MARK TISSINK

voorwoord door Lourens Visser, CIO Rijksoverheid

GRIP OP INFORMATIE BEVEILIGING

groei in leiderschap

het handboek voor beginnende informatiebeveiligers

Testimonials

"Een belangrijk Nederlands cybersecurity boek wat geschreven moest worden. Het is overzichtelijk, praktisch, meer dan actueel en eigenlijk verplichte kost voor iedere manager of ondernemer. Persoonlijk vind ik hoofdstuk 13 goed om hier nog even te benoemen. We hebben namelijk allemaal een eigen sociaal maatschappelijke verantwoordelijkheid niet de zwakste cyberschakel in de keten te worden. Lezen en aan de slag dus om onze digitale samenleving samen veilig te houden!"

Dimitri van Zantvliet, CISO Nederlandse Spoorwegen

"Informatiebeveiliging is niet uitsluitend een ICT-uitdaging, maar vooral een business-uitdaging. Informatiemanagement, het beleggen van eigenaarschap en het inzichtelijk maken van risico's zijn daarbij cruciaal. Mark snapt dat en legt dat haarfijn uit in zijn boek."

Hugo Leisink, senior adviseur bij het Nationaal Cyber Security Centrum

"Met dit boek worden alle onderwerpen die belangrijk zijn om de ICT veilig en betrouwbaar te houden op een plezierige en laagdrempelige wijze beschreven. Ook een mooi naslagwerk voor degene die alles al denken te weten over dit onderwerp."

Sophie Roozen, Executive director Internal Audit, Van Lanschot Kempen

"Met Grip op informatiebeveiliging brengt Mark een survivalgids voor het oerwoud zoals ik informatiebeveiliging ken. Het boek bereidt je gedegen voor en biedt helder richting zodat je met vertrouwen de reis aangaat.
Een complete beschrijving van alle aspecten die relevant zijn voor informatiebeveiliging en het beheer hiervan. Knap hoe Mark deze complexe en veelomvattende materie toegankelijk en uitnodigend beschrijft.
Een must read, niet alleen voor managers maar ook voor meer technisch georiënteerde IT-ers; zodat zij met wederzijds begrip de informatiebeveiliing binnen hun bedrijf kunnen verbeteren."

Jasper Rappard, Consultant Cyber Security & Application Performance bij Legian

"Zeer duidelijk en toegankelijk geschreven handleiding / introductie in informatiebeveiliging voor bestuurders. Junior informatiebeveiligers zullen dit zeker kunnen gebruiken als leidraad / naslagwerk."

Ralf Siebelt, Freelance Information Security Professional

"EINDELIJK een boek over informatiebeveiliging dat even toegankelijk als compleet is. Prachtig gepresenteerd middels een routekaart op een duidelijke en pragmatische manier. Een soepele mix van informatiebeveiliging, risicomanagement én leiderschap besprenkeld met praktijkvoorbeelden maakt het boek bijzonder boeiend"

Maike van Zutphen, Compliance/Privacy – Risk Officer & eigenaar, Rechtvaardig Advies

"Een vers perspectief welke informatiebeveiliging in de juiste bredere context plaatst - zonder je te vertellen wat je wel of niet móet doen.
Mark neemt je mee door de gangpaden van jouw organisatie en helpt je jouw eigen paradigma te verschuiven. Met praktische handvatten, begrijpelijke taal en zonder wollig te worden, kan dit boek iets op jouw salontafel toevoegen zelfs als je (nog) geen IB-professional bent."

Albert Groen, Adviseur Informatiebeveiliging, Dienst Justitiële Inrichtingen

"Na het lezen van het eerste hoofdstuk begrijp je direct wat informatiebeveiliging is en waar de verantwoordelijkheden en relaties binnen de organisatie liggen. Hierdoor helpt het boek mij, in de rol van Functionaris Gegevensbescherming, om het groter geheel te zien en de juiste vragen te kunnen stellen binnen de organisatie en als sparringpartner van de CISO te fungeren. Het boek leest lekker weg in begrijpelijk taal. Een aanrader voor niet- security specialisten, verantwoordelijke managers en andere geïnteresseerden"

Annuska van den Eijnden, Functionaris Gegevensbescherming Gemeente Waalre, Privacy Consultant Parell Groep B.V.

"Een verhelderende en vernieuwende kijk op het in de vingers (en grip) krijgen van informatiebeveiliging. Voor de beginnende IB'er een mooie routekaart, voor de doorgewinterde CISO een goed naslagwerk."

Jacques Eding, CISO, Openbaar Ministerie

"Ken je die dikke boeken over IT en IT-beveiliging? Van die CISA- of CISSP-trainingsboeken bijvoorbeeld? Dik, cryptisch en vol jargon.
Dat is dit boek juist niet! Mark heeft in zijn boek op een leuke en energieke manier een verhaal geschreven van de belangrijkste componenten op het gebied van informatiebeveiliging en hoe je in een organisatie hier praktisch mee kan omgaan."

Anske Jongsma, Senior IT Auditor bij Achmea

Grip op informatiebeveiliging
Groei in leiderschap

ISBN: 9789083152905
ISBN: 9789083152912 (eBook)
NUR: 800, 980

Eerste druk
1 oktober 2021

Auteur
Mark Tissink

Uitgever
MTiss Publish

Drukkerij
Real Concepts

Ontwerp
Eva Tissink

Portret auteur
Phina Kemper

Inhoudsopgave

Inleiding van het boek

Informatiebeveiliging is geen moeten. Dat is het nooit.
Het is wel continu het maken van de juiste keuzes.
Wat 'de juiste keuzes' dan ook precies zijn.

Informatiebeveiliging op orde krijgen is helemaal niet moeilijk. Als er maar voldoende aandacht, in de vorm van tijd en geld, aan gegeven wordt. Als het maar belangrijk genoeg gevonden wordt op de juiste niveaus in de organisatie. Om informatiebeveiliging goed uit te kunnen voeren zijn twee belangrijke ingrediënten nodig:

- Kennis
- Leiderschap

Dit boek biedt beide. Dit is het basishandboek voor de beginnende informatiebeveiliger voor wat betreft de kennis. Daarnaast wordt door de verschillende paragrafen heen elke lezer aangemoedigd om op de juiste momenten en op de juiste manier leiderschap te tonen.
En als het leiderschap op dit onderwerp aanwezig is, dan zal de verdere organisatorische, procesmatige en technische invulling haast als vanzelf volgen. Natuurlijk, het zal nog een flinke kluif zijn, maar het achterstallige onderhoud op dat thema zal ingelopen worden.

Wat maakt dit boek anders?
Afgelopen jaren heb ik vele bedrijven mogen helpen met hun informatiebeveiliging en heb ik meerdere trainingen verzorgd op dit gebied. Dit was van een beginnend niveau tot gevorderd, en elke keer viel het mij weer op, dat er altijd vanaf een ingezoomde positie wordt begonnen. Los van de organisatie, doelen en missie.
Vaak wordt er gestart met het kijken naar een applicatie of website.
En dan wordt de bril van de hacker opgezet om te kijken wat daarmee mis kan zijn. Hiermee komt informatiebeveiliging steevast als een te technisch en teveel op de IT-afdeling gefocust onderwerp in het gedimde licht te staan. En natuurlijk in de schijnwerpers wanneer het dan eindelijk een keer fout is gegaan. Die arme IT-manager kon er niets aan doen dat het onderwerp informatiebeveiliging niet in zijn geheel 'even' geïmplementeerd was in het gehele bedrijf.

Mijn doel met dit boek is een basishandleiding neer te zetten die nou eens niet vol staat met jargon, IT-techniek en andere specialistenpraat. Dit boek is ook niet compleet toegeschreven op een certificering voor persoon of bedrijf. Dit is gewoon een boek met een uiteenzetting die te begrijpen is. Die lekker wegleest. Waar je gemakkelijk doorheen komt én nog wat van leert. Dit boek beschrijft alle stappen om te komen tot grip op informatiebeveiliging, maar zonder leiderschap gaat dit niet werken.

Wat is de opbouw van het boek?
Het boek is opgedeeld in drie secties – input, verwerking, output – en deze secties zijn voorzien van een intro en outro. Binnen de secties zijn er dertien hoofdstukken. Elk hoofdstuk is op dezelfde manier opgebouwd. Na een introductie en de theorie volgt er een praktische aanpak. De hoofdstukken eindigen met praktijkvoorbeelden, praktische opdrachten en een conclusie.

Er zijn veel lijsten en overzichten in het boek opgenomen, wat ervoor zorgt dat je snel grip krijgt op informatiebeveiliging. In het boek verwijs ik in bijna elk hoofdstuk wel een aantal keer naar de 'boekbijlage pagina'. Deze is online te vinden op:

https://secure-it-is.nl/boek/bijlage

Hierop staan links naar gebruikte werkbladen, aanvullende cursussen of handige websites. Neem eens een kijkje wanneer het boek ernaar verwijst, en sla deze pagina op in je favorieten.

Hoe is dit boek te gebruiken?
Lees dit boek vooral niet van voor naar achter als je dat niet wilt. Ondanks dat het opgedeeld is in 3 duidelijke secties – input, verwerking, output – wil dat niet zeggen dat je ook bij de input moet beginnen. Weet je bijvoorbeeld al voldoende van informatiebeveiliging? Sla hoofdstuk 1 dan over en ga verder naar 2. Ben je nog niet klaar voor de inhoud en meer benieuwd naar het proces, dan begin je bij hoofdstuk 8. Of begin je graag met het einddoel in zicht, lees dan hoofdstuk 12 of 13 en werk vanaf daar terug.

Tot slot, waar ik spreek over ‘jouw organisatie’ bedoel ik de organisatie waar jij eigenaar van bent óf in dienst bent. Beide kunnen. Ik sta als coach/adviseur naast jou. Ik neem jou mee op het gebied van strategische en tactische informatiebeveiliging, om zo te komen tot een kwalitatieve, en daarmee beheerste, bedrijfsvoering.
Het is een vakgebied waar ook veel Engels wordt gebruikt. Deze termen heb ik waar dat relevant is in haakjes achter het Nederlandse woord gezet, of andersom.

En altijd geldt, kom je er bij een stap om welke reden dan ook niet helemaal uit. Laat het mij weten! Stuur mij een mail op info@marktissink.nl of plan op https://secure-it-is.nl/koffiebabbel een afspraak in en laten we volledig vrijblijvend bespreken waar jullie staan en waar ik eventueel mee kan helpen. Dit kan advies, coaching, training of een workshop zijn.

DEEL 1

INPUT

“To begin... BEGIN!”

William Wordworth

Begin bij het begin. Dat is vaak een goed advies. We kunnen informatiebeveiliging als organisatie of bedrijf lang genoeg uitstellen. Zo belangrijk is het nou toch ook weer niet. We komen er wel mee weg. We zijn te klein, ze pakken ons toch niet. Toch?
En die 'ze' kan dan natuurlijk duiden op toezichthouders. Of natuurlijk de criminelen, je weet wel, hackers.

Voordat we beginnen met het 'échte informatiebeveiligen' is het van belang dat we weten waar het over gaat. Dat we weten, waar we mee te maken hebben. En dat we het doel voor ogen krijgen.
Je bent tenslotte niet voor niets begonnen aan dit boek. Wil je gewoon nieuwe kennis opdoen over informatiebeveiliging? Of loopt de organisatie niet als een geoliede machine. Het hobbelt, kraakt en stoort. En daar heb je last van. Het kan natuurlijk ook nog zo zijn dat jij de taak hebt gekregen dit op te lossen voor jouw directie.

GEHEIM 1:

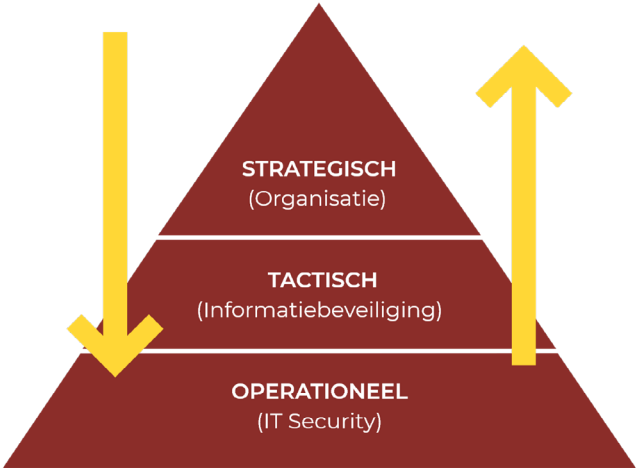
Informatiebeveiliging begint met tone at the top…
…maak de bestuurder (eind)verantwoordelijk.

Als het aan de bovenkant van de organisatie niet belangrijk gevonden gaat worden, dan gaat het niet werken.

Kortom, tijd om kennis te maken met mijn vakgebied!

Strategisch	De bedrijfsbrede organisatie
Tactisch	Informatiebeveiliging
Operationeel	IT Security

Deze moeten van boven naar beneden en van beneden naar boven op elkaar aansluiten. Op zo'n manier dat er één deugdelijke, kwalitatieve bedrijfsvoering ontstaat.



Gezien het geheel van informatiebeveiliging 'op orde te krijgen' een giga-opgave kan zijn bouwen we het langzaamaan op. Zoals altijd, begin bij het begin. En dat begint in het eerste hoofdstuk met kennis en met (vak)jargon. Zodat je mee kunt praten met de specialisten.
Om vervolgens in het hoofdstuk erna vast te stellen wat het doel is in onze organisatie met betrekking tot informatiebeveiliging.

De hoofdstukken drie tot zeven zijn vervolgens logisch opgebouwd aan de hand van het model wat in het eerste hoofdstuk wordt uitgelegd.

Als we de inventarisatie compleet hebben – dat is het doel van dit eerste deel – dan kunnen we door naar het 2e deel van dit boek. Daar gaan we al deze inzichten op een stelselmatige manier verder verwerken.

Alvast een mededeling: het is geen rechtlijnig proces.
Ook als je straks in het tweede of derde deel van dit boek bent, zul je merken dat je nog regelmatig naar dit belangrijke eerste deel gaat teruggrijpen.

1 SCOPE

WAAR HEBBEN WE HET OVER?

"Education can change the scope of the entire organization"

vrije vertaling van Nitin Nohria

Het lijkt zo flauw. Beginnen we het boek eindelijk, het eerste hoofdstuk, en dan hebben we het gelijk over 'de scope'. Maar dat is eigenlijk heel gangbaar. De scope beschrijft wat er wel bij hoort en ook vooral wat niet? Wanneer we bezig zijn met het vaststellen van verantwoordelijkheden is dit ontzettend belangrijk. Bij elke informatiebeveiligingsanalyse – of het creëren van een overzicht – gaat het in dit vak altijd over de scope. Dus lijkt het mij niet meer dan logisch om datzelfde te doen bij de start van dit boek en dit hoofdstuk.

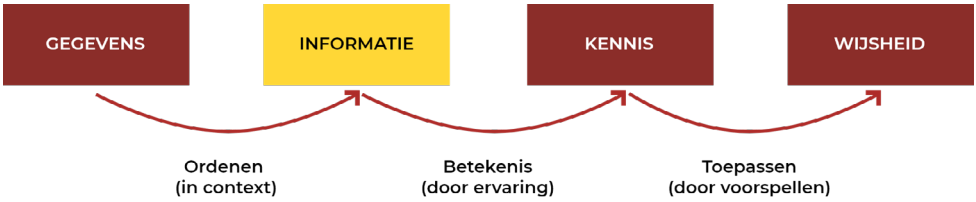
We gaan het dus hebben over informatiebeveiliging. Dit hoort wat mij betreft echt bij de basis bedrijfsvoering. Dit zou verweven moeten zijn in het DNA, in de kern, van de organisatie. Precies zoals je verwacht dat een directeur zorgt dat het bedrijf de kant op gaat die gewenst is. Die aansluit bij de visie. Sturen, controleren en beheersen. En dan zijn er drie belangrijke basisprincipes:

1) zorgen dat er geld verdiend wordt; en
2) zorgen dat het geld niet te hard wegstroomt; en
3) zorgen dat de kwaliteit van het product of de dienst op het gewenste niveau blijft.

In deze driehoek heeft informatiebeveiliging een groot aandeel als onderdeel van kwaliteitszorg.

1.1 Wat is informatiebeveiliging?

Informatiebeveiliging gaat over het beveiligen van informatie. De verzameling van gegevens (data) die in IT-systemen zijn opgeslagen moeten beschermd worden. Laten we daarbij de systemen van leveranciers waarop jouw bedrijfsdata staat, de laptops en andere apparaten, die medewerkers thuis hebben liggen ook niet vergeten. Tot slot gaat het ook over de afdrukken en dossiers die op de bureaus, in de archieven en in de werktassen liggen.
Op het moment dat de mens met deze gegevens in aanraking komt, bijvoorbeeld door een afdruk op papier of vertoning op een scherm, kan het door de ordening en context de stap gemaakt worden naar informatie.



Wanneer de mens hier vervolgens de betekenis en ervaring aan koppelt, kan de stap genomen worden naar kennis. Het voorspellen of toepassen van deze kennis kan leiden tot wijsheid.

Informatiebeveiliging gaat over de eerste twee: gegevens en informatie. In analyses zullen we altijd rekening moeten houden, wanneer deze informatie bij anderen terecht komt en wat zij ermee kunnen met hun kennis en wijsheid.

Informatiebeveiliging gaat over het toekennen van een waarde aan de verzamelingen van informatie. Om te zorgen dat het de juiste bescherming krijgt, passend bij die toegevoegde waarde. Niet te veel, want dat is te duur. Niet te weinig, want dan is het onvoldoende beschermd.

Hiervoor hebben we 3 kernkwaliteiten die we aan informatie koppelen, afgekort tot BIV.

3 KERNKWALITEITEN (BIV)

B **Beschikbaarheid** (availability) –
Hoe beschikbaar (en toegankelijk) moet deze informatie zijn?
Hoe vervelend is het als deze informatie niet beschikbaar is?
Of anders gevraagd; Wat is de schade als informatie er niet is als deze wel op dat moment benodigd is?

I **Integriteit** (integrity) –
Wat verlangen we van deze informatie als het gaat over de Juistheid, Volledigheid en Tijdigheid (JVT) ervan?
Hoe vervelend is het als deze informatie onvolledig is, fouten bevat of niet op het juiste moment de kwaliteit heeft die je wilt?

Of anders gevraagd; Hoeveel fouten kan het proces overkomen zonder problemen?

V **Vertrouwelijkheid** (confidentiality) –
Hoe goed willen (of moeten?) we deze informatie afschermen van onbevoegden?
Hoe erg is het als de informatie in kwaadwillende handen komt?
Of anders gevraagd: Hoeveel schade heb je als organisatie wanneer de gevoelige informatie onvoldoende beschermd wordt?

Wanneer je dit in het Engels gebruikt dan hebben we het altijd over de CIA. Deze afkorting is echt dé basis voor informatie in relatie tot de informatiebeveiliging. Hier refereer ik continu naar.

Let op! wanneer je zowel de Nederlandse als de Engelse termen in de organisatie gebruikt. De letters staan namelijk in een andere volgorde. Dit kan spraakverwarring opleveren met als gevolg dat er bijvoorbeeld te veel aandacht uitgaat naar beschikbaarheid en daardoor de vertrouwelijkheid te kort schiet.

1.2 Wat is informatiebeveiliging niet?

Hier maak ik graag altijd eerst een duidelijk onderscheid tussen informatiebeveiliging en het meer technische IT-security. Dit boek gaat (met name) over het eerste.

Daar waar het bij informatiebeveiliging gaat over het op tactisch en strategisch niveau inrichten van beleid en processen om meer grip te krijgen op de kwaliteit van informatie, gaat het bij IT Security over wezenlijk andere processen.

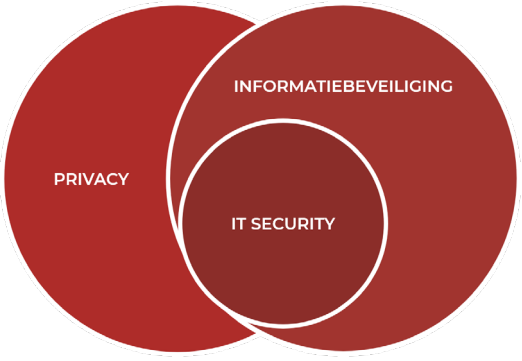
IT Security
De operationele inrichting van technische maatregelen. Het begint namelijk niet met kabels, software en andere techniek om digitale indringers buiten te houden. Natuurlijk, uiteindelijk gaat het ook over de ‘firewalls’, ‘intrusion-detection en -prevention systemen (IDS/IPS)’ en de ‘security incident event monitoring (SIEM)’. Maar dan als mogelijke resultaten van een organisatorische inrichting die goed op orde is en

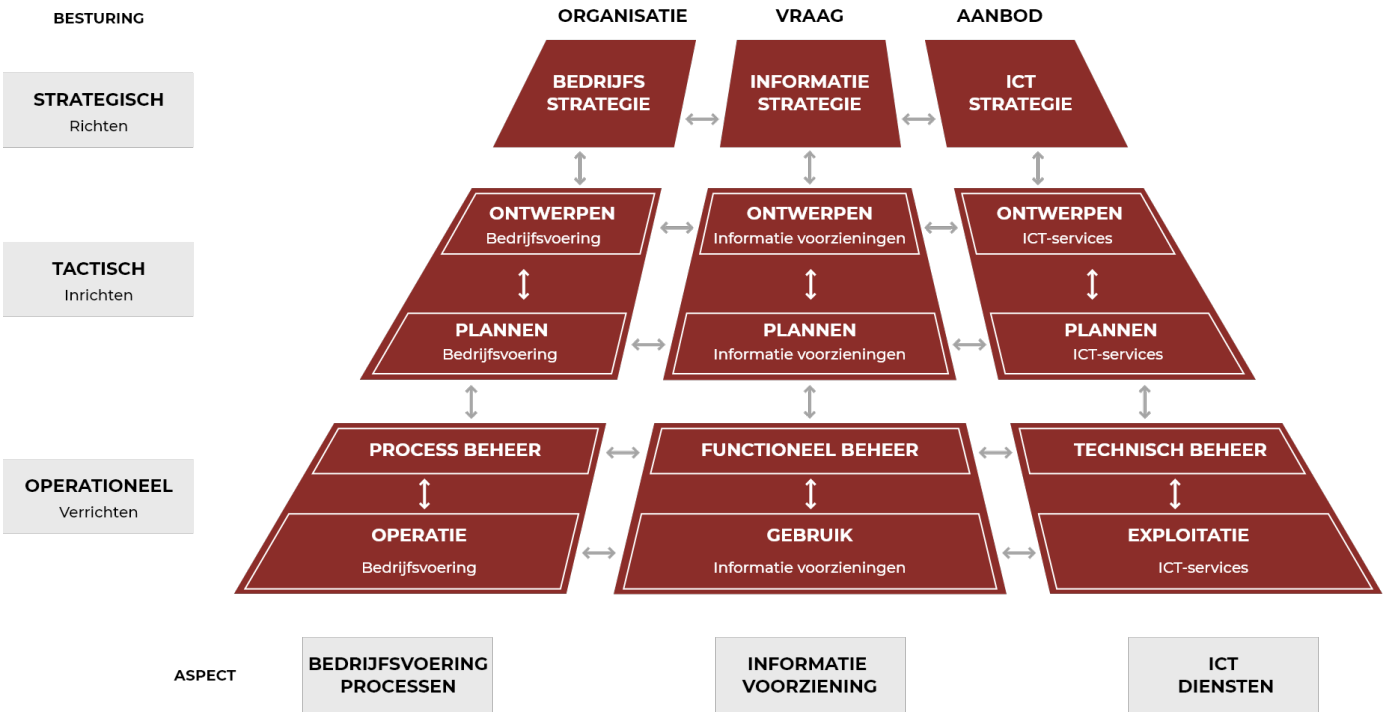
die gecombineerd is met een informatiebeveiligingsbeheersingsproces (dubbele woordwaarde).

Privacy

Ook even kort iets over privacy, of beter, persoonsgegevensbescherming. De GDPR (of, in het Nederlands, de AVG) waar je continu zoveel over hoort. Belangrijk... maar tevens ook een apart vakgebied. Er zit overlap in, maar ook zeker verschil. Het is gangbaar om informatiebeveiliging onder de IT-afdeling te plaatsen en privacy onder de afdeling Juridische Zaken. Over of deze plaatsing in de organisatie terecht is of niet kunnen specialisten ellenlange discussies voeren.
Het grote 'voordeel' wat privacy heeft ten opzichte van informatiebeveiliging is dat het een wet is. Met een toezichthouder en boetes. Hiervan is het geen keuze of je er wel of niet aan mee wilt doen. Voor informatiebeveiliging ligt dat iets genuanceerder.
Alhoewel, de GDPR/AVG vereist wel dat persoonsgegevens een 'passende beveiliging' verdienen. Ofwel, binnen de organisatie moeten we risicogebaseerd besluiten wat passend is.

Dus, informatiebeveiliging is geen privacy. Natuurlijk, ze versterken elkaar. Privacy heeft informatiebeveiliging hard nodig om de 'passende beveiligingsmaatregelen' goed toe te passen, maar het is wel degelijk een ander vakgebied. Wees je dus wel bewust dat het een ontzettend belangrijke eisensteller is. Hiermee bedoel ik dat eisen die de privacywet aan persoonsgegevens stelt, worden uitgewerkt in de informatiebeveiliging.




BESTURING
ORGANISATIE
VRAAG
AANBOD
STRATEGISCH
Richten
BEDRIJFS STRATEGIE
INFORMATIE STRATEGIE
ICT STRATEGIE
TACTISCH
Inrichten
ONTWERPEN
Bedrijfsvoering
ONTWERPEN
Informatie voorzieningen
ONTWERPEN
ICT-services
PLANNEN
Bedrijfsvoering
PLANNEN
Informatie voorzieningen
PLANNEN
ICT-services
OPERATIONEEL
Verrichten
PROCESS BEHEER
FUNCTIONEEL BEHEER
TECHNISCH BEHEER
OPERATIE
Bedrijfsvoering
GEBRUIK
Informatie voorzieningen
EXPLOITATIE
ICT-services
ASPECT
BEDRIJFSVOERING PROCESSEN
INFORMATIE VOORZIENING
ICT DIENSTEN

Informatiemanagement
Het is ook niet alleen informatiemanagement, waarbij er gezorgd wordt dat de juiste informatievraag vertaald wordt naar een oplossing in de informatievoorziening. Of dat het alleen een taak/zaak is voor de ICT-afdeling. Het begint altijd bij de (strategie van de) business. Zij bepalen de koers in de organisatie. Zij voeren de regie. Natuurlijk is het dan aan de vraag- en aanbodkant van belang dat de juiste tegenvragen gesteld worden. De IT-afdeling, of IT- of cloud-leverancier, is vervolgens degene die het moet gaan uitvoeren.
Dit boek gaat over alle negen vlakken[1], maar belangrijker, informatiebeveiliging beperkt zich niet tot één van deze negen.

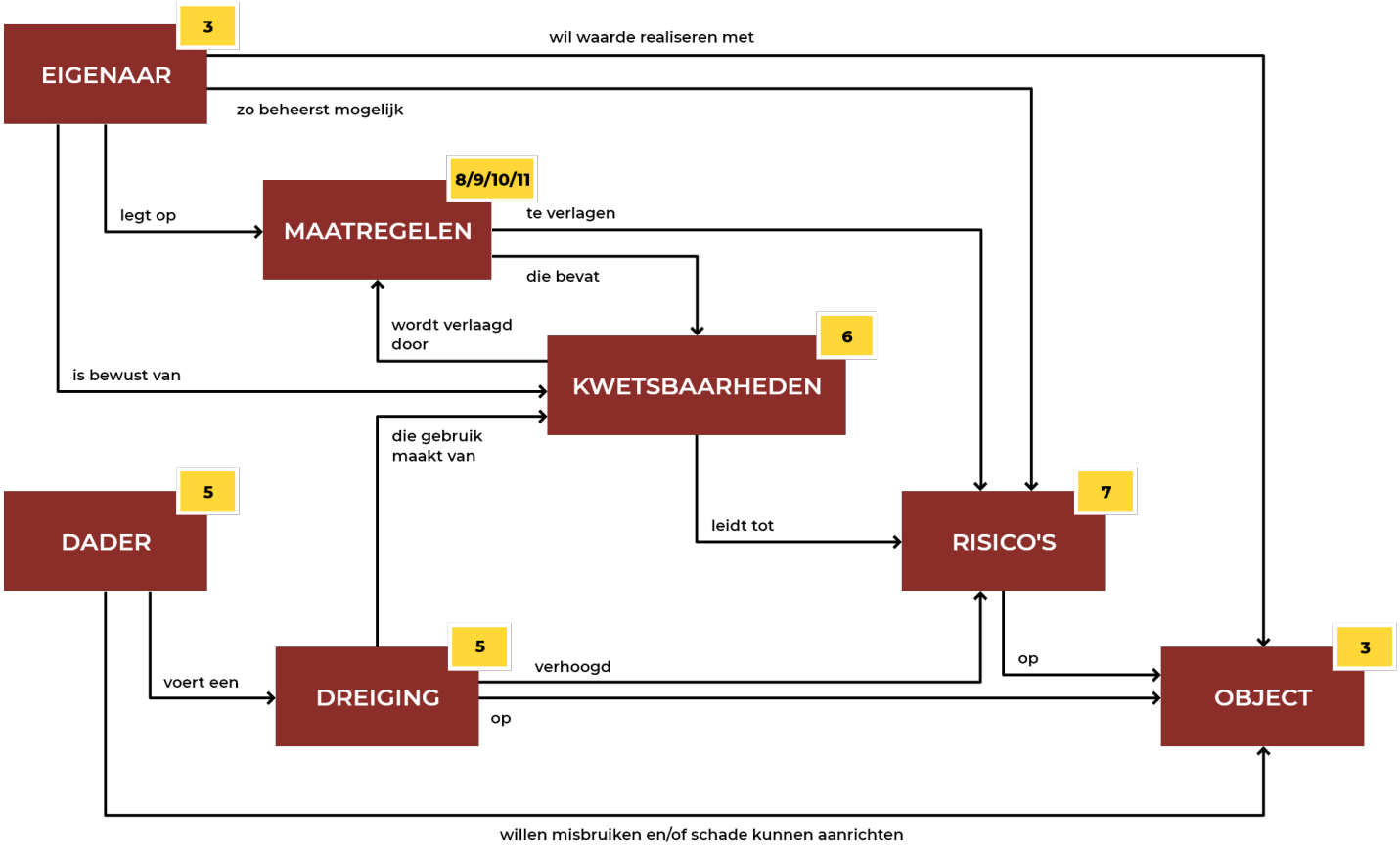
Architectuur

Het is ook geen architectuur. Hoewel een businessarchitectuur wel een belangrijk onderdeel kan zijn. Een goede architectuur kan helpen bij het op de juiste plaats implementeren van maatregelen. Informatie is dat wat door de organisatie stroomt middels (bedrijfs)processen.

1.3 Hoe hangt het vakgebied aan elkaar?

Voor mij als informatiebeveiliger is er op dit moment maar één model die het hele vakgebied op een juiste manier laat zien. Dat is het Security Model van Common Criteria. Dit model vormt dan ook de rode draad door dit hele boek. De elementen die dit vakgebied maken, staan namelijk niet los van elkaar, maar in samenhang. Wanneer we inzicht krijgen in één van de elementen geeft dit direct uitdagingen in de anderen. Het is van belang dat we op deze manier gaan kijken en de denkwijze volgen. Door deze samenhang te blijven zien, geeft het die belangrijke kwalitatieve beheersing in een organisatie waar we naar op zoek zijn.

Elk van deze termen heeft een apart hoofdstuk. Het gele vakje met cijfer verwijst naar het betreffende hoofdstuk. De onderwerpen worden kort toegelicht op de pagina daarna.


EIGENAAR
3
wil waarde realiseren met
zo beheerst mogelijk
legt op
MAATREGELEN
8/9/10/11
te verlagen
die bevat
wordt verlaagd door
KWETSBAARHEDEN
6
is bewust van
die gebruik maakt van
DADER
5
leidt tot
RISICO'S
7
voert een
DREIGING
5
verhoogd
op
op
OBJECT
3
willen misbruiken en/of schade kunnen aanrichten

Object (assets) –
Dat wat je bezit. Bij de boekhouding hebben ze het vaak over activa. Ook kun je de termen assets of bezittingen tegenkomen. Dit kan informatie zijn, maar ook apparatuur of software. En tot slot het meest waardevolle wat een organisatie bezit, de medewerkers. Alle objecten moeten we op de juiste manier beschermen.

Eigenaar (owner) –
Die ene persoon in de organisatie die moet beslissen wat er met deze informatie moet gebeuren. Of er meer of minder beveiliging op moet komen, uiteraard rekening houdend met de kosten.

Risico's (risk) –
Wat kan er misgaan met de informatie die we beschermen? Op welke manieren kan er tekortgeschoten worden in het naleven van de BIV? Wat is de kans dat dit gebeurt? Wat is de impact als dit gebeurt? Kortom: hoe groot is het risico?

Kwetsbaarheid (vulnerabilities) –
Waar zitten in onze organisatie de zwakheden bij objecten, producten of processen? Is het een technische, operationele of procedurele kwetsbaarheid?

Dreiging (threat) –
Wat is er in de buitenwereld aanwezig wat onze organisatie kan raken? Op welke manier kunnen deze gebruik maken van de kwetsbaarheden die er zijn? Hoe groot is deze dreiging?

Dader (threat agent/threat actor) –
Wie zou de dreiging uit te kunnen voeren? Wat zou het motief zijn, waarom zou een dader een dreiging bij een kwetsbaarheid willen gebruiken?

Maatregelen (countermeasures) –
Wat kunnen we eraan doen om te zorgen dat er minder risico/ kwetsbaarheid en/of dreiging is?

Vanuit dit model heb ik tevens een aantal belangrijke uitgangspunten uitgeschreven:

1. Elk object (bezit, asset) heeft een eigenaar
2. Elke dreiging heeft een dader
    2a. Dreigingen zijn er niet zonder dat iemand of iets – de dader – deze veroorzaakt
3. Een dreiging is op zoek naar kwetsbaarheden
4. Maatregelen neem je om het risico te verlagen
    4a. door kwetsbaarheden weg te nemen
    4b. door dreigingen weg te nemen
5. Elke maatregel introduceert nieuwe kwetsbaarheden/dreigingen/ risico's.

1.4 Praktische opdrachten

1.5 Conclusie

Als het goed is, heb je de kaders van informatiebeveiliging nu scherp en is de relatie tussen de verschillende hoofdstukken aangeduid. De grote rode draad is zichtbaar. Natuurlijk zoals het elke (vak)discipline goed betaamt, is er een hoop vakjargon aanwezig. De belangrijkste staan in dit hoofdstuk. Uiteraard zijn er meer en komen er ook steeds meer. Deze blijf ik continu aanvullen en toelichten in het boek.

De uitdaging voor jou is dat je continu vragen blijft stellen. Als er een term aangedragen wordt die je niet kent... vraag wat het betekent.

SECURE·IT·IS

SIMPLICITY | CREATIVITY | TRUST

KRIJG GRIP OP INFORMATIEBEVEILIGING, EN GROEI IN LEIDERSCHAP.

BESTEL HET GEHELE BOEK OP

SECURE-IT-IS.NL/BOEK

Informatiebeveiliging... leuker of simpeler wordt het niet!

Een toegankelijk boek voor elke directeur, manager of medewerker van een organisatie, die meer grip op informatiebeveiliging wil realiseren. Goed omgaan met de gevoelige informatie. Leiderschap tonen.

Hierna heb je minder last van:

1. Hack-gevolgen

Alle bestanden versleuteld middels ransomware
(Je wordt gechanteerd en mogelijk worden de klantgegevens online verhandeld)

2. Datalekken

Niet voldoen aan wetgeving, met kans op boetes
(en de gevolgen van imagoschade)

3. Gedoe met ICT

Niemand kan werken, omdat de website, applicatie of informatie alweer niet beschikbaar is
(en de oorzaak hiervan onduidelijk is)

4. Onnodige fouten

Waardoor gevoelige informatie op straat komt te liggen
(De medewerker die goedbedoeld de verkeerde dingen doet)

Dus pak dit boek aan, volg de praktische tips...

(of geef het cadeau aan de medewerker die dit samen met Mark Tissink mag oppakken)

... en Secure IT is!

Mark Tissink is auteur, trainer, coach & adviseur én expert op het gebied van informatiebeveiliging en risicobeheersing. Dit aangevuld met de softskills rondom (persoonlijk) leiderschap en communicatie.

Mark heeft het vermogen om de eerste stappen – die nodig zijn in een organisatie voor informatieveiligheid – uit te leggen op zo'n manier dat het begrijpelijk is voor elke medewerker in een organisatie.

https://marktissink.nl

9 789083 152905 >