

# BEVEILIGING PERSOONSGEGEVENS ALS ONDERDEEL VAN BEVEILIGINGSBELEID

Joris Hutter\*

■ Dikwijls wordt de beveiliging van persoonsgegevens als een juridisch onderwerp beschouwd en als een apart onderwerp in de organisatie behandeld. Dat is niet nodig en niet effectief. De nieuwe CBP Richtsnoeren 'Beveiliging van persoonsgegevens' zijn zodanig opgezet dat deze onderdeel kunnen worden van het algemene beveiligingsbeleid van de organisatie. Dit is effectiever dan een geïsoleerde aanpak op beveiliging van persoonsgegevens.

■ Het beveiligingsvakgebied is nu enkele tientallen jaren oud en organisaties kennen verschillende niveaus van volwassenheid. Omdat de privacydiscussie vaak juridisch is ingekleurd, is het nuttig om de belangrijkste succesfactoren op beveiliging te benoemen. De richtsnoeren lijken hier prima op aan te sluiten.

## Waar gaat het vaak mis?

Veel organisaties hebben een lage volwassenheid op het gebied van beveiliging en zijn te herkennen aan:

- Discussies over maatregelen, waarbij het onvoldoende duidelijk is wat beveiligd moet worden en wie daar belang bij heeft en waartegen de beveiliging moet zijn.
- Te weinig verbinding tussen beveiliging en de organisatie, cultuur, beleidsvoering en processen. Daarbij wordt tevens geklaagd dat het management geen interesse heeft voor beveiliging.
- Vaak staan aanpakken op zich ('silo-benadering'). Een veel voorkomende situatie is de toegangscontrole die afzonderlijk uit fysieke toegangscontrole, logische toegangscontrole en 'personele toegangscontrole' bestaat. Zelfs wanneer op één gebied vergaande maatregelen zijn ingevoerd, kan het geheel zwak zijn als de maatregelen niet goed op elkaar zijn afgestemd.
- Checklijst beveiliging. Om toch wat te bereiken wordt met checklijsten gewerkt. Als bijvoorbeeld

in de checklijst de eis staat dat er een terreinafscheiding moet zijn met een hekwerk van 2,2 meter hoog, dan wordt niet nagedacht of dat in deze concrete situatie ook werkelijk nodig is en of een andere vorm van terreinafscheiding niet passender is.

- Incident gedreven beveiliging. In overreactie op een incident worden kostbare maatregelen getroffen die al na een half jaar niet meer gebruikt worden.
- Kerkhof van niet-functionerende maatregelen. Veel maatregelen uit het maatregelenplan zijn niet of niet correct geïmplementeerd, of worden in de praktijk niet toegepast.
- Pas bij een incident wordt bij het management duidelijk dat de organisatie bloot heeft gestaan aan te grote risico's. Vaak blijkt reputatieschade met alle gevolgen van dien, veel groter dan de directe schade van het incident.

Voor veel privacy officers zal bovenstaande herkenbaar zijn. Zowel met de 'silo-benadering' als met de 'checklijst benadering' blijft het niveau van beveiliging van persoonsgegevens beperkt, waarbij er gelijktijdig er een beeld is dat er niks mag op privacy gebied. Beveiliging van persoonsgegevens wordt effectiever als deze aansluit op een goede en algemene beveiligingsaanpak van de organisatie.

---

\* **Joris Hutter** CISM is adviseur bij Hutter Security Risk Management ([www.hsrn.eu](http://www.hsrn.eu)) en bij Adviescentrum Bescherming Vitale Infrastructuur ([www.adviescentrumbvi.nl](http://www.adviescentrumbvi.nl)).

## Wat is dan wel een goede beveiligingsaanpak?

Organisaties met een hoog volwassenheidsniveau op beveiliging hebben over het algemeen de volgende kenmerken in hun aanpak:

### STAKEHOLDER BENADERING

Er hoeft alleen beveiligd te worden als er belangen zijn en belanghebbenden. Wie zijn precies de stakeholders en waaruit bestaat hun belang precies? Een vanzelfsprekende groep is natuurlijk het management, die continuïteit van de bedrijfsprocessen wil. Vanuit privacy kan hier aan worden toegevoegd: het individu waarvan persoonsgegevens worden verwerkt. Het is goed om ook de toezichthouder, in dit geval het College Bescherming Persoonsgegevens als een stakeholder te zien.

Als het duidelijk is wie de belangrijkste stakeholders zijn, kan de communicatie hier ook op worden afgestemd. Hierbij moet onderscheid worden gemaakt tussen communicatie vóór, tijdens en na een incident. Door gerichte communicatie met stakeholders kan waardering voor de beveiligingsaanpak worden gekregen en kan reputatieschade na een incident worden beperkt.

### INZICHT IN PROCESSEN, AFHANKELIJKHEDEN EN TE BESCHERMEN BELANGEN

Alleen met inzicht in processen en – daarbinnen – onderlinge afhankelijkheden, wordt het duidelijk waar de te beschermen belangen zich bevinden en wat de relatieve grootte is van een belang.

### ZICHT OP DREIGINGEN EN FAALFACTOREN

Er hoeft alleen beveiligd te worden als er potentiële dreigingen zijn en mogelijkheden tot falen. Het expliciet maken hiervan is voorwaarde om tot een effectief maatregelenplan te komen. Hierbij kan onderscheid gemaakt worden in:

- **Kwaadwillend handelen.** Zijn er motieven dat (cyber) criminelen belang hebben bij de persoonsgegevens? En hoe staat het met actievoerders? Heeft een klant of een medewerker belang om de eigen gegevens te wijzigen? Kunnen persoonsgegevens als bijeffect van een ander motief, bijvoorbeeld hacking, aangetast worden?
- **Nalatigheid en laakbaar handelen.** Wat zijn waarschijnlijkheid en mogelijkheden dat door onduidelijkheid, onverantwoordelijkheid en ongedisciplineerde bedrijfscultuur incidenten ontstaan? Denk bijvoorbeeld aan het verlies van een USB-stick.
- **Onvoldoende kennis en bewustzijn bij betrokkenen.** Wat voor type incidenten kunnen ontstaan doordat betrokkenen onvoldoende bewust zijn van hun rol in de beveiliging?

- **Organisatorisch falen.** Wat zijn de meest voor de hand liggende plaatsen waar organisatorisch gefaald kan worden? Denk in ieder geval aan interfaces tussen organisatieonderdelen, leveranciers en afnemers van informatie, bewerkers van informatie en servicepartijen die technische middelen ter beschikking stellen voor de informatievoorziening.
- **Technisch falen.** Wat zijn de meest kritieke technische componenten en interfaces voor het proces en voor verwerking en opslag van persoonsgegevens?
- **Omgevingsfactoren.** Denk bijvoorbeeld aan brand, overstroming of energieuitval.

### RISICO-OVERZICHT EN BESLUITVORMING OP RISICOBEBANDELING

Door inzicht in dreigingen en faalfactoren, inclusief waarschijnlijkheid, en de mogelijke effecten hiervan, is een risico-overzicht te maken. Dit kan gepresenteerd worden in een kwadrantmodel met impact en waarschijnlijkheid. Ook kunnen van een aantal kenmerkende risico's een scenario worden beschreven. Dit is een klein verhaaltje waarin vastligt door wie of wat een incident wordt veroorzaakt, hoe dat gebeurt en wat het effect is. Een dergelijk beeldend scenario maakt het risico concreet duidelijk en het wordt eenvoudiger om het maatregelenplan hierop te toetsen.

|        |   |                    |             |            |             |   |
|--------|---|--------------------|-------------|------------|-------------|---|
| Effect | 5 | Scenario 1         | Scenario 14 | Scenario 9 | Scenario 3  |   |
|        | 4 |                    | Scenario 5  | Scenario 6 |             |   |
|        | 3 | Scenario 2         | Scenario 13 | Scenario 7 | Scenario 15 |   |
|        | 2 | Scenario 12        | Scenario 10 | Scenario 8 | Scenario 11 |   |
|        | 1 |                    |             |            | Scenario 4  |   |
|        |   | 1                  | 2           | 3          | 4           | 5 |
|        |   | Waarschijnlijkheid |             |            |             |   |

Vanuit het risico-overzicht kan het management beslissingen nemen op wat de strategie is per type risico. Hiermee wordt bereikt dat de meeste aandacht en middelen naar de grootste risico's gaan en wordt voorkomen dat een dubbeltje met een kwartje wordt beveiligd.

### INTEGRALITEIT IN MAATREGELLEN, PASSENDE MAATREGELLEN

Integraliteit en evenwichtigheid in maatregelen kan vanuit verschillende invalshoeken worden beoordeeld:

- Risico gebaseerd, waarbij type en zwaarte van maatregelen gekoppeld zijn aan het risico.
- Beveiliging wordt gevormd mensen + procedures + technische voorzieningen. Deze drie aspecten moeten dan ook in samenhang gedefinieerd en onderhouden worden.
- Dit geldt ook voor informatiebeveiliging, fysieke beveiliging en mens aspecten. Deze maatregelen dienen in evenwicht te zijn, waardoor zij elkaar ook versterken.
- Maatregelen met een verschillend effect:
  - Andere inrichting van processen, waardoor het incident niet meer kan plaatsvinden. Indien een procesgang ook zonder persoonsgegevens uitgevoerd kan worden, kunnen in dit deel van het proces geen incidenten op persoonsgegevens ontstaan.
  - Maatregelen om de kans op een incident te verkleinen.
  - Maatregelen om het directe effect van een incident te beperken.
  - Maatregelen op alternatieve klantbediening.
  - Maatregelen op herstel van situatie.

### CONTROLE, HANDHAVING, VERANTWOORDING EN VERBETERING

Het stelsel van maatregelen dient gecontroleerd en gehandhaafd te worden inclusief sanctionering. Naar stakeholders dient verantwoording afgelegd te worden. Maar bovendien is dit een basis om verbeteringen door te voeren.

### CULTUUR EN NEMEN VAN VERANTWOORDELIJKHEID

De cultuur van de organisatie moet gericht zijn op een adequate beveiliging, waarbij iedere betrokkene vanuit de eigen rol een verantwoordelijkheid heeft en ook toont. Dit kan alleen gebeuren als beveiliging ook in het management is verankerd en het management het voorbeeld gedrag toont.

### KENNISNIVEAU EN GEBRUIK VAN STANDAARDEN

Op beleids- en op operationeel niveau dient voldoende kennis te zijn. Deze kan ontwikkeld worden of eventueel extern ingekocht. Met deze

kennis kan ook besloten worden waar en hoe standaarden worden toegepast en waar in maatwerk moet worden voorzien.

### PROGRAMMA AANPAK EN MANAGEMENT SYSTEEM AANPAK

Diverse organisaties sturen op een integraal programma van beveiliging-onderwerpen. Soms is een onderwerp een project dat uitgevoerd wordt, soms een permanente activiteit zoals bewustwording. Er zijn ook veel organisaties die een management systeem aanpak invoeren. Dit is een plan-do-check-act aanpak, waarin de onderwerpen van een programma-aanpak op een logische wijze zijn verwerkt en waar continue op verbetering wordt gestuurd. De ISO 27000 is een dergelijke aanpak.

### Beveiligingsrichtsnoer gelinkt aan algemene beveiligingsaanpak

Het richtsnoer 'Beveiliging van persoonsgegevens' vervangt de zogenoemde AV23 richtlijn en is minder voorschrijvend op type maatregelen. Belangrijke elementen zijn de bestuurlijke verankering van de beveiliging en dat deze via een management cyclus beheerd dient te worden. Ook dat de maatregelen passend moeten zijn, risico-gebaseerd en vanuit beveiligingsprofessionele gronden gekozen en gemotiveerd. Dit zijn kernelementen van iedere goede beveiligingsaanpak. Hiermee worden de risico's beheersbaar gemaakt, is de beveiliging kosteneffectief en kan verantwoording worden afgelegd op de gehanteerde aanpak.

Persoonsgegevens zijn, net als andere assets, bedrijfsmiddelen die beschermd moeten worden om de organisatieprocessen te kunnen uitvoeren. Beveiliging van persoonsgegevens heeft een aantal bijzondere kenmerken, maar is in systematiek niet anders dan beveiliging van andere bedrijfsmiddelen. Een integrale aanpak is veel effectiever dan een geïsoleerde beveiligingsaanpak op persoonsgegevens.

Is bovenstaande nieuw? Eigenlijk niet. De WBP impliceert al een managementaanpak op beveiliging. De nieuwe Europese verordening maakt nog expliciet dat bescherming van persoonsgegevens een management vraagstuk is. Het nieuwe richtsnoer 'Beveiliging van persoonsgegevens' sorteert hier prima op voor. ■