Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en ook associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. In zes bijdragen ontvouwt hij een Meetbare Maatregelen Aanpak voor de inrichting van een ISMS. Hij is te bereiken via: andre@octopus-ib.nl of via LinkedIn (1)

Even terug

Met mijn eerste bijdrage in IB Magazine 1 van dit jaar over de rol van de CISO dacht ik wel wat reacties los te zullen maken. Ik sloeg nogal van me af en spaarde niemand, ook mijzelf niet, maar wat bleef het stil! Ik werd door niemand op de vingers getikt, maar kreeg ook maar beperkte bijval. Met de mogelijkheid om online te reageren werd bijzonder weinig gedaan. Wat is dat met jullie, is de waarheid te pijnlijk of zijn jullie te lui om te reageren op mijn fouten en ongenuanceerde mening? Spreek je uit op LinkedIn of in mijn e-mail.

MMA

In mijn bijdrage in IB Magazine 2 vertelde ik over de 'implementatiekloof' en bood ik mijn inzichten aan, met het idee dat kritiek leveren belangrijk is, maar ook wel wat gemakkelijk. Wie kritiek levert moet ook een oplossing aanbieden en dat heb ik geprobeerd. Verwacht van mij geen diepe inzichten of doorwrochte beschouwingen met verwijzingen naar grote denkers. Ik schrijf gewoon op wat ik heb geleerd. Ik heb dit allemaal niet tussen hoofdgerecht en toetje bedacht, maar er een hele tijd over gedaan: jaren van fouten maken en peinzen over wat toch het probleem is. Ik kan het namelijk niet uitstaan dat wij - zoals ik in het eerste artikel betoogde - heel druk zijn, maar intussen maar weinig tot stand brengen én daarbij ook vaak niet blij zijn in ons werk.

GEDACHTEN OVER HET ISMS:

IB-Beleid en -eigenaarschap

Vandaag wil ik het hebben over enkele aspecten van het ISMS, het InformationSecurity ManagementSystem. Je kent het wel vanuit de standaarden ISO27001, NEN7510-1. Ik heb er lang mee geworsteld. Maar door schade en schande wijs geworden, denk ik nu dat er écht wel een ambachtelijke standaardmanier bestaat om een ISMS op te zetten. Passen en meten hoort erbij omdat organisaties verschillen, vooral het vinden en binden van de juiste spelers in de organisatie is een 'ding', maar verder…

Geen 'ding'

Even een voorafje: het is af en toe gewoon gênant mensen uit het vakgebied te horen praten over het ISMS alsof het een ding is, een database of een stapeltje documenten dat je koopt en dat je beveiliging magisch dichterbij brengt.
Wat ook niet helpt is dat sommige makers van 'tooltjes' (zoals ik het dan maar noem) de zegeningen van hun systeem/dienst zo breeduit meten dat het wel een oplossing móet zijn. De waarheid is dat ze vaak niet meer bieden dan een soort 'document-ophangrekje' aangevuld met een optie voor beheer van actiepunten (en misschien een risicoregister). Heel handig maar ook niet meer dan dat en zeker geen 'oplossing'.

Schaamlappen

Ook erg vind ik de aanbieders die je aanvullend ontzorgen met standaardteksten voor alles, van beleid, strategisch en tactisch tot procesdocumenten. Daarmee komt het hoofddoel van het ISMS, *nadenken over risico's en passende beveiliging niet dichterbij.* Erger nog, het zorgt voor een jaarlijks herhalend vinkjes-circus dat veel tijd vergt en ergernis oplevert. In de gemeentelijke wereld krijg je zelfs op verzoek een jaarlijkse update, zodat je inspanning wordt gereduceerd tot een druk op de knop… waarna een ingehuurde kracht toeziet op het bijeenrapen van je verdere papieren zodat je er weer voor een jaar vanaf bent. Het moet toch niet gekker worden… we noemen het ook wel ENSIA (2).

Maar het ergste van alles vind ik toch wel de aperte misleiding door partijen die een ISO-certificatie in vier weken aanbieden en dan de *zoek en vervang* ook nog voor je komen uitvoeren. Die in een paar weken een indrukwekkende papieren façade opbouwen en je mensen interviewtraining geven. Een handelwijze waarmee je dan ook nog (echt waar!) een certificering behaalt. Welke auditor je daar dan voor moet bellen weet ik niet, ik ga dit soort misleiding uit de weg.

Zélf nadenken

Ik kan het niet laten er hier ook opnieuw op te wijzen dat de BIO geen ISMS bevat, wel veel tekst die verwijst naar noodzakelijke elementen van besturing, maar het ISMS wordt alleen genoemd in een van de overheidsmaatregelen (H18). Ik vrees dat de lopende update weer een vervolg wordt op dit jaren geleden ingezette dwaalspoor.

Het ISMS in de ISO27001 is waar het allemaal om draait. Niet de controls vormen de norm (al denkt de BIO daar anders over), maar het geheel van beleid, besturing, eigenaarschap, maatregelen, monitoring, rapportage en lering. Het gaat om het geheel, het ManagementSystem dus, dat zoveel lijkt op dat uit de ISO9001, 'the HighLevelStructure'.

Dat is noodzakelijkerwijs voor elke organisatie anders en kan dus onmogelijk helemaal uit een standaardkoker komen. Doe wat een goede auditor doet en bestudeer elk '*moetje*' dat je vindt in de 27001 en denk na over wat het voor jouw organisatie betekent, kies voor een aanpak (goed gedocumenteerd) en houd je aan je voornemen. Meer wordt er niet gevraagd.

Communicatie

Liefst 85 pagina's telde het beleid voor informatiebeveiliging dat ik kortgeleden onder ogen kreeg. Vastgesteld door het bestuur, jawel. Wie denkt dat ze het hebben gelezen moet zijn vinger opsteken. Waartoe dient een document van 85 pagina's überhaupt? Dat wordt alleen gelezen als het een boek is met een leuke omslag, een belofte van spanning of genot. Anders wordt het nooit of te nimmer gelezen. Daarvoor hebben we samenvattingen uitgevonden, liefst in drie PowerPoint-dia's.

Bezweringen

Afgezien van de omvang is er nog iets mis met dergelijk beleid: de inhoud bestaat gewoonlijk uit bezweringsformules (of erger nog: herhaalt de teksten uit de norm). We spreken niemand aan, we stellen geen eisen, geen kaders en criteria. Wat denken we daarmee te bereiken?
Beleid moet iets in beweging zetten, het moet een helder doel communiceren en de randvoorwaarden aangeven waaronder dat doel bereikt moet worden. Het bestaat uit 5 W's:

- *Waarom* – je moet vragen vóór zijn en uitleggen waarom het beleid er überhaupt is;
- *Wie* – verantwoordelijkheid/eigenaarschap is de sleutel tot alles;
- *Wat* – zonder helder doel is elke inspanning te rechtvaardigen, mét alle de gewenste;
- *Waarmee* – reik middelen aan, anders gaat veel tijd verloren met zoeken;

- *Wanneer* – geef realistische tijdslijnen, en maak het SMART.

Het '*Hoe*' moet uit de organisatie komen, bij voorkeur van de 'Wie', die jóu komt vragen om hulp, dát moet het beleid bewerkstelligen.

Strategisch en tactisch

Het beleid dat het bestuur van de organisatie vaststelt moet zich beperken tot haar niveau: het strategische dat doelen stelt, de verantwoordelijken helder benoemt, de middelen daartoe aanreikt en dan het stokje doorgeeft aan het volgende niveau. In de NEN7510 wordt dit volgende niveau IBMF (3) genoemd. Die club (met leden uit de eerste én de tweede lijn (4)) kan zich namens het bestuur buigen over het tactisch beleid, wat dé norm (ISO27001) de 'kaders' noemt waartegen de *opzet, bestaan en werking* van de IB-maatregelen getoetst moeten worden.
Alle IB-beleid moet vastgeklonken worden aan de planning- & controlcyclus (die overal weer anders is), zoals NEN en ISO van ons eisen (in norm-eis 5.1b) tegen vrijblijvendheid.

Kaders (de halve Maesbrug)

Als je spreekt over kaders dan betekent dat 'ruimte afbakenen', minimale, functionele, eisen formuleren. NIVEA (5): de omzetting van controls naar passende en effectieve maatregelen moet gedaan worden door de 'control-eigenaren, zoals ik in mijn artikel in IB Magazine 2 betoogde. Die hebben behoefte aan kaders die worden meegegeven in de implementatie-opdracht, maar willen geen gedetailleerde voorschriften, want dan stopt het nadenken en wordt implementeren een invuloefening. Ook hier geldt: kórt én krachtig, want lange verhalen worden nu eenmaal niet gelezen.

Eigenaarschap

De hoeksteen van het ISMS is eigenaarschap. Daar merk je ook het verschil tussen ondernemers en managers. De eerste voelt zich volledig verantwoordelijk voor zijn eigendom, de tweede vaak alleen als je het hem 'duidelijk uitlegt'. Informatiebeveiliging staat nu eenmaal niet bovenaan de ambitielijst van de gemiddelde manager, hij scoort er niet makkelijk mee. Managers (en allen die zij managen) voeren nu eenmaal de opdracht van het bestuur uit, meestal met beperkte ruimte voor eigen inbreng. Dus zonder expliciete opdracht van het bestuur hangt IB maar al te vaak 'aan de laatste tiet' (6), conform (ontbrekende) opdracht. Al het andere krijgt voorrang.

Soorten

Wat een eigenaar moet doen is in het algemeen wel uit te leggen: hij moet goed zorgen voor zijn eigendom. Dus ook voor de informatieveiligheid ervan. Makkelijk toch?
Maar zoals ik al schreef in mijn artikel van april ligt dat net even anders: informatiebeveiliging is voor velen geen bekend onderwerp, geen routine- of ervaringskwestie. Dus is hulp geboden met middelen en adviezen door competente mensen. Dat is ónze rol: helpen met adviezen en middelen, maar we moeten daarbij níet op de stoel van de eigenaar gaan zitten, niet zijn taak overnemen.
In het artikel van april heb ik de control-eigenaar, de leverancier van informatieveiligheid, al een rol gegeven, hier behandel ik zijn klant: de vrager van informatiebeveiliging, de 'verwerkingseigenaar'.

Verwerkingseigenaar

Er zijn mensen die vinden dat de term verwerkingseigenaar eigenlijk 'informatie-eigenaar', 'proceseigenaar' of zelfs 'systeemeigenaar' moet zijn. Informatie moet mijns inziens horen bij een bedrijfsactiviteit, dat is de basis. Een afdelingsmanager (van een of een samenhangende groep bedrijfsactiviteit(en)) is in mijn ogen voor de informatieverwerking van zijn afdeling als 'verwerkingsverantwoordelijke' de natuurlijke kandidaat. De activiteit van zijn 'afdeling' genereert & gebruikt informatie en draagt dús verantwoordelijkheid. Er zijn vaak meerdere afdelingen zowel maker & gebruiker van informatie in gemeenschappelijke systemen, dus moet uit hun midden één de eigenaarrol op zich nemen en zo de anderen vertegenwoordigen. Ik gebruik heel bewust de AVG-term 'verwerking', om de relatie met de privacycollega's te benadrukken.
Geen van ons heeft nog alle IT in eigen huis, dus alle (cloud-

)diensten zijn verwerkingen mét een eigenaar ín de afdeling waar de gegevens gemaakt en gebruikt worden. Die is immers verantwoordelijk voor de uitbesteding.

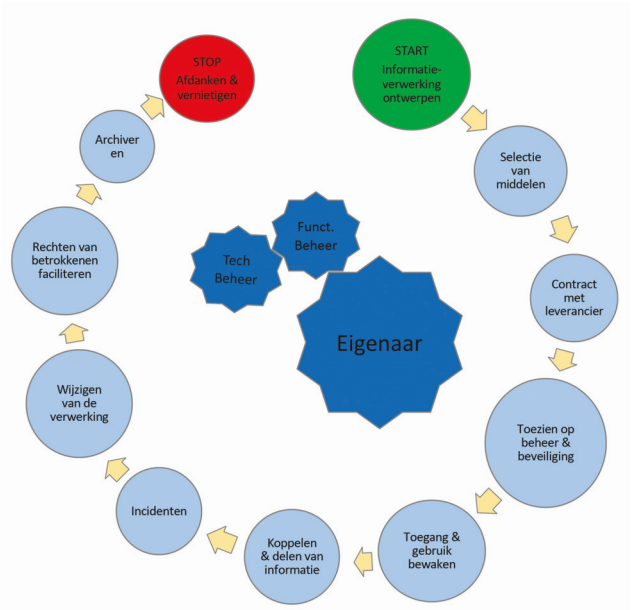
Beheersing loont

Ik heb het ook meegemaakt bij een gemeente dat output uit i-navigator (7) werd gebruikt om een verwerkingenlijst op te stellen. Die lijst telde toen 1215 regels. Dat zijn wel heel erg veel DPIA's en alleen al door de aantallen onwerkbaar voor eigenaren! Dus: beheers je, houd het werkbaar.

Beeld

Eigenaarschap gaat over de gehele periode van het bestaan van de informatieverwerking, de hele levenscyclus dus.

Om de breedte en diepte van dit eigenaarschap goed over te brengen, gebruik ik een eenvoudig beeld (zie figuur 1) dat de hele levenscyclus van een verwerking omvat, van concept tot en met afdanken. Daarbij horen ook het delen van informatie, de privacytaken en vooral: afdanken, goed opruimen, daar gaat nog wel eens wat fout.



Figuur 1: Eigenaarschap in de héle verwerkings-cyclus.

Tekst

Naast het beeld is de formele verankering van dit eigenaarschap van groot belang: het zijn immers managers, zoals eerder betoogd. Het volgende komt rechtstreeks uit beleid dat ik meestal gebruik (als toelichting op het beeld, Figuur 1).

- *Informatie*: tijdens het onderzoek naar een nieuw te starten informatieverwerking brengt hij de beveiligingseisen die aan de informatieverwerking worden gesteld in beeld middels een BIA (en soms een DPIA). Die eisen gaan over de Beschikbaarheid, Integriteit, Vertrouwelijkheid, Privacyklasse, Maximale uitvalduur, Maximaal gegevensverlies & de eisen uit de AVG (rechtmatigheid/doelbinding, proportionaliteit, subsidiariteit, dataminimalisatie);
- *Selectie*: op basis van de gevonden waarden moeten passende maatregelen worden gekozen en (bij uitvoering door derden) zekerheden dat die maatregelen ook effectief zijn. Hierbij laat de eigenaar zich adviseren door de tweede lijn (CISO/ISO).
- *Acceptatie*: bij de start van de verwerking wordt alle informatie rondom uitgevoerde BIA en DPIA, vereiste maatregelen en zekerheden gedocumenteerd en vastgelegd in het register van verwerkingen (hierna Register).
- *Overeenkomst*: alle afspraken rondom uitvoering van de beveiliging en privacy in de vorm van de overeenkomst (en eventuele verwerkersovereenkomst) worden door de **eigenaar** ondertekend en opgenomen in het Register;
- *Beheer*: de eigenaar laat zich actief informeren over beheer en beveiliging van de informatieverwerking, conform afspraken en eisen door de verantwoordelijken hiervoor.
- *Toegang en gebruik*: de eigenaar zet een autorisatiematrix op die gegevens en functionaliteit koppelt aan rollen/functies in/voor de verwerking (meest gebruikelijk in applicaties). Hierbij neemt hij 'functiescheiding' mee in de beoordeling van de rollen.
  De eigenaar verleent toestemming voor de toegang, het passende gebruik en ook beëindiging van toegang.
- *Instructie*: de eigenaar zorgt voor de nodige opleiding

Dit beleid hoort bij het algemene IB-beleid en moet door de bestuurder worden vastgesteld en gecommuniceerd naar alle verwerkingseigenaren.

en oefening voor de gebruikers om de informatieverwerking veilig te kunnen gebruiken zoals bedoeld.

- *Delen*: doorlopend bewaken en beoordelen van informatiekoppelingen en -verstrekkingen met andere verwerkingen binnen en buiten DLZ.
- *Wijzigen*: de eigenaar zorgt ervoor dat hij betrokken is bij alle wijzigingen die invloed kunnen hebben op de vereiste Beschikbaarheid, Integriteit of Vertrouwelijkheid of Privacy van zijn verwerking. Hij zorgt dat hij het laatste woord heeft bij grote wijzigingen in de informatieverwerking. Hij zorgt dan voor een (geactualiseerde) BIA en/of PIA.
- *Incidenten*: de eigenaar zorgt ervoor dat alle (vermoedens van) beveiligingsproblemen en datalekken tijdig gemeld worden. Hij zet in op beperking van de gevolgen, op onderzoek naar de oorzaken, melding bij de betrokkenen en definitief verhelpen van het lek;
- *Rechten van betrokkenen*: hij verwerkt verzoeken van betrokkenen in het kader van de AVG: informatie, inzage, rectificatie, beperking van de verwerking, overdraagbaarheid, bezwaar en vergetelheid.
- *Archiveren*: hij past de archiveringsregels en wettelijke bewaartermijnen toe.
- *Afdanken*: hij verwijdert tijdig alle informatie die niet meer nodig is voor de verwerking.

Dit beleid hoort bij het algemene IB-beleid en moet door de bestuurder worden vastgesteld en gecommuniceerd naar alle verwerkingseigenaren.
De CISO staat mijns inziens voor de taak dit beleid voor zijn organisatie aan te vullen en specifiek te maken én om optimale ondersteuning te leveren. Misschien kan hij/zij maar het beste starten met een cursus voor alle eigenaren. Hier is de eerste lijn namelijk aan zet!

Control-eigenaar

Over de control-eigenaar ga ik nu niets meer zeggen dan dat deze de leverancier van 'passende beveiliging', is, afgestemd op de eisen en wensen van de verwerkingseigenaar. Aan control-eigenaarschap en -implementatie heb ik heel mijn vorige artikel gewijd. Wat ik wel kwijt wil is dat deze eigenaar een expliciete opdracht van of namens het bestuur moet krijgen en ook de middelen nodig heeft (zoals 'gebruik de MMA') om dit realiseren. En natuurlijk ondersteuning van de CISO.

De volgende keer schrijf ik over bronnen van risico-informatie en een andere keer over het hierboven aangehaalde Register, de plek waar alle informatie te vinden is over verwerkingen, middelen, risico's, beveiliging enzovoorts.

Referenties

(1) https://www.linkedin.com/in/andrebeerten/
(2) www.ensia.nl
(3) Informatie BeveiligingsManagement Forum
(4) Bezoek www.iia.nl voor het nieuwe 3-lines model
(5) NIVEA - Niet Invullen Voor Een Ander
(6) Denk hierbij aan de big die het met de achterste en kleinste tiet van de zeug moet doen
(7) http://www.inavigator.nl/index.php/tags/gemeenten