Hoe verdeel je rollen en taken met betrekking tot informatiebeveiliging?

Security Officer: het schaap met de vijf poten?

Wanneer informatiebeveiliging expliciet op organisatieniveau benoemd wordt als aandachtsgebied, ontstaat er een nieuwe rol in de organisatie: die van de (Chief Information) Security Officer (ook wel SO of CISO). De rol van de SO is cruciaal om informatiebeveiligingsbeleid in een organisatie te implementeren, te verankeren en breed gedragen te krijgen. En daarmee ook om een informatiebeveiligingsmanagementsysteem (ISMS) en certificering (ISO 27001 of aanverwant) 'in de lucht te houden' en daadwerkelijk meerwaarde te laten hebben voor de organisatie. Niet iets om al te lichtzinnig mee om te gaan dus. Toch gebeurt het in de praktijk vaak dat de rol van SO 'als vanzelfsprekend' bij een IT-verantwoordelijke of bij een KAM-functionaris wordt neergelegd. Hoe logisch is dat? Welke kwalificaties en competenties vraagt de rol van SO? Zoek je die in één persoon binnen de organisatie, of is dat zoeken naar het schaap met de vijf poten?

Door Tobias op den Brouw en Gertjan de Beer

Het expliciet benoemen van informatiebeveiliging als bedrijfsbreed (kwaliteits-) aspect brengt structuur in wat de organisatie al doet. Het is niet langer iets wat 'de IT-afdeling erbij doet' – hoe goed ze het in de praktijk ook doet.

Deze aanvliegmethode van informatiebeveiliging stelt als doel om aantoonbaar voor informatie(systemen):

- de vereiste prestaties voor Beschikbaarheid, Integriteit en Vertrouwelijkheid te realiseren én te verbeteren en
- de noodzakelijke processen en maatregelen stabiel uit te voeren.

Voor de managementprincipes én de relevante maatregelen zijn er omvangrijke en eenvoudig te raadplegen internationale standaarden

vanuit diverse invalshoeken, zoals ISO 27001, COBIT, ITIL, en ISAE. Elke standaard kan voldoen, zolang deze:

- ingaat op maatregelen in de 'driehoek' mens, organisatie en techniek (waaronder fysieke maatregelen),
- de relevante maatregelen selecteert en prioriteert,
- daarbij aansluit bij de management-methoden voor het dagelijkse werk
- en bijdraagt aan organisatiedoelen.

Drie praktische, zeker niet uitputtende, voorbeelden van maatregelen:

- **vertrouwelijkheid** ontstaat bijvoorbeeld door **mensen** te ondersteunen in hun veranderproces: met bewustzijn dat leidt tot draagvlak en met middelen die het juiste gedrag makkelijk én nuttig maken;
- **integriteit** ontstaat bijvoorbeeld door een release**proces** met testactiviteiten;
- **beschikbaarheid** wordt bijvoorbeeld geborgd door voldoende **technische** redundancy.

Wie vult wat in?

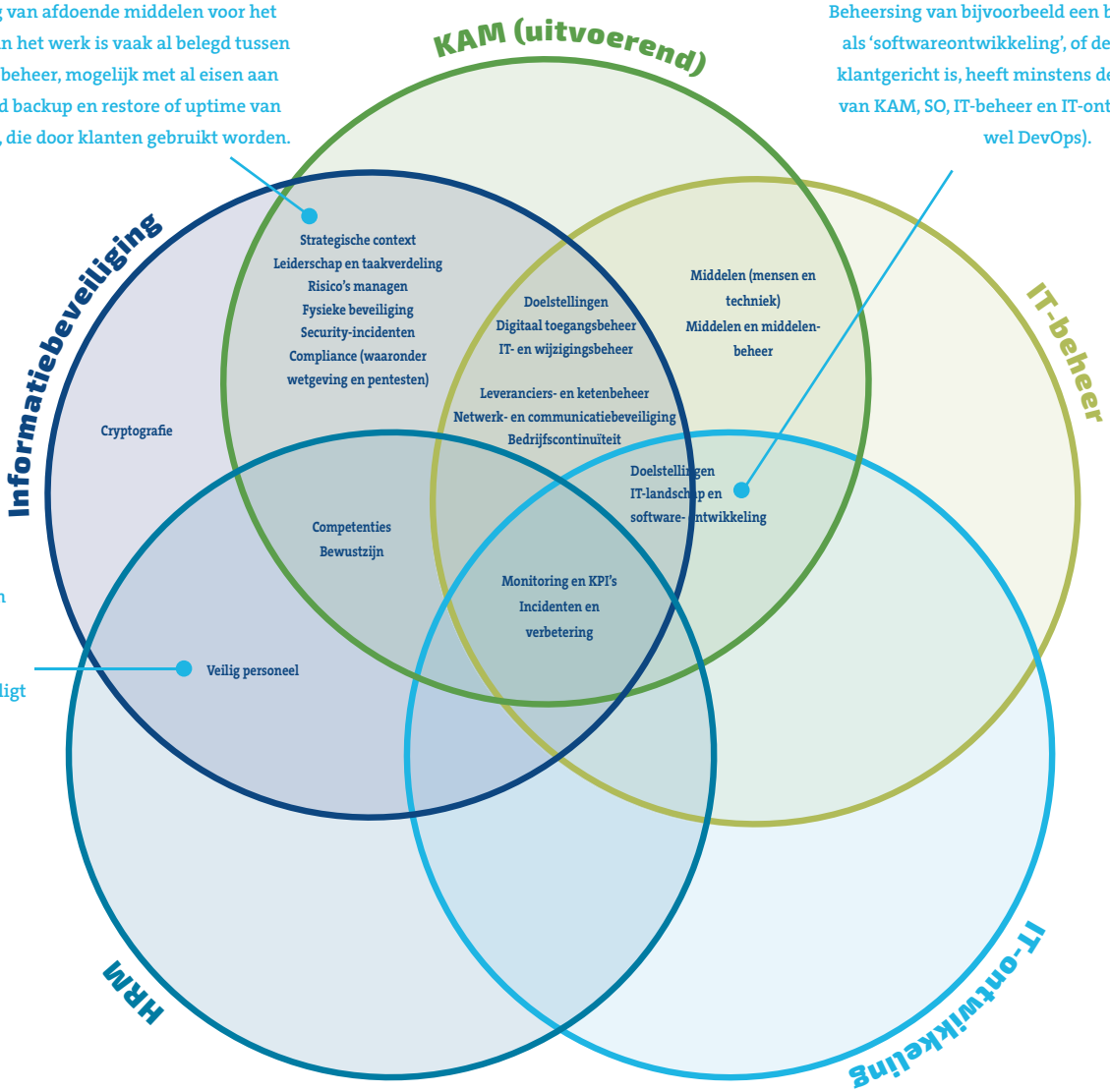
Vooropgesteld staat dat we het hebben over een rol, die ervoor zorgt dat bepaalde taken uitgevoerd worden. Deze rol hoeft niet per sé bij één (fulltime) persoon te liggen. Is de verantwoordelijkheid van deze (nieuwe) rol vooral het **managen** en ligt de uitvoering van taken bij anderen? Dan zijn operationeel en ontwikkelmanagement en coachen van collega's de kerncompetenties van de SO. De rol is dan veelal belegd bij een MT-lid (vaak van een IT-afdeling) of bij een fulltime KAM-manager. Bij de rol hoort dan ook de verantwoordelijkheid te rapporteren aan de directie en de directie-eisen vertalen naar nieuwe verbeteringen.

Dit is uiteraard makkelijker en doeltreffender met inhoudelijke (technische informatiebeveiligings-) kennis, maar met een breed veld zoals informatiebeveiliging kan één persoon niet alles weten. Als we beveiligingsonderwerpen voorlopig even splitsen naar expliciete rollen (of afdelingen), dan is de volgende afbeelding een gangbare invulling. We noemen de verantwoordelijke voor operationeel procesmanagement hier even 'KAM'.

Belangrijk bij de afbeelding: IT-ontwikkelingen staan niet stil en frameworks lopen altijd achter op de praktijk, maar veranderen wel mee. Een interessante verbetering in de ISO 27001-familie is dat in 2021 de beheersmaatregelen (nu op inhoudelijk hoofdstuk ingedeeld) qua indeling veranderen naar vier hoofdthema's: mensen, fysieke beveiliging, technische beveiliging en organisatorische aspecten. Zo sluit de norm al

Beheersing van afdoende middelen voor het uitvoeren van het werk is vaak al belegd tussen KAM en IT-beheer, mogelijk met al eisen aan bijvoorbeeld backup en restore of uptime van IT-systemen, die door klanten gebruikt worden.

Beheersing van bijvoorbeeld een breed onderwerp als 'softwareontwikkeling', of deze nu intern of klantgericht is, heeft minstens de inbreng nodig van KAM, SO, IT-beheer en IT-ontwikkeling (ook wel DevOps).



Beheersing van bijvoorbeeld 'screening van medewerkers' ligt vaker bij SO of HRM.

beter aan op de taakverdeling binnen bedrijven. Daarnaast zet de 2021-update dertien nieuwe controls explicieter neer, waaronder:

- cloud services (waarvoor ook specifieke normen 27017 en 27018 in opkomst zijn);
- data leakage prevention;
- vulnerability disclosure;
- ICT readiness for business continuity.

De verdeling van verantwoordelijkheid voor bestaande en nieuwe onderwerpen hangt af van:

- de branche waarin de organisatie acteert;
- de aard van de producten en/of diensten;
- de omvang en digitaliseringsgraad van de organisatie;
- de aanwezige kennis, competenties en al bestaande verdeling van verantwoordelijkheden en taken.

In de praktijk schuift de verantwoordelijkheid voor deze onderwerpen tussen verschillende personen, op basis van wat het bedrijf het meeste doet (kernprocessen) en welke rollen al zijn ingevuld. Hoe groter het bedrijf, hoe groter de kans op fulltime specialisten op elk vakgebied, maar ook hoe meer processen en IT-systemen er zijn die beheerst moeten worden. Voor elk onderwerp geldt dat een inhoudelijke 'kennishebber' (de uitvoerder) nodig is én een persoon die het onderwerp vertaalt naar organisatiebreed gedragen gedrag en de strategische doelen van de organisatie. Kortom, een persoon die het onderwerp 'managet'.

Typische rolinvulling SO

Voor een 'pure' kwaliteitsverantwoordelijke zijn specifieke onderwerpen als cryptografie, privacy-compliance of beveiliging van mobiele telefoons en laptops vaak nieuw en onbekend, waar die juist voor een SO en een IT-beheerder al bekender klinken. De kwaliteits- en security-verantwoordelijke vinden elkaar dan weer wel in managementprincipes zoals risico- en verandermanagement, het sturen op KPI's en controle-activiteiten zoals interne audit en management review. Wie is dan de beste eindverantwoordelijke? Zoals gezegd is dat de persoon die, naast managementvaardigheden, inhoudelijke kennis van de meeste onderwerpen meebrengt. Mits zijn of haar agenda dat toestaat natuurlijk. Ieder mens is natuurlijk anders, maar als we stereotypisch denken, dan:

Nr.	Thema	Gangbare invulling
1	Risico-identificatie, -beoordeling en -behandelmethodieken voor security-dreigingen en risico's	Uitbesteding
2	Begrijpelijke en toegankelijke regels voor collega's, ondersteuning bij gedrag	Samenwerking tussen KAM-manager, IT-manager en eventueel een communicatiedeskundig persoon
3	Specialistische thema's als cryptografie, verwerkersovereenkomsten, (evaluatie van) security in SLA en/of DAP met leverancier, compliance met wet- en regelgeving	Technisch of juridisch specialisten
4	Onafhankelijke praktijkcontroles of interne audits	Uitbesteding of opleiding en daarna auditors 'uitruilen' met andere organisaties
5	Projectmanagement dat voldoende aandacht geeft aan informatiebeveiligingsaspecten, met name wanneer een managementsysteem voor informatiebeveiliging grotendeels afwezig is	De directie of de IT-manager neemt deze taak aanvullend op zich
6	Classificatie van informatie	Uitbesteding
7	Business continuity Uitbesteding	Uitbesteding

is de KAM-manager:

- sterk in risico- en procesmanagement van de uitvoerende processen en gericht op bedrijfsdoelen en
- iemand die, afhankelijk van de kernactiviteit van het bedrijf, minder affiniteit heeft met beveiligingstechniek of relevante informatiebeveiligingswetgeving.

en is de IT (beheer)-manager:

- sterk in technische maatregelen en de monitoring daarvan;
- iemand die, afhankelijk van het type bedrijf, mogelijk minder draagvlak voor organisatiebreed veilig gedrag of andere 'soft' aspecten realiseert.

Invulling in de praktijk

Op basis van het voorgaande zijn de taakverdeling en bijbehorende voor- en nadelen duidelijk. En stel, er is de mogelijkheid een voldoende ervaren SO aan te stellen (fulltime, deeltijd, outsourced), dan kunnen tussen bijvoorbeeld directie, KAM-manager, SO, IT-manager en Hoofd Softwareontwikkeling de taken goed verdeeld worden. Als een dergelijke SO niet binnen de organisatie een vaste rol kan worden, of er te weinig tijd gemaakt kan worden voor deze rol, dan zijn de in het schema genoemde specialistische onderwerpen lastiger te verdelen. Een gangbare oplossing hiervoor is weergegeven in bovenstaande tabel.

Concluderend kunnen we stellen dat de vraag of de rol van SO vraagt om het 'schaap met de vijf poten' niet eenduidig te beantwoorden is, omdat dit per organisatie verschilt. Zeker is dat de taken en verantwoordelijkheden van een SO divers zijn en zowel een organisatorische (management) als een technische kant hebben. In organisaties met een IT-technisch kernproces zullen de competenties eerder in één persoon gevonden kunnen worden dan in andere organisaties. In die organisaties komt ook regelmatig de verdeling van taken over twee verantwoordelijken voor (één technisch, één procesgericht). In organisaties waar dit niet mogelijk of gewenst blijkt, is uitbesteding van de SO-rol een goede oplossing. Q

Over de auteurs

Tobias op den Brouw is Adviseur Informatiebeveiliging bij Certificerings-Advies Nederland.

Gertjan de Beer is Branchemanager Zakelijke Dienstverlening & IT bij Certificerings-Advies Nederland.