4.2 De organisatorische aspecten van informatiebeveiliging

> *When the general is weak and without authority; when his orders are not clear and distinct; when there are no fixed duties assigned to officers and men, and the ranks are formed in a slovenly haphazard manner, the result is utter disorganization.*
>
> SUN TZU, The Art of War – 510 v.C.

Goede informatiebeveiliging is mensenwerk. Technische hulpmiddelen zijn niet meer dan een vangnet voor onjuist menselijk handelen. Als alle medewerkers volledig risicobewust handelen volgens het beleid en als er geen inbreuken van buitenaf zouden zijn, hadden we dat vangnet niet nodig. Maar helaas, de wereld is niet utopisch; medewerkers openen bewust attachments bij e-mails en hackers proberen onze informatievoorziening te verstoren. Toch blijft staan dat voldoende aandacht voor de organisatorische 'zachte' kant van informatiebeveiliging veel problemen kan voorkomen.
In dit artikel wordt een aantal relevante aandachtspunten voor de organisatorische inrichting van informatiebeveiliging geschetst.

Auteur: **Ing. Ernst J. Oud CISA**, *senior manager bij Deloitte Enterprise Risk Services, is projectleider bij een aantal projecten waarin de Code voor Informatiebeveiliging wordt ingevoerd. Daarnaast is hij docent bij NEN en kerndocent bij de masters opleiding informatiebeveiliging Euforce aan de TU Eindhoven. E-mail: ernstoud@euronet.nl.*

Een fout is menselijk

Hoe onbetrouwbaar de diverse surveys ook zijn, keer op keer tonen ze aan dat de meeste beveiligingsincidenten door vaak onbewust menselijk handelen ontstaan. Zuiver theoretisch worden alle incidenten, behalve die welke door niet te beheersen natuurfenomenen ontstaan, veroorzaakt door de mens. Immers, ook uw firewall is ontworpen door mensen en fouten in het ontwerp leiden tot incidenten.
De praktijk leert helaas dat organisaties veel aandacht en financiële middelen richten op tastbare beveiligingstechniek en minder op de menselijke kant. Een niet goed beheerde firewall is echter zo mogelijk door het valse gevoel van veiligheid nog slechter dan geen firewall. Dat informatiebeveiliging als technisch bètavakgebied gezien wordt, is niet verwonderlijk; de bron van het vakgebied ligt in de wetenschappelijke wereld van wiskundigen en computertechnici. Niet voor niets droegen de computerexperts van een tiental jaren geleden nog witte jassen. Organisatorische aspecten hebben meer te maken met alfavakgebieden. Informatiebeveiligers zijn niet zo gewend over het hek naar die andere wereld te kijken.

Beveiliging is mensenwerk

Als beveiliging mensenwerk is dan is direct het probleem hoe we medewerkers zover krijgen dat zij dat ook zo zien. Medewerkers duidelijk maken wat hun rol is bij het genereren van het product of de dienst van de organisatie is te doen. Welke rol het beveiligen van informatie daarbij speelt wordt al moeilijker. Beveiliging is voor een aantal medewerkers zoals de security officer, de facilitaire en de ICT-medewerkers een dagelijkse activiteit, de andere medewerkers zien het niet als hun dagelijkse taak.

Voor de eerstgenoemde groep is informatiebeveiliging deel van de functie en daarom opgenomen in de functiebeschrijving. Voor hen wordt een hiërarchische structuur binnen het bedrijf opgezet. Voor de overige medewerkers moet beveiligingsbewustzijn gerealiseerd worden.

De norm op dit gebied, de Code voor Informatiebeveiliging, bevat tien maatregelen specifiek over organisatorische aspecten en tien maatregelen direct gericht op het personeel. Echter, over de plaats van de security officer in de organisatie of over de verantwoordelijkheden van een systeembeheerder leest u niets in deze norm.

Organisatorische beveiliging volgens de Code voor Informatiebeveiliging

In de Code voor Informatiebeveiliging [CvIB] vindt u in hoofdstuk 4 een klein aantal maatregelen met betrekking tot de organisatorische aspecten, met name over afstemming over dit onderwerp binnen en buiten de organisatie. In hoofdstuk 6 van de CvIB worden maatregelen besproken richting het personeel zoals screening, verantwoordelijkheden in de functiebeschrijving, opleiding en training, en incidentenbeheer.

Op veel meer plaatsen wijst de CvIB op het toewijzen van taken en verantwoordelijkheden. Afhankelijk van de grootte van uw organisatie en de door u in te voeren technische en procedurele maatregelen hebt u een grote of kleine beveiligingsorganisatie nodig. In uw beveiligingsorganisatie kunt u voor vrijwel alle in te voeren maatregelen verantwoordelijkheden onderscheiden op strategisch, tactisch en operationeel niveau. Op strategisch niveau is dat bijvoorbeeld het vaststellen van beleid, werkinstructies en de controle op naleving.

Op tactisch niveau moet iemand verantwoordelijk zijn voor het opstellen van de procedures die het beleid vertalen en op operationeel niveau moeten er werkinstructies geschreven worden. Op al deze niveaus liggen daarom taken. U kunt hierbij denken aan de security manager, de facilitair beheerder, de personeelsmanager, de security officer, de ICT-manager en de systeembeheerder(s). In een grote organisatie zijn dit aparte functies, maar in een kleine organisatie zijn ze wellicht gecombineerd. In dat laatste geval moet u wel denken hoe u functiescheiding aanbrengt. Controleren of het beleid nageleefd wordt, moet namelijk wel gescheiden blijven van het dagelijks beheer. Bij een kleinere organisatie is de controle op naleving van het beleid soms bij de externe auditor te beleggen.

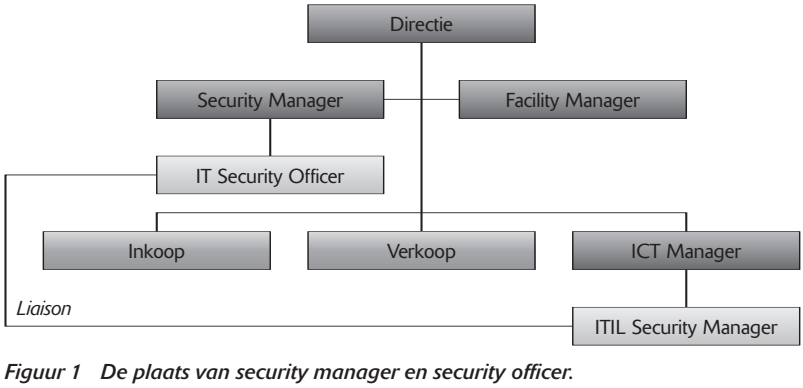
Het inrichten van een beveiligingsorganisatie krijgt binnen de CvIB

expliciet slechts tien paragrafen toegewezen. In tabel 1 worden de functies genoemd die u zou moeten benoemen om die tien maatregelen aan toe te kunnen wijzen.

Maatregel		Verantwoordelijke
4.2.1.1	Managementforum voor informatiebeveiliging	Security manager
4.2.1.2	Coördinatie van informatiebeveiliging	Security officer
4.2.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	Security officer, ITIL security manager, proceseigenaar
4.2.1.4	Autorisatieproces voor IT-voorzieningen	Proceseigenaar, ITIL security manager, ICT-manager
4.2.1.5	Specialistisch advies over informatiebeveiliging	Security officer, ITIL security manager, ICT manager
4.2.1.6	Samenwerking tussen organisaties	Security manager, ICT manager
4.2.1.7	Onafhankelijke beoordeling van informatiebeveiliging	Security officer, ITIL security manager, IT-auditor
4.2.2.1	Identificeren van risico's van toegang door derden	Proceseigenaar, ITIL security manager, security officer
4.2.2.2	Beveiligingseisen in contracten met derden	Proceseigenaar, security officer, juridische zaken
4.2.3.1	Beveiligingseisen in uitbestedingcontracten	Security officer, manager inkoop

Tabel 1 Verantwoordelijken voor hoofdstuk 4.2 van de CvIB.

In tabel 1 is uitgegaan van een formele rol voor informatiebeveiliging in de vorm van een security officer en een ITIL security manager binnen respectievelijk de gebruikersorganisatie en de ICT-organisatie. De eigenaar van het ICT-proces Security Management is in ITIL-terminologie de ITIL security manager. In figuur 1 is dit schematisch toegelicht.



Figuur 1 De plaats van security manager en security officer.

Bij grotere organisaties zijn veelal in de gebruikersorganisatie meerdere security officers aangesteld, onder leiding van een security manager. Naast de IT security officer is dan bijvoorbeeld een aparte functionaris voor de gegevensbescherming in het kader van de WBP aangesteld. De functienaam 'security manager' als hoofd van de afdeling Security en 'ITIL security manager' als verantwoordelijke voor Security Management binnen de ICT-organisatie moet goed onderscheiden worden. Duidelijk mag zijn dat elke medewerker verantwoordelijk is voor informatiebeveiliging. Het grootste deel van de genoemde functies zal bij u wel aanwezig zijn. Hebt u nog geen expliciete staffunctie security manager en/of security officer dan doet u er verstandig aan die functie te (laten) benoemen. Wellicht is het bij uw organisatie geen dagtaak. In dat geval zijn de activiteiten het beste onder te brengen bij een andere staffunctie of desnoods een lijnmanager waar al verantwoordelijkheden liggen voor bijvoorbeeld kwaliteit, administratieve organisatie of auditing.

Hierboven is aangegeven dat Security Management een staffunctie is. Security Management vereist onafhankelijkheid en gezien de controlefunctie is plaatsing in de lijn dan niet aan te raden.
Welke doelstelling heeft dit proces Security Management? In 'Management van Processen' wordt toegelicht dat de besturing van de organisatie als doelstelling heeft: koers bepalen, vertalen, coördineren en leren [Harjono 2001]. De security officer als manager van het proces Security Management moet dus samen met het management en de key-users (proceseigenaren) de doelstelling vastleggen, het pad daarnaar toe specificeren, dit vertalen naar activiteiten voor de organisatie, deze activiteiten coördineren en het leerproces (leren van fouten, incidenten en daardoor steeds beter worden) sturen. Mintzberg stelt dat een stafafdeling zoals de afdeling Security Management (hij noemt deze organizational subunit de 'Techo Structure') als belangrijkste taak heeft 'Standardization of Work Processes' [Mintzberg 1979]. In deze zin is de belangrijkste taak van de security officer een standaard werkproces voor (informatie)beveiliging voor – en met – de organisatie te ontwikkelen, uit te dragen en naleving te controleren.

In § M 2.193 van het Duitse 'IT Baseline Protection Manual' (zie www.bsi.bund.de) en in ISO TR 13335 (met name in § 8 van part 2, zie www.iso.ch) worden meer voorbeelden van de inrichting van de security organisatie gegeven. De laatste benoemt ook duidelijk de hiërarchische plaats en verantwoordelijkheden van het coördinerende orgaan ('an IT security forum, which typically resolves the interdisciplinary issues and approves directives and standards') en van de uitvoerend verantwoordelijke ('the corporate IT security officer, who acts as the focus for all IT security aspects within an organization').

Taken, functies, rollen en competenties opstellen

In de recente NGI-publicatie 'Taken, Functies, Rollen en Competenties in de Informatica' kunt u een beschrijving vinden van de meeste IT-gerelateerde functies [TFRC 2001].
Met betrekking tot informatiebeveiliging erkent deze publicatie vijf functies, de security officer, de security specialist, de beheerder informatiebeveiliging, de IT-auditor en de adviseur interne controle en beveiliging.

De *security officer* is in deze publicatie 'de eindverantwoordelijke voor het opstellen van het beveiligingsbeleid, vaak niet beperkt tot de informatievoorziening, meestal in een stafpositie. De security officer vult daarnaast het beleid in met concrete beveiligingsmaatregelen (tactisch niveau) en ziet toe op de realisatie van zijn beleid op operationeel niveau'. In figuur 1 wordt deze functie de 'IT security officer' genoemd.
Met betrekking tot de *security specialist* wordt gemeld dat deze 'een specialist is op het realiseren van beveiligingsmaatregelen in netwerken en op servers. De security specialist stelt concrete specificaties aan beveiligingssystemen op, selecteert, implementeert en beheert deze systemen. Indien er (nog) geen beveiligingsplan beschikbaar is, wordt dat ook door hem ontwikkeld. De security specialist is vaak ook betrokken bij het ontwerp en de realisatie van informatiesystemen'. Figuur 1 kent deze functie als IT security manager.
De *beheerder informatiebeveiliging* 'is operationeel verantwoordelijk voor de beveiliging van netwerken, servers en applicaties. In die zin draagt hij zorg voor de optimale implementatie van de beveiligingsmaatregelen en -systemen en de juiste parameterinstellingen. Vaak is de beheerder informatiebeveiliging ook degene die de autorisaties beheert, i.c. op aanvraag van verantwoordelijke lijnmanagers autorisaties aan medewerkers instelt'.
De *IT-auditor* 'is primair verantwoordelijk voor het toetsen van de kwaliteit van de informatievoorziening ten aanzien van de aspecten kwaliteit van systeem en gegevens, integriteit van gegevens, beveiliging en internet controle. De IT-auditor wordt betrokken bij projecten bij het ontwerpen en implementeren van de maatregelen op het gebied van de interne controle en beveiliging, toetst de voorgestelde maatregelen en geeft advies over verbetering daarvan'.
Van de *adviseur interne controle en beveiliging* ten slotte wordt opgemerkt dat die functie 'vergelijkbaar is met de IT-auditor maar niet is geaccrediteerd'.
In deze zeer bruikbare NGI-publicatie worden van de vijf genoemde functies de taken en de daarvoor benodigde competenties nauwkeurig omschreven. Met betrekking tot competenties wordt hieronder dieper ingegaan op de security officer en de security specialist (in ITIL-terminologie de security officer en security manager).

De security officer wordt geplaatst onder de taakcluster 'Beleid en Kaderstelling', de security specialist in de taakcluster 'Ontwikkelen Technische Infrastructuur'. Zoals uit figuur 1 blijkt zijn de twee functies elkaars 'liaison' en vullen zij elkaar aan. Competenties benodigd voor invulling van de twee functies komen dus ook grotendeels overeen. Taken uniek voor de security officer zijn 'opstellen informatiebeleid, opstellen informatieplan, opstellen plan voor interne controle en beheren correct gebruik applicaties'. Deze taken vereisen als kenmerkende competenties ervaring met bedrijfskunde en ervaring met organisatieleer. Een goede inleiding daarin is 'The Art of Management' (www.the-art.nl). Een unieke taak voor de security specialist is 'beheren server' wat meer technische ervaring met server technologie vereist dan de security officer tot de bagage zal rekenen.

Een hulpmiddel voor het toewijzen van taken

Als een organisatie middels risicobeoordeling bepaald heeft welke maatregelen men moet treffen om de risico's te minimaliseren moeten de maatregelen vertaald worden naar taken en activiteiten.
In 1995 verscheen de nu niet meer verkrijgbare NGI-publicatie 'Organiseren van gegevensbeveiliging' [NGI 1995]. Hierin was in bijlage D2 een kruisverwijzing opgenomen tussen de maatregelen uit de Code voor Informatiebeveiliging (versie 1994) en de taakclusters uit het indertijd recente NGI-rapport 'Taken en functie in de bestuurlijke informatica', de voorloper van de hierboven genoemde publicatie 'Taken, functies, rollen en competenties in de informatica' [TFRC 2001].
Om het toewijzen van taken voortvloeiend uit de maatregelen van de Code voor Informatiebeveiliging (versie 2000) te vergemakkelijken heeft de auteur speciaal voor dit artikel een nieuwe kruisverwijzing tussen CvIB:2000 en TFRC:2001 opgesteld. In tabel 2 hiervan een impressie.

CvIB	Taakclusters '93	Taakclusters '01
A.3.1.1	42 60	KBPB-1 OA-7 / OA-8
A.3.1.2	51 52 63 69	KBPB-4 / KBPB-5 BISF-4 / BISF-6 AA-10 EA-1
A.4.1.1	42 60	KBPB-1 OA-7 / OA-8
A.4.1.2	42 60	KBPB-1 OA-7 / OA-8
A.4.1.3	42 51	KBPB-1 KBPB-4 / KBPB-5
A.12.3.1	60	OA-7 / OA-8
A.12.3.2	51	KBPB-4 / KBPB-5

Tabel 2 Kruisverwijzing taakclusters 1993/2001 en CvIB (gedeelte).

De volledige tabel is kosteloos bij de auteur op te vragen. Met goede projectplanning en een implementatiemethodiek (zie bijvoorbeeld www.grib.org) kunnen de taken vervolgens ten uitvoer gebracht worden.

Borging lijn/staf, overlegorganen inrichten

In de CvIB wordt in maatregel 4.1.2 benoemd dat coördinatie van informatiebeveiliging noodzakelijk is. Beschreven wordt de inrichting van een multidisciplinair overlegorgaan tussen de primair voor beveiliging verantwoordelijke functies in de staf en de functies binnen de operationele lijn organisatie.
Tot de taken van een dergelijk overlegorgaan wordt dan o.a. gerekend 'het bereiken van overeenstemming over en het ondersteunen van initiatieven op het gebied van informatiebeveiliging in de gehele organisatie'. In de praktijk blijkt de inrichting van een coördinerend orgaan, een beveiligingscommissie, moeilijk.

Voor de direct betrokkenen is informatiebeveiliging zo vanzelfsprekend dat overleg niet noodzakelijk lijkt, voor de minder bij informatiebeveiliging betrokkenen heeft het primaire proces altijd meer prioriteit. Van de voorzitter van dit overleg – vaak de security officer – wordt dus tact, inlevingsvermogen en enthousiasme gevraagd om het overleg gaande te houden.
De agenda van een dergelijk overleg is bijvoorbeeld als volgt:

1. Opening
2. Inbreng punten voor agendapunt 6
3. Verslag vorig overleg
4. Actie- en verbeterpunten
5. Projecten
6. Wat verder ter tafel komt

Naast de genoemde beveiligingscommissie zijn meer overlegorganen nodig. In tabel 3 worden de minimaal noodzakelijk in te richten overlegorganen opgesomd.

Overlegvorm	Leden (minimum)	Frequentie
IB overleg (beveiligingscommissie)	ICT/security	Tweewekelijks
Werkoverleg security	Medewerkers security	Wekelijks
Werkoverleg ICT	Medewerkers ICT	Wekelijks
Wijzigingscommissie	Leden Change Management Board	Maandelijks
Management review	MT-leden	Jaarlijks
MT	MT-leden	Maandelijks
Werkoverleg security/beveiliging	Security officer, hoofd beveiliging	Dagelijks

Tabel 3 Voorbeelden van mogelijke overlegvormen.

Uw managementsysteem voor informatiebeveiliging moet na invoering gaan werken. De diverse personen in de beveiligingsorganisatie voeren de aan hen toegewezen taken uit. Daarbij komen allerlei problemen, opmerkingen en andere relevante zaken naar voren. Uit de uitgevoerde

audits komen verbeterpunten. Uw bedrijfsprocessen veranderen waarschijnlijk waardoor u opnieuw de risico's moet beoordelen. Kortom, er is regelmatig overleg noodzakelijk tussen alle betrokken partijen om acties te beleggen, voortgang te monitoren en problemen te bespreken. De bovengenoemde overlegorganen vormen dan als het ware de 'motor' voor uw managementsysteem.
De genoemde taken, verantwoordelijkheden, bevoegdheden en overlegorganen moeten in het informatie beveiligingsbeleid verwoord zijn. Daardoor kunnen alle medewerkers van de organisatie weten wie de aanspreekpunten zijn bij incidenten, bij vragen of voor het indienen van verbetervoorstellen. De CvIB meldt dat het informatiebeveiligingsbeleid moet bevatten 'een omschrijving van de algemene en specifieke verantwoordelijkheden voor het management van informatiebeveiliging, waaronder het rapporteren van beveiligingsincidenten'.

Wet- en regelgeving

Het zal u niet verbazen dat slechts weinig regelgeving bestaat m.b.t. de organisatorische inrichting van (informatie)beveiliging. In de Regeling Organisatie en Beheersing van De Nederlandsche Bank (zie http://www.dnb.nl/dnb/bin/doc/4201–tcm7-16520.pdf) worden in paragraaf 1.2.3 'Organisatorische maatregelen', een vijftal artikelen genoemd voor de financiële sector met name met betrekking tot de vastlegging van taken, verantwoordelijkheden en bevoegdheden, het opstellen van procedures en met betrekking tot functiescheiding.

Artikel 3 van het Voorschrift Informatiebeveiliging Rijksdienst (zie http://www.rijksarchiefinspectie.nl/wetgeving/overige–VIR1994.html) stelt dat in het beleidsdocument voor informatiebeveiliging vastgelegd moet zijn: 'de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden'. Dit document is bindend voor de Rijksdienst waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.

Voor veel organisaties is de Wet Bescherming Persoonsgegevens (WBP, zie www.overheid.nl) van belang. Deze beschrijft de (optionele) benoeming van de functionaris voor de gegevensbescherming. In artikel 64 van de WBP worden de taken van deze functionaris benoemd.

Afsluiting

In de publicatie HB231-2000, 'Organisational experiences in implementing information security management systems', worden van vijf organisaties de ervaringen met invoering van BS7799 (de Engelse brontekst van de Code voor Informatiebeveiliging) besproken [HB231 2000]. Een van de conclusies is: 'It is worth re-stating that organisational initiatives are more important than technical initiatives...'

Literatuur

[CvIB] Code voor Informatiebeveiliging, www.cvib.nl
[Hardjono 2001] Hardjono, T.W. en R.J.M. Bakker, *Management van processen*, Kluwer, 2001
[HB231 2000] *Organisational experiences in implementing information security management systems*, HB231-2000, Standards Australia, 2000
[Mintzberg 1979] Mintzberg, H., *The structuring of organisations*, Prentice Hall, Englewood Cliffs, 1979
[NGI 1995] *Organiseren van gegevensbeveiliging*, NGI, 1995 (niet meer verkrijgbaar)
[TFRC 2001] Op de Coul, J.C., *Taken, functies, rollen en competenties in de informatica*, NGI, 2001

Websites

www.the-art.nl
www.bsi.bund.de
www.iso.ch
www.grib.org
www.dnb.nl/dnb/bin/doc/4201–tcm7-16520.pdf
www.rijksarchiefinspectie.nl/wetgeving/overige–VIR1994.html
www.overheid.nl

Noot

1. Delen van dit artikel verschenen eerder in de *Praktijkgids Code voor Informatiebeveiliging,* Academic Service.