PBLQ

Safe in cyberspace
van awareness naar actie

voor een sterke publieke sector

PBLQatie 46

In samenwerking met

CIP centrum informatiebeveiliging en privacybescherming

SAFE IN CYBERSPACE
VAN AWARENESS NAAR ACTIE

Voor bestuurders, managers en veranderaars

ISBN 9789075239478

Ontwerp omslag en binnenwerk
Smidswater

SAFE IN CYBERSPACE
VAN AWARENESS NAAR ACTIE

Voor bestuurders, managers en veranderaars

Auteurs
Marcel Spruit
Boudien Glashouwer
Erik Dolle

PBLQatie nr. 46

Inhoudsopgave

Voorwoord

Met de digitalisering van onze samenleving is het hard gegaan. Digitale technologie is niet meer weg te denken op het werk en privé, en deze twee werelden lopen ook steeds meer door elkaar. En het zal steeds sneller gaan, van slimme thermostaten tot slimme steden. Bovendien worden apparaten en netwerken met elkaar verbonden en verknoopt.

We krijgen door het koppelen van bestanden, de uitwisseling en benutting in ketens en ontwikkelingen als open en big data steeds meer doorzoekbare en hoogwaardige gegevens. Via mobiele technologie kunnen we daar vanuit de hele wereld bij, wanneer we maar willen. Dat heeft onmiskenbaar voordelen; de keerzijde is dat we niet meer zonder kunnen. Als systemen stagneren, zijn we niet alleen ernstig onthand, maar allerlei maatschappelijke processen stagneren. Dit raakt al vrij snel onze primaire levensbehoeften. Bovendien zijn criminelen, spionnen en terroristen ook gedigitaliseerd. Zij zorgen voor een extra stroom dreigingen voor landen, organisaties en personen.

Het aantal incidenten is de afgelopen jaren schrikbarend toegenomen. Alle overheidssectoren hebben hiermee te maken gehad. Verscheidene waren langdurig in het nieuws. En omdat we weten dat veel organisaties hun incidenten niet openbaar maken, nemen we aan dat de afgelopen jaren het aantal incidenten veel groter was dan we gehoord en gelezen hebben. Dat strookt ook wel met expertschattingen dat in Nederland de schade door cybercrime ruim 8 miljard euro per jaar bedraagt, ofwel 1,5 procent van het bruto nationaal product. De schade door cyberspionage is daar nog niet eens in meegenomen.

Is het met al deze dreigingen wel veilig om het internet op te gaan? Zijn smartphones veilig? Wat zijn de risico's van big data? Hebben we nog iets privé? Kunnen verschillende organisaties veilig gebruik maken van dezelfde gegevensbestanden? Kunnen we incidenten voorkomen? Is het een race tegen de klok? Hoe pakken we dat dan aan en waar beginnen we?

Met dit soort vragen zitten bestuurders en managers van grote en kleine organisaties in de publieke sector. De afgelopen jaren is het bewustzijn dat er iets moet gebeuren gegroeid. Gremia zoals de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID), het Nationaal Cyber Security Centrum (NCSC), het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) en de Informatiebeveiligingsdienst voor gemeenten (IBD) hebben hier een belangrijke bijdrage aan geleverd.

Maar het blijft voor bestuurders en (verander)managers lastig om goede sturing te geven aan de informatieveiligheid binnen de eigen organisatie en bij partnerorganisaties. Dus genoeg aanleiding voor dit boekje dat in een notendop de hoofdzaken met betrekking tot informatieveiligheid schetst. Niet alleen wat het is, maar ook waar u in uw organisatie kunt beginnen. We bevelen de lezing van dit boekje dan ook van harte aan.

Ad Reuijl
Directeur Centrum voor Informatiebeveiliging en Privacybescherming

Leo Smits
Algemeen Directeur PBLQ

Hoofdstuk 1
Inleiding

Overheidsorganisaties zijn constant bezig hun elektronische dienstverlening aan burgers en bedrijven te verbeteren. Een papieren aangifte wordt een uitzondering. Het opvragen van gegevens of het indienen van een melding gaat via het digitale loket veel sneller en makkelijker dan via het fysieke loket. Het internet is daarbij onmisbaar. Uit recente onderzoeken van onder meer het NCSC (Nationaal Cyber Security Centrum) en de Taskforce BID (Bestuur en Informatieveiligheid Dienstverlening) blijkt dat veel overheidsorganisaties op het niveau van bestuur en management nog kennis ontberen over informatieveiligheid en het integreren ervan in de bedrijfsvoering.

Het realiseren van informatieveiligheid is dan ook geen kleinigheid. De digitalisering van onze maatschappij gaat snel. In hoog tempo dienen zich nieuwe digitale toepassingen aan. Enkele recente ontwikkelingen zijn cloud computing, BYOD (bring your own device), robots in de zorg en domotica in de huiskamer, 3D printen, zelfrijdende auto's en het Internet of Things. Hiermee komen naast kansen ook nieuwe dreigingen in beeld. Voorbeelden zijn DDoS-aanvallen, phishing, botnets, APT's (advanced persistent threats) en ransomware. Dit naast alle dreigingen die we al hadden, waaronder telefoon- en elektriciteitsuitval, ICT-falen, hacking en malware.

> "Het volume van de dreiging is toegenomen. Denk aan connectiviteit van de auto of de mate van digitalisering van de samenleving. En er is meer en meer professionele georganiseerde criminaliteit: 90% van de mail is spam."
> Leo Smits, Algemeen Directeur PBLQ, 2015

> "Het Duitse parlement dreigt al zijn 20 duizend computers te moeten vervangen vanwege een spionagehack. De vijandige software heeft zich in een maand tijd diep in het systeem gevreten en kon tot nu toe niet worden verwijderd."
>
> **de Volkskrant, 11 juni 2015**

Cybercrime kost de Nederlandse economie jaarlijks ruim 8 miljard euro, ofwel zo'n 1,5 procent van het bruto nationaal product (juni 2014). Er zijn zelfs studies die, weliswaar minder goed onderbouwd, veel hoger uitkomen. Veel incidenten ontstaan door onwetendheid of onoplettendheid van medewerkers. De mens is ondanks alle vooruitgang nog steeds de zwakke schakel. De meeste fouten worden onopzettelijk of te goeder trouw gemaakt. Toch neemt ook het aantal bewuste vergrijpen van medewerkers gestaag toe. Denk bijvoorbeeld aan het misbruik maken van voorkennis bij aanbestedingen en het inbreken op de privacy van anderen.

Voorbeelden van cyberincidenten in Nederland:

- Certificaten van DigiNotar vervalst, 2011.
- Beveiligingslekken van de overheid worden openbaar gemaakt, Lektober, 2011.
- Een pomp van een waterbedrijf wordt digitaal onklaar gemaakt, 2011.
- De gemalen van de gemeente Veere gehackt, 2012.
- De ontdekking van het spionagevirus Red October dat wereldwijd actief was, 2012.
- DigiD uit de lucht gehaald vanwege een beveiligingslek, 2013.
- Het afluisterschandaal van de NSA, 2013.
- 20% stijging van het aantal phishing mails, 2014.
- Meer dan 400.000 websites gekraakt door een Russische bende, 2014.
- Websites van rijksoverheid urenlang onbereikbaar na DDoS-aanval, februari 2015.
- Alle pc's van Friese gemeenten platgelegd door ransomware, juni 2015.
- 1.8 miljoen mensen zonder internet door DDoS-aanvallen op Ziggo, augustus 2015

Dit boekje beoogt bestuurders en (verander)managers praktische handreikingen te bieden die kunnen helpen bij het aansturen en professionaliseren van informatieveiligheid. Het richt zich op de managementaspecten van informatieveiligheid, zonder gebruik van vakjargon en 'overbodige' details. Want met name het management staat aan de lat voor het opstellen van een beleid voor informatieveiligheid en het laten definiëren, implementeren en controleren van een adequaat niveau van beveiliging van de informatievoorziening.

> "De DigiNotar-crisis en Lektober in 2011 hebben aangetoond dat de ICT-infrastructuur van gemeenten kwetsbaar is. Uit de acties rondom Lektober is gebleken dat de gemeentelijke beveiliging van de ICT-infrastructuur en de opgeslagen informatie niet bij alle gemeenten even goed op orde is."
>
> Baseline Informatiebeveiliging Nederlandse Gemeenten, KING/IBD, 2013

De uitdaging is te zorgen voor blijvende *awareness* in de organisatie ten aanzien van informatieveiligheid en die nadrukkelijk om te zetten in *actie*. Dit hoeft niet veel tijd te kosten als u de juiste opmerkingen maakt, de goede vragen aan de juiste personen stelt en de relevante terugkoppeling en rapportages vraagt. Dit boekje helpt u daarbij op weg.

Informatieveiligheid, informatiebeveiliging, of cybersecurity. Wat houdt dat in?

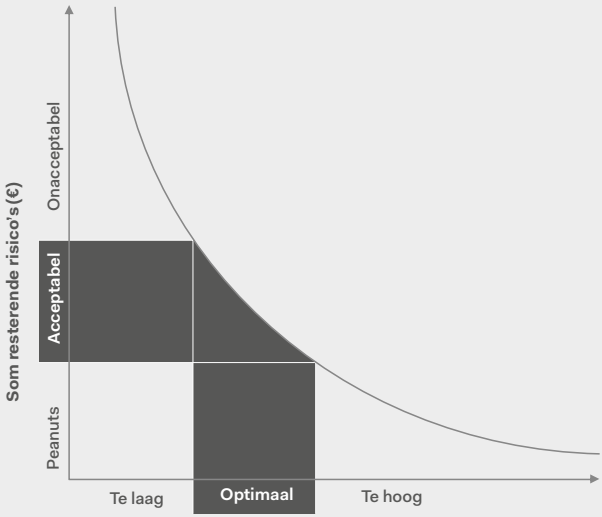
- Informatiebeveiliging is het proces (de weg) om tot informatieveiligheid (het resultaat) te komen.
- Cybersecurity is het onderdeel van informatiebeveiliging dat zich richt op het beveiligen van cyberspace (de ICT en het internet). In dit boekje stellen we voor het goede begrip cybersecurity gelijk aan informatiebeveiliging.

Hoofdstuk 2
Waarom informatiebeveiliging?

Na enkele jaren waarin informatieveiligheid hoog op de overheidsagenda heeft gestaan kan gemakkelijk het beeld ontstaan dat de publieke sector haar beveiliging op orde heeft. De bewustwording is weliswaar enorm toegenomen en steeds meer instrumenten zijn beschikbaar gekomen. Maar ook de digitalisering en de daarmee gepaard gaande dreigingen zijn toegenomen. Zonder passende informatiebeveiliging bereiken we geen smart city, laat staan een smart nation.

> "Er komt meer druk om de interne (ICT)-processen op orde te hebben: het belang voor je organisatie en daarbuiten is veel te groot. Meld daarom ICT-inbreuken. Op cybersecurity moet je niet willen concurreren, dus werk samen met het NCSC en met je branche!"
> Hans de Vries, Hoofd Nationaal Cyber Security Centrum, 2015

In elke organisatie en in contacten tussen organisaties is een grote variëteit aan gegevens te vinden. Een steeds groter deel hiervan is digitaal. Digitale gegevens bevinden zich in computersystemen, maar ook op laptops, smartphones, USB-sticks, toegangspassen, etc. De gegevens zijn nodig voor de administratieve processen, zoals planning en control, financiën en andere administraties, voor de dienstverlening en interactie met burgers en bedrijven en in sommige gevallen ook voor het besturen van vitale processen en systemen. Voor organisaties zijn de digitale gegevens zo belangrijk dat de organisaties veelal niet meer zonder deze gegevens kunnen functioneren. De grote diversiteit van de gegevens en de gegevensdragers maken de gegevens echter kwetsbaar voor een scala aan dreigingen. Denk bijvoorbeeld aan verlies, diefstal, vervalsing, fraude en hacking, maar ook aan brand, bliksem, waterschade en elektriciteitsstoring.



Figuur 1: De relatie tussen risico's en de kosten van maatregelen.

> "Het gijzelen van systemen en data wordt steeds eenvoudiger. Opsporing van daders helpt, maar blijkt niet voldoende om slachtofferschap te voorkomen."
> "Een vorm van cybercrime die grotendeels leunt op oplichting is niet gebaat bij teveel bekendheid bij potentiële slachtoffers. Daders moeten daarom blijven innoveren."
> Cyber Security Beeld Nederland 4, NCSC, juli 2014

Niet elke dreiging is even ernstig. Sommige dreigingen komen zelden voor, of leiden tot marginale schade. Maar andere dreigingen komen wel vaak voor en leiden misschien ook nog tot grote fysieke, materiële of imagoschade. Daarom is het niet zinvol om zomaar tegen alle dreigingen maatregelen te treffen. Beter is het om de belangrijkste dreigingen te identificeren en daartegen maatregelen te treffen.

Om die dreigingen te vinden, kijkt men niet alleen naar de dreigingen zelf, maar vooral naar de daaraan verbonden risico's. De risico's zijn namelijk een maat voor de schade die men kan verwachten door toedoen van de dreigingen. De schade kan financieel zijn, maar kan ook betrekking hebben op andere negatieve gevolgen, zoals imagoschade, of slachtoffers bij ongelukken.

> "De huidige informatietechnologie is zo complex geworden dat mensen deze niet langer zomaar veilig kunnen toepassen."
>
> Frank Katsburg, Chief Security Officer, Sociale Verzekeringsbank

Door beveiligingsmaatregelen te treffen, kan men de schade door optredende dreigingen reduceren (zie figuur 1). De som van de resterende risico's neemt dan af. Maar aan het treffen van maatregelen zijn uiteraard kosten verbonden, zowel voor het invoeren van de maatregelen, als voor het onderhouden ervan. Als er te weinig maatregelen worden getroffen, dan kunnen dreigingen tot hinderlijke of gevaarlijke situaties leiden. Daar staat tegenover dat als er te veel (of te zware) maatregelen worden getroffen, de organisatie dan 'penny wise, pound foolish' bezig is: men geeft euro's uit om dubbeltjes te beschermen. Dit lijkt misschien niet zo erg, maar het werpt ook onnodige barrières op bij het uitvoeren van het werk.

Al met al is het vinden van het optimum tussen te weinig en te veel beveiligen geen kleinigheid. Ook het selecteren van geschikte maatregelen is lastig. Daarbij spelen basisinformatiebeveiliging en risicoanalyse een rol. In het volgende hoofdstuk gaan we daar verder op in.

> "Goede informatiebeveiliging leidt tot een afname van het aantal en de impact van incidenten en daardoor een afname van het gevoel van urgentie ten aanzien van informatiebeveiliging."
>
> Piet Sennema, Secretaris Directeur Waterschap Aa en Maas, 2015

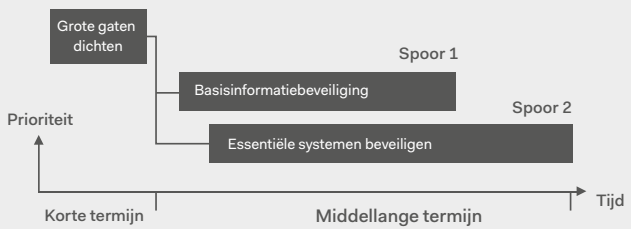
Na het selecteren van passende maatregelen moeten ze nog goed ingevoerd en onderhouden worden. Ook dit gaat niet vanzelf en vergt aan de ene kant kennis en inzicht en aan de andere kant tijd en geld. Dit maakt informatiebeveiliging een lastig onderwerp, dat echter broodnodig is voor de goede gang van zaken binnen een organisatie.

Hoofdstuk 3
Hoe wordt uw organisatie veilig?

Informatiebeveiliging begint bij bestuur en management. Het management stelt hiervoor beleid op, draagt het uit, wijst taken, verantwoordelijkheden en bevoegdheden toe en bewaakt de gang van zaken.

> "Door een 'foutje' van een meisje op Facebook beschouwde de halve wereld zich uitgenodigd voor haar feestje. De digitale wereld is inmiddels onlosmakelijk met de fysieke wereld verbonden, met alle kansen en risico's van dien. Gemeentelijke bestuurders moeten – net als op financiën – sturen vanuit de waarde van informatie en daarmee op informatieveiligheid."
>
> Larissa Zegveld, Directeur Kwaliteitsinstituut Nederlandse Gemeenten, VNG 2015

Als de informatiebeveiliging al goed geregeld is dan is het advies om vooral op de ingeslagen weg door te gaan. Als echter de informatiebeveiliging nog onvoldoende is vormgegeven, dan ligt er in eerste instantie werk voor het management. De volgorde van de globaal te nemen stappen is in figuur 2 getoond.



Figuur 2: De tweesporenaanpak.

3.1 **Grote gaten dichten**

Wanneer informatiebeveiliging nog onvoldoende is geregeld, dan is het nodig om eerst de urgente 'grote gaten' te dichten. Dit heeft betrekking op de dreigingen die morgen al tot een ernstig incident zouden kunnen leiden en waarvoor de beveiligingsmaatregelen echt niet kunnen wachten. Een ervaren informatiebeveiligingsfunctionaris kan in korte tijd een eerste inschatting maken welke dreigingen tot onacceptabele risico's leiden en daarom met spoed aangepakt moeten worden. Tegen deze dreigingen zijn direct maatregelen nodig, zonder overbodige rompslomp.

Bij het dichten van 'grote gaten' kunnen we denken aan het nemen van maatregelen tegen veel voorkomende en ernstige dreigingen zoals fraude, misbruik, hacking, malware en systeemuitval. Het gaat dan om maatregelen zoals functiescheiding, een autorisatiesysteem met logging, een firewall, antimalware en backup. Als er nog geen ervaren informatiebeveiligingsfunctionaris is, dan valt dat ook in de categorie 'grote gaten' en is snelheid geboden bij het zoeken en aanstellen van een geschikte functionaris. Zo nodig kan tijdelijk een externe op deze positie gezet worden.

De volgende stap heeft tot doel de informatiebeveiliging goed te regelen. Hierin onderscheiden we twee met elkaar samenhangende sporen. Het eerste spoor richt zich op het realiseren van een basisinformatiebeveiliging. Het tweede spoor richt zich op het grondig onder de loep nemen van de essentiële informatiesystemen om te kijken of voor deze systemen aanvullende maatregelen nodig zijn.

3.2 **Basisinformatiebeveiliging**

Nadat de grote gaten zijn gedicht, is het eerste spoor het realiseren van een basisinformatiebeveiliging. Dit is een samenhangende verzameling informatiebeveiligingsmaatregelen die (organisatie)breed wordt ingevoerd. Voor een brede invoering kunnen verschillende redenen zijn:

- De maatregelen werken van zichzelf al (organisatie)breed (bijvoorbeeld huisregels en gedragsrichtlijnen, inbraakbeveiliging van het pand, noodaggregaat tegen stroomstoring).

- De maatregelen gelden voor (bijna) iedereen in de organisatie (bijvoorbeeld de keuze van veilige (generieke) software, classificatierichtlijnen voor informatie, clear desk policy, beveiliging van berichtenverkeer met externe partijen).
- De effectiviteit of de efficiëntie van de maatregelen verbetert als ze breed toegepast worden (bijvoorbeeld centraal incidentmanagement, centrale firewall, standaard antimalware).

De basisinformatiebeveiliging is te beschouwen als een minimumniveau voor de informatiebeveiliging. In de praktijk is gebleken dat verschillende organisaties grotendeels op ongeveer dezelfde lijst maatregelen uitkomt, zelfs voor organisaties uit verschillende branches. Vandaar dat er richtlijnen zijn verschenen, waarin beschreven staat welke maatregelen normaal gesproken in de basisinformatiebeveiliging opgenomen zouden moeten worden.

De meest bekende richtlijn voor de basisinformatiebeveiliging is de 'Code voor Informatiebeveiliging'. Deze richtlijn is een internationale ISO-standaard geworden (ISO/IEC 27002). Verschillende overheidssectoren hebben hiervan een eigen richtlijn afgeleid. Voorbeelden zijn de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Interprovinciale Baseline Informatiebeveiliging (IBI) en de Baseline Informatiebeveiliging Waterschappen (BIWA). Ook bijvoorbeeld de zorg heeft een eigen afgeleide baseline informatiebeveiliging: NEN 7510.

De Code voor Informatiebeveiliging (of een daarvan afgeleide richtlijn) is te hanteren als een checklist om te controleren of alle benodigde basismaatregelen zijn getroffen. Een bijkomend voordeel van het toepassen van de Code voor Informatiebeveiliging is dat de inrichting van de informatiebeveiliging vergelijkbaar is met die van andere organisaties, bijvoorbeeld ketenpartijen, die deze Code ook gebruiken.

De Taskforce BID heeft voor de Rijksdienst een aantal operationele handreikingen uitgewerkt om het invullen van basisinformatiebeveiliging te ondersteunen. De handreikingen zijn te vinden op de website:
www.cip-overheid.nl/bir-operationele-producten-taskforce/.

Voorbeelden van handreikingen die daar te vinden zijn:
- een voorbeeld voor de invulling van informatiebeveiligingsbeleid;
- een handreiking voor de implementatie van de Baseline Informatiebeveiliging Rijksdienst;
- een methodische aanpak om een risicoanalyse uit te voeren;
- beleidsuitgangspunten ten aanzien van informatiebeveiliging voor cloud computing;
- beleidsuitgangspunten ten aanzien van informatiebeveiliging voor mobiele apparaten;
- uitgangspunten voor de invulling van antimalwarebeleid.

Ook de andere overheidssectoren hebben baselines voor informatiebeveiliging en ook voor hen zijn op het internet operationele handreikingen beschikbaar.

3.3 **Essentiële informatiesystemen beveiligen**

Het tweede spoor richt zich op de essentiële informatiesystemen, ofwel de informatiesystemen die zó belangrijk zijn voor de organisatie dat een stagnatie in deze systemen onacceptabele gevolgen heeft. Denk aan schade aan de omgeving, te laat betalen van uitkeringen, of het niet meer kunnen verlenen van belangrijke diensten. Dit kunnen administratieve informatiesystemen zijn, zoals de Basisregistratie Personen van een gemeente, het kentekenregister van de RDW, de uitwissingssystemen in een keten van het sociaal domein, of een Enterprise Resource Planning systeem, maar ook procesbesturingssystemen voor bijvoorbeeld verkeerslichten, waterbeheer en waterzuivering. Stagnatie in dergelijke systemen kan leiden tot grote schade voor de organisatie zelf, of voor de omgeving. Daarom worden hoge eisen gesteld aan de beveiliging ervan.

De eisen aan essentiële informatiesystemen zijn zo hoog dat men er niet op voorhand van uit kan gaan dat de basisinformatiebeveiliging voor deze systemen een voldoende beveiligingsniveau biedt. Het is daarom nodig om deze informatiesystemen en de risico's die daaraan kleven nader te analyseren om te bepalen of er als aanvulling op de basis-informatiebeveiliging nog extra maatregelen nodig zijn.

Hiervoor maakt men gebruik van risicoanalyse. Binnen de overheid worden verschillende methoden gebruikt die qua aanpak sterk op elkaar lijken, zoals IRAM (Information Risk Analysis Methodology) en A&K-analyse (Afhankelijkheids- en Kwetsbaarheidsanalyse). Het uitvoeren van een risicoanalyse is specialistenwerk, maar vraagt voldoende input vanuit de organisatie.

De gebruikelijke gang van zaken is dat eerst het management bepaalt welke processen kritisch zijn voor de organisatie of de omgeving. Dat kan bijvoorbeeld aan de hand van het financieel belang ervan, of het aantal klanten dat geraakt wordt. Ieder van deze processen heeft, of krijgt, een manager die als eigenaar van het proces kan worden beschouwd. De eigenaar stuurt zijn proces aan en is aanspreekbaar voor de goede gang van zaken in het proces. De eigenaar van een kritisch proces bepaalt welke informatiesystemen het betreffende proces ernstig kunnen verstoren.

Voor ieder van deze informatiesystemen wordt een risicoanalyse uit-gevoerd. De eigenaar van het proces is daarvoor verantwoordelijk. Elke risicoanalyse resulteert in een lijst met maatregelen die in aanvulling op de basisinformatiebeveiliging nodig zijn om het onderzochte systeem te beveiligen en de risico's te verkleinen. De aanvullende maatregelen vallen vervolgens onder dezelfde planning-, onderhoud- en controle-processen als de maatregelen in de basisinformatiebeveiliging.

3.4 **Inbedding informatiebeveiliging in reguliere organisatie**

Informatiebeveiliging is een normaal en noodzakelijk onderdeel van alle processen en procedures van de organisatie. Het is dan ook raadzaam om informatiebeveiliging niet als een apart fenomeen te organiseren, maar het op een natuurlijke manier in te bedden in de activiteiten van de organisatie en mee te nemen in de planning & controlcyclus van de organisatie. Dit bevordert niet alleen de aandacht voor informatiebeveiliging, maar zorgt er ook voor dat informatiebeveiliging mee kan liften met de bestaande planning-, onderhoud- en beheersingsprocessen in de organisatie, alsmede de reguliere verantwoording.

In eerste instantie is iedere overheidsorganisatie zelf verantwoordelijk voor de eigen informatieveiligheid. Zij bepaalt zelf hoeveel ze aan informatieveiligheid doet en mobiliseert zelf de kennis en ondersteuning voor informatieveiligheid uit de markt. Overheidsbreed kan de informatieveiligheid worden verbeterd door:

- Het invoeren van centrale sturing op informatieveiligheid, bijvoorbeeld door een Rijks-CISO (Chief Information Security Officer), of strakke regie op een keten.
- Het versterken van de sturing op informatieveiligheid door standaardisatie, (verplichte) zelfregulering, of wetgeving.
- Het centraal of sectoraal faciliteren van informatieveiligheid, bijvoorbeeld door kennisuitwisselingsplatforms.

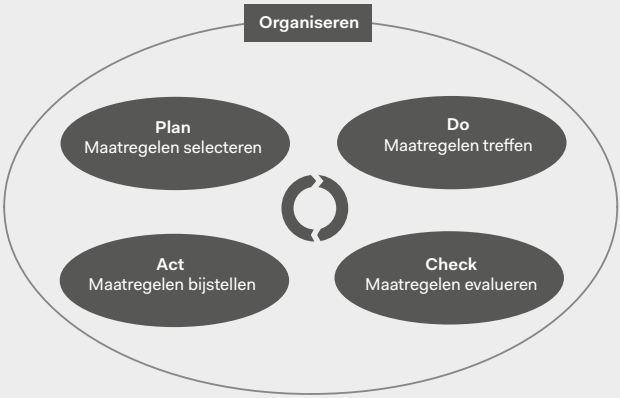
Hoofdstuk 4
Hoe blijft uw organisatie veilig?

Informatiebeveiliging is geen eenmalige exercitie maar een continu proces dat doorlopend aandacht nodig heeft. Door het in te bedden in de andere processen in de organisatie wordt voorkomen dat steeds ad hoc keuzes worden gemaakt.

4.1 PDCA-cyclus

De wereld verandert voortdurend en veranderingen komen steeds sneller, zodat regelmatig gecontroleerd dient te worden of alle getroffen maatregelen nog actueel zijn. Dit geldt zowel voor de basisinformatiebeveiliging, als de aanvullende maatregelen die volgen uit de risicoanalyses. Bovendien dient voor al deze maatregelen gecontroleerd te worden of ze nog goed werken. Informatiebeveiliging is dan ook een iteratief proces dat een PDCA-cyclus (plan-do-check-act) doorloopt (zie figuur 3):

- Plan: maatregelen selecteren.
- Do: maatregelen treffen.
- Check: maatregelen evalueren.
- Act: maatregelen bijstellen.



Figuur 3: De PDCA-cyclus voor informatiebeveiliging.

Randvoorwaardelijk voor de PDCA-cyclus voor informatiebeveiliging is het organiseren ervan. Uiteindelijk moeten eerst mensen taken, verantwoordelijkheden en bevoegdheden krijgen, voordat de stappen uit de PDCA-cyclus uitgevoerd kunnen worden.

> "De provincies hebben een standaardproces ontwikkeld dat erin voorziet dat op basis van een PDCA-cyclus jaarlijks een implementatieplan wordt opgesteld, waarvan de uitvoering wordt gemonitord. De resultaten worden gebruikt om over de voortgang te rapporteren en dienen tevens als input voor het opstellen van het volgende jaarplan."
>
> **Eindrapportage Taskforce Bestuur & Informatieveiligheid Dienstverlening, februari 2015**

4.2 **Informatiebeveiliging in (ICT-)projecten en programma's**

Bij vernieuwing of veranderingen in de informatievoorziening is het noodzakelijk al vroegtijdig informatieveiligheid als aspect mee te nemen. De nieuwe of gewijzigde producten of diensten van de informatievoorziening dienen tenslotte de werkprocessen op effectieve, efficiënte èn veilige wijze te ondersteunen.

Het aspect informatieveiligheid levert geen extra functionaliteit of prestaties. Meestal gaat het juist ten koste van functionaliteit en prestaties. Het is dan ook niet erg aantrekkelijk om veel aandacht te besteden aan informatieveiligheid. Toch is het belangrijk dat dit wel gebeurt, want het in een later stadium veilig(er) maken van onveilige producten of diensten is tijdrovend en duur en levert ook nog minder veilige resultaten op.

In de praktijk betekent dit dat informatiebeveiliging een aandachtspunt is in alle fasen van een project of programma. Zo is het bij de start, het projectplan, het ontwerp, de bouw of aanschaf, alsook het testen een terugkerend aandachtspunt.

In de project- of programmacyclus komt dat neer op onder meer:

- Het vaststellen van de veiligheidseisen. Hiervoor is in het algemeen een risicoanalyse nodig. De veiligheidseisen worden aan het project of programma meegegeven, opgenomen in het project- of programmaplan en meegenomen in het ontwerp.
- Bij het opzetten van een testplan worden de veiligheidseisen ook meegenomen. In het plan wordt beschreven op welke manier er getest wordt en hoe de acceptatie van de nieuwe of gewijzigde producten of diensten van de informatievoorziening plaatsvindt.
- Tijdens het ontwikkelen van nieuwe producten of diensten, of het wijzigen van bestaande producten of diensten, is informatieveiligheid een doorlopend aandachtspunt. Het verdient aanbeveling om ontwikkelmethoden en technieken te gebruiken die zijn geënt op 'security by design'.

Hoofdstuk 5
Wie heeft welke rol?

Informatiebeveiliging is een onderwerp dat iedereen in de organisatie raakt. Enkele actoren hebben een prominente rol in het realiseren van informatieveiligheid. Zij worden in dit hoofdstuk nader voor het voetlicht gebracht.

5.1 **De rol van de bestuurder**

Om succesvol invulling te kunnen geven aan hun werk kunnen bestuurders niet zonder goed informatiebeleid en optimaal werkende ICT-systemen. Bijvoorbeeld in het geval van een complex incident, zoals een brand bij een groot chemiebedrijf, waarbij meerdere partijen zijn betrokken en informatieuitwisseling en goed werkende systemen van cruciaal belang zijn om snel en accuraat te kunnen reageren.

Bij het goed uitvoeren van informatiebeveiliging spelen bestuur en management een cruciale rol. De bestuurder dient dit te zien ziet dit als een belangrijk onderdeel van zijn kaderstellende en controlerende taak. Accountability of rekenschap over dit onderwerp is daarbij onontbeerlijk.

> "Reputatie is een verborgen kroonjuweel van de organisatie. Gedrag, cultuur en vertrouwen zijn daarbij essentieel. Het is van groot belang om informatie over kwetsbaarheden en incidenten te delen en juist naar de boardroom te brengen. De boardroom moet de juiste vragen stellen."
>
> Annemarie Zielstra, Directeur Cybersecurity & Resilience TNO, 2015

5.2 **De rol van het management**

Het management maakt een inschatting van het belang van de verschillende delen van de informatievoorziening voor de organisatie, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management het beleid voor informatiebeveiliging op, draagt het uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Informatiebeveiliging is een integraal onderdeel van de bedrijfsvoering, specifiek gericht op het beheersen van de risico's ten aanzien van de informatiesystemen en de ICT-infrastructuur. Het heeft een sterke relatie met informatiemanagement. En net als de andere onderdelen van de bedrijfsvoering heeft de informatiebeveiliging regelmatig aandacht van het management nodig.

> "Vanwege de steeds verdergaande digitalisering en ontwikkelingen als het Internet of Things is het belangrijk dat we ons bewust blijven van de risico's. Laten we steeds blijven werken aan de juiste balans tussen gemak en dienstverlening èn privacy en informatieveiligheid."
> Bart Drewes, Hoofd Expertisecentrum Informatiebeleid, VNG, 2015

Het management heeft dan ook enige kennis en inzicht op het gebied van informatiebeveiliging nodig om de juiste keuzes te kunnen maken. Het management kan weliswaar allerlei werk op het gebied van informatiebeveiliging delegeren of uitbesteden, maar de eindverantwoordelijkheid ervoor en het maken van de primaire keuzes blijft op het bordje van het management liggen. Vanuit die verantwoordelijkheid kan het management reviews en audits uit laten voeren op de manier waarop de beveiligingsorganisatie is ingericht en functioneert.

Ook het aanwijzen van de medewerkers die een rol krijgen bij de informatiebeveiliging en het toewijzen van de daarbij behorende taken, verantwoordelijkheden en bevoegdheden gebeurt door het management. Hiermee maakt het management een begin met de invulling van infor-matiebeveiliging. Een goed begin is het halve werk. In dit geval

komt dat neer op het toewijzen van taken, verantwoordelijkheden en bevoegdheden aan capabele medewerkers die voldoende tijd en middelen krijgen om hun taken serieus uit te voeren.

> "Er wordt veel over informatiebeveiliging gepraat, maar het krijgt pas handen en voeten als je het ook oefent."
> **Steven Luitjens, Directie Digitalisering en Informatisering Overheid, Ministerie van BZK, 2015**

Omdat informatiebeveiligingsactiviteiten geen vanzelfsprekende voorkeurspositie hebben in het prioriteren binnen de organisatie, hebben de betreffende medewerkers nadrukkelijk ruggensteun nodig van het management. Er moet serieuze aandacht voor (en vraag naar) de rapportages over incidenten en de behaalde resultaten. Daarmee bevordert het management de discipline voor informatiebeveiliging.

> "Het zichtbaar eigenaarschap en persoonlijk commitment van het management, vormen de enige waarborgen voor het mobiliseren van voldoende aandacht voor informatieveiligheid binnen de organisatie."
> **Ad Reuijl, Directeur Centrum voor Informatiebeveiliging en Privacybescherming, 2015**

Bij het toewijzen van taken, verantwoordelijkheden en bevoegdheden spelen twee aspecten een rol:

1 Het eigenaarschap van processen en informatiesystemen.
2 De informatiebeveiligingstaken.

Als informatiebeveiliging in projectvorm op een hoger niveau wordt getild, dan is hiervoor bovendien nog een projectorganisatie nodig.

Het eigenaarschap van processen en informatiesystemen ligt in het algemeen bij lijnmanagers. Een lijnmanager is dan eigenaar van de processen en systemen binnen zijn organisatieonderdeel.

Als eigenaar zorgt de betreffende lijnmanager ervoor dat zijn processen en informatiesystemen voldoende beveiligd zijn. De taken die hiervoor uitgevoerd moeten worden, kan de manager delegeren of uitbesteden. Maar ook grote (verander)programma's verdienen in dit verband aandacht. Het aspect informatieveiligheid zal aandacht moeten krijgen in het handelen, de middelen, de systemen en de informatieuitwisseling van programma- en projectmanagement.
De belangrijkste informatiebeveiligingsfunctie is dan ook het management. Het management is uiteindelijk verantwoordelijk voor de centrale coördinatie en aansturing van informatiebeveiliging. Binnen het topmanagement, bijvoorbeeld het managementteam, is doorgaans één persoon de portefeuillehouder voor de organisatiebrede informatiebeveiliging c.q. informatieveiligheid.

5.3 **De rollen bij informatiebeveiliging**

De andere informatiebeveiligingstaken komen grotendeels terecht bij verschillende informatiebeveiligingsfuncties. De belangrijkste zijn:
- De informatiebeveiligingsfunctionaris.
- De functionaris gegevensbescherming.
- Het projectteam informatiebeveiliging.
- De IT-auditor.

De informatiebeveiligingsfunctionaris
De informatiebeveiligingsfunctionaris, ook wel (Chief/Concern) Information Security Officer of (C)ISO genoemd, is een deskundige op het gebied van informatiebeveiliging en informatieveiligheid en adviseur van het management. De informatiebeveiligingsfunctionaris ondersteunt bij het verbeteren van de informatiebeveiliging en daarmee de informatieveiligheid, maar is er niet voor verantwoordelijk. De verantwoordelijkheid blijft bij het management liggen.

De informatiebeveiligingsfunctionaris heeft een aantal taken:
- Is het aanspreekpunt op het gebied van informatiebeveiliging en informatieveiligheid voor het management.
- Ondersteunt het management bij het opstellen van het informatiebeveiligingsbeleid, het uitdragen van dit beleid en het bewaken van de naleving ervan.

- Zorgt ervoor dat de basisinformatiebeveiligingsmaatregelen worden getroffen en bewaakt de effectiviteit en de naleving ervan.
- Ondersteunt proces- en systeemeigenaren bij het uitvoeren van risicoanalyses en het realiseren van de daaruit voortkomende maatregelen.
- Ondersteunt bij het ontwerpen van beveiligingsmaatregelen en het implementeren en onderhouden van beveiligingsmiddelen.
- Legt een centrale registratie aan voor informatiebeveiligingsincidenten en stelt incidentenrapportages op voor het management.
- Ondersteunt het management bij het uitvoeren van self assessments en het overleggen met externe beveiligingspartijen.

De informatiebeveiligingsfunctionaris wordt in het algemeen in een stafpositie geplaatst. De functiewaardering en de omvang van de functie kan per organisatie verschillen door grootte en complexiteit van de problematiek. Globaal wordt gedacht aan ten minste hbo-niveau met een aanvullende informatiebeveiligingsopleiding en ervaring, alsmede projectleider-, verander- en communicatievaardigheden.

Naast een CISO en/of ISO kunnen er ook een of meer informatiebeveiligingsspecialisten zijn. Zij zijn met name deskundig in de technische aspecten van het beveiligen van informatietechnologie. Ze doen voorstellen voor benodigde beveiligingsmaatregelen en veelal implementeren en onderhouden ze deze ook. Daarnaast hebben ze een adviserende rol over informatiebeveiliging. Qua opleidingsniveau zit een informatiebeveiligingsspecialist veelal op hbo-niveau met aanvullende ICT-opleiding en ervaring. In bijzondere gevallen kan een hoger of lager opleidingsniveau nodig zijn.

De branchevereniging voor informatiebeveiligers, Platform voor Informatiebeveiliging (PvIB), heeft in 2014 nieuwe beroepsprofielen opgesteld voor informatiebeveiligingsfunctionarissen.

De functionaris gegevensbescherming
De functionaris gegevensbescherming (FG), ook wel privacyfunctionaris, Privacy Officer (PO), of Data Protection Officer (DPO) genoemd, is degene die in de organisatie advies geeft en toezicht houdt op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp), oftewel de privacywet. Een FG is, na invoering van de Europese

Privacyverordening, al verplicht als een organisatie persoonsgegevens van 5000 personen of meer op jaarbasis verwerkt.

De functionaris gegevensbescherming heeft een aantal taken:
- Legt een inventarisatie aan van de informatiesystemen waarin persoonsgegevens worden verwerkt.
- Ontwikkelt interne protocollen, procedures en een gedragscode voor het verwerken van persoonsgegevens.
- Beoordeelt Privacy Impact Assesments (PIA's) en adviseert over het toepassen van privacybevorderende technologie en beveiligingsmaatregelen (privacy by design).
- Is het 'loket' voor vragen en klachten van mensen binnen en buiten de organisatie over het verwerken van persoonsgegevens.
- Houdt toezicht op de toepassing en naleving van de protocollen, procedures en gedragscodes voor het verwerken van persoonsgegevens.

Het komt voor dat organisaties de rol van de functionaris gegevensbescherming combineren met die van informatiebeveiligingsfunctionaris. Voor de meeste overheidsorganisaties is het echter beter om beide functies onafhankelijk van elkaar in te vullen, omdat beide functies voldoende complexiteit in zich dragen voor een eigen specialisatie.

Het projectteam informatiebeveiliging
Als de informatiebeveiliging in projectvorm wordt verbeterd, dan is hiervoor een projectorganisatie nodig. Dit is in ieder geval nodig als het verbeteren van de informatiebeveiliging niet door de beschikbare mensen naast hun dagelijkse werkzaamheden uitgevoerd kan worden. Dit is veelal het geval als informatiebeveiliging vanuit een duidelijke achterstandspositie op een redelijk niveau gebracht moet worden. Binnen het projectteam moet dan voldoende oog zijn voor het integreren van informatiebeveiliging in de organisatie.

De IT-auditor
De IT-auditor (ook wel EDP-auditor genoemd) ondersteunt het management en de financial auditor bij het vormen van een oordeel over informatiebeveiligingsaangelegenheden. Het is wenselijk deze verantwoordelijkheid niet bij de informatiebeveiligingsfunctionaris te beleggen, omdat de laatste een belangrijke rol speelt bij het realiseren van informatiebeveiliging. Vanuit een oogpunt van onafhankelijke oordeelsvorming is het beter om beide functies gescheiden te houden. De beroepsorganisatie voor IT-auditors is de NOREA.

"Hoe meer mensen goed zijn opgevoed en opgeleid in het veilig omgaan met gegevens, des te minder incidenten er optreden door onopzettelijke fouten. In het Verenigd Koninkrijk en Israël heeft men dit goed begrepen. Daar krijgt iedereen verplicht ICT-onderwijs. Hierdoor vergroot het inzicht in en de affiniteit met ICT, maar ook het inzicht in de kwetsbaarheden ervan en het draagvlak voor noodzakelijke beveiligingsmaatregelen."

Verkenning informatieveiligheid buitenland, Taskforce BID, 2014

Hoofdstuk 6
Informatiebeveiliging met anderen

Organisaties staan niet op zichzelf. Niet alle expertise is in eigen huis: soms is het effectiever of efficiënter om producten te kopen, expertise in te huren, of taken uit te besteden. Daarnaast werken overheidsorganisaties op structurele of incidentele basis samen met andere publieke en private partijen in ketens en netwerken.

6.1 **Inkoop en inhuur**

In een aantal gevallen kan het aantrekkelijk te zijn om (beveiligings)producten te kopen, of expertise in te huren. Het is dan wel nodig om vroegtijdig aan mogelijke leveranciers kenbaar te maken welke veiligheidseisen worden gesteld aan de producten of medewerkers. In plaats van het opnemen van deze eisen in een bestek of aanbestedingsdocument en ze achteraf te toetsen, werkt het in de praktijk beter om gedurende het inkoop- of inhuurtraject hierover in gesprek te blijven.

Eisen met betrekking tot de veiligheid van producten kunnen betrekking hebben op:
- Beveiligingsnormen waaraan het product voldoet.
- Reviews die op het product zijn uitgevoerd.
- Certificaten die het product heeft.
- Ingebouwde beveiligingsmaatregelen.

Eisen met betrekking tot de veiligheid van ingehuurde mensen kunnen betrekking hebben op:
- Blijken van integriteit (bijvoorbeeld een VOG).
- De te volgen gedrag- en geheimhoudingsregels.
- Bekendheid met relevante veiligheidsstandaarden.
- Controle en toezicht door de opdrachtgever.

Meer informatie over informatiebeveiliging bij inkoop en inhuur is te vinden in bijvoorbeeld de *CIP-publicaties Grip op Secure Software Development* en *Grip op Beveiliging in Inkoopcontracten.*

6.2 **Uitbesteding**

Het realiseren van informatieveiligheid in een organisatie is lastig. Het lijkt dan ook aantrekkelijk om dit uit te besteden. Vooral als de automatisering al geheel of gedeeltelijk is uitbesteed aan een externe partij, dan ligt het voor de hand dat zij de beveiliging er wel bij kunnen doen. Daar zitten echter twee adders onder het gras.

Ten eerste is informatiebeveiliging meer dan het treffen van beveiligingsmaatregelen in de automatisering. Informatiebeveiliging omvat ook het aansturen en coördineren van de informatiebeveiliging en het beveiligen van de niet-geautomatiseerde informatiesystemen. Dit valt niet onder de automatisering en kan dan ook niet neergelegd worden bij de externe partij waaraan de automatisering is uitbesteed.

Ten tweede is uitbesteden geen wondermiddel. Uitbesteden betekent niet dat alleen de dienstverlener werk verricht, maar dat beide partijen een inspanning leveren, dus ook de opdrachtgever, in dit geval de eigen organisatie. De regieorganisatie speelt hierbij een belangrijke rol. Het werk van de regieorganisatie is niet uit te besteden.

Uitbesteden mag dan geen wondermiddel zijn, in veel situaties kan het zeer nuttig zijn. We kunnen voor uitbesteden onderscheid maken tussen de volgende twee zaken:

- Het uitbesteden van informatiebeveiligingstaken of diensten. Bijvoorbeeld het uitbesteden van de inrichting en het beheer van de firewall aan een daarin gespecialiseerd bedrijf.
- Het (mee) uitbesteden van het aspect informatieveiligheid. Bijvoorbeeld het uitbesteden van (een deel van) de automatisering. Normaal gesproken zorgt de externe dienstverlener dan ook voor het beveiligen van deze automatisering.

Uitbesteden kan gebeuren aan een commerciële externe marktpartij, maar ook aan een Shared Services Organisatie,

of een andere organisatie. In alle gevallen is, gezien vanuit de uitbestedende organisatie, sprake van een externe partij.

Voor- en nadelen
Uitbesteden heeft voordelen, maar ook nadelen. Voordelen zijn onder meer dat een in informatiebeveiliging gespecialiseerde leverancier dit beter kan regelen, en wellicht, door schaalvoordelen ook nog goedkoper. De eigen organisatie kan zich dan weer toeleggen op haar kerntaken.

Uitbesteden heeft echter ook nadelen, zoals de afhankelijkheid van de dienstverlener, inflexibiliteit door "afspraak is afspraak", extra kosten voor onder andere winst- en risicomarge, de kosten voor de noodzakelijke transitie en een beperkte looptijd van het contract. In de praktijk rekenen veel organisaties zich rijk bij het maken van plannen voor uitbesteding. Als de uitbesteding eenmaal gerealiseerd is, blijkt de situatie veelal minder rooskleurig te zijn. Dan blijkt bijvoorbeeld een beveiligingsdienst niet zo goed(koop) te zijn als gedacht, of bij een automatiseringsdienst blijkt de beveiliging niet ingecalculeerd te zijn. Voor uitbesteden geldt: "bezint eer ge begint".

> "De overheid mag haar hoofd niet verliezen bij alle technologische kansen die zich nu voor doen. Een veilige samenleving vereist zorgvuldige afspraken."
> Anneke van Zanen-Nieberg, Algemeen directeur Auditdienst Rijk, 2015

Service Level Management
Als een organisatie tot uitbesteden wil overgaan dan wordt in de besluitvormingsfase aan de hand van een business case beoordeeld of, en in welke mate, uitbesteding zinvol is. In de selectiefase wordt een geschikte dienstverlener geselecteerd en daar worden afspraken mee gemaakt. De afspraken komen in een formeel document, een Service Level Agreement (SLA). Als de uitbesteding betrekking heeft op het aspect informatieveiligheid van, bijvoorbeeld, uit te besteden automatisering, dan komen in de SLA voor de betreffende automatisering de afspraken over de beveiliging te staan. Aangezien de organisatie zelf eindverantwoordelijk is voor de informatieveiligheid, dient zij zelf aan te geven welk beveiligingsniveau nodig is.

Na het afsluiten van de SLA vindt de transitie plaats naar de dienstverlener. In de dienstverleningsfase is de uitbesteding een feit en levert de dienstverlener de overeengekomen diensten.

De dienstverlener is weliswaar verantwoordelijk voor de te leveren diensten, maar de uitbestedende organisatie zal, als opdrachtgever, de dienstverlening moeten bewaken en de dienstverlener moeten aansturen. Dit is een continue activiteit die wordt belegd bij een specifiek organisatieonderdeel, de regieorganisatie. De meeste organisaties hebben het aansturen van hun externe partijen ondergebracht in één regieorganisatie, maar er kunnen meerdere regieorganisaties zijn.

In de regieorganisatie voor de partijen die beveiligingsdiensten leveren, zitten medewerkers met kennis en inzicht op het gebied van informatieveiligheid, en kennis en inzicht op het gebied van aansturing van externe partijen. Het goed aansturen van externe partijen in de vorm van Service Level Management wordt gemakkelijk onderschat, zowel in belang als in moeilijkheidsgraad. Het is belangrijk dat in de regieorganisatie capabele medewerkers zitten met voldoende tijd en middelen.

Toetsing
Om de dienstverlening bij de dienstverlener op locatie te kunnen controleren, kan de regieorganisatie audits uitvoeren, of een onafhankelijke auditorganisatie dit laten doen. Een IT-auditor kan, na toetsing namens de eigenaar, over de aangetroffen situatie een zogenaamde Third Party Mededeling doen. In beide gevallen dienen hierover duidelijke afspraken te zijn gemaakt over de invulling en de betaling van de kosten in de SLA. Bovendien zijn afspraken nodig over hoe beide partijen omgaan met de geconstateerde gebreken.

6.3 **Samenwerkingsverbanden**

Informatieveiligheid binnen ketens en netwerken is een lastig onderwerp. Omdat informatiesystemen en informatiestromen steeds meer met elkaar verknoopt raken, kan het zicht op de herkomst en de betrouwbaarheid van de gegevens vertroebelen. Organisaties in een keten of netwerk kunnen gelijke doelen, belangen en terminologie hebben, maar in het algemeen is dat niet het geval.

Veelal is er vanuit een organisatie in de keten of het netwerk geen goed zicht op de hele keten c.q. netwerk. Het is dan ook een illusie om de informatiebeveiliging voor de hele keten c.q. netwerk in kaart brengen, laat staan te specificeren. Het is al mooi als alle aangesloten partijen dezelfde standaarden gebruiken voor hun basisinformatiebeveiliging en risicoanalyse.

Toch is er in een keten of netwerk wel het één en ander aan informatieveiligheid te doen. Voor iedere aangesloten organisatie begint het bij het op orde brengen van de informatieveiligheid in de eigen organisatie. Bij voorkeur wordt gebruik gemaakt van gemeenschappelijke standaarden voor de basisinformatiebeveiliging en risicoanalyse. Vervolgens wordt in kaart gebracht welke informatiesystemen gegevens krijgen van of leveren aan andere (externe) informatiesystemen. Voor alle ingaande informatiestromen worden afspraken gemaakt over de herkomst en de betrouwbaarheid van de betreffende gegevens en de eventuele bewijzen ervan. Voor alle uitgaande informatiestromen worden afspraken gemaakt over gebruiksrechten en plichten van de betreffende gegevens, in hoeverre er beperkingen zijn voor 'doorleveren' en de eventuele toetsing ervan.

Hoofdstuk 7
Praktische tips

In de voorgaande hoofdstukken zijn aspecten genoemd waarvan de manager in een overheidsorganisatie zich bewust zou moeten zijn. In dit hoofdstuk geven we enkele praktische tips waarmee u direct aan de slag kunt.

1 Controleer of uw beeld klopt
Informatieveiligheid is cruciaal. Onderzoeken uit de praktijk laten zien dat veel cyberdreigingen op een organisatie afkomen. Als manager sta je hier veelal niet bij stil. Zonder goede informatiebeveiliging zouden aan de lopende band incidenten optreden. Gelukkig zijn er binnen vrijwel elke organisatie al heel wat maatregelen getroffen. Vaak geïnitieerd door de betrokken uitvoerende medewerkers, zoals ICT- en personeelsfunctionarissen. Veel incidenten worden hierdoor al voorkomen.
Maar niet allemaal.

Managers krijgen in het algemeen te weinig informatie over informatieveiligheid, zodat zij hun ideeën over wat er kan gebeuren, en de ernst ervan, te weinig kunnen baseren op objectieve feiten. Daardoor onderschatten ze wellicht het belang en laten het ad hoc karakter van informatiebeveiliging toe. Het gaat te ver om van alle managers te vragen om zich inhoudelijk te verdiepen in de laatste onderzoeksrapporten, maar het is wel verstandig als zij zich kort en bondig en op regelmatige basis op de hoogte laten stellen door deskundigen van binnen of van buiten de organisatie. Dit bevordert bovendien de dialoog over informatiebeveiliging en informatieveiligheid tussen het management en andere medewerkers met taken op het gebied van informatiebeveiliging.

2 Investeer in goede mensen
Informatiebeveiliging is complex en specialistisch werk. Daarvoor zijn goede informatiebeveiligers nodig. Niet overal zijn de informatiebeveiligingsrollen toereikend ingevuld. Het komt geregeld voor dat beveiligingstaken worden toegewezen aan medewerkers die daar niet voldoende tijd voor hebben of de benodigde integrale kennis en inzicht missen om deze taken effectief en efficiënt aan te pakken. Daardoor ondersteunen zij het

management onvoldoende. Het is dan ook van belang om te investeren in goede en goed geschoolde informatiebeveiligers.

Informatiebeveiligers zijn veelzijdige mensen. Zij zijn thuis in de kenmerken en eisen van de business, de informatievoorziening en de (informatie) technologie. Ze kunnen goed plannen, analyseren en communiceren. Zij hebben kaas gegeten van veranderprocessen. Ze kennen nieuwe toepassingen en technologie, zoals cloud computing, BYOD (bring your own device) en het Internet of Things, alsook nieuwe dreigingen, zoals phishing, botnets, APT's (advanced persistent threats) en ransomware. Het is dan ook niet makkelijk om voldoende goede informatiebeveiligers te vinden. Toch is het de verantwoordelijkheid van het management om ervoor te zorgen dat deze mensen er zijn.

Goede informatiebeveiligers vinden en aannemen is cruciaal voor informatieveiligheid, maar niet voldoende. Informatiebeveiligers kunnen tegenwoordig overal werk vinden. Daarom is het belangrijk om deze mensen aan de organisatie te binden met uitdagend werk, voldoende autonomie, goede ontplooiingsmogelijkheden en een redelijke beloning. Bovendien is het nodig om informatiebeveiligers ook op langere termijn op niveau te houden, zowel voor hun ontplooiing, als voor hun effectiviteit in de organisatie. Daarom hebben informatiebeveiligers regelmatig training, bijscholing en stimulans nodig. Daar moet tijd voor vrijgemaakt worden. Door de waan van de dag lijkt er nooit een goed moment voor (bij)scholing en training te zijn, daarom is het verstandig om dit soort activiteiten stringent in te roosteren, met volledig commitment van het management.

3 Geef het goede voorbeeld en werk aan bewustwording
Informatiebeveiliging is een zaak van managers én medewerkers. Medewerkers zijn in principe van goede wil, maar kijken wel naar de managers. De managers moeten dan ook het goede voorbeeld geven. Dit is noodzakelijk voor de medewerking van de medewerkers, maar er komt meer bij kijken.

De activiteiten voor informatiebeveiliging kunnen het best op een natuurlijke manier zijn ingebed in de processen van de organisatie en het handelen van de medewerkers.

Hierdoor zullen medewerkers de activiteiten voor informatiebeveiliging niet zo makkelijk over het hoofd zien en niet als extra belasting ervaren. Het management dient erop toe te zien dat informatiebeveiliging op een dergelijke natuurlijke manier wordt ingebed en hun informatiebeveiligers daarbij steunen.

Informatieveiligheid staat of valt met het draagvlak voor de informatiebeveiligingsmaatregelen die getroffen worden. Het draagvlak hiervoor wordt gelegd door de medewerkers te betrekken bij het selecteren en implementeren van deze maatregelen. Aan de andere medewerkers moet de redelijkheid van de maatregelen uitgelegd kunnen worden. Vervolgens moeten de maatregelen natuurlijk wel ingevoerd worden zoals ze naar de medewerkers zijn besproken en uitgelegd.

Last but not least moeten medewerkers wel weten wat ze moeten doen om veilig met informatie te werken. Medewerkers moeten dan ook voldoende geïnformeerd zijn. Dit geldt vooral voor medewerkers die nieuw zijn, of een andere taak of functie hebben gekregen.

4 Inventariseer wet- en regelgeving

Elke organisatie moet zich houden aan de vigerende wet- en regelgeving. Hiervan is inmiddels een hele verzameling die geheel of gedeeltelijk gericht zijn op informatiebeveiliging. Voorbeelden zijn:

- De Wet Bescherming Persoonsgegevens.
- De Archiefwet.
- De Wet Meldplicht Datalekken.
- De Wet Computercriminaliteit.
- De Telecommunicatiewet.
- De Auteurswet.

Het is verstandig om vroegtijdig de relevante wet- en regelgeving te inventariseren en de informatiesystemen en informatiebeveiliging daarop af te stemmen. Ook is het verstandig zicht te houden op nieuwe regels, zoals de Europese privacyverordening die naar verwachting in 2016 van kracht wordt.

Een bijkomend voordeel is dat het dan ook mogelijk is om de benodigde inspanningen en producten voor de verschillende wet- en regelgeving op elkaar af te stemmen. Bovendien hoeft men niet meer bang te zijn op

enig moment verrast te worden door een controlerende instantie.

5 Gebruik standaarden
Informatiebeveiliging heeft een lange historie. In de loop van de tijd hebben veel organisaties hun ervaringen gebundeld in richtlijnen. Bij voldoende brede erkenning kunnen deze doorgroeien tot standaarden. De organisatie hoeft zelf dan ook geen wielen uit te vinden. Het is handiger om geschikte richtlijnen en standaarden te zoeken en die te gebruiken. Dat heeft als bijkomend voordeel dat de informatiebeveiliging te vergelijken is met die van andere organisaties die dezelfde richtlijnen en standaarden gebruiken.

Op het gebied van informatiebeveiliging springen een paar standaarden er qua relevantie uit. De belangrijkste hiervan zijn ISO/IEC 27001 en 27002 en de daarvan afgeleide baselines voor informatiebeveiliging voor de verschillende overheidssectoren. Deze standaarden zijn binnen elke middelgrote en grote organisatie zeer goed toepasbaar. Ze schetsen een reeks maatregelen met een organisatiebrede scope op de volgende aandachtsgebieden:
- Beveiligingsbeleid.
- Organisatie van informatiebeveiliging.
- Beheer van bedrijfsmiddelen.
- Beveiligingseisen ten aanzien van personeel.
- Fysieke beveiliging en beveiliging van de omgeving.
- Beheer van communicatie- en bedieningsprocessen.
- Toegangsbeveiliging.
- Verwerving, ontwikkeling en onderhoud van informatiesystemen.
- Beheer van informatiebeveiligingsincidenten.
- Bedrijfscontinuïteitsbeheer.
- Naleving.

Daarnaast zijn voor iedere sector ook sectorspecifieke verdiepende richtlijnen en standaarden beschikbaar. Sommige hiervan zijn ook buiten de eigen sector goed toepasbaar. Bijvoorbeeld de CIP-publicatie Grip op Secure Software Development.

6 Actualiseer procedures
Incidenten zijn veelal te herleiden tot het overtreden van procedures. Procedures uit het verleden, die wellicht ooit goed zijn ingevuld, maar

die al jaren niet worden nageleefd. En als de procedures gevolgd zouden worden, dan draaien de primaire processen in de soep. Aan zulke procedures heeft de organisatie niets; ze zijn alleen te gebruiken voor zwartepieten na een incident. Ook informatieveiligheid komt met zulke procedures geen stap verder. Procedures zijn alleen zinvol als ze kort en duidelijk zijn, nodig zijn, passen bij de organisatie en de processen, gedragen worden door de medewerkers en geregeld worden geactualiseerd.

7 Integreer informatiebeveiliging
Informatiebeveiliging staat niet op zichzelf. Het behoort op een natuurlijke manier te zijn ingebed in de processen van de organisatie. Informatiebeveiliging kan daarvoor het beste worden meegenomen in de normale planning & control cyclus van de organisatie. Hierdoor wordt informatiebeveiliging een vanzelfsprekend aandachtspunt van de organisatie. Voor het informatiebeveiligingsbeleid gelden dan dezelfde regels als voor de overige activiteiten die de organisatie draaiende moeten houden: er wordt jaarlijks beleid bijgesteld, bij de budgetaanvraag wordt een kosten/batenafweging gemaakt, acties worden benoemd, de benodigde mensen en middelen worden inzichtelijk gemaakt en jaarlijks wordt verantwoording afgelegd.

Hierbij kan het beste zoveel mogelijk gebruik gemaakt worden van bestaande procedures. De voor informatiebeveiliging benodigde activiteiten kunnen hierin veelal prima worden opgenomen. Informatiebeveiliging wordt dan ‘vanzelf’ een integraal onderdeel van de processen van de organisatie. Bovendien kan in de periodieke risicoanalyse van de primaire processen de kwetsbaarheid van de informatiesystemen worden meegenomen. Daaruit komen immers de eisen met betrekking tot de informatiebeveiliging.

8 Test uw informatieveiligheid
Eventuele gaten in de informatiebeveiliging kunnen ook zichtbaar gemaakt worden met penetratietesten (ethische hacking) en social engineering (mystery guests). Met een penetratietest wordt door een deskundige van buitenaf via het internet getest hoe goed de beveiliging van de informatiesystemen is. Met social engineering wordt door een deskundige getest in hoeverre de medewerkers van de organisatie bestand zijn tegen aanvallers die misbruik maken van menselijke zwakheden.

Daarnaast kan het geen kwaad om op regelmatige basis reviews of beveiligings- en privacy-audits uit te laten voeren. Deze geven goed inzicht in de getroffen maatregelen op organisatorisch en technisch gebied. Verder kunt u bij het ontwikkelen of inkopen van nieuwe systemen specifieke controles eisen zoals een privacy impact assessment (PIA) en kwaliteitsmetingen van de software.

9 Leer van incidenten

Incidenten laten de zwakke kanten van de informatiebeveiliging zien. Als de informatiebeveiliging nog niet op orde is, dan geven de incidenten bovendien een indicatie van de dreigingen die zoal voorkomen. Veel (kleine) incidenten zullen echter niet eens opgemerkt worden, omdat daarvoor geen detectie is geregeld. En als ze wel worden opgemerkt, dan is het onvoorspelbaar waar de meldingen daarover terechtkomen en of er überhaupt iets mee gedaan wordt. Bovendien zijn medewerkers zich er vaak niet van bewust dat ze naast elkaar slachtoffer zijn van dezelfde dreigingen. En ieder voor zich maken ze daar geen melding van.

Daardoor ligt het werkelijke aantal incidenten en de daaruit resulterende schade in de praktijk meestal beduidend hoger dan het management denkt. Er kan een volledig misplaatst gevoel van veiligheid ontstaan, omdat “bij ons nooit wat gebeurt”. Het lijkt of de informatiebeveiliging wel op orde is, terwijl het tegendeel het geval is. Een goede registratie van incidenten, klein en groot, en een periodiek rapportage daarover, kan het inzicht in de dreigingen, incidenten en opgelopen schade verbeteren. Dit kan helpen bij het beter stellen van prioriteiten.

Een bijzondere plaats nemen ernstige incidenten op het gebied van informatiebeveiliging in. Uiteraard komt ieder incident ongelegen. Toch zit er ook een positief kantje aan. Een incident kan namelijk gebruikt worden om de medewerkers met hun neus op de feiten te drukken. Een incident, en vooral een ernstig incident, geeft aan dat er wat schort aan de informatiebeveiliging. De meeste medewerkers onderkennen in een dergelijke situatie het falen van de informatiebeveiliging en hun aandeel daarin en zijn bereid daar wat aan te doen. Meestal zijn ze zelfs bereid om zich ook nog extra in te spannen voor het verbeteren van andere aspecten van de informatiebeveiliging. Deze bereidheid duurt echter maar enkele dagen tot weken en verdwijnt dan weer. Na een ernstig incident is dus een snelle reactie nodig om van dit effect te kunnen profiteren.

10 Leer van anderen

Informatiebeveiliging is een onderwerp waar elke organisatie aan moet werken. Veel organisaties hebben hier al waardevolle ervaringen mee opgedaan in de praktijk. Veelal zijn deze organisaties bereid hun ervaringen met u te delen. Start het overleg op en wissel ervaringen uit. Het Centrum voor Informatiebeveiliging en Privacybescherming heeft de afgelopen jaren een platform gecreëerd waarin kennis wordt ontwikkeld en uitgewisseld. Hierin werken overheden en marktpartijen samen. Koepelorganisaties, zoals de VNG, dragen bij aan het ontwikkelen en delen van kennis, door het organiseren van informatiebijeenkomsten, opstellen van factsheets en praktische handreikingen en het delen praktijkervaringen. Ook ander overheidslagen organiseren dit soort zaken. Laat u zo nodig bijstaan door een ervaren adviseur.

Hoofdstuk 8
Tot slot

Informatiebeveiliging is geen keuze; informatiebeveiliging moet! Bij onvoldoende aandacht is de informatieveiligheid in het geding en kunnen gegevens over burgers en bedrijven aangetast raken, of in verkeerde handen komen. De bedrijfsvoering van organisaties kan in gevaar komen. Hoge kosten en een slecht imago zijn het gevolg.

Met een toenemend gebruik van het internet en steeds nieuwe functionaliteiten komen er steeds nieuwe dreigingen bij. Cybercriminelen, cyberspionnen en cyberterroristen vormen in het huidige tijdvak dreigingen die niet meer gebagatelliseerd mogen worden. Mede daardoor neemt de kans op incidenten met een grote impact toe. Dit soort incidenten kan het vertrouwen van burgers en bedrijven in publieke organisaties aantasten. Dat kan de overheid zich niet permitteren. Voldoende aandacht voor informatiebeveiliging is dan ook broodnodig.

Informatiebeveiliging kent vele technische, organisatorische en menselijke aspecten. Het aandachtsgebied is verre van triviaal. Aan de andere kant verschilt het aansturen ervan niet zo erg veel van het aansturen van andere bedrijfsprocessen. Eigenlijk stoelt het aansturen van informatiebeveiliging vooral op alertheid, gezond verstand en het inzetten van goede mensen. Veel tijd hoeft dat het management niet te kosten, maar op zijn tijd enige gerichte aandacht is wel noodzakelijk.

Hoewel de verleiding misschien groot is, is het niet verstandig te bezuinigen op de capaciteit en vooral ook de kwaliteit van de medewerkers voor informatiebeveiliging. Het functioneren van uw organisatie is dusdanig afhankelijk van betrouwbare informatie dat u en de burger de zekerheid moeten hebben dat deze in goede handen is.

In dit boekje hebben we de belangrijkste ins en outs van informatiebeveiliging en informatieveiligheid voor u als manager geschetst. Als u uw informatiebeveiliging goed op de rails heeft, dan zijn ook nieuwe cyberdreigingen voor u hanteerbaar.

Bedenk echter wel dat informatiebeveiliging geen eenmalige exercitie is; het is een continu proces dat steeds gerichte aandacht nodig heeft.

Checklist voor de manager

Informatieveiligheid op niveau krijgen

De volgende vragen kan de manager of bestuurder zich stellen ten aanzien van het op niveau krijgen van de informatieveiligheid:

- Heeft u geïnventariseerd waar mogelijk 'grote gaten' in de informatiebeveiliging zitten en heeft u die allemaal gedicht?
- Heeft u een beleid voor informatieveiligheid opgezet, dit duidelijk naar de organisatie gecommuniceerd en bewaakt u zichtbaar de navolging ervan?
- Is het eigenaarschap van alle processen en informatiesystemen duidelijk belegd en zijn de betreffende managers zich bewust van de consequenties daarvan?
- Heeft u een basisinformatiebeveiliging ingevoerd en is het onderhoud en de bewaking ervan in de organisatie belegd?
- Heeft u geïnventariseerd welke informatiesystemen kritisch zijn en worden daar risico-analyses voor uitgevoerd?
- Heeft u ervaren medewerkers, waaronder een informatiebeveiligingsfunctionaris, die u kunnen ondersteunen bij het ontwerpen en inrichten van informatiebeveiliging?
- Worden de andere medewerkers voldoende betrokken bij het selecteren en implemen-teren van informatiebeveiligingsmaatregelen?
- Is informatiebeveiliging op een natuurlijke manier ingebed in de activiteiten van de or-ganisatie en het handelen van de medewerkers?
- Als u gebruik maakt, of wil gaan maken, van uitbesteding, heeft u daarvoor dan een goede business case en een adequate regieorganisatie?
- Heeft u geïnventariseerd welke wet- en regelgeving voor uw organisatie relevant is en voldoen de organisatie en eventuele externe dienstverleners daar ook aan?
- Maakt u gebruik van standaarden voor informatiebeveiliging, zoals de ISO/IEC 27001 en 27002 of daarvan afgeleide sectorale standaarden (bijvoorbeeld de BIR)?

Informatieveiligheid op niveau houden

De volgende vragen kan de manager of bestuurder zich stellen ten aanzien van het op niveau houden van de informatieveiligheid:

- Heeft u regelmatig contact met deskundigen van binnen en van buiten de organisatie om u op de hoogte laten stellen van de status van de informatiebeveiliging?
- Besteedt u voldoende aandacht aan informatiebeveiliging en geeft u zelf het goede voorbeeld?
- Heeft u ervaren medewerkers, waaronder een informatiebeveiligingsfunctionaris, die u kunnen ondersteunen bij het op niveau houden van informatiebeveiliging?
- Is informatiebeveiliging op een natuurlijke manier ingebed in de activiteiten van de or-ganisatie en het handelen van de medewerkers?
- Heeft u een accurate registratie van alle gesignaleerde incidenten, klein en groot, zodat u lering kunt trekken uit de opgetreden incidenten?
- Worden regelmatig audits uitgevoerd op de informatiebeveiliging binnen de organisatie, en indien van toepassing bij de externe dienstverleners?
- Heeft u overleg met andere organisaties om regelmatig ervaringen op het gebied van informatiebeveiliging uit te wisselen?
- Neemt u bij veranderingen in de informatievoorziening tijdig informatieveiligheid mee als een cruciaal thema?
- Heeft u aandacht voor de informatieketens en -netwerken waar uw organisatie deel van uitmaakt en de risico's die u daarin loopt?

Literatuur

1. *Baseline Informatiebeveiliging Rijksdienst,* Ministerie van BZK, 2012.
2. *Baseline Informatiebeveiliging Nederlandse Gemeenten,* KING-IBD, 2013.
3. *Baseline Informatiebeveiliging Waterschappen,* Unie van Waterschappen, 2013.
4. *Beroepsprofielen informatiebeveiliging,* M. Spruit en F. van Noord, Platform voor Informatiebeveiliging, 2014.
5. *Cybercrime kost Nederland jaarlijks 8 miljard,* http://www.volkskrant.nl/recensies/cybercrime-kost-nederland-jaarlijks-8-miljard~a3669671/. De Volkskrant, 2015
6. *Cybersecuritybeeld Nederland CSBN-4,* Nationaal Cyber Security Centrum, 2014.
7. *Eindrapportage Taskforce Bestuur & Informatieveiligheid Dienstverlening,* Taskforce BID, 2015.
8. *Grip op beveiliging in inkoopcontracten,* CIP, 2014.
9. *Grip op Secure Software Development (SSD),* CIP, 2015.
10. *Handreiking Cybersecurity voor de bestuurder,* CSR, 2015.
11. *ICT-beveiligingsrichtlijn voor webapplicaties,* NCSC, 2012 en 2015.
12. *Informatiebeveiliging voor de overheid*, een paktische aanpak, Het Expertse Centrum, Papernote nr. 12. Boudien Glashouwer e.a., 2002.
13. *Informatiebeveiliging onder controle,* P. van Houten, M. Spruit en K. Wolters Pearson, 2015.
14. *Integratie van informatiebeveiliging,* M. Spruit, Informatie, nr. 8, 2006, blz. 8-11.
15. *Interprovinciale Beseline Informatiebeveiliging,* IPO, 2010.
16. *Nationale Cybersecurity Strategie 2,* NCTV, 2013.
17. *NEN-ISO/IEC 27001: 2013 nl, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen,* NEN, 2013.
18. *NEN-ISO/IEC 27002: 2013 nl, Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging,* NEN, 2013.
19. *Opgeruimd staat netjes? Uitbesteden van ICT in de publieke sector,* C. Wauters, M. Spruit en M. Vermeulen. SDU, 2008.
20. *The cost of cyber crime,* Detica and The Cabinet Office, 2011.
21. *Verkenning informatieveiligheid buitenland,* Taskforce BID, M. Spruit en N. Ducastel, 2014.
22. *Voorschrift Informatiebeveiliging Rijksdienst 2007,* Ministerie van BZK, 2007.
23. *Zakboekje preventie cybercrime, voor management en bestuur van gemeenten,* Marcel Spruit, Boudien Glashouwer, Het Expertise Centrum, 2008.

Trefwoorden

Audit
Een onderzoek naar de kwaliteit van een product, proces of organisatie door een onafhankelijke partij.

Basisinformatiebeveiliging (baseline voor informatiebeveiliging):
Een samenhangende verzameling informatiebeveiligingsmaatregelen die organisatie breed worden ingevoerd.

Beschikbaarheid
De mate waarin informatie op de juiste momenten beschikbaar is voor gebruikers.

Beveiligingsmaatregel
Een product of proces dat beoogt te voorkomen dat een dreiging tot een incident leidt, of anders de schade beperkt.

Business case
Een document waarin alle motieven, voor- en nadelen, risico's en keuzemogelijkheden van een te nemen beslissing zorgvuldig zijn beschreven en gewogen.

Cloud
Modern synoniem voor het internetdomein.

Cloud computing
Het via het internet beschikbaar stellen van ICT-middelen.

Contract
Een formele overeenkomst waarin twee of meer partijen afspraken vastleggen.

Cybercrime
Criminaliteit waarbij gebruik wordt gemaakt van het internet.

Cybersecurity
Het beveiligen van de cyberspace, ofwel de ICT en het internet.

Cyberspionage
Spionage waarbij gebruik wordt gemaakt van het internet.

Cyberterrorisme
Terrorisme waarbij gebruik wordt gemaakt van het internet.

Dreiging (bedreiging)
Een proces of gebeurtenis die in potentie tot een incident kan leiden.

ICT
Informatie- en communicatietechnologie**.**

Impact
De gevolgen van een dreiging die zich manifesteert.

Incident
Een ongewenste gebeurtenis die tot schade – financieel of anderszins – heeft geleid.

Informatiebeveiliging
Het treffen en onderhouden van een samenhangend pakket maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorziening te borgen.

Informatiesysteem
Een systeem voor het verzamelen, bewerken, opslaan, distribueren en presenteren van gegevens.

Informatieveiligheid
Het niveau van beschikbaarheid, integriteit en vertrouwelijkheid van de informatie voorziening.

Informatievoorziening
De verzameling informatiesystemen en de daarvoor benodigde infrastructuur.

Integriteit
De mate waarin informatie is zoals die bedoeld is, dus correct, compleet, actueel, etc.

Opdrachtgever
Een organisatie(onderdeel) die een gegeven partij een formele opdracht geeft, bijvoorbeeld voor uitbesteding.

Preventie
Het voorkómen van een incident.

Regieorganisatie
Een organisatieonderdeel waar de regievoering ten aanzien van een of meer dienstverleners is belegd, oftewel de aan-sturing van de dienstverlener(s) vanuit de opdrachtgever.

Repressie
Het reduceren van de schade na een opgetreden incident.

Risico
De jaarlijks te verwachten schade door het manifesteren van een of meer dreigingen.

Risicoanalyse
Een methode die inventariseert welke risico's er zijn, welke daarvan onacceptabel zijn en welke maatregelen de risico's kunnen reduceren.

Risicomanagement
Het proces dat beoogt risico's te inventariseren en te beheersen.

Schade
De negatieve gevolgen van een incident, financieel of anderszins. Schade omvat de directe schade, bijvoorbeeld om een beschadigd onderdeel te vervangen, en de gevolgschade, bijvoorbeeld het verlies van klanten.

Service Level Agreement (SLA)
Een formele overeenkomst waarin het kwaliteitsniveau van te leveren diensten beschreven staat. Een SLA kan deel uitmaken van een contract.

Service Level Management (SLM)
Het proces of de functie waarin zich de afstemming tussen de opdrachtgever en de dienstverlener afspeelt.

Shared service organisatie (SSO)
Een organisatie die ontstaat als meerdere partijen een deel van hun activiteiten samenvoegen en al dan niet op afstand plaatsen.

Uitbesteding
Het beleggen van taken en verantwoordelijkheden bij een of meer externe dienstverleners.

Vertrouwelijkheid
De mate waarin de toegang tot informatie beperkt is tot de-genen die daartoe bevoegd zijn.

PBLQ

De publieke sector functioneert sterk wanneer zij met afnemende middelen in staat blijft om met gezag te voldoen aan de steeds veranderende eisen en verwachtingen vanuit haar omgeving. Sterk opereren vraagt van de leidinggevenden en medewerkers van publieke organisaties een voortdurende ontwikkeling, zowel individueel als collectief. Dit geheel is een complex samenspel van persoonlijke, bestuurlijke, organisatorische en ICT veranderingen.

Onze drijfveer

PBLQ wil organisaties bijstaan in bovengenoemde complexe maatschappelijke uitdagingen. Uitdagingen die mensen in deze organisaties aangaan met kracht en inspiratie, zodat zij een verandering kunnen realiseren. Een verandering die zich uit in nieuw beleid en aanpassing van strategie en uitvoering, om op die manier de kwaliteit van diensten in de publieke sector te verbeteren. De medewerkers van PBLQ hebben de kennis en het vermogen om aan deze ontwikkelingen een bijdrage te leveren. Daarmee dragen wij bij aan een sterke publieke sector. Dit kan met het ontwikkelen van mens en organisatie door een opleiding, een betere inrichting van de processen en/of een slimmer gebruik van ICT. Vooruitgang is wat wij met elkaar willen bereiken. PBLQ geeft graag de in het werk opgedane kennis terug aan de publieke sector. Daarom organiseert PBLQ regelmatig symposia met en voor haar relaties en brengt jaarlijks een aantal zogenaamde PBLQaties uit.

Wat doet PBLQ?

Advies en Management
PBLQ adviseert en ondersteunt organisaties in de publieke sector bij vragen over communicatie, informatie, organisatie en beleid op het

snijvlak van bestuur en ICT. Onze opdrachten lopen uiteen van strategisch (IT) en communicatie advies, audits en contra-expertises tot de rol van verandermanager. Bovendien zorgen de Informatiemanagement Academie (IMAC) en het Traineeprogramma ervoor dat steeds meer professionals werken aan een succesvolle verbinding tussen bestuur en ICT.

Leren en ontwikkelen
PBLQ ontwikkelt mensen en organisaties binnen de publieke sector. Dit doet PBLQ al meer dan 35 jaar met toonaangevende opleidingen en coachings- en adviestrajecten. De aanpak van PBLQ is persoonlijk, professioneel en sluit altijd nauw aan bij de specifieke leervraag. De uniciteit van de publieke sector vraagt immers om vakmanschap op maat.

Onderzoek
PBLQ levert een bijdrage aan maatschappelijke vraagstukken, door met innovatieve oplossingen de werkwijzen en processen van organisaties in het publiek domein te verbeteren. Het onderzoek staat voor vernieuwing en procesverbetering met een nadruk op realiseerbaarheid.

Waar zijn wij actief?
PBLQ definieert de publieke sector breed. Tot de publieke sector rekenen wij niet alleen het Rijk, provincies en gemeenten, maar bijvoorbeeld ook ZBO's, agentschappen, inspecties, pensioenfondsen, woningbouwcorporaties, zorginstellingen en onderwijsinstellingen. Kortom, alle organisaties die geheel of gedeeltelijk met gemeenschapsgelden worden gefinancierd. Onze klanten acteren op verschillende bestuurslagen en in diverse domeinen zoals: Openbaar bestuur, Economie en Innovatie, Financiën, Werk en Inkomen, Onderwijs, Cultuur en Wetenschap, Openbare orde en Veiligheid, Infrastructuur en Milieu, Welzijn en Zorg.

Binnen deze domeinen werken wij aan thema's als: decentralisaties, veiligheid, digitale overheid, Europa en Internationaal, Programma's en grote ICT projecten, en leren en ontwikkelen.

De oorsprong
PBLQ is een bundeling van krachten van de voormalige organisaties HEC, ROI, VDMMP en Zenc. HEC en ROI zijn als overheidsstichtingen opgericht in 1988 respectievelijk 1992 om kennis en ervaring op

persoonlijke, bestuurlijke, organisatorische en ICT aspecten op te bouwen en deze via advies- en opleidingsdiensten weer terug te geven aan de overheid. Zenc is in 2000 ontstaan vanuit de missie het openbaar bestuur te verbeteren met innovatieve oplossingen. VDMMP is in 2006 opgericht om met name in het veiligheidsdomein zorg te dragen voor communicatie(advies), beleid, onderzoek en trainingen en is in 2015 onder de vlag van PBLQ gekomen. De vier organisaties hebben een lange historie van dienstverlening aan de publieke sector in Nederland en hebben daarin een bijzondere expertise en netwerk opgebouwd en zijn samen gegaan onder de naam PBLQ.

Kwaliteit

PBLQ hecht veel waarde aan kwaliteit en wetenschappelijke verankering. Uiteraard hebben we een kwaliteitsmanagementsysteem en zijn we ISO 9001:2000 gecertificeerd. PBLQ HEC is aangesloten bij de ROA (Raad voor Organisatie-Adviesbureaus) en PBLQ ROI werkt volgens de gedragscode van de NRTO (Nederlandse Raad voor Training en Opleiding). Om te waarborgen dat onze kennis hoog blijft, is een groot aantal hoogleraren verbonden aan PBLQ. Zij werken mee in projecten, treden op in de opleidingsactiviteiten en verzorgen, indien nodig, de kwaliteitsbewaking.

Meer informatie kunt u vinden op www.pblq.nl.

De volgende papernotes en PBLQaties zijn verschenen:

- *Informatisering: spel zonder grenzen (1994)* – prof. dr. E.J.J.M. Kimman
- *Het recht van overheidsinformatisering (1995)* – mr. V.A. de Pous
- *Lichtsporen en luchtspiegelingen (1996)* – drs. S.B. Luitjens (red.)
- *Designing electronic document infrastructures (1997)* – dr. J.J.M. Uijlenbroek
- *Voorbij 2000 ... (1997)* – drs. S.B. Luitjens, mw. H. Krijgsman-Heersink en mr. V.A. de Pous
- *Oups! (1998)* – dr. B. Scheepmaker
- *Digitaal Documentbeheer (1998)* – dr. J.J.M. Uijlenbroek
- *Op weg naar E-day; De euro in de overheidsinformatisering (1998)* – drs. J.A. Perlee en drs. M. Rijn
- *Overheidsinformatisering: het taaie ongerief (1999)* – prof. ir. P.A. Tas en drs. S.B. Luitjens
- *E-commerce; Elektronisch zaken doen bij de overheid (2000)* – ir. P.P van der Hijden, dr. A. Jonk, drs. A.W.M. Lasance en dr. J.J.M. Uijlenbroek
- *Beheerst beheren; beheer van ICT voorzieningen uit managementoptiek (2000)* – ir. H.A. Spanjersberg en mr. dr. ir. Th.J.G. Thiadens
- *Het Resultaat Geteld; Over verantwoording en informatievoorziening (2000)* – dr. R. van Dael, drs. W.J. van Gelder en dr. A. Jonk
- *Overheid in het web; Naar een toegankelijke overheidssite (2001)* – dr. A.G. Arnold, drs. L.C. Swennen, drs. P.B. Nederkoorn en R.M. Herpel
- *De politieke partij in de netwerksamenleving (2002)* – dr. A. Jonk en G. van Velzen (red.)
- *Informatiebeveiliging voor de overheid (2002)* – mw. B.J. Glashouwer RE RI CISA, drs. M. de Graaf, ir. J.M. Meij, mw. drs. P. Mettau en ir. P. Wielaard
- *De I-functie verklaard (2002)* – dr. R. van Dael en drs. I. Henneman
- *Aanbesteden van ICT projecten (2003)* – mr. J.C.H. van Berkel, ir. A. Bloembergen, dr. A. Jonk en C. Kolk
- *Van ontwijken naar uitwijken (2003)* – dr. M.E.M. Spruit, ing. G.A. Ven, drs. W.B.M. Vrouwenvelder en ir. P. Wielaard
- *Andere overheid, andere bedrijven, andere systemen (2004)* – ir. L.H.M. Matthijssen, dr. R. van Dael en F. Heijink
- *De moderne informatiehuishouding van de digitale overheid, het archief op het bureau (2005)* – dr. A.G. Arnold en mw. B.J. Glashouwer RE RI CISA
- *mijnoverheid.nl'; publieke dienstverlening in de toekomst (2005)* – mw. drs. P. Mettau
- *De ontbrekende dialoog. Over nieuwe ambtenaren, nationale politici en de noodzaak tot dialoog (2005)* - drs. J.F. Jeekel

- *Excellent Public Leadership. 7 competencies for Europe (2005)* - dr. K.M. Becking en mw. drs. N. Hopman
- *SONAR – Aansturen van complexe overheidsprojecten (2005)* – drs. G.H.P. van den Berg en S.A.J. Munneke
- *Meesterlijk besturen. De burgemeester als leider (2006)* - dr. K.M. Becking en drs. G. Rensen MCM (red.)
- *Vernieuwend leiderschap. Persoonlijke reflecties uit de praktijk (2006)* - dr. K.M. Becking en mw. drs. N. Hopman (red.)
- *De uitvoeringsorganisaties in Europa; Niet langer een muurbloem (2006)* – drs. E.J. Mulder
- *Eitjes tikken; Bij het afscheid van Siep Eilander (2006)* – drs. M.M. Frequin, drs. S.B. Luitjens en drs. L.J.E. Smits
- *Bestuurscultuur en strategie. Een onderzoek naar de cognitieve kaart van topambtenaren (2007)* - dr. C.J.M. Breed
- *Naar een goed gebruik van het burgerservicenummer (BSN) (2007)* – mw. drs. P.R.B. Heemskerk, mr. drs. T.F.M. Hooghiemstra, mr. J.N. van Lunteren, mw. drs. P. Mettau en drs. D. Schravendeel
- *Voor alle zekerheid; Over adviezen, audits en contra-expertises: een gids voor ICT-opdrachtgevers in de publieke sector (2007)* – ir. A Bloembergen, drs. A. Glass en ir. C.L. Wauters EMEA
- *Gedwongen nering; ICT dienstverlening in een gebonden klant-leverancier relatie (2007)* – drs. M.F.M. Bom en dr. ir. K. Rijniersce
- *Elf Bommen en Granaten; Columns van Rob Meijer in de Automatiseringsgids (2007)* – drs. R.A.M. Meijer
- *Canon van de Nederlandse ambtenaar (2008)* - drs. A.G. Wirschell (red.)
- *Opgeruimd staat netjes? Uitbesteden van ICT in de publieke sector (2008)* – ir. C.L. Wauters EMEA, dr. M.E.M. Spruit en ing. M.R. Vermeulen MCM
- *Zakboekje preventie cybercrime (2008)* – mw. B.J. Glashouwer RE RI CISA en dr. M.E.M. Spruit
- *Exploring Identity Management and Trust (2008)* – drs. N. Ducastel, mw. drs. P.R.B. Heemskerk, mr. M.W.I. Hillenaar, mr. drs. T.F.M. Hooghiemstra, mw. drs. B.M. van Rijt, drs. D. Schravendeel, drs. L.J.E. Smits en dr. J.M. van Veen
- *20 jaar HEC 1988–2008 (2008)* – mw. drs. B.M. van Rijt-Valkenburg
- *Games in het openbaar bestuur; Wat zijn de spelregels? (2008)* – mw. drs. M. van de Vecht MPIM
- *The Devil is in the Detail (2009)* – mw. Ms C.I. Langejans MA
- *Langs elkaar heen; Over geïntegreerde dienstverlening in het publieke domein (2009)* – drs. G.H.P. van den Berg, mr. drs. T.F.M. Hooghiemstra, drs. O. Kinkhorst, mr. J.N. van Lunteren, B. Luxemburg, dr. A. van Venrooy en mw. drs. J. Vosse MPIM

- *Eerlijk bestek; Handleiding praktisch aanbesteden (2009)* – mr. J.C.H. van Berkel en ir. P. Wielaard
- *Referentiearchitecturen: niet alleen voor architecten! (2009)* – drs. R.A.M. Meijer, mw. J.M. van Rooij MScFS en mw. drs. M. Stam MPIM
- *Duurzaam bestuur(d); Bouwstenen voor duurzame bedrijfsvoering en groene ICT (2009)* – drs. J.A.B. Walschots MPIM, drs. A.M. Jansen en drs. A. de Jager
- *Effectief leiderschap in een innovatieve praktijk. Het project MSHR: 'Failure is not an option' (2010)* - prof. dr. M. Thaens
- *Op de golven van Europa (2010)* – drs. L.J.E. Smits, mr. drs. T.F.M. Hooghiemstra, drs. E.J. Mulder, mw. drs. M. van Beurden, mr. A.W.H. Docters van Leeuwen en mr. L.J. Brinkhorst
- *Leren van de Buren (2010)* – drs. L.J.E. Smits, mr. J.N. van Lunteren, drs. J.E. van Veenen, ir. M.R. Vermeulen MCM, drs. J. Romme MPIM, drs. M.A. de Rooij MCM, drs. E. Linke en drs. A.M. de Kamper
- *7. 10 jaar HEC Traineeprogramma, "verbinder word je niet zomaar" (2010)* – dr. A.G. Arnold en mw. D. Sytsema
- *De informatiepositie van de patiënt (2010)* – mw. drs. R.A.E. Gerads, mr. drs. T.F.M. Hooghiemstra, dr. A.G. Arnold en mw. drs. A.D. van der Heide MCM
- *Beter slim gejat dan slecht bedacht. Over de internationale uitwisseling van ICT best practices (2010)* – drs. J. Romme MPIM
- *Eyes only – Over de ragfijne balans van de duivelsdriehoek: het evenwicht tussen functionaliteit, veiligheid en geld (2011)* – N. Laagland, drs. J.P. Otter en ir. P. Wielaard
- *9. Lissabon in Den Haag – De gevolgen van het Verdrag van Lissabon voor politiek en bestuur in Den Haag (2011)* – drs. E.J. Mulder, mw. L. Abrahamse MA en mw. drs. I. de Boer
- *Web 2.0 & Social Media 'een routekaart' (2011)* – drs. G.H.P. van den Berg, mw. drs. S. Naghib-Bukman, drs. M.A. de Rooij MCM en drs. C. van der Werf
- *Portfoliomanagement; Een hoofdtaak van de CIO (2011)* – drs. A. Beetsma, ir. H. van Beusekom, drs. A.M. Bos, U. Groen MMC, drs. R.A.M. Meijer, ir. P. van Rotterdam, mw. ir. F.F. Westbroek en drs. C. van der Werf
- *Loonaangifteketen. De aorta van BV Nederland (2011)* – M.D. van Dijk, M.G.M. Driessen RA, C.H.A.M. Ewalds RA RC, mw. drs. D. Meijer, drs. M. de Roos EMIA RO, E.J.M. Ruiterman, mw. drs. W.N. Sonneveld EMIA RO en ir. C.L. Wauters EMEA RE
- *De CIO kan het niet alleen (2011)* – drs. C. van der Werf en dr. J.M. van Veen

- *TRENDS – Het Haagse leger? 14 experts over de toekomst van de publieke sector (2012)* – mr. drs. T.F.M. Hooghiemstra, mw. L. Wijnants en mw. drs. B.M. Valkenburg (red.)
- *Businesscases: het kompas van de bestuurder (2012)* – drs. R.A.M. Meijer, mw. drs. W.N. Sonneveld EMIA RO en drs. N. van Baarsen RE RI
- *Europa: wat doe je ermee? EU-professionalisering voor overheden (2012)* – mw. mr. M. Baptist-Fruin, drs. E.J. Mulder en drs. P. van Wersch
- *Risicomanagement: Bouwen aan zekerheden. Ingrediënten voor succes (2012)* – dr. K.F.C. de Bakker PMP, R.J. Mollema RE RA en ir. C.L. Wauters EMEA RE
- *De kinderopvangketen. Het verbinden van beleid, uitvoering en ICT (2012)* – drs. M. de Rooij
- *De burger kan het niet alleen. Digitale dienstverlening die past bij digitale vaardigheden van burgers (2013)* – mw. drs. Y. Bommeljé en P.A. Keur MSc
- *TRENDS – De publieke sector innoveert. 15 experts over innovatie binnen de publieke sector (2013)* – mw. C.N. van den Burg, mw. drs. D. Meijer, prof. dr. M. Thaens en mw. L. Wijnants (red.)
- *12. Wijzer – Investeren in ervaren talent (2013)* – drs. C. Fortunati en drs. M. Kessels
- *Evidence based loopbaanbeleid (2013)* – mw. C.M.F. Schellekens MSc.
- *Eindrapportage Programma SPEER. Terugblik op de invoering van ERP bij Defensie (2013)* – J.G. van der Burg, ir. J. Vos, dr. R. Schimmel, A.A.H. van Poecke MBA, ir. W. Helleman, mw. drs. D. Meijer en drs. J.E. van Veenen
- *Leren van decentraliseren lessen uit Fonkelveen (2014)* – dr. P.G. Castenmiller, drs. A.G. Wirschell
- *TRENDS - Veiligheid en innovaties in de publieke sector (2014)* - prof. dr. M. Thaens, mw. drs. B.M. Valkenburg en mw. L. Wijnants (red.)
- *TRENDS – Trends, Trends en nog eens Trends. Ontwikkelingen en innovaties in de publieke sector (2015)* – prof. dr. M. Thaens en 27 andere experts
- *Over leren en ontwikkelen en de kwaliteit van de Rijksdienst (2015)* - drs. Christa Fortunati

Internet of things, complexe informatienetwerken, bring your own device en big data. De maatschappij wordt digitaler; de dreigingen nemen toe. De uitdaging voor de overheid is om er voor te zorgen dat de beschikbaarheid van de dienstverlening is gegarandeerd en gevoelige gegevens niet op straat komen te liggen. 100% veiligheid bestaat echter niet; incidenten zullen onherroepelijk blijven optreden.

Voor bestuurders en managers bij de overheid is het de uitdaging om de goede maatregelen te treffen, zodat de kans op de grootste problemen wordt verkleind. Mocht zich toch een beveiligingsincident voordoen, dan is het belangrijk dat de organisatie in staat is om weer snel de dienstverlening te hervatten. Het vereist bewustwording van de eigen verantwoordelijkheid, het stellen van de goede vragen en steeds aandacht geven aan informatiebeveiliging. Leren van incidenten en van andere organisaties helpt om de informatieveiligheid te verbeteren.

Deze publicatie geeft bestuurders en managers een aantal belangrijke aandachtspunten en praktische tips om direct mee aan de slag te gaan.

ISBN 978-90-75239-47-8