GvIB Expertbrief – Maart 2005
ISSN 1872-4876, Jaargang 1 – Nr. 1

Functies en rollen in de informatiebeveiliging

Paul Overbeek

Bart Bokhorst

Dirk Brouwer

Ben Elsinga

Leo van Koppen

Renato Kuiper

Fred van Noord

De aanleiding voor deze expertbrief is de wildgroei aan functiebenamingen in de informatiebeveiliging en risicomanagement. Ook de samenhang tussen de functies onderling, en de relatie met functies in de rest van de organisatie is niet helder. Er zijn nog andere onbeantwoorde vragen. Zoals, zijn carrièrepaden uit te stippelen, en welke opleidingsbehoeften zijn er eigenlijk. Ook de aanbiedende kant zou gebaat zijn bij een beter beeld van de feitelijke opleidingsbehoeften in de markt.

http://www.gvib.nl/
✉ expertbrief@gvib.nl

2

OP WEG NAAR EENDUIDIGE FUNCTIES EN ROLLEN IN DE INFORMATIEBEVEILIGING

BaMa-structuur vraagt om herkenbare beveiliging

De aanleiding voor deze expertbrief is de wildgroei aan functiebenamingen in informatiebeveiliging en risicomanagement. Ook de samenhang tussen de functies onderling, en de relatie met functies in de rest van de organisatie is niet helder. Er zijn nog andere onbeantwoorde vragen. Zoals, zijn carrièrepaden uit te stippelen, en welke opleidingsbehoeften zijn er eigenlijk. Ook de aanbiedende kant zou gebaat zijn bij een beter beeld van de feitelijke opleidingsbehoeften in de markt.

In het ledenbestand van het GvIB zijn maar liefst 200 verschillende functieaanduidingen geïdentificeerd. Ook de certificeringen rijzen de pan uit. Min of meer bekend zijn: MSIT, CISSP, CISM, ISSMP, CISA, CIA. Hoe verhouden deze letterafkortingen zich tot bijvoorbeeld ing., drs., mr., RE of RA? Sommige ‘opleidingen’ bieden tegen betaling van 500 dollar een cursus die zorgt voor een mooie afkorting achter de naam. Hoe passen deze opleidingen bij carrièrepaden en functies? Welke kwaliteiten en vaardigheden passen überhaupt bij een functie?

Een team bestaande uit Dirk Brouwer (information security manager), Renato Kuiper (security architect), Bart Bokhorst (information security manager in het ontwerpproces), Fred van Noord (adviseur informatiebeveiliging en interim service manager), Leo van Koppen (docent), Ben Elsinga (facilitator in dit proces) en Paul Overbeek (als ghostwriter), heeft zich bovenstaande vragen gesteld. Het uiteindelijke doel is duidelijkheid te krijgen over de functienamen in informatiebeveiliging en risicomanagement en de competenties, taken, en verantwoordelijkheden die bij een functie horen. Hiermee wordt het ook mogelijk om de ontwikkeling van loopbaanpaden te stimuleren, en een ‘common body of knowledge’ te adopteren voor ontwikkeling van competenties, al dan niet binnen een opleiding.

ONDERZOEKSVRAGEN

De onderzoeksvragen die dit expertteam uiteindelijk wil beantwoorden zijn:

- ***Organisatieperspectief***: welke rollen/functies zijn er te onderscheiden op het gebied van informatiebeveiliging/risicomanagement, en welke namen krijgen deze rollen en functies. Het eindresultaat van deze onderzoeksvraag wordt een overzicht met functienamen, functie-eisen, overzichten met taken-verantwoordelijkheden-bevoegdheden (TVBs), persoonlijke competenties, kennis en vaardigheden. Wellicht kan een koppeling worden gemaakt tussen deze profielen en opleidingen en certificeringen.
- ***Individueel perspectief***: welke stadia van ontwikkeling kan een ‘informatiebeveiliger’ of ‘risicomanager’ doorlopen.
  Het eindresultaat van deze onderzoeksvraag is meer duidelijkheid over de ontwikkelingspaden die een professional kan doorlopen en de competenties die daarin bijdragen.

Het is niet de bedoeling dat deze onderzoeksvragen in één keer in het isolement van deze 'expertgroep' worden beantwoord. Van belang is om tot stellingname te komen en om discussiepunten te formuleren, die in de discussie met beroepsgenoten en andere belanghebbenden nader uitgewerkt worden en in een relatief korte doorlooptijd een breed gedragen beeld te verkrijgen.
De doelstelling is in een brede discussie via de website van het GvIB en in een forumdiscussie, in een relatief korte doorlooptijd tot een redelijk breed gedragen beeld te komen. Dit artikel is een fase in een proces, en hopelijk een "baken op het pad naar verdere volwassenheid van ons vakgebied."

ORGANISATIEPERSPECTIEF

Als vertrekpunt dient een risicomanagement proces. Voorbeelden zijn het information security management system (ISMS) zoals dat in de Code voor Informatiebeveiliging is beschreven of het risicomanagementproces van het COSO en COBIT-model. In een organisatie wordt veelal onderscheid gemaakt tussen het operationele, tactische en strategische niveau, en wordt onderscheid gemaakt in een MBO-, HBO- of universitair werk- en denkniveau, overigens niet persé een één op één relatie.

Vanuit het organisatieperspectief wordt onderscheid gemaakt naar gewone functies en verbijzonderde functies. Voor wat betreft de gewone functies worden gewone medewerkers en gewone managers onderscheiden, ieder met die competenties (kennis, vaardigheden en attitude) die álle medewerkers c.q. managers zouden moeten hebben, ongeacht hun positie in de organisatie.
Voor wat betreft de verbijzonderde functies wordt de wildgroei in aanduidingen als een hindernis ervaren. De werkgroep stelt voor een zo beperkt mogelijk aantal functies te hanteren. Over de functie 'information security manager' groeit consensus. Alle andere aanduidingen worden niet als zelfstandige specifieke functies gezien, maar eerder als rollen of specialisaties. Voorbeelden hiervan zijn de 'beveiligingsarchitect', de 'risico-analist', de 'autorisatiebeheerder' en de 'cryptograaf'. Wat opvalt, is dat het grote aantal functieaanduidingen niet leidt tot herkenning in de markt. De vele tientallen certificeringen helpen ook niet. De werkgroep roept hier op tot terughoudendheid.
Wat ook opvalt, is de verwarring tussen functies en rollen. Iemand kan in een functie, bijvoorbeeld 'senior beleidsmedewerker', prima verschillende rollen op beveiligingsgebied invullen, bijvoorbeeld risicoanalist en continuïteitscoördinator.

Dan zijn er nog de tijdelijke rollen. De werkgroep merkt op dat een aanduiding voor een fenomeen dat tijdelijk extra aandacht vraagt, snel wordt verward met een functie. Een evident voorbeeld hiervan is de 'anti-spam-medewerker'. Binnen korte tijd is deze 'functie' een normaal onderdeel van, bijvoorbeeld, de anti-virus-software beheer. Maar ook van een 'Beveiligingsarchitect' kan je je afvragen of dit daadwerkelijk een functie is, of dat de behoefte aan deze rol is ontstaan omdat binnen de natuurlijke positionering van de juiste rol de kennis ontbreekt. De stille wens hierbij is dat de natuurlijke functies op enig moment voldoende 'basiskennis' hebben om het beveiligingsaspect als normaal onderdeel van hun takenpakket aan boord te nemen.

4

INDIVIDUEEL PERSPECTIEF

De ontwikkeling van een informatiebeveiliger is als volgt gedefinieerd (conform: www.ics2.org):

- 1e niveau: aanstormend talent zonder veel relevante ervaring;
- 2e niveau: een ethische all-round professional met relevante kennis en ervaring;
- 3e niveau: specialisatie naar security management of beveiligingsarchitectuur of andere vakinhoudelijke specialisaties.

In plaats van over niveaus wordt ook wel van (groei-)fasen gesproken.

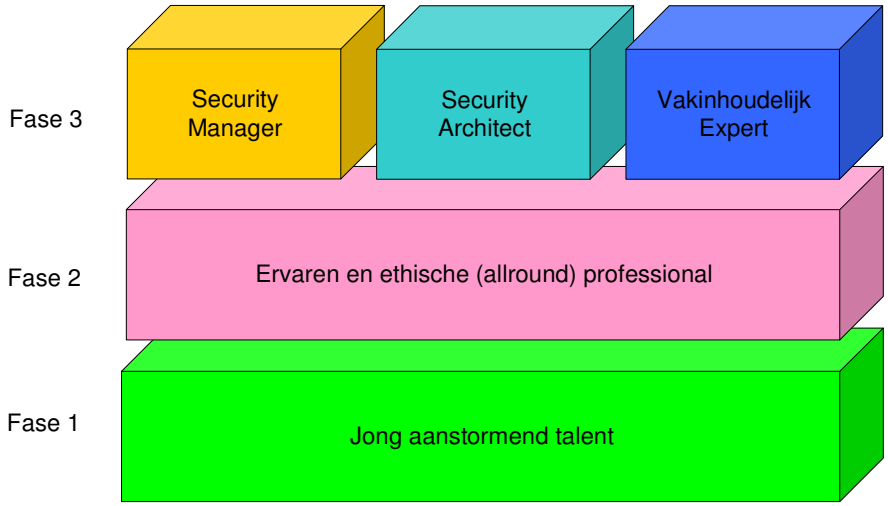
Vanuit het indivueel perspectief wordt onderscheid gemaakt naar de drie niveaus en naar de aspecten kennis, ervaring en persoonlijke vaardigheden.
Het basisniveau biedt voldoende kennis en ervaring, en de bijpassende persoonlijke vaardigheden om binnen een niet-gespecialiseerde functie de beveiligingsproblematiek voldoende te kunnen plaatsen en te (laten) adresseren. Het basisniveau is wat je al je medewerkers aan bagage mee zou willen geven en waarvan je stilletjes hoopt dat al je managers dit ook in huis hebben. Ook vallen in deze categorie de “wannabe’s”, leergierig en met affiniteit voor informatiebeveiliging. Mensen die het vak bij wijze van spreken in hun genen hebben zitten.

Op het tweede niveau vinden we de personen die zich professioneel met alle aspecten van het vak bezighouden. Ze hebben een HBO of academische vooropleiding en hebben minimaal vijf jaar ervaring in diverse onderdelen van de informatiebeveiliging. Het ideaal is dat deze personen in samenwerking met personen uit andere disciplines er voor zorgen dat informatiebeveiliging in de oplossingen wordt ingebouwd, in plaats van later aangebouwd. Ook is de informatiebeveiliger op het tweede niveau in staat om in teamverband een risico analyse uit te voeren en dit op managementniveau te presenteren.

Het derde niveau is dat van, bijvoorbeeld, de information security manager. Deze heeft vaak een staffunctie, met een beperkt aantal ‘direct reports’ en dito leidinggevende verantwoordelijkheden. Zijn rol is een coördinerende of ondersteunende voor de rest van de organisatie. Hij moet in staat zijn om het hele speelveld, dus met alle aspectgebieden van de informatiebeveiliging (fysiek, HRM, juridisch, lijn, audit, techniek), te overzien, daar de prioriteiten te kunnen bepalen, en hij moet óók nog in staat zijn om met voldoende gezag en draagvlak activiteiten te laten gebeuren op plekken van de organisatie waar hij zelf geen lijnverantwoordelijkheid draagt. Dit niveau vraagt veel van persoonlijke vaardigheden, managementcapaciteiten, en vraagt tevens een goede inhoudelijke bagage.

Een ander voorbeeld van het derde niveau is dat van de specialist. Op een beperkt gebied heeft de betrokkene een hoog kennis en ervaringsniveau. Een specialist wordt primair aangesproken op zijn inhoudelijke kennis, en minder op zijn persoonlijke vaardigheden. Voorbeelden van specialistenrollen zijn de cryptoloog, de risico-analist en de beveiligingsarchitect. Net als de risico-analist is de beveiligingsarchitect (voor zover verbijzonderd in een aparte rol) onderdeel van een team dat diverse disciplines voor haar rekening neemt. Alleen op deze wijze maakt informatiebeveiliging een integraal onderdeel uit van de bedrijfsvoering en ondersteunende bedrijfsmiddelen zoals ICT.

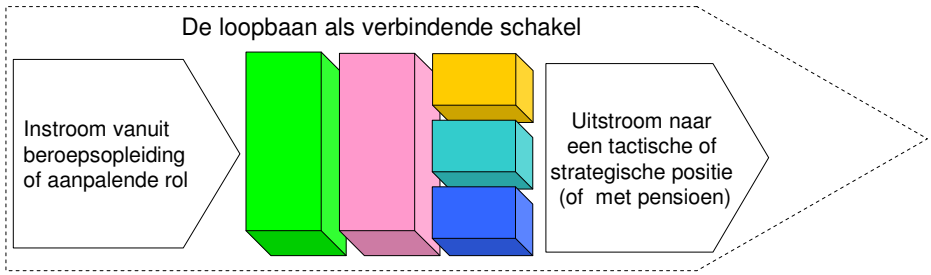
De ontwikkelingsfasen van een informatiebeveiliger:
Van jong talent tot een ervaren grijsaard



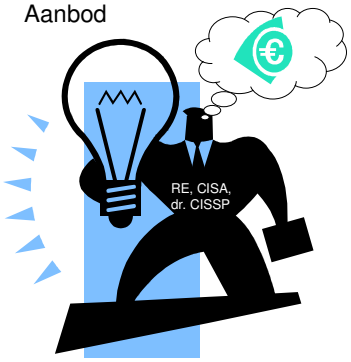
LOOPBAAN

Een loopbaan, of carrière, is het groeipad van het individu in een organisatie. In een loopbaan kunnen beveiligingsfuncties/rollen zijn opgenomen, en andere functies. De werkgroep is van mening dat voorbeeld carrièrepaden behulpzaam kunnen zijn bij het aantrekken van talent. Er wordt wel eens verzucht dat, zodra je in de beveiliging zit, er alleen binnen de beveiliging een carrièrepad is, en dat dit pad ook nog eens zeer kort is.
De vraag kan overigens worden gesteld of dit niet voor álle beroepen geldt. Immers, geldt niet voor alle beroepen een structuur van ‘krullenjongen – gezel – meester’.
Een loopbaan in informatiebeveiliging moet geen doodlopende weg zijn, en ook niet persé een laatste stap in een carrière. Dat, zo vindt de werkgroep, is eerder een teken van zwakte en zal talenten afschrikken. Daar moet de carrièreontwikkeling van een organisatie dan wel op anticiperen. Een managementfunctie in de informatiebeveiliging biedt iemand de gelegenheid iedere uithoek van het bedrijf te verkennen, zijn persoonlijke vaardigheden te ontwikkelen en zich zo klaar te stomen voor een functie als CIO of CFO van het bedrijf.
Er zijn tal van dwarsverbanden met andere functies in de organisatie te onderkennen, neem bijvoorbeeld de relatie met de auditfunctie en corporate risicomanagement. De werkgroep is van mening dat er op dit gebied ruimte is voor verbetering. Voorbeelden zijn nodig van succesvolle loopbanen, met uitzicht op de top.

6



Aanbod



Vraag

UITSPRAKEN OVER ORGANISATIE- EN INDIVIDUEEL PERSPECTIEF

Organisatieperspectief

Wat is bijvoorbeeld een *information security manager*? Er zijn veel verschillende beelden. Het is een staffunctionaris, met verstand van de business. Hij zorgt voor coördinatie, prioriteitenstelling en beweging. 'Getting the job done, by others'. En ook voor het laten draaien van de managementcyclus: plan – do – check – act. De werkgroep heeft voorkeur voor een functiebeschrijving met daarin het woord 'manager', dat al meer wordt gehanteerd in de Nederlandse taal dan het Amerikaanse 'officer'.

En de 'functie' *beveiligingsarchitect*, is dat daadwerkelijk een aparte functie, of is het eigenlijk een rol die binnen een gewone functie, systeemontwerp, zou moeten kunnen worden uitgevoerd. Dat wil zeggen, als die kennis er binnen die gewone functie is: de ICT architect dient beveiligingskennis in zijn bagage te hebben! En dat wordt als de kern van het probleem gezien: zolang het kennisniveau binnen de gewone functies te laag is, zullen deze functies geflankeerd zijn met vergelijkbare functies met het voorvoegsel 'informatiebeveiliging'. En zodra dit kennis deficiënt is opgelost, dan zullen deze 'beveiligingsfuncties' ook weer verdwijnen. De beveiligingsarchitect verdwijnt zodra er binnen de functie systeemontwerp voldoende beveiligingskennis is.

Er is dus maar één bijzondere functie, namelijk de information security manager. Daarnaast zijn er specialistische (of gewone) rollen, waarbij een 'rol' gedefinieerd is als een onderdeel van een takenpakket. In die optiek is 'auditor', volgens de werkgroep, ook een rol. Maar, de inhoud van de rol houdt een zekere afstand tot zijn object in. Daarom zal, zodra de omvang van de organisatie dat mogelijk maakt, de 'auditor' een verbijzonderde rol zijn.

In 2004 is het beroepscompetentieprofiel *Digitaal Rechercheur* ontwikkeld. De digitaal rechercheur signaleert en onderzoekt cybercriminaliteit. Dit doet hij door nieuwe onderzoeken te initiëren, digitaal bewijsmateriaal veilig te stellen en onderzoek te verrichten naar en op bewijsmateriaal. De opleiding zou moeten worden geplaatst in het reguliere onderwijs. De rechercheurfunctie, ook de digitale rechercheur, wordt typisch ingestoken op MBO-niveau. Het beschreven competentieniveau voor de digitale variant lijkt echter hoger, eerder HBO. Is dit een kenmerk van een normale ontwikkeling in een beroep, of zijn de eisen te ambitieus?
Is een digitaal rechercheur niet in de eerste plaats een rechercheur met kennis van automatisering? De relatie met informatiebeveiliging is dan beperkt en dan zou deze functie geen specifieke beveiligings- of risicomanagementfunctie zijn.

De Engelsen zeggen het zo mooi: security should be built IN, rather than built ON. Verbijzonderde functies leiden tot probleemisolatie en tot eilandgedrag. Eigenlijk hoor je geen aparte beveiligingsarchitectuur te hebben, maar moeten de beveiligingsaspecten zijn ingeweven in de gewone architectuur.

De beveiligingsfunctionaris is te vergelijken met de kwaliteitsfunctionaris. Toen ‘kwaliteit’ als issue op kwam, ontstonden er op de allerlei plekken kwaliteitsfunctionarissen. Vervolgens zorgden ze er zelf voor dat er een normaal geïntegreerd kwaliteitsproces op gang kwam. En momenteel zie je dat de aparte kwaliteitsfunctionarissen niet overal meer nodig zijn. Ze zijn er alleen nog waar ze daadwerkelijk waarde toevoegen. Over 20 jaar zal ‘de informatiebeveiligings-functionaris’ ook niet meer bestaan. De ‘rol’ zal naar verwachting ingebed zijn in die van een compliance-manager. Er is ook in functies een soort levenscyclus ontstaan, die bij een probleem, dat meestal een tijdelijk kennisdeficiënt is, een functie creëert, die na verloop van tijd weer opgeheven kan worden.

De beveiligingsfunctie is een normale functie maar dan met extra kennis en een bij de functie passende attitude. Natuurlijk moet informatiebeveiliging in de ontwikkelingscyclus van informatiesystemen geborgd te zijn. Maar wie zorgt daar voor? Je moet altijd vooraan in het proces zitten en telkens blijkt dat verbijzonderde functies er te laat bij (kunnen) zijn. We moeten de functies die vóórop in een proces zitten, uitzoeken, en die moeten we verrijken met extra benodigde beveiligingskennis. De information security manager zal er goed voor moeten waken dat het kennisniveau binnen die functies voldoende is. Vanuit die ‘normale’ functies moet herkenning van de problematiek plaats kunnen vinden, en moet men desgewenst via de information security manager er een specialist bij kunnen halen. Die specialist brengt extra kennis met zich mee opgedaan in het werkveld of dankzij een speciale opleiding, al dan niet voorzien van een titel. Het komt dus toch weer neer op het inbedden van kennis in de gewone processen. De information security manager is, net als gewone manager, of ITIL-manager, dus een gewone procesmanager. Het enige bijzondere is wellicht dat veel van de activiteiten van het security management proces binnen andere processen worden uitgevoerd, wat een extra beroep doet op coördinerende kwaliteiten.

De functie informatiebeveiliging lijkt twee basiscompetenties te bevatten: analyseren en adviseren. Dit geldt zowel voor information security managers als beveiligingsarchitecten. Een informatiebeveiliger werkt nooit alleen, en vaak is hij ondersteunend. Als hij er niet is, staat er niet direct iets stil.

De werkgroep is ook te rade gegaan bij een klassieker op het gebied van functiebeschrijving, namelijk het overzicht 'Taken, Functies, Rollen en Competenties in de Informatica', door ir. Johan C. Op de Coul (ISBN 90-440-0343-7) dat destijds onder auspiciën van het NGI is uitgegeven. De werkgroep is van mening dat de overzichten in dit boek niet bruikbaar zijn voor informatiebeveiliging.

Het 'speelveld' waarbinnen informatiebeveiliging zich beweegt is nog niet gedefinieerd. Waar gaat het eigenlijk om? Fysieke beveiliging, technische beveiliging, risicomanagement, juridische aspecten, personele aspecten? Of raakt informatiebeveiliging aan elk van die aspecten, en misschien nog wel meer, en kan de 'informatiebeveiliger', afhankelijk van persoonlijke ambities en aan- of afwezigheid van interne druk zichzelf een profiel geven. Welke verwachtingen zijn, vanuit het bedrijf gezien, reëel? Het lijkt erop dat een toekomstig werkgever én zijn HRM-afdeling, vooralsnog in het duister tasten, en maar moeten hopen dat de match tussen persoon en functie-uitoefening past.

Uitspraken over het individu

Het onderwijs is van oudsher ingericht om kennis over te dragen. Gelukkig wordt nu de slag gemaakt naar een competentiegerichte opleidingsvorm. Persoonlijke vaardigheden zijn echter moeilijk aan te leren. Ook is persoonlijke 'groei' lastig te meten. Onmisbare persoonlijke kenmerken als loyaliteit, integriteit en overtuigingskracht zijn vrijwel niet aan te leren, en slechts beperkt te meten. Toch zijn dit kernbegrippen in de persoonlijke kenmerken die een professional in de informatiebeveiliging nodig heeft. Wellicht moeten deze kenmerken dan worden aangedragen vanuit andere hoeken. De gedragscomponent kan bijvoorbeeld input krijgen vanuit een coachende rol, en natuurlijk ook vanuit het tonen van voorbeeldgedrag. Het onderwijs is traditioneel ingericht op kennis, en minder op persoonlijke vaardigheden. Toch lijkt het aspect 'persoonlijke vaardigheden en persoonlijke kenmerken' nu juist voor beveiliging van grote importantie. Zou dit niet vragen om een meer op de praktijk gerichte opleiding Informatiebeveiliging bijvoorbeeld op HBO-niveau? Of is dit maar een deel van de oplossing?

Voor het vakgebied zou het goed zijn om tot een concretisering van competenties te komen. Wat maakt een beveiligingsfunctie bijzonder? Genoemd is reeds de combinatie van kennis, vaardigheden en attitude of gedrag. Maar is hier niet sprake van een 'vertrouwensfunctie'? En zou dit aspect dat niet een zwaarder accent moeten hebben?

Informatiebeveiliging heeft naast de vakinhoudelijke aspecten ook kenmerken vanuit de sociaal-wetenschappelijke disciplines zoals organisatieontwikkeling en –verandering en psychologie. Dat vraagt het vermogen interdisciplinair vraagstukken op te lossen in de beroepspraktijk. Er zitten allerlei aspecten in: organisatie, mens, techniek, juridische aspecten. Zowel vanuit de alfa als de beta-hoek is er genoeg te beleven.

Overigens is een zwaarder beroep op persoonskenmerken zoals integriteit en loyaliteit overal om ons heen te zien. De Amerikaanse Sarbanes Oxley wetgeving spreekt zich uit over de ethiek van het management, en Tabaksblat heeft het over de persoonlijke integriteit van de bestuurder. Het beeld wordt duidelijk: informatiebeveiliging verbreedt zich! Dat vraagt om specialismen, nieuwe competenties en dus een bijstelling in opleidingen en opleidingsniveaus. Echter niet in titels.
Deze verbreding maakt het domein van informatiebeveiliging alleen maar interessanter.

TOT SLOT

Het werkgroep pleit voor een beperkt aantal opleidingsrichtingen. De titels zouden aan moeten sluiten bij de bestaande internationale niveaus van bachelor, master en PhD als het gaat om het niveau. De werkgroep stelt voor twee 'master' aanduidingen te gebruiken: de master of information security management MIS-M, en de master of information security technique MIS-T, beide op (post) HBO-niveau. De Master-opleidingen zouden zich daarbij kwalitatief en inhoudelijk moeten kunnen meten aan de RE-opleidingen. Certificering van opleidingen voor de twee gebieden is noodzakelijk, ook in internationaal verband. De werkgroep ziet geen behoefte aan certificeringen op persoonsniveau. Daar zijn er simpelweg te veel van en een certificaat is geen aanduiding meer van het niveau waarop iemand zich bevindt.

Zoals gezegd is dit 'white paper' een stap in een proces. De werkgroep ontvangt daarom graag commentaar en input op de volgende vragen:

- Welke taakelementen zijn relevant/belangrijk in de twee opleidingsrichtingen (MIS-M en MIS-T)?
- Idem, welke kennis, vaardigheden en attitude worden verwacht?
- Welke loopbaanpaden zijn er?
- En zijn twee opleidingsrichtingen genoeg?
- Wat zijn de voor- en nadelen van de inrichting van een verbijzonderde functie voor informatiebeveiliging?
- Moet er voor informatiebeveiliging een opleiding komen op HBO en op universitair niveau, of kunnen deze niveaus worden gecombineerd door middel van een post HBO opleiding? Hoe sluit deze opleiding van bijvoorbeeld aan op een HBO-Informatica opleiding?
- Is het van belang dat de vakinhoudelijke expert (fase 3) eerst de fase van de allround professional (fase 2) doorloopt?

Dit artikel beschrijft voornamelijk de rol- en competentie aspecten van de informatiebeveiliger, maar hoe kunnen opleidingen en de werkzaamheden van de informatiebeveiliger en de auditor goed op elkaar worden afgestemd? Op welke wijze kan een persoon "switchen" tussen de rollen informatiebeveiliger en auditor?

U kunt uw reactie op dit artikel sturen naar expertbrief@gvib.nl

Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

10 LITERATUURLIJST

Voor het tot stand brengen van de expertbrief 'Functies en rollen in de informatiebeveiliging' heeft de werkgroep de volgende literatuur geraadpleegd:

Bokhorst, Bart (2004, 2005), *Functies in de informatiebeveiliging, een visie op ordening, deel 1 en 2* , Informatiebeveiliging 7, 2004 en Informatiebeveiliging 1, 2005

Coul, J. C. op de (2001) , *Taken, functies, rollen en competenties in de informatica,* Den Haag

Dunn Lex, Kuiper Renato (2003), *Security-architectuur, modekreet of bruikbaar?,* Informatiebeveiliging 8

ECABO (2004), *Beroepscompetentieprofiel* Digitaal Rechercheur, www.ecabo.nl

HBO-I stichting (december 2004), *Bachelor of ICT, een competentiegerichte profielbeschrijving*, ISBN 90-9018970-x

Hoek Cobie van der, Koppen Leo van, Spruit Marcel, (2004), *Competenties van de Informatiebeveiliger,* Tinfon 4

(ISC)2 (2005), *Support throughout Your Information Security Career,* www.isc2.org

Meeuwisse Henk (oktober 2004) *Ïnformatiebeveiliging vraagt sterke sturing*, Automatiseringgids 44, en cursusmateriaal NEN 7510 (Informatiebeveiliging in de Zorg)

Noord Fred van, Blankendaal Hans, (2004), *Nieuwe Opleidingen voor Informatiebeveiligers,* Informatiebeveiliging 4

Tittel Ed, Lindros Kim (2004) *Careers and Certification Tips, Charting a path through the security certification landscape,* http://searchsecurity.techtarget..com/tip/1,289483,sid14_gci990011,00.html?track=NL-105&ad=487582

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

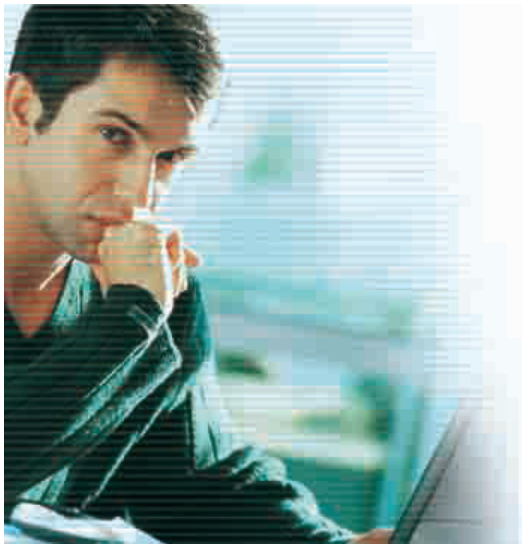
Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

12

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm