VOLWASSENHEIDSMODEL

INFORMATIEBEVEILIGING

3-Pijlermodel

Afbeelding van Renjith Krishnan / FreeDigitalPhotos.net

De Haagse Hogeschool, TNO en de waterschappen voeren samen het RAAK-project Veilig Water uit. Dit project is in december 2013 gestart en heeft een doorlooptijd van twee jaar. Het heeft tot doel de informatiebeveiligingsprofessionals meer grip te laten krijgen op de informatiebeveiliging. Hiervoor worden binnen het project kennis en praktisch inzetbare hulpmiddelen ontwikkeld.

Opdrachtgever: RAAK-project Veilig Water

Auteur: Marcel Spruit

Versie: 1.3

Datum: 4 april 2017

Inhoudsopgave

1 Inleiding

Na een reeks incidenten op het gebied van informatieveiligheid, waaronder het hacken van op afstand bestuurbare sluizen, de Diginotar-affaire en Lektober, is het duidelijk geworden dat binnen de overheid de informatieveiligheid nog onvoldoende geregeld is. Mede daarom is een RAAK-project gestart waarin de Haagse Hogeschool, TNO, het Nationaal Cyber Security Centrum en de waterschappen samenwerken om methoden en technieken te ontwikkelen die overheidsorganisaties kunnen ondersteunen bij het verbeteren van hun informatieveiligheid.

Informatieveiligheid is geen eenmalige actie, maar een zaak die regelmatig terugkomt op de tafel van de bestuurder. Het vraagt om een procesmatige aanpak waarbij tijdig bijstelling plaats kan vinden op basis van nieuwe of gewijzigde risico's of dreigingen. Dat vraagt om heldere keuzes (de goede dingen doen), competenties (de dingen goed doen) en verantwoordelijkheden (de dingen goed beleggen). Het is niet vanzelfsprekend dat dit allemaal goed geregeld is. Het is dan ook nodig om te kunnen bepalen hoever overheidsorganisaties met het regelen ervan zijn gevorderd en in hoeverre ze op het gebied van informatieveiligheid in control zijn, oftewel hoe volwassen ze zijn op het gebied van informatiebeveiliging.

In de literatuur zijn verschillende modellen beschreven om de volwassenheid van de informatiebeveiliging te meten. Uit vooronderzoek is gebleken dat de bestaande modellen niet zonder meer voldeden aan de gestelde criteria,[1] te weten:

- Het meet alle relevante aspecten van de volwassenheid.
- Het is gericht op informatiebeveiliging.
- Het is toepasbaar op overheidsorganisaties.
- Een meting kan binnen één dag worden uitgevoerd.

Daarom is een nieuw model opgesteld waarmee het mogelijk is om door middel van interviews de volwassenheid van de informatiebeveiliging van een organisatie binnen één dag te bepalen. Dit model is opgesteld op basis van de bestaande volwassenheidsmodellen uit de literatuur.

Dit rapport beschrijft het model voor het meten van de volwassenheid van de informatiebeveiliging bij een organisatie. De organisatie kan de resultaten van de meting gebruiken om te bepalen hoe ze scoort voor de volwassenheid van de informatiebeveiliging.

[1] M.A. Jahan, *Het ontwikkelen van een genormeerde meetmethode waarmee de volwassenheid van informatiebeveiliging in een organisatie (snel en efficiënt) kan worden bepaald*, De Haagse Hogeschool, 2 april 2013.

2 Volwassenheid informatiebeveiliging

In het kader van informatiebeveiliging worden door de medewerkers van een organisatie, lopend van topmanagers tot operationele en ondersteunende medewerkers, activiteiten met betrekking tot informatiebeveiliging uitgevoerd. Als de organisatie informatiebeveiliging adequaat heeft ingericht, dan geldt, met betrekking tot de activiteiten in het kader van informatiebeveiliging, dat:

- de goede activiteiten worden uitgevoerd;
- deze activiteiten goed worden uitgevoerd;
- de uitvoering en aansturing ervan goed zijn belegd.

Niet elke organisatie zal informatiebeveiliging even adequaat hebben ingericht. Op ieder van de genoemde aspecten kan een organisatie namelijk steken laten vallen. De mate waarin een organisatie met betrekking tot de activiteiten voor informatiebeveiliging voldoet aan de drie genoemde aspecten, is het volwassenheidsniveau van informatiebeveiliging in de organisatie.

Het volwassenheidsniveau van informatiebeveiliging kunnen we bepalen door de genoemde aspecten te scoren. We krijgen dan drie scores (s_1,s_2,s_3), waarin:

- s_1 = de mate waarin de goede activiteiten voor informatiebeveiliging worden uitgevoerd.
- s_2 = de mate waarin de betreffende activiteiten goed worden uitgevoerd.
- s_3 = de mate waarin uitvoering en aansturing van deze activiteiten goed zijn belegd.

De score voor ieder van de aspecten kan lopen van 1 tot 5, waarbij 1 aangeeft dat het betreffende aspect nog niet is gerealiseerd en 5 aangeeft dat het aspect volledig is gerealiseerd.

De drie aspecten wegen niet even zwaar. Het uitvoeren van de goede activiteiten weegt het zwaarst, want als je de verkeerde activiteiten doet, wordt informatiebeveiliging sowieso niets. Als de werkwijze en de belegging volwassener worden, wordt de beveiliging effectiever, maar zelfs zonder dat werken de maatregelen toch, zij het minder effectief. De werkwijze en de belegging wegen daarom beide, en in dezelfde mate, minder zwaar. Dit leidt tot de volgende gewichten:

- s_1: x 3.
- s_2: x 2.
- s_3: x 2.

Het volwassenheidsniveau van informatiebeveiliging, M_{IB}, is het gewogen gemiddelde van de drie scores (s_1,s_2,s_3). In formule weergegeven:

$$M_{IB} = \frac{s_1 \times 3 + s_2 \times 2 + s_3 \times 2}{3 + 2 + 2}.$$

Als de drie scores (s_1,s_2,s_3) bijvoorbeeld (2,3,3) zijn, dan is het volwassenheidsniveau van informatiebeveiliging 18 / 7 = 2.6.

In de volgende paragrafen worden de drie aspecten en de mogelijke scores kort toegelicht.

Opgemerkt dient te worden dat het volwassenheidsniveau van informatiebeveiliging niet hetzelfde is als het veiligheidsniveau. Zo kan een organisatie die voor volwassenheid van informatiebeveiliging op

5 zit (het maximum), op basis van deze volwassenheid hebben gekozen om een bepaalde gangbare beveiligingmaatregel, bijvoorbeeld uitwijk, niet te implementeren. In dit geval is deze maatregel dan ook niet nodig, of zelfs ongewenst, voor de betreffende organisatie. Het maximale niveau voor volwassenheid impliceert dat de organisatie zeer serieus en professioneel met informatiebeveiliging omgaat en zeker niet dat ze alle denkbare beveiligingsmaatregelen treft, maar wel alle benodigde maatregelen.

Het volwassenheidsniveau van de informatiebeveiliging van een organisatie heeft één waarde. Dit in tegenstelling tot het veiligheidsniveau dat kan variëren over de verschillende onderdelen van de organisatie. Zo kan een organisatie er bewust voor kiezen om het computercentrum zwaar te beveiligen en de kantoortuin licht te beveiligen. Een organisatie met een hoge volwassenheid heeft dit zeer goed onderbouwd en afgewogen en zeer adequaat gerealiseerd en geconsolideerd. Een organisatie met een lage volwassenheid is het overkomen en dan is het zeer wel mogelijk dat het, waarschijnlijk voor de kantoortuin, niet het benodigde veiligheidsniveau is.

2.1 Het uitvoeren van de goede activiteiten

Voor het bepalen van de mate waarin de goede activiteiten voor informatiebeveiliging worden uitgevoerd, wordt de standaard ISO 27001 als uitgangspunt gebruikt. ISO 27001 is een internationale standaard norm voor het inrichten van een managementsysteem voor informatiebeveiliging, oftewel een Information Security Management System (ISMS).[2] De standaard beschrijft een procesbenadering voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS in een organisatie. De belangrijkste onderdelen van het ISMS zijn:

- Informatiebeveiliging beleid opstellen.
- Risico's identificeren en analyseren.
- Beveiligingsmaatregelen selecteren en invoeren.
- Restrisico's accepteren.
- Beveiligingsincidenten detecteren en registreren.
- Awareness meten en verbeteren.
- Informatiebeveiliging controleren.
- ISMS evalueren en verbeteren.

We definiëren vijf niveaus aan de hand van de mate waarin informatiebeveiliging is ingevoerd. Deze vijf niveaus zijn weergegeven in onderstaand schema.

[2] *ISO/IEC 27001:2013; Information technology – Security techniques – Information security management systems – Requirements*, ISO, 2013.

Niveau		Maatregelen voor informatiebeveiliging	Status van informatie-beveiliging	Nieuw aspect t.o.v. onderliggend niveau
1	Reactief	Maatregelen voor informatiebeveiliging worden pas getroffen nà incidenten, om herhaling te voorkomen	De meeste informatie-beveiligings-maatregelen ontbreken	–
2	Ad hoc	De meest gebruikelijke beveiligingsmaatregelen zijn getroffen	Maatregelen voor informatiebeveiliging zijn op ad hoc basis getroffen (bijv. op basis van bekendheid)	Proactief treffen van een beperkt aantal beveiligingsmaatregelen
3	Baseline	Alle relevante maatregelen uit een baseline voor informatiebeveiliging zijn getroffen en de implementatie ervan wordt beheerd en gecontroleerd	Er is een beheerd en gecontroleerd basisniveau voor informatie-beveiliging	Implementatie van een basisniveau voor informatiebeveiliging, inclusief het beheer en de controle ervan
4	Baseline plus	Op basis van risicoanalyse zijn, waar nodig, aanvullende maatregelen getroffen en ook deze worden beheerd en gecontroleerd	Risicoanalyse wordt ingezet om te bepalen in hoeverre extra informatiebeveiliging nodig is	Aanvullende maatregelen op basis van risicoanalyse worden beheerd en gecontroleerd meegenomen
5	ISMS	Alle processen van een managementsysteem voor informatiebeveiliging (ISMS) zijn volledig ingevoerd en gecontroleerd	Er is een volledig en gecontroleerd managementsysteem voor informatiebeveiliging (ISMS)	Implementatie van een gecontroleerd ISMS

De parameter s_1 (de mate waarin de goede activiteiten voor informatiebeveiliging worden uitgevoerd) krijgt een waarde van 1 tot 5, overeenkomend met de opeenvolgende niveaus *reactief* tot *ISMS*.

2.2 Het goed uitvoeren van de activiteiten

Voor het bepalen van de mate waarin de activiteiten voor informatiebeveiliging goed worden uitgevoerd, wordt het Capability Maturity Model (CMM) als uitgangspunt gebruikt. Het CMM is een door het Software Engineering Institute van de Carnegy Mellon University ontwikkeld referentiemodel voor het verbeteren van de kwaliteit van organisaties voor softwareontwikkeling.[3] In het CMM worden vijf niveaus gedefinieerd voor het kwaliteitsniveau van de werkwijze in de organisatie. Hoewel het CMM specifiek gericht is op organisaties voor softwareontwikkeling, kan het concept van gedefinieerde kwaliteitsniveaus voor de werkwijze ook toegepast worden in andere domeinen, waaronder informatiebeveiliging. Analoog aan het CMM onderscheiden we vijf niveaus voor het kwaliteitsniveau van de werkwijze met betrekking tot de activiteiten voor informatiebeveiliging. Deze vijf niveaus zijn weergegeven in onderstaand schema.

[3] Software Engineering Institute, *The Capability Maturity Model: Guidelines for Improving the Software Process*, Addison Wesley, 1995.

Niveau		Karakterisering van werkwijze	Status van informatie-beveiliging	Nieuw aspect t.o.v. onderliggend niveau
1	Initieel	Men werkt ad hoc	Er wordt niets afgestemd over informatiebeveiliging	–
2	Herhaald	Men gebruikt good practices en stemt het werk onderling af	Ervaringen en good practices voor informatiebeveiliging worden vastgelegd en toegepast	Het gebruik van good practices voor informatiebeveiliging
3	Gedefinieerd	Men werkt conform gedefinieerde en vastgelegde procedures	Standaarden en vaste procedures voor informatiebeveiliging worden (gecontroleerd) toegepast	Het volgen van vastgelegde procedures voor informatiebeveiliging
4	Gemanaged	Men meet de efficiëntie van informatiebeveiligingsactiviteiten en past deze zo nodig aan om de efficiëntie ervan te vergroten	De kwaliteit van de activiteiten voor informatiebeveiliging wordt gemeten en zo nodig bijgestuurd	Efficiëntieverbetering van informatiebeveiligingsactiviteiten
5	Geoptimaliseerd	Men toetst of de informatiebeveiligingsactiviteiten de business faciliteren en past ze zo nodig aan om het nut ervan te vergroten	De informatiebeveiligingsactiviteiten worden afgestemd op de behoefte van de organisatie	Effectiviteitsverbetering van informatiebeveiligingsactiviteiten

De parameter s_2 (de mate waarin de betreffende activiteiten goed worden uitgevoerd) krijgt een waarde van 1 tot 5, overeenkomend met de opeenvolgende niveaus *initieel* tot *geoptimaliseerd*. Ieder niveau wordt pas behaald als de karakterisering van de werkwijze (de tweede kolom in de tabel) zowel in opzet, bestaan als werking is gerealiseerd. Zo wordt bijvoorbeeld niveau *gedefinieerd* pas behaald als geconstateerd is dat in de organisatie zowel in opzet, bestaan als werking wordt gewerkt conform de gedefinieerde en vastgelegde procedures.

2.3 Het goed beleggen van de uitvoering en aansturing

Organisaties baseren hun management normaal gesproken op het concept integraal management.[4] De volle eindverantwoordelijkheid voor alle processen en systemen van de organisatie ligt in eerste instantie bij de strategische top van de organisatie. Anders gezegd: de top is de eigenaar van de processen en systemen. De eigenaar bepaalt welke middelen voor de processen en systemen worden ingezet, wat de betreffende middelen moeten kunnen (functionaliteit en kwaliteit) en wie dat tegen welke kosten dient te realiseren.
Desgewenst kan de top bepaalde processen of systemen delegeren naar een organisatieonderdeel. Het management van het betreffende organisatieonderdeel wordt dan de eigenaar van de naar haar gedelegeerde processen of systemen. Dit is vooral nuttig als het gaat om processen of systemen die vooral, of zelfs uitsluitend, gebruikt worden door het betreffende organisatieonderdeel.
Informatiebeveiliging met betrekking tot een bepaald proces of systeem is een aandachtspunt van de eigenaar van het betreffende proces of systeem. Informatiebeveiliging met betrekking tot organisa-

[4] H. Buurma & C. Jacobs (red.), *Integraal management, inspirerend leiderschap in de publieke sector*, Lemma, 2007.

tiebrede processen en systemen is een aandachtspunt van de strategische top van de organisatie. Informatiebeveiliging met betrekking tot processen en systemen die naar een bepaald organisatieonderdeel zijn gedelegeerd, zijn een aandachtspunt van de eigenaar ervan, te weten het management van het betreffende organisatieonderdeel.
Voor de belegging van informatiebeveiliging kunnen we verschillende niveaus onderscheiden, zoals weergegeven in onderstaand schema.[5,6]

Niveau		Houding van topmanagement	Status van informatiebeveiliging	Nieuw aspect t.o.v. onderliggend niveau
1	Onbezorgd	Topmanagement vindt informatiebeveiliging niet relevant en meer iets voor anderen	Niemand is verantwoordelijk voor informatiebeveiliging	–
2	Ontluikend	Topmanagement vindt dreigingen m.b.t. de informatievoorziening relevant en vindt specifieke aanpak van informatiebeveiliging nodig	Informatiebeveiliging is een stafaangelegenheid	Informatiebeveiliging is belegd bij specifieke rollen of (staf)functies
3	Beheerst	Topmanagement vindt dat informatiebeveiliging een verantwoordelijkheid is van het lijnmanagement	Informatiebeveiliging is een lijnmanagementaangelegenheid	Informatiebeveiliging staat op de managementagenda
4	Geïntegreerd	Topmanagement beschouwt informatiebeveiliging als een integraal onderdeel van de bedrijfsvoering	Informatiebeveiliging is een topmanagementaangelegenheid en is opgenomen in de planning & control cyclus	Informatiebeveiliging is geïntegreerd in de bedrijfsvoering
5	Genetwerkt	Topmanagement vindt geïntegreerde informatiebeveiliging zo cruciaal dat zij hiervoor samenwerking met partnerorganisaties noodzakelijk vindt	Organisaties werken samen om informatiebeveiliging gezamenlijk aan te pakken als onderdeel van de dagelijkse bedrijfsvoering	Geïntegreerde informatiebeveiliging strekt zich uit over meerdere organisaties

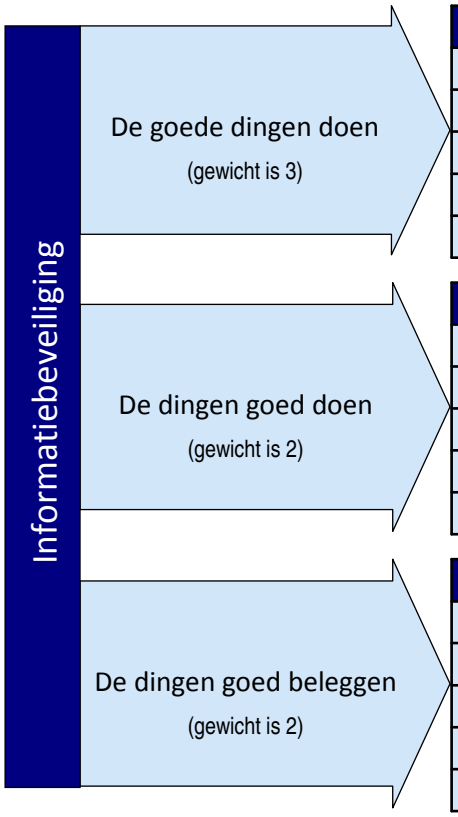
De parameter s_3 (de mate waarin uitvoering en aansturing van deze activiteiten goed zijn belegd) krijgt een waarde van 1 tot 5, overeenkomend met de opeenvolgende niveaus *onbezorgd* tot *genetwerkt*.

2.4 Samenvatting

Het hierboven beschreven model voor het meten van de volwassenheid van informatiebeveiliging is samengevat in onderstaande figuur. Het volwassenheidsniveau van de informatiebeveiliging van een organisatie heeft één waarde die aangeeft hoe serieus en professioneel de organisatie omgaat met informatiebeveiliging. Het volwassenheidsniveau is het gewogen gemiddelde van de behaalde niveaus op de drie aspecten. Evenals voor de drie aspecten loopt de schaal voor het volwassenheidsniveau van 1 tot 5.

[5] P. Overbeek e.a., *Informatiebeveiliging onder controle*. Pearson Education, Amsterdam, 2005.

[6] *Partnering for cyber resilience*, World Economic Forum, 2012.



Niveau	Status van informatiebeveiliging
1 – Reactief	De meeste beveiligingsmaatregelen ontbreken
2 – Ad hoc	Maatregelen zijn op ad hoc basis getroffen
3 – Baseline	Er is een beheerd en gecontroleerd basisniveau voor IB
4 – Baseline plus	Aanvullend wordt risicoanalyse ingezet
5 – ISMS	Er is een volledig en gecontroleerd ISMS

Niveau	Status van informatiebeveiliging
1 – Initieel	Er wordt niets afgestemd
2 – Herhaald	Good practices worden vastgelegd en toegepast
3 – Gedefinieerd	Gedefinieerde en vastgelegde procedures
4 – Gemanaged	Kwaliteit wordt gemeten en zo nodig verbeterd
5 – Geoptimaliseerd	Effectiviteit gemeten en zo nodig verbeterd

Niveau	Status van informatiebeveiliging
1 – Onbezorgd	Niemand is echt verantwoordelijk
2 – Ontluikend	IB is een stafaangelegenheid
3 – Beheerst	IB is een lijnmanagementaangelegenheid
4 – Geïntegreerd	IB is een integrale directieaangelegenheid
5 – Genetwerkt	Geïntegreerde IB strekt tot buiten de organisatie

3 Succesfactoren informatiebeveiliging

Op basis van het volwassenheidsmodel voor informatiebeveiliging uit het vorige hoofdstuk zijn succesfactoren voor informatiebeveiliging geformuleerd. Deze factoren zijn in onderstaande tabel weergegeven.

Succesfactoren voor informatiebeveiliging	Gerealiseerd		
	Ja	Deels	Nee
De directie heeft een beleid voor informatiebeveiliging opgesteld, heeft hierover goed gecommuniceerd en bewaakt zichtbaar de navolging ervan			
Er is een sluitende inrichting van de informatiebeveiligingsorganisatie, met voldoende ervaren mensen en alle benodigde bevoegdheden			
Het eigenaarschap van kritische processen en informatie- en ICT-systemen is adequaat ingevuld en geborgd			
Awareness ten aanzien van informatieveiligheid wordt geborgd door goede informatieverstrekking, actieve participatie en voorbeeldwerking			
Met alle relevante leveranciers en ketenpartijen zijn afspraken met betrekking tot informatiebeveiliging gemaakt en die worden gecontroleerd			
Er is een baseline voor informatiebeveiliging ingevoerd en de actualiteit en naleving van de maatregelen wordt geborgd			
Voor alle kritische processen en informatie- en ICT-systemen is een actuele risicoanalyse beschikbaar en de follow up ervan wordt geborgd			
Alle kritische componenten van de informatievoorziening worden gemonitord op potentieel schadelijke dreigingen			
De betrouwbaarheid van alle kritische componenten van de informatievoorziening wordt regelmatig getoetst			
Alle incidenten met betrekking tot de informatievoorziening worden adequaat gemeld, geregistreerd en gerapporteerd			
De organisatie en processen voor de informatiebeveiliging worden regelmatig geaudit door ervaren auditors			

4 Verbeterpad informatiebeveiliging

Als van de organisatie het ambitieniveau en het gemeten volwassenheidsniveau aanzienlijk verschillen dan is het in één stap verbeteren van de informatiebeveiliging tot het beoogde niveau veel gevraagd. Het is dan realistischer om stapsgewijs te verbeteren. Een voorstel voor stapsgewijze verbetering van een niveau lager dan 2.7 naar een niveau 4.0 is hieronder gegeven. Het volwassenheidsniveau van de informatiebeveiliging gaat hierin vanuit het uitgangsniveau via niveau 2.7 naar een niveau van 3.7. Daarna kan dan gewerkt worden aan verdere groei tot 4.0.

Eerste stap

Te bereiken volwassenheid: 2.7
Doelen:

- Informatiebeveiligingsorganisatie inrichten.
- Basismaatregelen treffen.
- Toetsing organiseren.

Activiteiten:

- De directie stelt zelf informatiebeveiligingsfunctionarissen (waaronder een CISO) aan met voldoende expertise, goed beschreven mandaat en rapportage aan de directie.
- De directie laat door de informatiebeveiligingsfunctionarissen een beleid voor informatiebeveiliging (inclusief procesautomatisering) opstellen en communiceert hier goed over.
- De directie laat door de informatiebeveiligingsfunctionarissen het eigenaarschap van processen en systemen vastleggen en maakt hierover managementafspraken met de eigenaren.
- De directie laat door de informatiebeveiligingsfunctionarissen een effectieve incidentenregistratie inrichten (inclusief kwartaalrapportage – dashboard – voor directie).
- De directie laat de informatiebeveiligingsfunctionarissen regelmatige (bijvoorbeeld 2x/jaar) penetratietesten en fotorondes organiseren om kwetsbaarheden op te sporen.
- De directie regelt zelf jaarlijkse interne audits door een ervaren auditor (niet zijnde een eigen informatiebeveiligingsfunctionaris).
- De directie laat een paragraaf over informatiebeveiliging in de jaarrapportage opnemen.
- De informatiebeveiligingsfunctionarissen stellen een lijst met urgente maatregelen op en coordineren de implementatie hiervan.
- De informatiebeveiligingsfunctionarissen leggen relevante ervaringen en good practices op een goed toegankelijke wijze vast.

Tweede stap

Te bereiken volwassenheid: 3.7
Doelen:

- Invoeren baseline (op basis van de relevante standaard baseline en risicoanalyse op organisatieniveau).
- Verbeteren van awareness t.a.v. informatiebeveiliging.
- Integratie van risicoanalyses, calamiteitenmaatregelen en managementafspraken.

Activiteiten:

- De informatiebeveiligingsfunctionarissen coördineren de implementatie van een baseline voor informatiebeveiliging, inclusief beheer van de maatregelen en borging van de naleving.
- De informatiebeveiligingsfunctionarissen verbeteren de awareness ten aanzien van informatiebeveiliging door goede informatieverstrekking, actieve participatie en voorbeeldwerking.
- De informatiebeveiligingsfunctionarissen regelen met de eigenaren dat afspraken worden gemaakt met alle relevante externe partijen m.b.t. informatiebeveiliging (inclusief controle).
- Voor ieder kritisch proces en systeem wordt in opdracht van de eigenaar een integrale risicoanalyse uitgevoerd en de benodigde maatregelen getroffen.
- Het onderwerp ICT-calamiteit wordt meegenomen in de calamiteitenplan en de calamiteitenorganisatie en er wordt ook met ICT-calamiteiten geoefend.
- De directie regelt jaarlijkse externe audits van de gehele informatiebeveiliging.

Verdere groei

Voor het behalen van volwassenheid 4.0 is nodig dat tevens de volgende zaken worden geregeld:

- Volledige integratie van informatiebeveiliging in de planning&control-cyclus.
- Effectieve communicatie van directie en management over geaccepteerde risico's.
- De directie geeft opdracht voor en autoriseert risico- en gap-analyses voor bedrijfskritische informatiesystemen.

Bijlage A: Interviewvragen

Onderstaande vragen worden gebruikt bij de interviews van functionarissen uit de organisatie waarvoor het volwassenheidsniveau van informatiebeveiliging wordt bepaald.

De vragen zijn open vragen. Bij voorkeur worden de interviews afgenomen door een ter zake deskundige interviewer. Voor verscheidene vragen is het nodig om door te vragen om zeker te stellen dat de vraag goed is begrepen en voldoende genuanceerd is beantwoord.

Om kleuring door meningen en vooringenomenheid zoveel mogelijk te voorkomen heeft het de voorkeur om interviews uit te voeren met verschillende functionarissen, namelijk:

- iemand uit het managementteam;
- iemand die de beveiliging van de procesautomatisering goed kent (indien van toepassing);
- iemand die de beveiliging van de administratieve automatisering goed kent;
- iemand die niet werkzaam is in een ICT- of beveiligingsfunctie.

De organisatie

1. In welke branche/sector valt uw organisatie?
2. Hoeveel medewerkers heeft uw organisatie?
3. Over hoeveel locaties/vestigingen is de organisatie verdeeld?
4. Hoeveel medewerkers werken op de locatie/vestiging waar u werkt?
5. Heeft uw organisatie ICT(-diensten) uitbesteed?
   Zo ja, welke ICT(-diensten) betreft het?
6. Heeft uw organisatie één of meer functionarissen voor informatiebeveiliging?
   Zo ja, hoeveel (in fte) voor administratieve automatisering en hoeveel voor procesautomatisering?
   Maakt één van deze functionarissen deel uit van directie/managementteam?
   Zo nee, rapporteert één van deze functionarissen direct aan directie/managementteam?

Uw functie

7. Welke functie bekleedt u in uw organisatie?
8. Bent u lid van directie/managementteam?
   Zo nee, rapporteert u direct aan directie/managementteam?
9. In welke mate bent u betrokken bij informatiebeveiliging in uw organisatie?

De ICT

10. Gebruikt uw organisatie ICT voor het aansturen of monitoren van een maatschappelijk vitaal proces?
11. Gebruikt uw organisatie ICT voor een intern bedrijfskritisch proces?
12. Gebruikt uw organisatie ICT voor procesautomatisering (ICS- of SCADA-systemen)?
    Zo ja, waarvoor worden deze systemen gebruikt en wat is het belang ervan?
    Worden systemen voor procesautomatisering op afstand gemonitord en/of bestuurd?

Zijn de netwerken voor administratieve automatisering en procesautomatisering fysiek en/of logisch van elkaar gescheiden?
Hoe wordt ongeautoriseerde toegang door derden voorkomen?
Welke andere maatregelen zijn getroffen om de procesautomatisering te beveiligen?

13. Is op uw ICT en informatievoorziening specifieke wet- of regelgeving van toepassing?
Zo ja, welke?

Volwassenheid informatiebeveiliging

14. Heeft uw organisatie de ambities met betrekking tot informatiebeveiliging geformuleerd en vastgesteld?
Zo ja, hoe wordt dit bij de medewerkers onder de aandacht gebracht?
En hoe worden de ambities vertaald in werkafspraken over informatiebeveiliging?
Wordt hier ook de procesautomatisering (scada-systemen) bij betrokken?
15. Worden ervaringen en good practices voor informatiebeveiliging vastgelegd?
Zo ja, waar en hoe?
16. Waar ligt in uw organisatie de verantwoordelijkheid voor informatieveiligheid?
Geldt dit voor zowel administratieve automatisering als procesautomatisering?
17. Weten de verantwoordelijken voor informatiebeveiliging van elkaar wie waarvoor verantwoordelijk is?
Zo ja, hoe is dat geregeld?
En als één van deze mensen tijdelijk is uitgeschakeld, worden diens taken dan overgenomen?
18. Zijn de leden van directie/managementteam goed op de hoogte van het belang van informatiebeveiliging en de risico's die de organisatie op het gebied van de informatievoorziening loopt?
Geldt dit ook voor de procesautomatisering?
19. Staat het onderwerp informatiebeveiliging wel eens op de agenda van directie/managementteamoverleg?
Zo ja, hoe vaak?
20. Heeft de organisatie een calamiteitenplan/continuïteitsplan (voor de primaire processen)?
Zo ja, hoe volledig en actueel is het, hoe vaak worden er calamiteitenoefeningen gedaan en in hoeverre dekt het plan ICT- en scada-calamiteiten?
21. Geven leden van directie/managementteam het goede voorbeeld met betrekking tot het opvolgen van informatiebeveiligingsmaatregelen?
22. Maakt uw organisatie gebruik van een gecontroleerd basisniveau van informatiebeveiliging?
Zo ja, is dit gebaseerd op een externe standaard/baseline (bijv. ISO 27002, BIR, BIG, BIWA) en geldt deze ook voor de procesautomatisering?
En in welke mate is deze geïmplementeerd?
23. Worden regelmatig penetratietests en social engineering tests uitgevoerd?
24. Wordt regelmatig een self-assessment uitgevoerd op het geïmplementeerde niveau van informatiebeveiliging (door een IT-auditor en niet alleen door een accountant)?
25. Op welke wijze worden medewerkers bewust gemaakt van het belang van informatiebeveiliging en de van hun gevraagde inzet?
Betreft dat de administratieve automatisering, de procesautomatisering, of beide?
26. Met welke frequentie worden wachtwoorden gewijzigd in de administratieve automatisering en de procesautomatisering?
27. Is voor elk (kritisch) proces en informatiesysteem bekend wie de 'eigenaar' ervan is?
Geldt dit ook voor de procesautomatisering?
28. Maakt informatiebeveiliging deel uit van de planning & control cyclus?
Zo ja, waar blijkt dat uit?

29. Wordt aandacht besteed aan informatiebeveiliging in alle fasen van de levenscyclus van componenten, waaronder onderhoud en vernietiging?
30. In hoeverre worden medewerkers betrokken bij het selecteren en implementeren van beveiligingsbeleid en beveiligingsmaatregelen?
31. Maakt uw organisatie gebruik van een standaard op het gebied van risicomanagement of governance (bijv. Cobit, COSO, ISO 27001, ISO 27005)?
    Zo ja, welke is/zijn dit en in welke mate is/zijn deze geïmplementeerd?
    Is er sprake van een Information Security Management System?
32. Worden de kritische componenten van de automatisering gemonitord om beveiligingsincidenten te signaleren?
33. Als een medewerker een beveiligingsincident constateert, moet deze dan gemeld worden?
    Zo ja, aan wie?
    Geldt dit ook voor minder veilige of verdachte omstandigheden op de werkvloer?
34. Worden beveiligingsincidenten aan directie/managementteam gerapporteerd?
    Zo ja, om welke incidenten gaat het en hoe wordt hierover gerapporteerd?
35. Worden risicoanalyses uitgevoerd voor de kritische informatiesystemen?
    Zo ja, gebeurt dit ook voor niet-kritische informatiesystemen?
    En voor de procesautomatisering?
    Hoe vaak worden deze analyses geactualiseerd?
    Wordt er na een risicoanalyse een gap-analyse uitgevoerd en bijgehouden?
36. Wie autoriseert de risico-/gap-analyses voor bedrijfskritische informatiesystemen?
37. Worden de geaccepteerde restrisico's naar de medewerkers gecommuniceerd?
38. Zijn er afspraken over informatiebeveiliging gemaakt met ketenpartijen en leveranciers?
    Zo ja, omvat dit ook de leveranciers voor procesautomatisering?
    En hoe worden de afspraken geborgd en wie is daarvoor verantwoordelijk?
39. Heeft uw organisatie een informatiebeveiligingsplan?
    Zo ja, wanneer is dat voor het laatst geactualiseerd?
    Omvat het ook de procesautomatisering?
    Wie is verantwoordelijk voor de uitvoering en de controle van de in het plan gedefinieerde activiteiten?
40. Wanneer is de laatste risicoanalyse voor een bedrijfskritisch informatiesysteem uitgevoerd?
    Om welk systeem ging het?
41. Wordt (een deel van) de ICT van uw organisatie regelmatig (bijv. jaarlijks) geaudit en/of getest?
    Zo ja, gebeurt dit door, of in opdracht van, een externe toezichthouder?
    In hoeverre zijn de aanbevelingen hieruit geïmplementeerd?
    Is de toetsing ten behoeve van een certificatie gedaan (bijv. ISO 27001)?
    Maakt de procesautomatisering deel uit van de audit?
    Wanneer heeft de laatste IT-audit plaatsgevonden?
    Wanneer heeft de laatste penetratietest plaatsgevonden op de administratieve automatisering?
    En op de procesautomatisering?

Bijlage B: Analyseschema

In onderstaand schema is aangegeven hoe de antwoorden op de vragen uit de vragenlijst in bijlage A input geven aan het bepalen van volwassenheidsniveaus. Per volwassenheidsfactor is aangegeven van welke vragen de antwoorden worden gebruikt.

Per volwassenheidsfactor staat bij ieder niveau welke uitspraak uit de interviews meetelt voor het betreffende niveau en bij welke vraag deze uitspraak gegeven zou moeten zijn. Als alle vermelde uitspraken bij een niveau genoemd zijn, dan wordt het betreffende niveau gehaald. Op dezelfde wijze wordt bepaald of ook het daaropvolgende niveau wordt gehaald. Etc.

Voor het eerste niveau dat niet geheel wordt gehaald, kan nog een deel van een niveau worden gehaald. Dit deelniveau is de som van de waarden die tussen haakjes achter de uitspraken staan die in de interviews gedaan zijn.

Als een niveau deels gehaald is dan tellen uitspraken die zijn vermeld bij hogere niveaus niet mee.

Factor s_1

De mate waarin de goede activiteiten voor informatiebeveiliging worden uitgevoerd.

Input zijn de antwoorden op vraag (zie bijlage A): 12, 14, 16, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32, 33, 34, 35, 37, 38, 41.

Niveau 1: De meeste informatiebeveiligingsmaatregelen ontbreken
er is informatie (1.0)

Niveau 2: Maatregelen voor informatiebeveiliging zijn op ad hoc basis getroffen
12, 22: de meest gebruikelijke informatiebeveiligingsmaatregelen zijn getroffen (1.0)

Niveau 3: Er is een gecontroleerd basisniveau voor informatiebeveiliging
14: er is een actueel informatiebeveiligingsbeleid opgesteld en dat omvat proces- en andere automatisering (0.05)
14: het informatiebeveiligingsbeleid wordt effectief uitgedragen en in werkafspraken verwerkt (0.1)
16: beveiliging van proces- en andere automatisering zijn op elkaar afgestemd (0.1)
20: er is een ICT-calamiteitenplan/continuïteitsplan en dat wordt geoefend (0.05)
21: de directie geeft zichtbaar het goede voorbeeld met betrekking tot informatiebeveiliging (0.05)
22: er is een baseline voor informatiebeveiliging geïmplementeerd (0.2)
23: af en toe worden penetratietests uitgevoerd (0.1)
23: af en toe worden social engineering tests uitgevoerd (0.05)
24: af en toe worden self-assessments uitgevoerd door een IT-auditor (0.05)
25: medewerkers worden bewust gemaakt van het nut van informatiebeveiliging (0.1)
27: elk proces/systeem (zowel proces- als andere automatisering) heeft een gedocumenteerde eigenaar (0.1)

38: afspraken over informatiebeveiliging met externe beheerders en leveranciers (0.05)

Niveau 4: Risicoanalyse wordt ingezet om te bepalen in hoeverre extra informatiebeveiliging nodig is
23: regelmatig worden penetratietests uitgevoerd (0.1)
23: regelmatig worden social engineering tests uitgevoerd (0.1)
24: regelmatig worden self-assessments uitgevoerd door een IT-auditor (0.1)
27: alle proces-/systeemeigenaren geven invulling aan hun eigenaarschap (0.3)
35: op alle kritische informatiesystemen worden risico- en gap-analyses uitgevoerd (0.3)
37: de geaccepteerde restrisico's worden gecommuniceerd (0.1)

Niveau 5: Er is een gecontroleerd managementsysteem voor informatiebeveiliging (ISMS)
28: informatiebeveiliging maakt deel uit van de planning & control cyclus (0.2)
29: er is aandacht voor informatiebeveiliging in alle fasen van de levenscyclus van componenten (0.05)
30: medewerkers participeren bij het specificeren en implementeren van informatiebeveiliging (0.1)
31: er wordt een standaard voor risicomanagement of governance gebruikt (0.1)
32: alle netwerken worden gemonitord op informatiebeveiligingsincidenten (0.1)
33: alle beveiligingsincidenten worden aangemeld en geregistreerd (0.2)
34: beveiligingsincidenten worden aan de directie gerapporteerd (0.05)
41: er wordt regelmatig een IT-audit op de informatiebeveiliging uitgevoerd door een externe IT-auditor (0.2)

Factor s_2

De mate waarin de betreffende activiteiten goed worden uitgevoerd.

Input zijn de antwoorden op vraag (zie bijlage A): 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 28, 33, 39.

Niveau 1: Er wordt niets afgestemd over informatiebeveiliging
er is informatie (1.0)

Niveau 2: Ervaringen en good practices voor informatiebeveiliging worden vastgelegd en toegepast
15: ervaringen en good practices voor informatiebeveiliging worden vastgelegd (0.3)
17: de verantwoordelijken voor informatiebeveiliging weten van elkaar wie waarvoor verantwoordelijk is (0.4)
17: als een informatiebeveiliger tijdelijk is uitgeschakeld dan worden diens taken overgenomen (0.3)

Niveau 3: Standaarden en procedures voor informatiebeveiliging worden (gecontroleerd) toegepast
14: het informatiebeveiligingsbeleid wordt effectief uitgedragen en in werkafspraken verwerkt (0.2)
20: er is een vastgesteld ICT-calamiteitenplan/continuïteitsplan en dat wordt geoefend (0.2)
22: de getroffen beveiligingsmaatregelen zijn gecontroleerd geïmplementeerd (0.4)
39: er is een actueel informatiebeveiligingsplan dat zowel proces- als andere automatisering omvat (0.2)

Niveau 4: De kwaliteit van de informatiebeveiligingsactiviteiten wordt gemeten en zo nodig bijgestuurd

23: af en toe worden penetratietests uitgevoerd (0.2)
23: af en toe worden social engineering tests uitgevoerd (0.1)
24: af en toe worden self-assessments uitgevoerd door een IT-auditor (0.3)
33: alle beveiligingsincidenten worden aangemeld en geregistreerd (0.4)

Niveau 5: De informatiebeveiligingsactiviteiten worden afgestemd op de behoefte van de organisatie

13, 18, 19: de directie kent het belang van informatiebeveiliging, weet welke regelgeving daarvoor van toepassing is en agendeert het onderwerp geregeld (0.2)
23: regelmatig worden penetratietests uitgevoerd (0.2)
23: regelmatig worden social engineering tests uitgevoerd (0.1)
24: regelmatig worden self-assessments uitgevoerd door een IT-auditor (0.3)
28: informatiebeveiliging maakt deel uit van de planning & control cyclus (0.2)

Factor s_3

De mate waarin uitvoering en aansturing van deze activiteiten goed zijn belegd.

Input zijn de antwoorden op vraag (zie bijlage A): 6, 13, 14, 16, 18, 19, 27, 28, 34, 35, 36, 38.

Niveau 1: Niemand is verantwoordelijk voor informatiebeveiliging

er is informatie (1.0)

Niveau 2: Informatiebeveiliging is een stafaangelegenheid

6: er zijn één of meer functionarissen aangewezen voor informatiebeveiliging van de procesautomatisering (0.2)
6: er zijn één of meer functionarissen aangewezen voor informatiebeveiliging van de andere automatisering (0.2)
16: de belangrijkste taken voor informatiebeveiliging zijn expliciet belegd (0.6)

Niveau 3: Informatiebeveiliging is een lijnmanagementaangelegenheid

27: elk proces/systeem (zowel proces- als andere automatisering) heeft een gedocumenteerde eigenaar (0.2)
35: de eigenaren geven opdracht voor assessments en (risico)analyses voor hun (informatie)systemen (0.4)
35: de eigenaren bewaken de implementatie van de benodigde maatregelen (0.4)

Niveau 4: Informatiebeveiliging is een topmanagementaangelegenheid en is opgenomen in de planning & control cyclus

14: het informatiebeveiligingsbeleid wordt effectief uitgedragen en in werkafspraken verwerkt (0.2)
13, 18, 19: de directie kent het belang van informatiebeveiliging, weet welke regelgeving daarvoor van toepassing is en agendeert het onderwerp geregeld (0.1)
28: informatiebeveiliging maakt deel uit van de planning & control cyclus (0.3)
34: beveiligingsincidenten worden aan de directie gerapporteerd (0.2)
36: de directie autoriseert risico-/gap-analyses voor bedrijfskritische informatiesystemen (0.2)

Niveau 5: Organisaties werken samen om informatiebeveiliging gezamenlijk aan te pakken als onderdeel van de dagelijkse bedrijfsvoering

38: er zijn vergaande gecontroleerde afspraken over informatiebeveiliging gemaakt met ketenpartijen/leveranciers (1.0)

Volwassenheid informatiebeveiliging

De volwassenheid van informatiebeveiliging, $M_{IB} = \frac{s_1 \times 3 + s_2 \times 2 + s_3 \times 2}{3 + 2 + 2}$.