Herman de Bruine is docent Integrale Veiligheidskunde en onderzoeker Cybersecurity aan de Haagse Hogeschool. Herman is bereikbaar via h.debruine@hhs.nl. Fabio Lucero Garau is student Integrale Veiligheidskunde aan de Haagse Hogeschool. Fabio is bereikbaar via f.j.lucerogarau@student.hhs.nl. Marcel Spruit is lector Cyber Security & Safety aan de Haagse Hogeschool. Marcel is bereikbaar via m.e.m.spruit@hhs.nl.

Een praktisch volwassenheidsmodel voor informatiebeveiliging

Recente incidenten met ransomware tonen aan dat veel organisaties hun informatiebeveiliging nog niet op orde hebben. Informatiebeveiliging op orde brengen vraagt naast technische middelen ook om beleid en informatiebeveiligingsbewustzijn bij medewerkers. Deze combinatie betekent dat het een illusie is te denken dat organisaties van de ene op de andere dag hun informatiebeveiliging op orde kunnen hebben. Er is behoefte aan een model waarlangs organisaties stappen kunnen zetten om hun informatiebeveiliging op orde te brengen.

In dit stuk wordt een praktisch volwassenheidsmodel voor informatiebeveiliging gepresenteerd, mede gebaseerd op het Capability Maturity Model en ISO 27001. Dit volwassenheidsmodel helpt de stand van zaken rond informatiebeveiliging in beeld te brengen en geeft aanwijzingen wat de prioriteiten van een organisatie zouden moeten zijn om de informatiebeveiliging te verbeteren.

In 2017 kwamen meerdere wereldwijde ransomware-aanvallen in het nieuws. Daardoor werden honderdduizenden organisaties getroffen, waaronder veel grote organisaties (1). Ransomware gijzelt computersystemen en als er niet betaald wordt, gaan bestanden verloren. Opvallend is dat vaak het niet up-to-date zijn van software de mogelijkheid gaf voor de verspreiding van en schade door de ransomware. Aanvallen als deze tonen de noodzaak voor organisaties om te zorgen dat zij hun informatiebeveiliging op orde hebben. Onder informatiebeveiliging worden in dit stuk niet alleen de technische beveiligingsvoorzieningen in ICT-systemen verstaan, maar ook de fysieke beveiligingsvoorzieningen (bijvoorbeeld toegangsbeheersing tot ruimtes) en organisatorische beveiligingsvoorzieningen (bijvoorbeeld protocollen voor het omgaan met vertrouwelijke informatie). Hierbij volgen we de definitie en indeling als in van Houten et al (2015) (2).

Door de toenemende invloed van ICT op onze samenleving wordt de rol van informatiebeveiliging steeds belangrijker voor publieke en private organisaties, maar betekent dit dat organisaties voldoende maatregelen nemen op het gebied van informatiebeveiliging? Uit rapporten van onder meer het Rathenau Instituut (3), de Rekenkamer Rotterdam (4) en het ministerie van J&V (5) blijkt dat er nog voldoende te verbeteren valt op het gebied van informatiebeveiliging. De weerbaarheid van organisaties is nog niet in alle sectoren op orde. Ook de (Rijks)overheid voldoet op het gebied van de informatiebeveiliging niet altijd aan haar eigen standaarden (3).

Volwassenheidsniveaus

In kwaliteitsmanagement is gebleken dat organisaties niet in één stap naar optimale kwaliteit gaan, maar dat dit een groeiproces is waarin een aantal fasen te onderscheiden is. Een voorbeeld hiervan wordt beschreven in het INK-model (6). Ook binnen de informatievoorziening zijn groeimodellen ontwikkeld. Zo is er voor softwareontwikkeling het Capability Maturity Model (CMM) (7). Zowel INK als CMM gaan uit van fasen in de ontwikkeling van organisaties, waarbij vastgesteld wordt op welk niveau een organisatie zich bevindt, om daarna daarbij passende ontwikkelacties te kunnen ondernemen. In CMM worden

deze fasen volwassenheidsniveaus genoemd en wij zullen deze term ook hanteren.

Het ligt voor de hand om de CMM-benadering te volgen, maar CMM kenmerkt zich door een grote hoeveelheid vragen en is tegelijkertijd beperkt tot alleen het beoordelen van de werkwijze binnen de organisatie. CMM is gericht op het 'hoe' en niet zozeer het 'wat' en 'wie'. Daarnaast geldt dat CMM gericht is op softwareontwikkeling, niet op informatiebeveiliging en veiligheidsbewustzijn. De doelstelling was om te komen tot een volwassenheidsmodel voor informatiebeveiliging waarmee organisaties zelfstandig het niveau van hun informatiebeveiliging kunnen vaststellen (zelfevaluatie) en op basis hiervan verbeterpunten hiervoor formuleren.

Het volwassenheidsmodel voor informatiebeveiliging is in de loop van 2016 en 2017 ontworpen en verbeterd. Toetsing van de eerste versie is in december 2016 en januari 2017 uitgevoerd met behulp van 25 derdejaars hbo-studenten van de opleiding Integrale Veiligheidskunde (8) die minimaal 32 uur per week in dienst zijn van een organisatie. Aan de studenten is gevraagd de informatiebeveiliging van hun eigen organisatie, met behulp van de eerste versie van het model, te beoordelen.

Opbouw van het volwassenheidsmodel

Het volwassenheidsmodel bestaat uit twee componenten. De aandachtsgebieden en de volwassenheidsniveaus. Als eerste worden de aandachtsgebieden behandeld.

Aandachtsgebieden

De aandachtsgebieden zijn ontleend aan ISO-normering voor managementsystemen. Daarbij is gekozen voor de zogenaamde ISO High Level Structure die de gemeenschappelijke basis is waarop de verschillende normen van ISO zijn gebouwd, zoals 9001 voor kwaliteitssystemen, 27001 voor informatiebeveiliging en 14001 voor milieu.

In ISO 27001 zijn de volgende aandachtsgebieden benoemd (9):

a. **Context van de organisatie:** het in kaart brengen van belanghebbenden, welke eisen zij stellen, en welke raakvlakken en afhankelijkheden er zijn.
b. **Leiderschap:** het tonen van leiderschap en betrokkenheid door het opstellen en communiceren van informatiebeveiligingsbeleid en het verdelen van rollen, verantwoordelijkheden en bevoegdheden om dit beleid ook te kunnen uitvoeren.
c. **Planning:** het in kaart brengen en beoordelen van risico's en kansen op het gebied van informatiebeveiliging, op basis hiervan maatregelen nemen en de voortgang van de uitvoering ervan bewaken.
d. **Ondersteuning:** het beschikbaar stellen van middelen, competenties van medewerkers benoemen en medewerkers hiervoor toerusten, werken aan bewustzijn van de medewerkers, communiceren over informatiebeveiliging en het onderhouden van gedocumenteerde informatie erover.
e. **Uitvoering:** op operationeel niveau uitvoeren van informatiebeveiliging door het uitvoeren van risicobeoordeling en het implementeren van maatregelen.
f. **Evaluatie van prestaties:** het evalueren van de prestaties (ook door audits) op het gebied van informatiebeveiliging, vastlegging daarvan en een actieve rol van het management daarbij.
g. **Verbetering:** omgaan met afwijkingen en het nemen van corrigerende maatregelen.

Vanuit deze zeven aandachtsgebieden zijn voor het volwassenheidsmodel de volgende negen aandachtsgebieden gedefinieerd:

1. **Beleid en risico's (10):** de mate van bekendheid en begrip van informatiebeveiligingsbeleid bij medewerkers en de afstemming hierover met partners.
2. **Maatregelen:** de mate waarin er een complete set van maatregelen is ingevoerd, liefst in de vorm van een Information Security Management System.
3. **Protocollen/regelgeving:** de mate waarin rond informatiebeveiliging risico's up-to-date zijn en protocollen of regels aanwezig zijn.
4. **Bekendheid met beleid, risico's en dreigingen:** de bekendheid hierover bij medewerkers en de bekendheid en afstemming erover met partners.
5. **Rol staf/lijn/directie:** de mate waarin het management informatiebeveiliging als eigen verantwoordelijkheid ziet.
6. **Toerusting van medewerkers:** de mate waarin medewerkers zijn toegerust rond informatiebeveiliging en informatiebeveiligingsbewustzijn wordt bevorderd.
7. **Processen:** de mate waarin bij procesanalyse aandacht besteed wordt aan informatiebeveiligingsrisico's en -maatregelen.
8. **Procesmanagement:** de mate waarin bij procesmanagement aandacht besteed wordt aan informatiebeveiliging.
9. **Meten en evalueren:** de mate waarin binnen de besturing van organisatie (bijvoorbeeld via de Planning & Control-cyclus) aandacht is voor informatiebeveiliging.

In tabel 1 is aangegeven hoe de ISO-aandachtsgebieden terugkomen in de aandachtsgebieden van ons model.

Aandachtsgebied model	Aandachtsgebieden ISO (zie pagina 5)
1.Beleid en risico's	a. Context van de organisatie: het in kaart brengen van belanghebbenden, welke eisen zij stellen, en welke raakvlakken en afhankelijkheden er zijn. c. Planning: het in kaart brengen en beoordelen van risico's en kansen op het gebied van informatiebeveiliging.
2. Maatregelen	c. Planning: op basis van risico's en kansen maatregelen nemen en de voortgang van de uitvoering ervan bewaken. d. Ondersteuning: het beschikbaar stellen van middelen, communiceren over informatiebeveiliging.
3. Protocollen/ regelgeving	d. Ondersteuning: het onderhouden van gedocumenteerde informatie.
4. Bekendheid met beleid, risico's en dreigingen	b. Leiderschap: het tonen van leiderschap en betrokkenheid, door het opstellen en communiceren van informatiebeveiligingsbeleid.
5. Rol staf/ lijn/ directie	b. Leiderschap: het verdelen van rollen, verantwoordelijkheden en bevoegdheden om dit beleid ook te kunnen uitvoeren.
6.Toerusting van medewerkers	d. Ondersteuning: competenties van medewerkers benoemen en medewerkers hiervoor toerusten en werken aan bewustzijn van de medewerkers.
7. Processen	e. Uitvoering: op operationeel niveau uitvoeren van informatiebeveiliging door het uitvoeren van risicobeoordeling en het implementeren van maatregelen op procesniveau.
8. Procesmanagement	e. Uitvoering: bewaken implementatie van maatregelen op procesniveau.
9. Meten en evalueren	f. Evaluatie van prestaties: het evalueren van de prestaties (ook door audits) op het gebied van informatiebeveiliging, vastlegging daarvan en een actieve rol van management daarbij. g. Verbetering: omgaan met afwijkingen en het nemen van corrigerende maatregelen.

Tabel 1 – Aandachtsgebieden ISO.

In de tabel is goed te zien dat in de eerste aandachtsgebieden (1. beleid tot en met 5. rolverdeling) afgeweken is van de volgorde in ISO. De reden hiervoor is dat het model ontworpen is om de praktijk van informatiebeveiliging op de werkvloer zichtbaar te maken. Dit betekent dat gefocust wordt op wat de kennis en ervaring van medewerkers is met informatiebeveiliging binnen hun organisatie. Eerst wordt gevraagd naar de inhoud van het beleid en maatregelen, daarna naar de bekendheid van het beleid, de rol van management en staf bij de uitvoering van informatiebeveiligingsbeleid en de toerusting van medewerkers. Volgend onderdeel is de uitvoering van het beleid op procesniveau waarbij onderscheid wordt gemaakt tussen de inhoud (risicobeoordeling en maatregelen) en de wijze van sturing bij het implementeren van maatregelen. Tenslotte is er aandacht voor het meten en evalueren en de wijze waarop dit verankerd is in de Planning & Control-cyclus binnen de organisatie.

Volwassenheidsniveaus

Er zijn vijf volwassenheidsniveaus onderscheiden in de omgang met informatiebeveiliging: Onbewust, Reactief, Systemen in ontwikkeling, Systemen op orde en systemen die zowel geïnternaliseerd zijn alsook op partners afgestemd. De inspiratie hiervoor komt uit verschillende bronnen: het CMM-model van Carnegie Mellon (Paulk et al 1993), het maturitymodel van Crosby (1979) (11) en het INK-managementmodel (12).

In CMM en Crosby wordt niet verwezen naar de samenwerking met externe partners, bij het INK-model is dit wel het geval (13). Er is ervoor gekozen in het vijfde niveau ook de externe partners mee te nemen, omdat veel organisaties in hun informatievoorziening interactie hebben met partners, waardoor afstemming van informatievoorziening en informatiebeveiliging met partners een noodzaak is geworden (14).

Volwassenheidsniveau	Omschrijving*
1. Onbewust	Aandacht voor IB als er een (groot) incident is geweest. Er is geen IB-beleid.
2. Reactief	Aandacht voor IB vooral na incidenten. Er is IB-beleid gemaakt n.a.v. incidenten en er zijn maatregelen genomen om herhaling te voorkomen.
3. Systemen in ontwikkeling	Er is proactief IB-beleid (naast incidenten zijn ook bedreigingen meegenomen). Dit wordt nog niet door iedereen op dezelfde wijze gehanteerd.
4. Systemen op orde	Er is proactief IB-beleid, uniform gehanteerd binnen de organisatie. Er is sturing op IB in de Planning & Control-cyclus.
5. Geïnternaliseerd en op partners afgestemd	IB-beleid wordt door medewerkers naar de geest gehanteerd en doorlopend verbeterd. Het IB-beleid is afgestemd met partners.

**IB = informatiebeveiliging*

Tabel 2 – Volwassenheidsniveaus.

Figuur 1 – Volwassenheidsmodel.

Hanteren van het volwassenheidsmodel

In het hanteren van de volwassenheidsniveaus geldt dat ze cumulatief zijn: elk volgend niveau behoudt de goede elementen van het niveau ervoor en voegt daar extra elementen aan toe. Bij elk van de aandachtsgebieden zijn stellingen geformuleerd die het volwassenheidsniveau voor dit aandachtsgebied illustreren (zie figuur 1).

Als voorbeeld de regel in het model rond protocollen/regelgeving:

- **Onbewust:** men werkt inzake informatiebeveiliging volgens de gedachte: 'zo doen we het hier nu eenmaal'.
- **Reactief:** voor sommige kritische informatiebeveiligingsrisico's zijn er protocollen of regels. Na incidenten worden protocollen of regels op- of bijgesteld.
- **Systemen in ontwikkeling:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels, controle op naleving nog vooral na incidenten.
- **Systemen op orde:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels. Deze worden bij-

gesteld als er iets niet goed blijkt te zijn of ze niet worden nageleefd.
- **Geïnternaliseerd:** voor alle relevante informatiebeveiligingsrisico's zijn protocollen of regels. Deze worden periodiek doorgelicht of ze nog passend/effectief zijn.

Om het volwassenheidsniveau (15) te bepalen in het geval van de protocollen/regelgeving wordt gekeken naar het bestaan van protocollen (zijn er protocollen, dan niveau 2), de dekking (volledig dekkend, dan niveau 3), de actualiteit (dan niveau 4) en ten slotte of ze proactief worden doorgelicht en met partners besproken (dan niveau 5).

Het is de bedoeling dat per score door de beoordelaar een feitelijke onderbouwing wordt geleverd waarom het betreffende niveau gescoord is. Bijvoorbeeld bij niveau 2: het benoemen van de bestaande protocollen en het aangeven waar nog behoefte aan is. Voor niveau 3 geldt dat aangegeven wordt hoe de naleving van de protocollen gecontroleerd wordt, enzovoort.

Van elk van de aandachtsgebieden kan zo het niveau worden bepaald. De niveaus kunnen per aandachtsgebied verschillen. Dit levert een profiel van de scores op de aandachtsgebieden.
Het uitgangspunt van het volwassenheidsmodel is dat de organisatie zo sterk is als de zwakste schakel. Het overall volwassenheidsniveau wordt daarmee de laagste score van de aandachtsgebieden. Dit maakt het prioriteren van de benodigde verbeteringen die uit de diagnose komen relatief eenvoudig: verbeter het zwakste aandachtsgebied. Mochten alle aandachtsgebieden zich op hetzelfde volwassenheidsniveau bevinden dan impliceert het model een volgorde van 1 (beleid) naar 9 (evaluatie) conform de PDCA- of Deming-cirkel. Als er onvolledigheid in het beleid is, dan dient dat als eerste te worden weggenomen. Daarna de concrete uitwerking in maatregelen, de voorlichting en toerusting. Vervolgens de uitwerking op uitvoeringsniveau en tenslotte de meting en evaluatie ervan.

Uitkomsten van de test van het volwassenheidsmodel

Zoals beschreven is het model getest door studenten van de opleiding Integrale Veiligheidskunde. Hen is gevraagd de scores te bepalen voor de organisatie waarin zij werken en deze scores toe te lichten. De rapportages van 30 studenten zijn beoordeeld door de onderzoekers. Zij hebben hen van commentaar/nadere vragen voorzien, met het verzoek de rapportages hierop aan te passen. De vragen betroffen vooral de concrete onderbouwing van de score. Uiteindelijk

	sector	beleid	maatregelen	protocollen	bekendheid risico's	rol staf / lijn	toerusting mdw	processen	processmgt	meten en evalueren	niveau	prioriteit
1	Overheid	4	2	3	3	5	2	2	4	3	2	maatregelen
2	Overheid	2	3	3	1	4	1	2	2	2	1	bekendheid
3	Overheid	4	3	5	2	5	3	5	4	2	2	bekendheid
4	Overheid	4	3	3	5	4	3	3	5	1	1	evalueren
5	Overheid	5	3	4	4	4	4	4	4	5	3	maatregelen
6	Overheid	2	2	2	2	4	1	2	2	4	1	toerusting
7	Overheid Vitaal	5	3	3	5	4	2	4	5	4	2	toerusting
8	Overheid Vitaal	3	2	2	4	4	2	3	2	2	2	maatregelen
9	Overheid Vitaal	2	2	2	2	3	1	1	3	1	1	toerusting
10	Profit	3	4	2	3	3	1	1	1	1	1	toerusting
11	Profit dienstverlening	2	2	2	2	5	1	2	2	1	1	toerusting
12	Profit dienstverlening	2	2	4	3	2	1	2	1	1	1	toerusting
13	Profit dienstverlening	2	2	2	2	3	1	2	2	1	1	toerusting
14	Profit dienstverlening	5	2	1	2	3	1	1	2	1	1	protocollen
15	Profit Industrie	2	2	3	3	3	2	3	2	1	1	evalueren
16	Profit Infrastructuur	2	2	2	2	4	1	1	2	1	1	toerusting
17	Profit offshore	2	2	2	2	3	2	1	2	1	1	processen
18	Profit productie	1	3	1	3	4	1	1	2	1	1	beleid
19	Verzekering	2	3	1	2	3	1	2	1	1	1	protocollen
20	Zorg	1	2	2	1	2	1	2	1	1	1	beleid
21	Zorg	2	2	2	2	3	2	1	2	1	1	processen

Figuur 2 - Een overzicht van de scores van verschillende organisaties op het maturitymodel.

zijn na aanvulling 21 uitwerkingen ontvangen, die van voldoende kwaliteit waren. Een tweetal studenten gaf aan dat het informatiebeveiligingsbeleid van hun organisatie (dat ze in termen van volwassenheidsniveau zelf inschatten op niveau 4) niet toestond dat ze de rapportage van concrete voorbeelden konden voorzien; deze uitwerkingen zijn niet meegenomen in deze rapportage.

De beelden van de organisaties zijn zeer uiteenlopend. Overall valt op dat er nog weinig organisaties op volwassenheidsniveau 3 (systemen in ontwikkeling) of hoger zitten. Er zijn een aantal organisaties die op zich relatief hoog zouden kunnen scoren, maar één element ontbreekt (zoals organisaties 4 en 7). Er zijn ook organisaties die nog helemaal aan het begin staan (organisaties 18 en 20).

Conclusies

In dit stuk is een praktisch volwassenheidsmodel gepresenteerd voor informatiebeveiliging op basis van de aandachtspunten uit de ISO High Level Structure en de volwassenheidsniveaus uit CMM en het INK-model. Een conceptversie is uitgetest door studenten Integrale Veiligheidskunde. Met een beperkte ondersteuning was het model goed door hen te hanteren. De ondersteuning bestond vooral uit het 'doorvragen' op aspecten en het verhelderen van wat onder een baseline informatiebeveiliging wordt verstaan. Op basis van deze ervaringen lijkt het

De uitkomsten geven een negatief beeld van de volwassenheid

dat binnen een organisatie een inhoudelijk deskundige (security officer, CISO, of een andere medewerker die zich bezighoudt met informatiebeveiliging) met behulp van het volwassenheidsmodel relatief snel kan vaststellen wat het niveau van de informatiebeveiliging in de organisatie is. Hiervoor hoeven ze geen uitgebreide opleiding te krijgen omdat hun eigen inhoudelijke kennis volstaat. Wel dient de uitvoerder bij voorkeur enige ervaring met auditen te hebben (16); hierbij kan overigens aangesloten worden op auditortrainingen die rond (kwaliteits)managementsystemen gebruikelijk zijn. Uit de resultaten van het model kan snel duidelijk worden op welk vlak de verbeterpunten voor de organisatie liggen met betrekking tot de informatiebeveiliging en in welke volgorde deze het best opgepakt kunnen worden.

De uitkomsten van werken met het model geven een negatief beeld van de volwassenheid op het gebied van informatiebeveiliging van de organisaties die zijn beoordeeld. Dit beeld was consistent met de indruk die de studenten over hun organisatie hadden. Het beeld was wellicht enigszins positiever geweest als er over de twee niet meegenomen organisaties, waarvan het volwassenheidsniveau door de betrokken studenten rond 4 werd ingeschat, gedetailleerder informatie beschikbaar was geweest. Hier staat echter tegenover dat bij informatiebeveiliging transparantie een belangrijke waarde is, waaraan deze organisaties niet voldoen.

Referenties

(1) http://www.nu.nl/internet/4692084/aantal-slachtoffers-ransomware-wannacry-loopt-200000.html

(2) P. van Houten, M. Spruit & K. Wolters (2015). Informatiebeveiliging onder controle. Amsterdam, Pearson

(3) G. Munnichs, M. Kouw & L. Kool (2017). Een nooit gelopen race – over cyberdreigingen en versterking van weerbaarheid. Den Haag, Rathenau Instituut

(4) Rekenkamer Rotterdam (2017). In Onveilige Handen. Rotterdam, Rekenkamer Rotterdam.

(5) Cybersecuritybeeld Nederland CSBN 2017 (2017). Den Haag, NCTV

(6) Zie bijvoorbeeld: Hadjono en Hes (1993). De Nederlandse kwaliteitsprijs en onderscheiding, Deventer, Kluwer

(7) Zie bijvoorbeeld: M. Paulk, C. Mark, C. Weber, B. Curtis, M. Chrissis (1993). Capability Maturity Model for Software, Version 1.1. Technical Report. Pittsburgh, Software Engineering Institute, Carnegie Mellon University en zie J. Herbsleb, D. Zubrow, D. Goldenson, W. Hayes & M. Paulk (1997). Software Quality and the Capability Maturity Model. Communications of the ACM 40(6), 30-40

(8) Als onderdeel van het vak Cybersecurity

(9) NEN-ISO/IEC 27001 (nl), Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

(10) Onder risico's worden ook de termen dreigingen, assets en kwetsbaarheden meegenomen (termen die gebruikelijk zijn binnen het security-veld)

(11) P. Crosby (1979). Quality is Free. New York, McGraw Hill

(12) R. Emmerik (2012). Kwaliteitsmanagement, tweede editie. Amsterdam, Pearson.

(13) De volwassenheidsniveau lijken het meest op de dimensies van het INK-model, waarbij t.o.v. het INK-model een 'nul'-niveau is ingevoerd

(14) World Economic Forum (2012). Partnering for Cyber Resilience - Risk and Responsibility in a Hyperconnected World - Principles and Guidelines. Geneve, World Economic Forum

(15) Het model is ontwikkeld om te kijken naar een hele organisatie, maar kan ook op afdelingsniveau worden gehanteerd. Bij het organisatieniveau geldt dat de beveiliging zo sterk is als de zwakste schakel, de score wordt dan bepaald door de 'zwakste' afdeling (met een belangrijke rol rond het beveiligen van informatie). Wel kunnen de punten die moeten worden opgepakt dan verschillen van afdeling tot afdeling

(16) Met name de diepgang en concreetheid van de voorbeelden ter onderbouwing van de bepaling van het volwassenheidsniveau is cruciaal