Organisatie van de informatiebeveiliging en vertrouwelijkheid van informatie

Hoe professionals in een organisatie samenwerken en de belangen van de organisatie worden beschermd

dr. Clemens H.J. Willemsen

ISBN: 978-94-0360-917-1

Gedrukt en gepubliceerd door: Managementboek

Inhoudsopgave

1 INLEIDING 5
2 ROLVERDELING 8
3 VERTROUWELIJKHEID IN RELATIE TOT RUBRICERING 17
3.1 De onderscheiden standaarden 17
3.2 Een verbeterd begrippenkader vertrouwelijkheid 42
3.3 Methoden en tools 51
4 DATACLASSIFICATIE EN RISICOMANAGEMENT 52
4.1 Inleiding risicomanagement 52
4.2 Aanvulling op het verbeterd begrippenkader 56
4.3 Methoden en tools 63
4.4 Incidentmanagement 69
5 AFSLUITING 76
BIJLAGE 1. LITERATUURLIJST 79
BIJLAGE 2. VERBETERD BEGRIPPENKADER INTEGRAAL 82
BIJLAGE 3. RECAPITULATIE DREIGINGEN 86

Lijst van figuren

Fig. 1. Onderwerpen van dit boekwerk 6
Fig. 2. Organisatie van de informatiebeveiliging 8
Fig. 3. Verhouding BVA en CISO inzake te beschermen belangen. 12
Fig. 4. Losse begrippen 17
Fig. 5. Relaties tussen begrippen. 50
Fig. 6. Dataclassificatie versus risicomanagement. 54
Fig. 7. ISO- en NIST-standaarden. 55
Fig. 8. Begrippen dataclassificatie uitgebreid met risicomanagement. 62
Fig. 9. Octave. 66
Fig. 10. Relaties tussen begrippen integraal. 78

Lijst van tabellen

Tab. 1. Standaarden organisatie en vertrouwelijkheid 7
Tab. 2. Functionarissen rijksoverheid 14
Tab. 3. Taken CISO en BVA 16
Tab. 4. Begrippen en betekenis vertrouwelijkheid 21
Tab. 5. Basisbeveiligingsniveaus BIO 24
Tab. 6. Rubricering VIR-BI 26
Tab. 7. Handleiding rubricering VIR-BI 29
Tab. 8. Rubricering Verenigd Koninkrijk 31
Tab. 9. Aanval en effect Verenigd Koninkrijk 32
Tab. 10. Rubricering KLPD 34
Tab. 11. Rubricering Politie 34
Tab. 12. Soorten te beschermen belang 35
Tab. 13. Rubricering Defensie 36
Tab. 14. Merking Defensie 38
Tab. 15. Rubricering gemeenten 39
Tab. 16. Rubricering België 41
Tab. 17. Onderscheiden rubriceringsniveaus 42
Tab. 18. Belangen België versus Nederland 43
Tab. 19. Begrippenkader vertrouwelijkheid 48
Tab. 20. Relaties tussen categorieën 49
Tab. 21. Vertrouwelijkheid versus rubricering 50
Tab. 22. Risico volgens ISO 27000 53
Tab. 23. Begrippenkader risicomanagement 59
Tab. 24. Motief en methode van dreiging 60
Tab. 25. Information risk assessment methodology 63
Tab. 26. Kwetsbaarheden en blootstellingen 67
Tab. 27. Incidentmanagement doelstellingen 72
Tab. 28. Incidentmanagement in enge zin 74
Tab. 29. Incidenten schaal 1 tot 10 76
Tab. 30. Taken per functionaris 77
Tab. 31. Onderscheiden tools 77
Tab. 2-1. Begrippenkader integraal 85
Tab. 2-2. Recapitulatie dreigingen 87

1 Inleiding

Informatiebeveiliging (IB) speelt in alle geledingen van een organisatie. De rol en taakinvulling van de Chief Information Security Officer (CISO) verschilt daarbij nogal van een fulltime functie bij een grote ICT-organisatie tot de (parttime) rol van informatie-beveiliger bij een beleidsdirectie. Daarbij kun je van mening verschillen of het een taak, functie of beroep is [Functieprofiel CISO, p. 14][1]. De rol vereist in alle gevallen een grote vakinhoudelijke deskundigheid op het gebied van informatiebeveiliging en kennis van de bedrijfsprocessen in de organisatie. De afgelopen 30 jaar heb ik ervaren dat informatie-beveiliging een zeer boeiend werkterrein is dat je vooral samen met andere IB-professionals, proceseigenaren en opdrachtgevers moet doen.

Als je zoals ik de CIO van een beleidsdirectie adviseert en IB een aspect is van je werk maar niet de hoofdtaak dan moet je op een praktische wijze invulling geven aan deze taak. Ik deel graag mijn ervaringen met de professionals in het veld en hoop dat zij daar hun voordeel mee kunnen doen.

Ik richt mij in het bijzonder in dit boekwerk op de onderwerpen:

- Organisatie en rolverdeling
  De onderscheiden organisaties en functionarissen dienen nauw samen te werken zowel tussen organisaties als daarbinnen. Enkele standaarden gaan daar nader op in doch deze dienen voor een specifieke overheidsdienst nader te worden verbijzonderd.
- Relatie vertrouwelijkheid en rubricering[2]
  Ik merk in de praktijk dat rubricering van informatie niet iets van zelf sprekends is als het gaat om het afschermen van informatie terwijl vertrouwelijkheid (ook wel genoemd exclusiviteit[3]) wel als belangrijk aspect van informatiebeveiliging wordt onderkend.

---

[1] [xx] verwijst naar de literatuurlijst in bijlage 1.

[2] Rubricering is de term bij de rijksoverheid en dataclassificatie daarbuiten. Op zich is rubricering een meer specifieke term en heeft dataclassificatie buiten het gebied van informatiebeveiliging een ruimere betekenis. Rubricering heeft alleen betrekking op vertrouwelijkheid. Waar is spreek over dataclassificatie beperk ik mij tot vertrouwelijkheid hoewel dataclassificatie ook betrekking kan hebben op beschikbaarheid en integriteit. Buiten deze context heeft classificatie een ruimere betekenis zodat ik deze kortere benaming verder niet gebruik.

[3] Doorgaans spreekt men over exclusiviteit met dezelfde betekenis dat direct aangeeft dat het om uitsluiten van toegang tot informatie gaat terwijl de term vertrouwelijkheid meer slaat op hoe de omgang met informatie dient plaats te vinden.

De relatie tussen deze beide concepten is niet altijd even duidelijk en ik hoop daar in dit boekwerk verheldering in aan te brengen.

- (Data)classificatie wordt vaak los gezien van risicomanagement (en incidentmanagement) of alleen als voorwaarde hiertoe. Ik breng beide werelden met elkaar in verband en laat de verschillen zien.

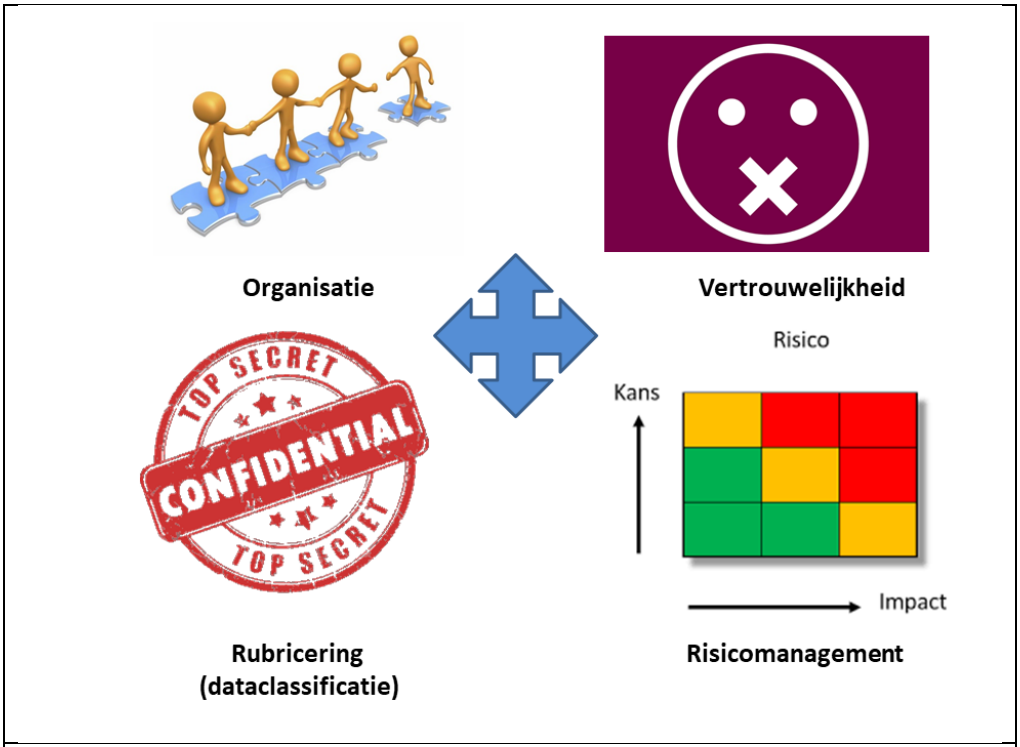

Fig. 1. Onderwerpen van dit boekwerk

In al deze gevallen demonsteer ik de onderwerpen aan de hand van de standaarden die gebezigd worden bij de (rijks)overheid. Ik ga bij rubricering en risicomanagement bewust niet in op de maatregelen die vervolgens genomen kunnen worden om de vertrouwelijkheid en/of rubricering te waarborgen hetgeen ik verderop onderbouw. "*In de beperking toont zich eerst de meester*" aldus Goethe.

Standaarden

Bij de diverse standaarden die worden gebruikt bij de overheid is de genoemde verdeling in verantwoordelijkheden en de relatie tussen vertrouwelijkheid en rubricering niet altijd eenduidig dan wel wordt daar

weinig aandacht aan geschonken. De standaarden die bij de overheid worden gebruikt zijn in het bijzonder de volgende:

standaard	*geldig voor*
1. Baseline Informatiebeveiliging Overheid (BIO)	Overheid in brede zin
2. besluit Voorschrift Informatiebeveiliging Bijzondere Informatie (VIR-BI) 2013	Rijksoverheid
3. Handleiding rubricering (VIR-BI) 2015	Rijksoverheid
4. Rubriceringsregeling Politie 2015 (intern document)	Politie
5. Rubricerings – en merkingsysteem Defensie 2017	Defensie
6. Handreiking dataclassificatie voor gemeenten inzake de BIO	Gemeenten
7. Het NBA-volwassenheidsniveau voor informatie-beveiliging	Alle organisaties
geen standaard maar ter referentie	
8. Beleidslijn informatieveiligheid & privacy dataclassificatie	Sociale zekerheid België
9. Besluit van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (2013/488/EU)	Europese overheden
Tab. 1. Standaarden organisatie en vertrouwelijkheid	

Veel onderwerpen uit (2) het **VIR-BI** komen grotendeels uit de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is de vertaling van de British Standards 7799 die later als ISO 17799 als internationale standaard voor informatiebeveiliging in organisaties is gepubliceerd als voorloper van de ISO 27002. De Code voor Informatie-beveiliging bestaat thans uit twee delen: een norm (ISO 27001) en een 'code of practice' (ISO 27002). De ISO 27002-standaard is een best practice van beveiligingsmaatregelen (‘controls’) om informatie-beveiligingsrisico’s aan te pakken met betrekking tot de betrouwbaar-heid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van ISO 27001. De (1) **Baseline Informatie-beveiliging Overheid** is eveneens gestructureerd volgens ISO 27001, bijlage A en ISO 27002. Waar relevant neem ik verderop wel ISO 27001/2 mee doch niet als standaard voor de overheid in de voorgaande tabel. Verderop geef ik aan hoe de ISO-standaarden zich onderling verhouden.

Ik bespreek deze standaarden inzake verantwoordelijkheden tussen partijen en inzake rubricering. Ten eerste vanwege het hier voor genoemd belang om dat onderscheid te maken en het tweede omdat ik constateer dat er aanzienlijke verschillen zijn in de aanduiding van niveaus van vertrouwelijkheid en de al dan niet onderkende relatie

tussen vertrouwelijkheid en rubricering alsmede tussen dataclassificatie en risicomanagement.

2 Rolverdeling

De positie van de informatiebeveiliging op diverse niveaus

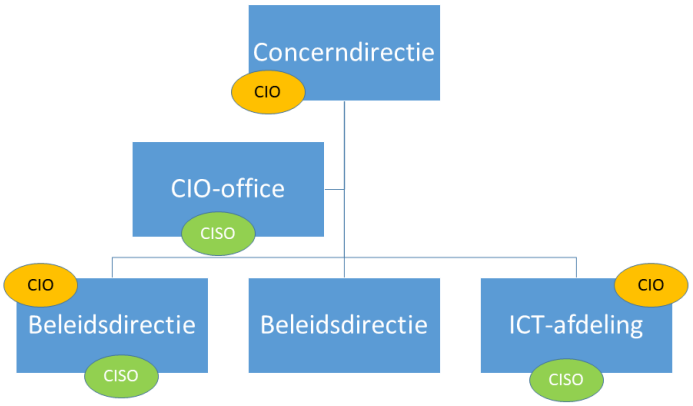

Fig. 2. Organisatie van de informatiebeveiliging

Aan de top van de organisatie, doorgaans als onderdeel van het CIO-office[4], stelt de CISO de kaders vast voor de organisatie als geheel en is (eind)verantwoordelijk voor de informatiebeveiliging van de gehele organisatie. De ICT-organisatie kan een eigen CISO hebben en elke beleidsdirectie een CISO. Ik schets de mogelijke situatie in algemene zin in figuur 1 en niet alleen voor het bedrijfsleven. Voor de rijksoverheid valt te denken aan het bureau van de (plv.) Secretaris-generaal als de concerndirectie, een Directie informatievoorziening als CIO-office en een Directoraat-generaal als beleidsdirectie. Bij een gemeente valt achtereenvolgens te denken aan het bureau van de gemeentesecretaris, een bedrijfsvoeringsexpertise centrum en een dienst zoals Stedelijke Ontwikkeling. De positie van de onderscheiden CIO's kan natuurlijk per organisatie verschillen.

[4] Taalkundig gezien is Chief Information Office juister maar CIO-office is gangbaar.

De beleids-CISO heeft daarbij een relatie met de concern-CISO als het gaat om toe te passen standaarden plus het afleggen van verantwoording via de planning- en controlcyclus. De relatie met de ICT-CISO is niet minder van belang waar het gaat om systemen waarvoor de beleidsdirectie opdrachtgever is en de ICT afdeling opdrachtnemer; de laatste als ontwikkelaar en/of beheerder. De beleids-CISO haalt informatie op bij de ICT-CISO (of ICT-CISO's) om dit te aggregeren voor de concern-CISO. Denk hierbij aan beveiligingsincidenten en - risico's. De CISO heeft "*specifieke inhoudelijke kennis van de uitvoerings-processen binnen het betreffende domein en ondersteunt de proces-eigenaar bij het uitvoeren van de risicoafweging en het bepalen van beveiligingsmaatregelen*" [Functieprofiel CISO, p. 6]. Al met al is de CISO 'slechts' een adviseur van het management.
In dit spinnenweb van verantwoordelijkheden is het handig om de RASCI-methodiek[5] te gebruiken om de rollen specifieker te maken. De CISO is op het niveau van de beleidsdirectie verantwoordelijk ('responsible'), zijn CIO is eindverantwoordelijk ('accountable'), de concern-CISO is informerend ('informative') en de ICT-CISO is raadplegend ('consultive'). Het is goed om dit onderscheid te maken omdat je het alleen samen kunt doen. Elke CISO heeft in beginsel een onafhankelijke positie ten opzichte van het lijnmanagement zodat een directe rapportagelijn naar en overleg met de CIO mogelijk is.

[ISO 27002] stelt (6.1.1): "*Alle verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging behoren te worden gedefinieerd en toegewezen in het bijzonder voor het risicobeheer. Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren; niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht*". Denk hierbij b.v. aan de CISO bij een directie en een informatiebeveiliger bij een organisatieonderdeel of locatie. Verder stel zij: "*Veel organisaties benoemen een manager informatiebeveiliging die de algehele verantwoordelijkheid draagt voor de ontwikkeling en implementatie van informatiebeveiliging en om de identificatie van beheersmaatregelen te ondersteunen*". Dat kan worden gezien als de manager.

Ik beperk mij verder tot de hoofdtaken van deze functies en ga niet in detail een profiel opstellen voor de CISO. Bij de rijksoverheid wordt een (rijks)beveiligingsambtenaar (BVA) of beveiligingsautoriteit onderkend die verantwoordelijk is voor de integrale beveiliging waar informatie-

[5] **R**esponsible, **A**ccountable, **S**upportive, **C**onsultive en Informative.