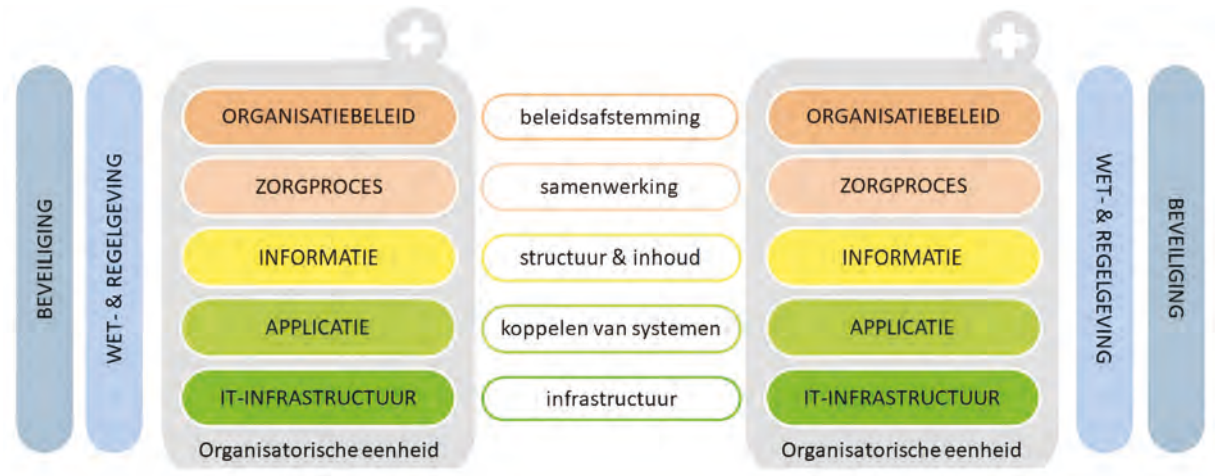
Auteur: André Beerten is sinds 2015 zelfstandig adviseur informatiebeveiliging en associate bij Verdonck, Klooster en Associates. Hij werkte eerder bij KPN, Getronics en het Groene Hartziekenhuis. Hij is te bereiken via: andre@octopus-ib.nl of via https://www.linkedin.com/in/andre-beerten/.

Gedachten over een 'Register'

OF HOE WE ZONDER INFORMATIE NIET KUNNEN BEVEILIGEN

Een plek waar voor alle betrokkenen bij informatiebeveiliging (en privacy, laten we die vooral niet vergeten) passende informatie vindbaar is noem ik het 'Register'. De informatie over informatie en beveiliging die onmisbaar is voor IB-inspanningen. En volgens mij ook voor een betrouwbaar beeld van de gevraagde 'passende beveiliging': daar hoort ook alle informatie over opzet-bestaan-werking van beveiliging in thuis, ongeacht de methode en middelen die je hanteert voor beveiliging. Waarom? Omdat de 'business', oftewel de vragers van beveiliging moeten weten hoe de beveiligers (de control-eigenaren) presteren. De risicoverantwoordelijkheid ligt immers in de business en niet bij de ondersteunende afdelingen (of zie jij dat anders?). En natuurlijk is zo'n register handig als de auditor wil weten hoe je de boel beveiligt.



Figuur 1: Datamodel van het Register.

Het beheersen van risico's is het hoofddoel van informatiebeveiliging. Beheersen begint met kennis van de scope, het bereik van je domein. De ISO27001 begint daar in hoofdstuk 4 niet voor niets ook mee, waar de grenzen, context en belanghebbenden bij het domein moeten worden verkend.

Strategisch

De kennis van je domein moet je onder meer een beeld geven van je 'risico-omgeving': wat is de betekenis van informatie in je branche, welke informatie verwerkt je organisatie, hoe groot is je afhankelijkheid, wat zijn bekende bedreigingen van beschikbaarheid, integriteit en vertrouwelijkheid ervan. Het geeft het belang aan van informatie en informatiebeveiliging voor je economische activiteit, waardoor de leiding een generieke beveiligingsambitie en een 'risk-appetite' kan formuleren waar je organisatie mee aan de slag kan. Het is 'chef-sache'.

Tactisch

Op tactisch niveau zet je deze ambitie en appetite om in beleidsregels en een concrete aanpak, waar betrokkenen mee aan de slag kunnen. Die vertaalslag kan alleen succesvol zijn als een betrouwbaar beeld bestaat van het informatielandschap ín de organisatie, gekoppeld aan verantwoordelijkheden ten aanzien van specifieke risico's per bedrijfsproces oftewel informatieverwerking en de daarvoor gebruikte middelen/diensten. Op basis van dit specifieke beeld kan beveiliging aangepakt worden. ISO, NEN & BIO vragen in control 8.1.1 om dat beeld 'Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris te worden opgesteld en onderhouden' (1). De opdracht gaat duidelijk niet (alleen) over de uitgereikte laptops, telefoons, usb-sticks, DVD's, etc.

Operationeel

De beveiligers, zij die de controls uit de norm moeten vertalen naar passende maatregelen, kunnen dat alleen doen als de informatie uit de strategische en tactische analyses hen bereikt. En niet alleen moet die informatie 'vindbaar' zijn, maar ook gestructureerd worden aangeboden, geordend naar risico, verwerking en control.
Dus een correlatie van risico's, verwerkingen, systemen/diensten en controls moet gelegd kunnen worden, anders vinden de beveiligingsinspanningen 'blind' plaats.

Wat ik waarneem

Ik heb in de tientallen organisaties waar ik heb gewerkt of opdrachten heb vervuld nog geen voorbeeld gezien van een Register zoals ik dat hierboven beschrijf.
Er zijn wel deelregistraties, zoals van IT-spullen en van het 'register van verwerkingen' van de PO/FG, maar die zijn vaak niet actueel en worden ook niet gedeeld in de organisatie en zijn niet of moeilijk te correleren.

‘Cruciale randvoorwaarde voor succes is ‘Eigenaarschap van risico’s, verwerkingen en controls’

Dat betekent dat betrokkenen voortdurend in het duister tasten over de stand van de beveiliging, over hoeveel systemen er zijn, wie die beheert, waar ze staan, welke cloud services we gebruiken en waarvoor, hoe de beveiliging per verwerking/systeem/dienst moet worden aangepakt en dan hebben we daarbij nog de onderwerpen eigendom, classificatie, toegang, koppelen etc... die ook allemaal aan beveiliging raken. CISO’s, PO’s, FG’s én control-eigenaren tasten vaak in het duister.

Voorbeeld van een Register-concept

Ik heb onlangs zijdelings kennis gemaakt met een model dat een beeld geeft van de mogelijke opbouw van zo’n Register en van de gebruiksdoelen: het NICTIZ 5-laags infra-model. In dat model staat het delen van informatie door partijen centraal, geordend naar functionele lagen. Deze structuur lijkt mij zeer handig voor het – conceptuele – datamodel van het Register.

Elk van de informatielagen kan (een groep van) eigenaren hebben die zorgen voor de actualiteit en betrouwbaarheid (en compleetheid) van de informatie. Gebruikers, zoals control-eigenaren, weten waar de informatie waar ze zich op baseren vandaan komt en hoeven niet meer op zoek.
Het Register (2) moet zélf natuurlijk ook een eigenaar hebben. Die zoek ik in de kolom informatiemanagement (in het 9-vlaks-model van Maes), tussen business en IT, waar overzicht de eerste opdracht is.

Voorbeeld van Register-beleid

Ik deel hier met jullie mijn voorstel voor een beleid dat dit Register instelt. Zoals het mij betaamt is dit artikel geen stuk met vrome wensen, maar geef ik (hoop ik) helder instructies aan benoemde rollen, waarop gehandhaafd kan worden. Cruciale randvoorwaarde voor succes is `Eigenaarschap van risico’s, verwerkingen en controls’, zoals ik dit al eens omstandig heb betoogd in een eerder artikel in dit blad.

Tactisch beleid Register

Elke organisatie heeft voor haar beheersing van de informatievoorziening behoefte aan een helder, actueel en compleet overzicht van haar informatiesystemen & -diensten eindverantwoordelijken voor beheer en beveiliging. Vooral bij incidenten is een dergelijk actueel en compleet overzicht van groot belang om snel te kunnen handelen. Dit beleidsdocument biedt kaders voor realisatie van een dergelijk overzicht.

Doel

Eén informatiepunt over de informatieverwerkingen in het domein: gestructureerde vastlegging en beschikbaarstelling van tactische en operationele (stuur-)informatie over projecten en middelen van de organisatie.
Specifieke doelen zijn:

- Ondersteunen van interne processen (ontwikkeling, beheer, veiligheid) voor gemak, snelheid en actualiteit;
- Procesverbetering, lagere (zoek-)kosten voor medewerkers, minder fouten, snellere analyse en response op incidenten;
- Makkelijker toezicht op de realisatie van kwaliteitseisen van opdrachtgevers en toezichthouders, zoals privacy en informatiebeveiliging.

Persoonsgegevens

Informatie over de verwerking van persoonsgegevens (welke gegevens waar, hoeveel, gebruiksbeperking, verwerker) moet tactisch en operationeel beschikbaar zijn. Ook voor informatiebeveiliging is er behoefte aan een intern `register’ waarin duidelijk wordt hoe elke verwerking compliant is en waar bewijzen gevonden kunnen worden van implementatie van risk-controls ten behoeve van privacy.

Bereik van het Register

De Registereigenaar (informatiemanagement dus) zorgt ervoor dat het Register de volgende informatie bevat:

- In de breedte: alle projecten, producten, informatieverwerkingen en middelen (waaronder interne applicaties, databases en hulpmiddelen voor beheer & onderzoeken);
- In de lengte: gedurende de hele levenscyclus, van idee tot en met afdanken;
- In de diepte: alle informatie rond opdrachtgever, risico's/gevraagde beveiliging (uit de BIA en DPIA), verantwoordelijkheden & (beheer-)afspraken, toegangsverlening (matrix & autorisaties), audits, koppelingen en documentatie over opzet, bestaan en werking van informatiebeveiligings- en privacy maatregelen.

Kwaliteit

Het Register moet een juiste, complete en actuele informatiebron zijn voor alle informatie-gerelateerde vragen (informatie over informatieverwerking). Om dat te bereiken zorgt de Register-eigenaar voor regelmatige toetsing van de kwaliteit van de informatie van het Register en onderneemt herstelacties door de bronnen aan te spreken. De eigenaar rapporteert hierover aan het IBMF/ de stuurgroep informatiebeveiliging.

Eigendom

Het Register of masterlist kent twee samenwerkende (groepen) eigenaren:

- Van functionaliteit en beschikbaarheid van de voorziening. Deze bepaalt ook in afstemming met de CISO inhoudelijke ambitie: welke informatie komt er wel/niet in het Register);
- Van de juistheid, toepasselijkheid, tijdigheid en compleetheid van de informatie in de masterlist: dit ligt bij eigenaren van verwerkingen en controls zoals verder uiteengezet in het 'Beleidsbijlage eigenaarschap van informatieverwerkingen' en de 'Beleidsbijlage eigenaarschap van controls'.

De tabel in het kader geeft een begin van een overzicht van de relatie informatie <> verantwoordelijke. De Register-eigenaar zorgt voor communicatie en overleg met alle betrokkenen.

(Een begin van) een inhoudsopgave van het Register

- Het verwerkingenregister van Privacy, aangevuld met alle overige 'verwerkingen'
    - o aangevuld met (of samenvallend met) bedrijfsprocessen
    - o aangevuld met de verwerkte informatie en classificatie
    - o informatie uit BIA & DPIA en andere risicobronnen:
        - alle risico-informatie, classificatie etc.
        - alle afspraken/voornemens (Maatwerk-Maatregelen) rondom beveiliging en toezicht, met agenda-/actiekoppelingen ('geactiveerd' dus die leiden tot signalen die tot actie aanzetten) voor actief toezicht op de beheerder/leverancier;
- Gerelateerde hardware en software, maar ook diensten (alle 'Cloud' etc.). Daar horen dan ook nog de diensten van 'vaste' en mobiele telefonie, Internet-lijnen, housing, hosting en beheer voor x systemen)) onder;
    - o koppelingen en (kritieke) afhankelijkheden;
    - o zicht op de gehele leverketen:
      applicatie < hoster < houser < implementatiepartner < servicepartner < leverancier HW & SW
      (misschien mis ik nog wat..);
    - o rollen rondom beheer (FB, AB, TB), gebruik, toezicht etc;
    - o niet alleen interne rollen, maar ook externe rollen (de BIA/DPIA heeft dat hopelijk in beeld gebracht). Daarbij hoort contactinformatie en operationele info zoals vastgelegd in een DAP, maar ook service-windows, responsetijden, hersteltijden, escalatie informatie;
- Alle contractuele informatie etc. etc..

Referenties

(1) In de ISO27001-2022-versie geldt een vergelijkbare opdracht: 'Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden'.

(2) Hét Register, ik schrijf het doelbewust met een hoofdletter.