Risico's vinden en erover communiceren

Eigenaarschap van de derde soort [1]

Ik ben geen specialist in risicomanagement, heb er nog niet eens een cursus in gevolgd, maar vat het gewoon op als de kerntaak van de CISO en de kerndoelstelling van het ISMS: *beheers informatierisico's met passende maatregelen*. Vanuit die gedachte deel ik met jullie mijn praktische inzichten, inclusief hun beperkingen. Dus weet je het beter, heb je een vraag of opmerking, deel het met me, dan komen we in gesprek en kan ik wat leren. Ik ga in deze bijdrage zeker ook niet in op alle prachtige methoden die er bestaan, omdat dat maar afleidt van de kern: *wie* doet het risicovinden en -beoordelen, *waar* in de organisatie en in welke fase in het ISMS (en ook een beetje *hoe*). De norm zwijgt daarover, dus schrijf ik erover.

Risico's (ongeplande gebeurtenissen met (negatieve) invloed op de informatiehuishouding van je organisatie) zijn de *raison d'être* van informatiebeveiliging. Zonder risico's geen CISO, geen ISO/NEN/BIO en geen ISMS (en natuurlijk geen firewalls, virusscanners, cryptografie et cetera). Het kennen of vermoeden van informatierisico's is van groot belang voor ons als beroepsgroep, dus moeten we het zoeken naar, vinden en opvolgen van risico's goed organiseren. ISO27001 geeft de opdracht in 6.1.2 om een (herhaalbare) methode voor het identificeren en beoordelen van informatierisico's vast te stellen. De CISO (2) moet dus aan de bak.

Mijn stelling: risico's voor je informatieverwerking vind je niet op één plek in je organisatie en niet met één zoekmethode.

Dé methode

Ik heb gerespecteerde collega's (die ik óók waardeer) die bijna heilig geloven in 'dé risicoanalyse' - zoals de norm die ook lijkt te vragen - waarbij een groep mensen (vaak een kamer vol adviseurs) zich buigt over een lange lijst dreigingen. Deze groep weegt de dreigingen naar kans en impact en het resultaat is – bijvoorbeeld - een prioriteitstelling van de ruim 112 controls. Soms worden ze voorzien van wat achtergrondinformatie.

Werkt deze werkwijze?

Mijn vragen bij dé methode zijn:

- **Compleetheid:** kan een groep adviseurs en experts over genoeg kennis & informatie beschikken om álle dreigingen en kwetsbaarheden te kennen?
- **Kwaliteit:** kan een groep adviseurs en experts over genoeg kennis & informatie beschikken om álle scenario's en potentiële impacts te doordenken?
- **Actualiteit:** als de inspanning groot is, ga je hem dan wel vaak genoeg herhalen terwijl het dreigingsbeeld intussen wel verandert?
- **Toepasbaarheid:** heeft de informatie uit de analyse de juiste vorm en detaillering om te gebruiken voor het doel?

Mijn beeld is dat dé risicoanalyse in een project een korte impact kan hebben, maar snel verwordt tot een vinklijstje voor acties en zo maanden of jaren op agenda's kan staan, maar steeds minder steun krijgt. Zolang de lijst niet is afgewerkt, maakt een nieuwe poging tot inventarisatie niet veel kans. Daarnaast zet de beschikbaarheid van een 'lijst' niet aan tot zélf nadenken. Daarom vermijd ik 'dé risicoanalyse'. Ik doe het daarom anders.

Risico's zijn overal

Ik doe het anders, ik onderscheid de volgende bronnen van risico-informatie:

1. het bestuur van de organisatie (RvB),
2. de 'verwerkingseigenaren',
3. de 'control-eigenaren',
4. de CISO,
5. alle medewerkers in de organisatie.

1.Bestuur

De eerste (en belangrijkste) bron van risico-informatie is voor mij het bestuur. Het bestuur is namelijk de risico-eigenaar in laatste instantie (of gelijk Harry S. Truman: *'the buck stops here'*). Het bestuur geeft de opdracht tot beveiligen niet voor de lol. Het kost namelijk aandacht, tijd, geld en die zijn, zo heb ik geleerd, nergens ongelimiteerd voorhanden. Het gaat ten koste van de dingen die een RvB écht graag wil, namelijk bedrijfsdoelen bereiken.

De risico-opvatting van het bestuur is essentiële informatie voor het ISMS: het verwoordt ambitie en richting van 'de baas'. Iedereen die een rol speelt in de informatiebeveiliging van de organisatie moet die motivatie kennen en vertalen naar zijn eigen handelen, maar dit geldt vooral de verschillende 'eigenaren'.

Je kunt verslag maken van de sessie met de RvB, met daarin aangemerkt een 'risk-appetite' met van die gekleurde vakjes (een 'heat map') met een schuine lijn die aangeeft welk risico wel en welk risico niet wordt behandeld. Dat werkt vooral goed voor de auditor, maar het is ook een mogelijke basis voor een aanvalsplan.

Gevoel en betrokkenheid

Of de risico-informatie vanuit de RvB helemaal compleet en juist is, boeit mij eerlijk gezegd niet zo, want het gaat er primair om dat de RvB betrokken is en dat kan (en *durft* te) tonen aan de hele organisatie. IB is *'spooky stuff'* voor de gemiddelde bestuurder, dus als je ze al een uitspraak kunt ontlokken, heb je maximaal gescoord.

Natuurlijk moet je ze helpen met enige inspiratie uit - voor de RvB - herkenbare bronnen zoals het NCSC, de 'big 4' en de branche-organisatie. Laat in een interactieve sessie ook de IT-manager en de controller aanschuiven om support te leveren. Wat een formeel - door het bestuur - vast te stellen resultaat oplevert.

Rapportage

De risicobeleving van de RvB levert je ook een prachtkans op om de in de norm gevraagde doelen voor het ISMS te formuleren en je periodieke rapportage over het ISMS en de projectvoortgang hierop af te stemmen. De herkenning dat je concreet aan de slag gaat met hun *wakkerligpunten* zal hen verrassen en bij de les houden. EN het 'eigenaarschap' bij hen verder verankeren. Het vormt het zeer belangrijke startpunt van je ISMS.

Communicatie

De uitkomsten van de Bestuurlijke RisicoAnalyse (BRA), zoals ik hem noem, moeten conform de eis in 'de norm' gedeeld worden met 'relevante personen'. Als het kan door de RvB zélf en bij elke gelegenheid. Ik vind dat iedereen in de organisatie de bestuurlijke risicoboodschap moet ontvangen 'from the horses mouth'. Een uitstekend beginpunt van een veiligheidscultuur.

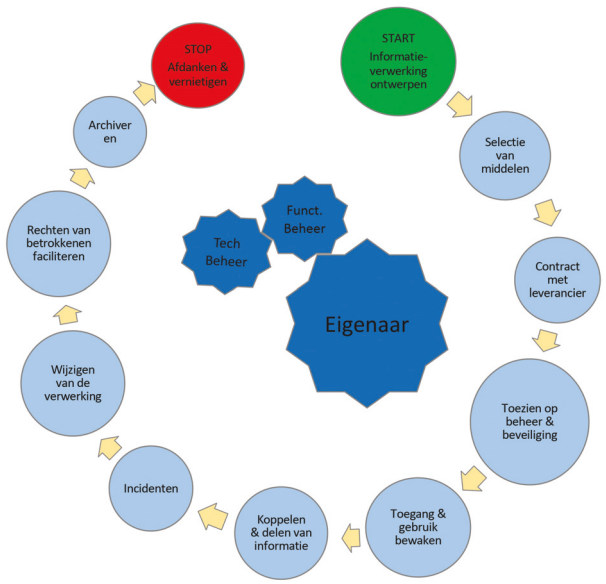
2.De Verwerkingseigenaren

Deze groep duiden we ook vaak aan als proces- of systeemeigenaren. In mijn tweede artikel heb ik hun takenpakket breed uitgemeten en een van de belangrijke taken (ze zijn allemaal belangrijk, natuurlijk) is het in kaart brengen van de specifieke risico's rond de informatieverwerking. Namens het bestuur moet die verantwoordelijkheid expliciet belegd zijn en leiden tot bijvoorbeeld een 'aangeklede' BIA of DPIA (dus met meer dan alleen een BIV-klasse (3)).

Aangeklede BIA

Een aangeklede BIA bevat voor mij primair een analyse van de 'scope', het bereik van de verantwoordelijkheid: voor welke informatieverzamelingen, systemen en diensten ben ik als eigenaar verantwoordelijk. En wie verrijkt en gebruikt 'mijn' informatie, wie heeft toegang, wie beheert wat? Niet zelden is dit gesprek voor de betrokkenen een ontdekkingsreis. Er duiken soms ook spoken uit het verleden op zoals oude systemen 'in de kelder', contracten die nooit opgezegd zijn et cetera.

Natuurlijk doen we ook even een 'BIV-je', maar we moeten vooral in gesprek raken over *verwerkingsrisico's* die vermijdbaar of behandelbaar zijn. Deze moeten gewogen en gecommuniceerd



Figuur 1 - Eigenaarschap in de hele verwerkingscyclus

worden.

Communiceren

Door de BIA/DPIA met de aangewezen verwerkingseigenaar in een gesprek te verkennen vestigen we 'eigenaarschap'. Dat is ook weer een bijdrage aan de veiligheidscultuur.

Uitkomsten van het gesprek moeten uiteraard niet op de plank belanden. Ik hoor jullie denken 'natuurlijk niet', maar ik vraag me wel eens af wat er dan wél mee gebeurt?

De uitkomsten (BIV-klasse én specifieke risico's voor de hele verwerkingsscope) dienen opgenomen te worden in het risicoregister. Ik zal daar later dit jaar (in IB Magazine 6) meer over schrijven. Dít is de informatie waarmee de control-eigenaar (IB Magazine 2) aan de slag moet.

3.De Control-eigenaren

Door de control-eigenaren wordt 'passende veiligheid' geleverd. Ze doen dit (als het goed is) door optimaal aan te sluiten bij de wensen en eisen van de directie en van verwerkingseigenaren, wetgeving en brancheregels, de risicobeelden van NCSC, Z-Cert et al én de operationele kennis van direct betrokkenen. Althans zo moet het mijns inziens gebeuren. Dit loffelijk streven wordt optimaal ondersteund door mijn MMA (zie artikel in IB Magazine 2 van dit jaar).

Met die MMA registreren we bij dit streven de tekortkomingen en óók de 'restrisico's die we daarbij vanuit operationeel perspectief bezien: wat kan er fout gaan nu we het niet volledig in de klauwen hebben?

Niemand kan beter inschatten wat die restrisico's zijn dan de control-verantwoordelijke (met zijn mensen), liefst in een goed gesprek met de CISO.

Communiceren

Al te vaak zijn de (operationele) restrisico's welbekend maar dringen niet door tot de bestuurder. Dat vindt zijn oorzaak vooral in de manier waarop erover gecommuniceerd wordt: inhoudelijk, anekdotisch en incidenteel. Als je er daarentegen in slaagt de aansluiting te vinden bij de beleving van de 'business' word je gehoord en ontstaat ruimte voor verbetering.

Alle risico's in de organisatie verdienen een plek in het risicoregister, dat risico's naar aard en urgentie moet onderscheiden. Het risicoregister is dé manier om de boodschap aan het bestuur over te brengen, mits structureel/regelmatig en via de juiste boodschapper bezorgd (stuurgroep en/of CISO). Want het bestuur is immers '*where the buck stops*'.

4.De CISO

De CISO zorgt voor een eenvoudig en toegankelijk risicoregister dat 'geconsumeerd' (gekend, geanalyseerd) wordt, door zowel control-eigenaren als het bestuur van de organisatie. Geïmplementeerde controls geven direct antwoord op dreigingen, de bestuurder zorgt voor de middelen om dat te kunnen realiseren. Verder zorgt de CISO dat signalen van binnen en buiten de organisatie over dreigingen en risico's een plek vinden in het register en de passende weging ontvangen.

Bronnen

'De normen' stellen dat iemand contact moet houden met overheden en andere relevante organisaties (ISO/NEN/BIO 6.1.3 en 6.1.4). Voor risico-informatie uit de buitenwereld, zoals branche-organisaties en partijen in het vakgebied (NCSC, Z-CERT, DTC en uiteraard open bronnen) moet dat de CISO zijn.

Business-impacts of BIV

Operationele risico's blijk je niet goed in business-impacts te kunnen uitdrukken, zo heb ik gemerkt in de praktijk. Een falende bescherming tegen malware kan zoveel verschillende effecten hebben en dat geldt ook voor een openstaande deur of een falende screening. Dus heb ik me aangeleerd bij operationele (rest-)risico's met BIV en de kwalitatieve beoordeling 'laag-

midden-hoog' te werken. Dit uiteraard aangevuld met een beschrijving van de mogelijke gevolgen en een plan voor mitigatie.

5.Alle andere medewerkers

Het melden en verwerken van (vermoedens van) zwakke plekken heeft een prominente plek in de norm. Ik denk dat veel organisaties het best aardig hebben geadresseerd, omdat het een manier is om 'awareness' te bevorderen. Of het ook het gewenste resultaat heeft, daar heb ik vrees ik geen beeld bij.

Wél word ik verdrietig van het woord awareness dat nog steeds breed gebruikt wordt. Immers, vrijwel alle rokers zijn zich bewust van hun ongezonde gedrag, maar dat verandert hun gedrag níet. Dat je aan veel meer knoppen moet draaien om het gewenste gedrag te bewerkstelligen bij je medewerkers is genoegzaam behandeld in goede artikelen, onder andere van de hand van Inge Wetzer.

Melden en verwerken

Natuurlijk moet er een simpele en goed vindbare meldmogelijkheid bestaan van dreigingen, kwetsbaarheden en security-incidenten met aansluitend ook een snelle verwerking (triage) en opvolging. Opname in het algemene risicoregister (ook al zijn ze gemitigeerd) lijkt me ook verstandig, omdat je meldingen dan meeneemt in perioderapportages en deze bij herhalingen ook een hogere prioriteit kunt geven.

Het risicoregister

Het risicoregister bevat alle informatie over actuele dreigingen en gewogen risico's. Ik gebruik daarvoor de voorspelbare opzet van impact in businesstermen (financiën, reputatie, processen et cetera) dus met relatie naar impact op proces-/bedrijfsniveau. Verder natuurlijk de berekening **kans*impact** voor prioritering, mitigerende actie, relatie met control & control-eigenaar en de status.

Houd daarbij de scoring eenvoudig: onderscheid niet meer dan drie niveaus voor kans en impactcategorieën, hoe je dat doet is weer een ander onderwerp. Heldere ideeën om de gevonden risico's te mitigeren mogen natuurlijk niet ontbreken, voorzien van gebudgetteerd geld, tijd & mensen.

Rapporteren

Het register moet regelmatig op de bestuurstafel belanden en niet in de organisatorische kleilaag vastlopen. Daar ligt een belangrijke taak voor de CISO, als maker en bewaker van het ISMS. Als de Bestuurlijke RisicoAnalyse succesvol was dan zal de bestuurder ook ontvankelijk zijn geworden voor andere risicoboodschappen en er iets mee willen doen. **Overal geldt: cultuur begint bij de toon in de bestuurskamer ('the tone at the top').**

Accepteren, vermijden en overdragen

Ik schrijf hier vooral over het identificeren en behandelen van risico's, maar we hoeven ze niet per se te behandelen we mogen ze ook accepteren, dat hoort bij ondernemerschap. *'Zonder risico's geen kansen'*, zegt de ondernemer. Maar we zijn veel vaker *'manager'* dan *'ondernemer'* en een manager is inherent *'risico-avers'*. Dus formuleren we overwegingen -'criteria' zegt de norm - om risico's te accepteren of over te dragen. In relatie tot norm-controls hoor ik vaak op luchtige toon 'comply or explain', alsof je altijd zomaar mag accepteren, onbeargumenteerd. Ik denk dat een 'explain' gekoppeld moet zijn aan een formeel proces en formele acceptatie, daar ga ik hier verder niet op in.

Samenvattend

Risico's voor je informatieverwerking vind je niet op één plek en niet met één zoekmethode. Ik zie eigenaren op verschillende niveaus (strategisch, tactisch en operationeel) die op verschillende manieren risico's moeten vinden (actief en passief).

De communicatie over risico's van 'vinders' naar 'behandelaren van risico's' en omgekeerd over de stand van de behandeling (beheersing met controls) is de kern van je ISMS (je PDCA-cyclus). Een belangrijk hulpmiddel daarbij is je risicoregister dat de basis vormt voor rapportage naar het bestuur.

De rapportage naar het hoogste organisatieniveau is je doorlopende 'awareness'-actie 'naar boven', dat daardoor de uitdaging op zijn bordje krijgt om te kiezen uit de vier opties: accepteren, vermijden, behandelen of overdragen.

Referenties

(1) Vrij naar Steven Spielberg, naast eigenaarschap van 1. verwerkingen en 2. controls.

(2) De term CISO gebruik ik hier - in arren moede - als dekmantel voor alle soorten adviseurs en coördinatoren informatiebeveiliging, ook waar er geen sprake is van een 'concern'.

(3) BIV – Beschikbaarheids-, Integriteits- en Vertrouwelijkheidsklasse.