1 Inleiding

Informatiesystemen vormen het zenuwstelsel van onze samenleving. Ze worden gebruikt om gegevens op te slaan, transacties vast te leggen, berekeningen uit te voeren, contacten te leggen, nieuwe producten te verkopen en organisaties te besturen. Ook maken ze het mogelijk informatie met andere organisaties of personen uit te wisselen. Zonder informatiesystemen kunnen de meeste organisaties niet functioneren.

Informatiesystemen zijn in hoge mate gebaseerd op informatietechnologie. Het gebruik hiervan is niet zonder risico's. Informatietechnologie is immers vatbaar voor allerlei bedreigingen, menselijk en niet-menselijk. Wat gebeurt er als kritische systemen voor langere tijd uitvallen? Als er wordt geknoeid met belangrijke gegevens? Als vertrouwelijke informatie 'op straat' komt te liggen? De gevolgen kunnen ernstig zijn: denk aan gemiste orders, verlies van vertrouwen van klanten en andere stakeholders, juridische claims of negatieve publiciteit. Een verantwoordelijk manager zal zich inspannen om zulke incidenten te voorkomen of de schade ervan te beperken door passende maatregelen te treffen. Dit is het werkterrein van *informatiebeveiliging*. Hoewel dit terrein inmiddels ook bekend is onder verschillende synoniemen, waaronder *cybersecurity* en *cyberresilience*, geven wij er in dit boek de voorkeur aan om voornamelijk de term informatiebeveiliging (in het Engels: *information security*) te blijven hanteren.

Informatiebeveiliging is een verzamelnaam voor de processen die ingericht zijn om de betrouwbaarheid van de informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Aangezien betrouwbaarheid een kwaliteitsaspect is, kan informatiebeveiliging dus beschouwd worden als een onderdeel van de kwaliteitszorg. Maar even goed is informatiebeveiliging onderdeel van de interne beheersing van organisaties (*corporate governance*).

Informatiebeveiliging staat sinds de boekhoudschandalen aan het begin van deze eeuw bij onder meer Enron en WorldCom zeer in de belangstelling. Wetten als de Amerikaanse Sarbanes-Oxley Act en richtinggevende documenten als de Code Tabaksblat (sinds 2018 als Code Van Manen verankerd in de Nederlandse wet) legden de basis voor de verplichting voor organisaties een stelsel van maatregelen op het gebied van interne beheersing ingericht te hebben en de effectiviteit hiervan expliciet door het management te laten bevestigen. Voorbeelden van zulke maatregelen zijn het inrichten van controletechnische functiescheidingen, het uitvoeren van geautomatiseerde controles en het waarborgen van de herleidbaarheid van transacties tot individuele medewerkers. Voor het realiseren van zulke maatregelen is informatiebeveiliging een noodzakelijke voorwaarde. Corporate governance kan niet zonder informatiebeveiliging. Maar meer nog dan een onderdeel van de kwaliteitszorg of de interne beheersing van organisaties is informatiebeveiliging voor veel organisaties een voorwaarde om te overleven: organisaties die de beveiliging van informatie niet goed voor elkaar hebben, worden door de publieke opinie als onbetrouwbaar gezien en kunnen daardoor lijden aan een slecht imago, hetgeen moeilijk te herstellen is.

Eén ding is duidelijk: informatiebeveiliging is allang geen specialisme meer dat voorbehouden is aan een select groepje professionals: het hoort bij de taken en verantwoordelijkheden van elke manager en medewerker.

Het is algemeen bekend dat informatiebeveiliging soms op gespannen voet staat met andere zaken die voor organisaties van groot belang zijn. Denk aan openheid, gebruiksvriendelijkheid en efficiency. Wie te hoge eisen aan de beveiliging stelt, snijdt zichzelf in de vingers. Maar een te laag beveiligingsniveau is ook niet verantwoord. Het vinden van de goede balans is noodzakelijk om zowel de werkbaarheid als het beveiligingsniveau optimaal te houden.
Het realiseren van een evenwichtige informatiebeveiliging is een uitdaging van formaat. Al in de ontwerpfase van informatiesystemen moet rekening gehouden worden met de bedreigingen die in de praktijk op kunnen treden. Daarbij beperkt informatiebeveiliging zich niet tot de informatietechnologie; het omvat ook processen die niet direct met informatietechnologie te maken hebben, zoals beveiliging van gebouwen, personeelsbeleid en toezicht. Naast technologie spelen zaken als management, organisatie, certificatie en wet- en regelgeving een belangrijke rol.
Bovendien zijn standaarden in zo'n breed vakgebied onontbeerlijk. Het gebruik van standaarden neemt in dit boek dan ook een centrale plaats in. Technische standaarden, maar ook processtandaarden. Door standaarden te gebruiken, kan worden geprofiteerd van de jarenlange ervaring van toonaangevende organisaties.
Bij het gebruik van zulke standaarden past enig voorbehoud. Informatiebeveiliging staat in de organisatie niet op zichzelf; voor een optimaal effect dient zij geïntegreerd te zijn in de andere bedrijfsprocessen. Bovendien kan informatiebeveiliging niet los worden gezien van technologische, organisatorische, maatschappelijke en economische ontwikkelingen:

Technologie
Door steeds krachtigere en mobielere informatietechnologie, de explosieve groei van het aantal aan elkaar gekoppelde systemen en het steeds intensievere gebruik ervan verandert niet alleen het object van beveiliging, maar ook het bedreigingenbeeld. Nieuwe technologieën brengen nieuwe bedreigingen met zich mee, maar maken ook nieuwe beveiligingsmaatregelen mogelijk.

Organisatie
Organisatorische veranderingen zijn zeer actueel. Het toenemend belang van interne beheersing, maar ook fusies, overnames, een toenemende verantwoordelijkheid van de individuele medewerker ('empowerment') en de uitbesteding van informatiediensten zijn ontwikkelingen die hun effect op informatiebeveiliging niet missen.

Maatschappij
Ook maatschappelijke ontwikkelingen hebben een invloed op informatiebeveiliging. Denk aan nationale en internationale wet- en regelgeving, de trend tot marktwerking en deregulering, de maatschappelijke betekenis van privacy, de toenemende individualisering van de burger, de strijd tegen het internationale terrorisme en contacten tussen verschillende culturen.

Economie
Ten slotte zijn er economische ontwikkelingen die het vakgebied informatiebeveiliging aanzienlijk beïnvloeden. Voorbeelden zijn de toenemende globalisering van ondernemingen en markten, maar ook de verdere groei van de digitale handel tussen bedrijven en burgers en tussen bedrijven onderling.

De invloed van deze ontwikkelingen zal in dit boek uitgebreid aan de orde komen. Duidelijk zal worden dat informatiebeveiliging niet moet worden gezien als een rigide bouwwerk, maar als een flexibel arsenaal aan functies en maatregelen om informatie en informatiesystemen in een sterk veranderende omgeving adequaat te kunnen beschermen.
De indeling van dit boek is als volgt:

- Deel I behandelt de grondslagen van informatiebeveiliging.
  - Hoofdstuk 2, Begrippenkader, bevat een referentiekader met de begrippen die in relatie tot informatiebeveiliging een rol spelen.
  - Hoofdstuk 3, Informatiebeveiliging in perspectief, positioneert informatiebeveiliging als discipline en als proces in de organisatie. Ook de relaties met andere processen in de organisatie komen aan bod.
  - Hoofdstuk 4, Juridische aspecten, behandelt de juridische aspecten van informatiebeveiliging. Hierin komt de relevante nationale en internationale wet- en regelgeving aan de orde.
  - Hoofdstuk 5, Informatiebeveiligingsstandaarden, gaat in op de verschillende standaarden die er op het gebied van informatiebeveiliging zijn, de relatie die ze met elkaar hebben en de specifieke behoeften die de standaarden afdekken, alsook de certificatie van informatiebeveiliging.
- Deel II behandelt management en organisatie van informatiebeveiliging.
  - Hoofdstuk 6, Organisatie van informatiebeveiliging, gaat over het organiseren van de informatiebeveiliging zelf.
  - Hoofdstuk 7, Uitbesteden van informatiebeveiliging, beschrijft de manier waarop organisaties om kunnen gaan met de toenemende mate waarin informatiebeveiliging niet meer zelf wordt gedaan, maar wordt overgelaten aan derde partijen.
  - Hoofdstuk 8, De menselijke factor, behandelt de relatie tussen menselijk gedrag en informatiebeveiliging. Er wordt onder meer ingegaan op menselijk falen en het beveiligen daartegen.
  - Hoofdstuk 9, Securityarchitectuur en ontwerpcriteria, bespreekt de samenhang tussen de diverse onderdelen van informatiebeveiliging en de architectuurraamwerken die hiervoor bestaan.
  - Hoofdstuk 10, Risicoanalyse, beschrijft het fenomeen risicoanalyse en gaat in op het uitvoeren ervan.
- Deel III behandelt informatiebeveiligingsmaatregelen.
  - Hoofdstuk 11, Preventie, behandelt preventieve informatiebeveiligingsmaatregelen.
  - Hoofdstuk 12, Detectie, behandelt detectieve informatiebeveiligingsmaatregelen.
  - Hoofdstuk 13, Respons, behandelt responsieve (repressieve) informatiebeveiligingsmaatregelen.

Dit boek is bedoeld voor general managers, securitymanagers, security officers, informatiemanagers, informatiebeveiligers, IT-managers en IT-auditors. Het is geschikt als studieboek voor bachelor/hbo-opleidingen, master/doctorale opleidingen en postdoctorale opleidingen op het gebied van onder meer cybersecurity, informatiebeveiliging, informatiemanagement, accountancy en IT-auditing.

DEEL I

GRONDSLAGEN VAN INFORMATIEBEVEILIGING

2 Begrippenkader

Informatiebeveiliging richt zich op het beschermen van informatiesystemen (in de ruime zin van het woord) en de gegevens daarin. Om informatiebeveiliging goed te kunnen plaatsen worden in dit hoofdstuk de relevante begrippen met betrekking tot informatiebeveiliging uitgewerkt. In hoofdstuk 3 volgt dan de invulling en positionering van 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;
- archieven.

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

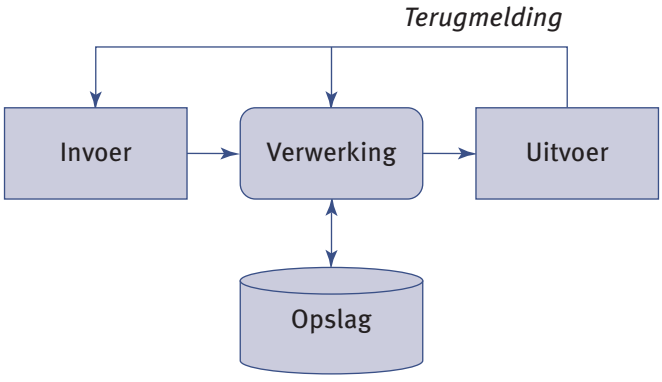
- Het *procesbelang*: de mate waarin bedrijfsprocessen, die gebruikmaken van de betreffende gegevens, van belang zijn voor de organisatie.
- De *onmisbaarheid* voor de bedrijfsprocessen: het belang van de betreffende gegevens voor de bedrijfsprocessen die er gebruik van maken.
- De *herstelbaarheid*: 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 betreffende 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 desbetreffende 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, waarbij de waarde van de gegevens ook in de tijd kan variëren. Denk hierbij bijvoorbeeld aan een persbericht over een bedrijfsovername door een beursgenoteerde onderneming. De informatiewaarde van deze gegevens is voor de beurs een hele andere dan twee weken na het uitkomen van het persbericht. Met andere woorden: twee ontvangers van dezelfde gegevens kunnen er verschillende informatie aan ontlenen. 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). Een bijzonder voorbeeld is *big data*: een grote verzameling gegevens waarvan het vooraf niet duidelijk is welke informatie de gebruiker hieraan kan ontlenen. 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.

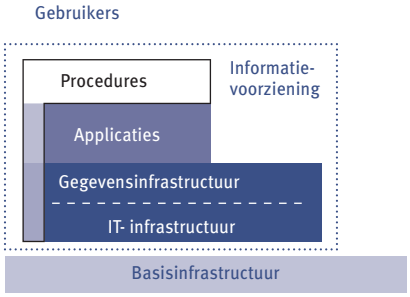
FIGUUR 2.1 De relatie tussen gegevens en informatie

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 kennen, 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 wordt gerealiseerd 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, 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 *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 om het betreffende onderdeel goed te laten functioneren. Alle onderdelen kunnen bovendien mensen en documentatie omvatten, ten behoeve van het functioneren van de betreffende onderdelen. Voor de overzichtelijkheid is dat niet in de figuur aangegeven.
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 heeft 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.

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 *privacy*, *controleerbaarheid*, *nauwkeurigheid* en *robuustheid*. De aandacht voor het kenmerk privacy is de laatste jaren zodanig 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 het (deel)aspect privacy respectievelijk controleerbaarheid apart in de schijnwerpers te zetten.

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