), en zo nodig een corrigerende reactie bevat (terugmelding) (zie figuur 2.2). Een informatiesysteem kan worden ingezet om één of meer bedrijfsprocessen te monitoren, te ondersteunen of te besturen. Een informatiesysteem kan de volgende componenten bevatten: apparatuur, programmatuur, gegevens, procedures en mensen. We spreken van een geautomatiseerd informatiesysteem als het informatiesysteem voornamelijk gerealiseerd is met informatietechnologie.



FIGUUR 2.2 Een informatiesysteem.

Informatietechnologie (IT), ook wel *informatie- en communicatietechnologie* (ICT) genoemd, is de technologie (apparatuur en programmatuur) die nodig is voor het beschikbaar stellen van een of meer geautomatiseerde informatiesystemen.
Een *applicatie* is de programmatuur waarin de specifieke functionaliteit van een informatiesysteem geprogrammeerd is. Een applicatie omvat de toepassingsprogrammatuur (applicatieprogrammatuur) en de bijbehorende gegevensverzamelingen, inclusief de daarop van toepassing zijnde procedures en documentatie.
Een *gegevensinfrastructuur* is het geheel van een of meer gegevensverzamelingen die door meerdere applicaties gebruikt (kunnen) worden, inclusief de daarop van toepassing zijnde procedures en documentatie, dat beschikbaar is voor een of meer informatiesystemen.
Een *IT-infrastructuur* is het geheel van automatiseringsmiddelen voor het opslaan, bewerken, transporteren en representeren van gegevens ten behoeve van gegevensinfrastructuren en applicaties. De IT-infrastructuur bestaat uit de componenten apparatuur, basisprogrammatuur (onder andere besturingssystemen en beheersoftware voor computers en netwerken) en communicatievoorzieningen, inclusief de daarop van toepassing zijnde procedures en documentatie.



FIGUUR 2.3 De componenten van de informatievoorziening.

De (geautomatiseerde) *informatievoorziening* (IV) is het geheel van IT-infrastructuur, gegevensinfrastructuur, applicaties en organisatie, dat tot doel heeft om te voorzien in de informatiebehoefte van de processen van een organisatie. De informatievoorziening van een organisatie kan ook beschouwd worden als de verzameling informatiesystemen en de gegevens- en IT-infrastructuur van de betreffende organisatie.

De onderdelen van de informatievoorziening zijn schematisch weergegeven in figuur 2.3. Van het onderdeel 'organisatie' is alleen de component 'procedures' weergegeven (zwart omlijnd). De gebruiksprocedures zijn aangegeven in wit. De overige onderdelen omvatten ieder procedures (en documentatie) om het betreffende onderdeel goed te laten functioneren. Aan procedures kunnen mensen gekoppeld zijn voor het uitvoeren ervan. Zo zijn voor de onderhoudsprocedure van een applicatie een of meer software engineers nodig. Soms worden deze mensen bij de informatievoorziening gerekend.
In de figuur is de locatie van de verschillende onderdelen van de informatievoorziening in het midden gelaten. Doordat de verschillende lagen rechtstreeks maar bijvoorbeeld ook via het internet met elkaar in verbinding kunnen staan, kan het zijn dat de verschillende lagen van de informatievoorziening op verschillende locaties zijn gerealiseerd. Vooral door de opkomst van *cloud computing* worden de verschillende lagen van de informatievoorziening steeds vaker op verschillende locaties gerealiseerd, en soms door verschillende organisaties. In hoofdstuk 7 zullen we nader ingaan op uitbesteden.
De *basisinfrastructuur* maakt geen deel uit van de informatievoorziening, maar schept wel noodzakelijke voorwaarden voor het functioneren van de informatievoorziening. Vanuit de informatievoorziening zullen dan ook eisen gesteld worden aan de basisinfrastructuur. De basisinfrastructuur omvat onder meer:

- elektriciteitsvoorziening;
- airconditioning;
- gebouwen en ruimten;
- kasten en meubilair.

Een uitgebreidere verhandeling over gegevens, informatie en informatiesystemen is te vinden in Stair en Reynolds, 2018, en in Laudon en Laudon, 2019.

2.2 Bedreiging, kwetsbaarheid en risico

Bij het beveiligen van de informatievoorziening spelen de begrippen bedreiging, kwetsbaarheid en risico een belangrijke rol.

2.2.1 Bedreiging

Een *bedreiging* is een proces of gebeurtenis met in potentie een verstorende invloed op de betrouwbaarheid van een object[1]. In het kader van informatiebeveiliging betreft het dan (onderdelen van) de informatievoorziening: apparatuur, programmatuur, gegevens, procedures en mensen.
Bedreigingen kunnen worden onderverdeeld naar de *aspecten van betrouwbaarheid* die ze negatief beïnvloeden. Betrouwbaarheid omvat de aspecten beschikbaarheid, integriteit en vertrouwelijkheid:

- *Beschikbaarheid* (B) is de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers.
- *Integriteit* (I) is de mate waarin gegevens of functionaliteit juist en volledig zijn.
- *Vertrouwelijkheid* (V) is de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

1 De term *object* wordt hierbij breed geïnterpreteerd: het betreft alle zaken van waarde. In het Engels wordt hiervoor vaak de term *asset* gebruikt.

Bedreigingen kunnen nog verder worden onderverdeeld op basis van de *kenmerken* die ieder aspect van betrouwbaarheid heeft (zie tabel 2.1). Naast de genoemde kenmerken zijn er nog andere kenmerken die hiervan afgeleid zijn, zoals *toegankelijkheid*, *nauwkeurigheid* en *robuustheid*. De aandacht voor het kenmerk *privacy* is de laatste jaren zo toegenomen dat het soms als een apart betrouwbaarheidsaspect wordt beschouwd, maar in feite is het een onderdeel van het aspect vertrouwelijkheid, waarbij dit aspect specifiek betrekking heeft op persoonsgegevens. Ook *controleerbaarheid* wordt nogal eens als een apart betrouwbaarheidsaspect vermeld, maar in feite is het een onderdeel van het aspect beschikbaarheid. Echter, voor mensen en partijen die betrokken zijn bij privacybescherming of controle kan het zinvol zijn om de kenmerken privacy en controleerbaarheid apart in de schijnwerpers te zetten.

ASPECT	KENMERK	BEDREIGING	VOORBEELDEN VAN BEDREIGING
Beschikbaarheid	Tijdigheid	Vertraging	Overbelasting van infrastructuur
	Continuïteit	Uitval	Defect in infrastructuur
	Vindbaarheid	Onvindbaar	Onvindbaar bestand (bijvoorbeeld door ontbrekende indexering)
	Controleerbaarheid	Oncontroleerbaar	Ontoegankelijk bestand (bijvoorbeeld door ontbrekende toegangsrechten)
Integriteit	Correctheid	Wijziging	Ongeautoriseerd wijzigen van gegevens Malware-infectie Typefout
	Volledigheid	Verwijdering Toevoeging	Ongeautoriseerd wissen van gegevens Ongeautoriseerd toevoegen van gegevens
	Geldigheid	Veroudering	Gegevens niet up-to-date houden
	Authenticiteit	Vervalsing	Frauduleuze transactie
	Onweerlegbaarheid (non-repudiation)	Verloochening	Ontkennen bepaald bericht te hebben verstuurd
Vertrouwelijkheid	Exclusiviteit	Onthulling Misbruik	Afluisteren van netwerk Hacking Privégebruik
	Privacy	Aantasting van persoonlijke integriteit	Uitlekken van gevoelige persoonsgegevens

TABEL 2.1 **Aspecten en kenmerken van betrouwbaarheid en daaraan gerelateerde bedreigingen.**

We zullen ons in de rest van dit boek beperken tot de onderverdeling naar de genoemde drie aspecten van betrouwbaarheid: beschikbaarheid, integriteit en vertrouwelijkheid. Een geheel andere indeling van bedreigingen is die naar de *bron* (veroorzaker) ervan. Zo kunnen mensen enerzijds al dan niet opzettelijk bepaalde bedreigingen veroorzaken, zoals fouten, inbraak, fraude, sabotage, hacking, et cetera; anderzijds kunnen zwakheden in bijvoorbeeld apparatuur en programmatuur leiden tot verstoringen.

Verstoringen kunnen ook veroorzaakt worden door externe invloeden, zoals het weer (denk aan schade door bliksem, storm, overstromingen, et cetera).
Op grond van hun verschillende bronnen kunnen bedreigingen in de volgende groepen worden onderverdeeld:

- Menselijke bedreigingen:
  - onopzettelijk foutief handelen, zoals vergissingen, door gebruikers, beheerders, gasten, of extern personeel;
  - opzettelijk foutief handelen, zoals diefstal, inbraak, hacking, sabotage, of fraude.
- Niet-menselijke bedreigingen:
  - invloeden van buitenaf, zoals een aardbeving, storm, bliksem, wateroverlast of brand;
  - storingen in de basisinfrastructuur, zoals uitval van elektriciteit;
  - storingen in apparatuur, programmatuur of gegevensbestanden.

Als we inzoomen op opzettelijk foutief handelen, dan kunnen we de volgende categorieën *aanvallers* onderscheiden:

- De *amateur*: deze persoon heeft algemene kennis van beveiliging en informatiesystemen en heeft slechts de beschikking over eenvoudige, vrij verkrijgbare middelen.
- De *professional*: deze persoon heeft *inside-kennis* van de aan te vallen systemen en/of de beschikking over professionele middelen.
- De *criminele organisatie*: deze groep beschikt over zeer ruime financiële middelen en is in staat om op uitgebreide schaal professionele mensen en middelen in te zetten.
- De *activistische of terroristische organisatie*: ook deze aanvalscategorie beschikt over zeer ruime middelen. Bovendien werken de mensen in hun ogen voor een 'goed doel'.
- De *staatsorganisatie*: een (organisatie van een) staat beschikt ook over zeer ruime middelen. Ook in dit geval werken de mensen voor een 'goed doel'.

De mate waarin een of meer van de genoemde categorieën aanvallers een organisatie als doelwit kan hebben, heeft consequenties voor het beveiligen van de betreffende gegevens en daarmee ook voor het budget dat voor informatiebeveiliging nodig is.

2.2.2 Kwetsbaarheid

De *kwetsbaarheid* van een object voor een bedreiging is de mate waarin dit object gevoelig is voor die bedreiging. Deze gevoeligheid ontstaat doordat een of meer karakteristieken van het object het mogelijk maken dat de bedreiging een negatieve invloed uit kan oefenen op het object. Zo is apparatuur bijvoorbeeld gevoelig voor fysiek geweld, terwijl programmatuur gevoelig is voor digitaal geweld.
Het begrip kwetsbaarheid is altijd gerelateerd aan enerzijds een of meer objecten en anderzijds een of meer bedreigingen. Zo kan men bijvoorbeeld de kwetsbaarheid onderzoeken van de computerruimte (verzameling objecten) voor brand (bedreiging).
De kwetsbaarheid van een object kan in het algemeen slechts beperkt kwantitatief bepaald worden. Een geschikte weergave kan bijvoorbeeld gebaseerd zijn op kwalitatieve kwetsbaarheidsniveaus (laag, midden, hoog), zoals toegepast in tabel 2.2.

	BEDREIGING								
	B			*I*			*V*		
Object	Diefstal	Sabotage	Kort-sluiting	Typefout	Fraude	Malware	Afluis-teren	Hacking	Privégebruik
Documen-tatie	ooo	o	–	ooo	–	–	–	–	oo
Tekstverwer-kingspakket	o	ooo	–	o	oo	ooo	–	ooo	ooo
Pc	ooo	ooo	oo	o	oo	ooo	ooo	ooo	ooo
Elektriciteits-voorziening	o	oo	ooo	–	–	–	–	–	o

– = n.v.t.; o = laag; oo = midden; ooo = hoog

TABEL 2.2 **De kwetsbaarheid van verschillende objecten voor enkele bedreigingen, onderverdeeld naar de betrouwbaarheidsaspecten (B, I, V).**

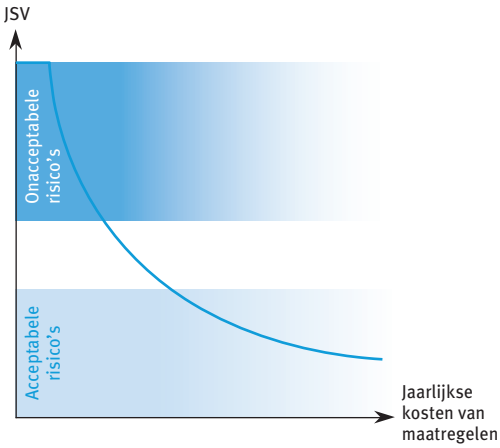
2.2.3 Risico

Een *risico* is een combinatie van de kans dat een bedreiging zich manifesteert en de mogelijke schade hiervan. Dit kan gezien worden als de gemiddelde schade over een gegeven tijdsperiode die verwacht wordt doordat een of meer bedreigingen leiden tot een verstoring van een of meer objecten van de informatievoorziening. Dit betekent dat er sprake is van een risico als een of meer objecten van de informatievoorziening door een of meer bedreigingen getroffen kunnen worden. De grootte van het risico is dan gelijk aan de te verwachten schade maal de kans dat de schade in een gegeven tijdsperiode optreedt. Daarmee is een risico dus te beschouwen als *kans op schade in een gegeven tijdsperiode* × *schade*, oftewel de schadeverwachting over de gegeven tijdsperiode. Een schadeverwachting op jaarbasis wordt aangeduid met de eenheid *Jaarlijkse Schade Verwachting* (JSV), of *Annual Loss Expectancy* (ALE).
De in aanmerking te nemen schade is al dan niet van financiële aard en omvat:

- De *directe schade* aan rechtstreeks getroffenen, zoals personen, apparatuur, programmatuur, gegevensverzamelingen en gebouwen.
- De *indirecte schade*, oftewel de *gevolgschade*, zoals verstoring van bedrijfsprocessen, het overtreden van wetten, het verlies van opdrachten en imagoschade.

Een risico heeft altijd betrekking op een of meer objecten, en op een of meer bedreigingen waarvoor die objecten een zekere kwetsbaarheid hebben. In het kader van de informatiebeveiliging hebben risico's betrekking op de objecten van de informatievoorziening en de bedreigingen die daarop in kunnen werken. Een voorbeeld van een risico is sabotage van een computer. Stel dat een dergelijke sabotage gemiddeld één keer in de tien jaar voorkomt en dat de directe en indirecte schade tezamen gemiddeld € 200.000 per keer is, dan is de te verwachten schade per jaar € 20.000. De JSV voor dit risico is dan € 20.000.
Alle risico's, uitgedrukt in JSV, met betrekking tot de objecten van de informatievoorziening kunnen bij elkaar opgeteld worden tot de JSV voor de gehele informatievoorziening. Zo ontstaat een schadepost die de organisatie gemiddeld per jaar kan verwachten voor de informatievoorziening als gevolg van manifestaties van bedreigingen. De organisatie kan een zeker kostenniveau verwerken zonder dat daardoor de bedrijfsprocessen in gevaar gebracht worden. Tot dit niveau zijn de risico's acceptabel.

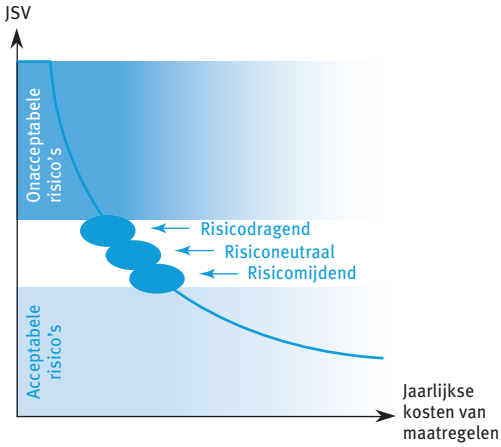
Er is echter ook een kostenniveau waarboven de bedrijfsprocessen zeker in gevaar gebracht worden. Een dergelijk kostenniveau is te allen tijde onacceptabel. Tussen de twee genoemde niveaus ligt een gebied waarin de jaarlijkse kosten voor schade kunnen leiden tot een weliswaar ernstige maar niet fatale[2] verstoring van de bedrijfsprocessen (zie figuur 2.4).



FIGUUR 2.4 De relatie tussen de schadeverwachting en de kosten van maatregelen.

Door het treffen van *beveiligingsmaatregelen* is het mogelijk om risico's te verkleinen. Dit kan enerzijds gerealiseerd worden doordat de maatregelen de kans verlagen dat de bedreigingen zich manifesteren, en anderzijds doordat de kwetsbaarheid van de objecten wordt verkleind. In beide gevallen wordt de schadeverwachting kleiner. Er moeten echter wel eerst kosten worden gemaakt om de beveiligingsmaatregelen te treffen. Deze kosten betreffen de initiële kosten voor het ontwerpen, realiseren en implementeren van de maatregelen, maar ook de steeds terugkerende kosten voor het onderhoud ervan. Een vermindering van de functionaliteit van de informatievoorziening moet ook als een kostenpost worden gezien. Uiteindelijk is het mogelijk om de kosten die gemoeid zijn met het treffen van beveiligingsmaatregelen uit te drukken in jaarlijkse kosten. Vervolgens kunnen deze kosten gerelateerd worden aan de schadeverwachting (JSV). Het resultaat is een dalende kromme: hoe meer wordt uitgegeven aan beveiligingsmaatregelen, hoe lager de schadeverwachting. In feite is de relatie geen monotone kromme, maar een stapvormige kromme die ontstaat doordat elke nieuwe beveiligingsmaatregel de schadeverwachting een stukje laat dalen ten opzichte van de vorige set maatregelen.
Een organisatie kan op verschillende manieren omgaan met de risico's die kunnen leiden tot ernstige (maar niet fatale) verstoringen van de bedrijfsprocessen. Zij kan er bijvoorbeeld voor kiezen om relatief weinig risico's te lopen: de organisatie investeert dan zo veel in beveiliging als redelijkerwijs mogelijk is. In dat geval werkt de organisatie *risicomijdend*. Als de organisatie onder het motto 'wie niet waagt, die niet wint' relatief veel risico's durft te accepteren, werkt zij *risicodragend*. Als de organisatie voor de gulden middenweg kiest, werkt zij *risiconeutraal* (zie figuur 2.5).

2 Een analoge redenering is te houden voor één enkele schade, die al dan niet gedragen kan worden door een organisatie.

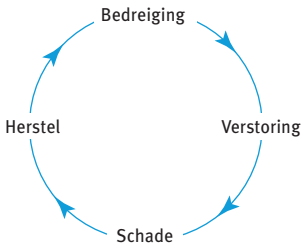


FIGUUR 2.5 Risicodragend, risiconeutraal en risicomijdend.

Om inzicht te krijgen in de aard en de grootte van risico's, alsmede in de kosten en de effectiviteit van beveiligingsmaatregelen, kan men een risicoanalyse[3] uitvoeren (zie hoofdstuk 12). Hoe in een bepaalde situatie omgegaan moet worden met risico's, is een aspect van het informatiebeveiligingsbeleid (zie paragraaf 6.3.1).

2.3 Beveiligingsmaatregelen

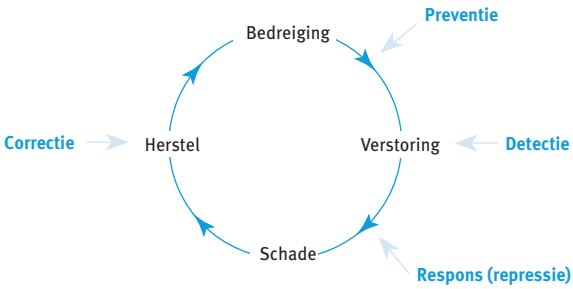
Een risicoanalyse leert tegen welke bedreigingen beveiligingsmaatregelen getroffen moeten worden. Het vervolgens op goed geluk implementeren van maatregelen levert zo goed als zeker een set maatregelen op die niet effectief is. Om een samenhangend pakket beveiligingsmaatregelen op te stellen waarmee de betrouwbaarheid van informatievoorzieningsprocessen gewaarborgd kan worden, is inzicht nodig in de werking van maatregelen en de onderlinge relaties ertussen.
Beveiligingsmaatregelen zijn gericht op een bepaald moment van de *incidentcyclus* (*event cycle*; zie figuur 2.6).



FIGUUR 2.6 De incidentcyclus.

3 In het Engels wordt hiervoor de term *risk assessment* gebruikt. In het Engels wordt de term *risk analysis* ook wel gebruikt, maar dan als onderdeel van *risk assessment* en dus met een beperktere reikwijdte dan het Nederlandse *risicoanalyse*.

In de incidentcyclus worden vier stappen onderscheiden. Allereerst is er een *bedreiging*: iets wat zou kunnen gebeuren. Als dit zich manifesteert bij een daarvoor kwetsbaar object, spreken we van een *verstoring*, oftewel een *beveiligingsincident*. Een beveiligingsincident is een incident dat de betrouwbaarheid van de informatievoorziening verstoort. Door een incident ontstaat *schade* aan gegevens of aan middelen, en dat vraagt om *herstel*.
Bij ernstige incidenten is na verloop van tijd een evaluatie nodig: wat ging er fout, hoe is het veroorzaakt en hoe kan dit in de toekomst voorkomen worden. Bovendien kan een meldingsprocedure voor beveiligingsincidenten ervoor zorgen dat de evaluatie van de effectiviteit en efficiëntie van de huidige beveiligingsmaatregelen plaats kan vinden op basis van inzicht in *alle* incidenten. Hiervoor moet een beroep gedaan kunnen worden op logging- en auditfiles, en natuurlijk op de registraties uit het IT-beheerproces.
In al de stappen van de incidentcyclus kan ingegrepen worden met passende (beveiligings)maatregelen. Parallel aan de incidentcyclus bestaat dan ook een *beveiligingscyclus*, die vier fasen doorloopt: preventie, detectie, respons (repressie) en correctie (zie figuur 2.7).



FIGUUR 2.7 De beveiligingscyclus,

Analoog aan de beveiligingscyclus kunnen we beveiligingsmaatregelen indelen (zie figuur 2.8):

- preventieve maatregelen;
- detectieve maatregelen;
- responsieve (repressieve) maatregelen;
- correctieve maatregelen.

Preventieve maatregelen zijn maatregelen die tot doel hebben te voorkomen dat bedreigingen tot een verstoring leiden. Deze maatregelen worden ook wel eerstelijnsmaatregelen genoemd, omdat deze maatregelen beschouwd kunnen worden als de eerste 'schil' van de beveiliging.
Preventieve maatregelen kunnen weer worden onderverdeeld in permanente en getriggerde maatregelen. *Permanente maatregelen* beveiligen continu, zonder dat ze opgestart hoeven te worden. Bij deze maatregelen is het vaak niet zichtbaar wanneer ze effectief zijn. Een voorbeeld hiervan is het gebruik van onbrandbare vloerbedekking: de vloerbedekking doet continu en onzichtbaar zijn brandwerende werk. *Getriggerde maatregelen* beveiligen daarentegen pas nadat ze zijn opgestart. Hiervoor is het nodig dat een zich manifesterende bedreiging al dan niet automatisch opgemerkt wordt, waarna een opstartsignaal, oftewel een *trigger*, voor die beveiligingsmaatregel gegenereerd wordt. Een voorbeeld hiervan is het gebruik van een *uninterruptible power supply*