De nieuwe Code voor Informatiebeveiliging

Dr. ir. P.L. Overbeek RE

De Code voor Informatiebeveiliging mag zich in een grote populariteit verheugen. Standaarden als de Code worden iedere vijf jaar geactualiseerd. De veranderingen in de Code laten zien welke ontwikkeling IT heeft doorgemaakt, en nog doormaakt. Ter gelegenheid van deze nieuwe versie zijn tevens enkele onderzoeken uitgevoerd naar de stand van zaken op beveiligingsgebied.

De nieuwe Code voor Informatiebeveiliging

De Code voor Informatiebeveiliging is sinds 1994 in gebruik in Nederland, als vertaling van de Engelse Code of Practice for Information Security Management (British Standard BS7799). De Code wordt in Nederland veel gebruikt, vooral bij grotere bedrijven. En de populariteit is nog steeds groeiende. In het kader van het periodiek onderhoud aan standaarden is nu een revisie van de Code verschenen. In dit artikel wordt eerst de nieuwe Code zelf geïntroduceerd. Vervolgens worden de verschillen tussen de nieuwe en de oude versie besproken. De veranderingen in de Code laten goed zien welke ontwikkeling de IT heeft doorgemaakt, en nog doormaakt. Ter ere van de introductie van de nieuwe versie zijn enkele onderzoeken uitgevoerd naar de actuele stand van zaken op beveiligingsgebied, en de rol van de Code hierin. Enkele opvallende trends worden gepresenteerd.

Code voor Informatiebeveiliging 2000

De *Code voor Informatiebeveiliging* is een leidraad voor praktische informatiebeveiliging. De Code is ontwikkeld in antwoord op de vraag naar praktische hulpmiddelen voor beveiliging van informatie in computers en netwerken. De Code biedt een gemeenschappelijke basis voor bedrijven om beveiligingsbeleid te ontwikkelen, maatregelen te selecteren, de nodige plannen op te stellen, en zo tot 'beveiliging op maat' te komen. In deze paragraaf wordt de Code zelf beschreven, en wordt ingegaan op het werken met de Code.

Achtergrond

Ons vakgebied mag zich verheugen in een ruime belangstelling van de media. Dat is goed, want het stimuleert dat over het onderwerp wordt gesproken. De incidenten die ons via de pers bereiken zijn echter niet illustratief voor de huidige stand van zaken. Het grootste deel van de incidenten wordt niet door hackers veroorzaakt, maar door de eigen medewerkers in de omgang met gebrekkige techniek. Ook vindt het merendeel van de beveiligingsincidenten niet bij het Pentagon plaats, maar bij u, en waarschijnlijk zonder dat u dat weet. Informatiebeveiliging is zich aan het ontwikkelen van een specialisme, dat het domein was van hoogopgeleide staffunctionarissen met grijze haren, naar een normaal gemanaged proces. In dit proces wordt het evenwicht gezocht tussen de beveiligingsmaatregelen: fysieke afscherming, technische hulpmiddelen, ondersteunende procedures en dat geheel ingebed in een passende organisatie.

Juist met het oog op het evenwicht tussen de maatregelen is de Code voor Informatiebeveiliging ontwikkeld: als een goed toegankelijk hulpmiddel, ook voor de niet-beveiligingsspecialisten. De Code richt zich op managers en werknemers die verantwoordelijk zijn voor het opzetten, implementeren en onderhouden van de informatiebeveiliging in hun bedrijf.

De Code biedt basisprincipes voor het management voor de bescherming van informatie. In de eerste plaats is het doel van de Code om in eigen huis orde op zaken te kunnen stellen. Bovendien is de Code bedoeld als referentiekader, als gemeenschappelijke basis, voor (elektronische) zakenpartners. In het zakelijk verkeer moet men op elkaar kunnen vertrouwen. Dat geldt zeker wanneer organisaties afhankelijk worden van de beveiliging bij partners waarmee elektronisch zaken wordt gedaan, bijvoorbeeld bij gebruik van elektronische handel (electronic commerce) of elektronische post. De Code beoogt hiermee tevens het vertrouwen in het handelsverkeer tussen bedrijven te bevorderen.

De Code voor Informatiebeveiliging is ontstaan in Engeland als een samenbundeling van *best practices* voor informatiebeveiliging. Aan de Code wordt meegewerkt door grote en kleine bedrijven, om het draagvlak zo groot mogelijk te houden. Deelnemende bedrijven zijn bijvoorbeeld British Telecom, Marks & Spencer, Midland Bank, Shell en Unilever. In het schrijversteam wordt samengewerkt door mensen uit Engeland, Duitsland, Noorwegen en Nederland. Er is ook een Nederlandse vertaling. De Nederlandse versie is totstandgekomen onder supervisie van het Nederlands Normalisatie Instituut. Gebruik van de Code wordt onder andere gestimuleerd door organisaties als het Ministerie van Economische zaken, het Ministerie van Verkeer en Waterstaat, de Nederlandse Vereniging van Banken, Electronic Commerce Platform Nederland, FENIT en VNO/NCW, die hiermee het belang van informatiebeveiliging voor moderne organisaties onderschrijven. De Code wordt veel gebruikt als referentiekader door professionals in de informatiebeveiliging. De Code bestaat uit twee delen: deel I beschrijft het managementraamwerk en de te treffen beveiligingsmaatregelen, deel II beschrijft de eisen die in verband met certificatie worden gesteld.

Uitgangspunten van de Code

Het doel van beveiliging is enerzijds het waarborgen van de continuïteit van de bedrijfsprocessen en anderzijds het minimaliseren van eventuele schade, direct of indirect, die ontstaat uit beveiligingsincidenten. Dit doel wordt bereikt door het treffen van een evenwichtig pakket preventieve maatregelen (het voorkomen van beveiligingsincidenten), alsmede repressieve en correctieve maatregelen (gericht op het beperken van de negatieve gevolgen van incidenten). Overigens richt de Code zich niet alleen op de beveiliging van informatie in computers en netwerken, maar op alle vormen van informatie, dus bijvoorbeeld ook de informatie die opgeslagen is in papieren documenten, op videobanden, in antwoordapparaten, dicteerapparaten en palmtops.
De Code baseert zich daarbij op de bekende drie-eenheid: vertrouwelijkheid, integriteit en beschikbaarheid. Informatie is één van de bedrijfsmiddelen en de bescherming daarvan kan van essentieel belang zijn voor het behoud van de concurrentiepositie, de winst en het imago van een organisatie. De afhankelijkheid van de bedrijfsprocessen van informatiesystemen neemt nog steeds toe. Helaas neemt tegelijkertijd de kwetsbaarheid van de informatiesystemen ook toe, bijvoorbeeld door de toenemende afhankelijkheid van externe netwerken zoals het Internet, de steeds complexere software en het gedeelde gebruik van infrastructuren door 'vriend' en 'vijand'.

Tabel 1. De tien hoofdcategorieën voor beveiliging.

Beveiligingscategorieën	Trefwoorden uit de categorie
Beveiligingsbeleid	* Doelstellingen voor informatiebeveiliging vastleggen in het beleidsdocument: beschrijving van de te bereiken of na te streven situatie in termen van de bedrijfsbelangen. Het beleid wordt goedgekeurd en uitgedragen door het management. Het halen van de doelstellingen wordt aangestuurd en gecontroleerd.
Organisatie van de beveiliging	* Inrichten van de organisatie met beveiligingsfuncties, verantwoordelijkheden, bevoegdheden en taken, coördinatie, samenhang en rapportagelijnen, autorisatieprocessen. Verantwoordelijkheid voor afspraken over samenwerking met derden wordt expliciet gemaakt.
Classificatie en beheer van de bedrijfsmiddelen	* Weten wat je in huis hebt door inzicht in de aanwezige bedrijfsmiddelen en hun verantwoordelijke 'eigenaar'. Gebruik van classificatieschema's voor informatie en systemen koppelt het belang van informatie en andere middelen aan specifieke beveiligingsmaatregelen.
Personeel	* Succesvolle informatiebeveiliging begint bij betrouwbaar, zorgvuldig en goed opgeleid personeel. Daarvoor is nodig: training, security awareness, veilig gedrag op de werkvloer, aannamebeleid en functioneringsbeoordeling. Personeel moet weten hoe te reageren op beveiligingsincidenten.
Fysieke beveiliging en omgeving	* Beveiliging van en in de infrastructuur vereist onder andere toegangscontrole bij de poort, fysieke beveiliging van computerruimten, decentrale computers en mobiele apparatuur. Toegang tot rondslingerende papieren wordt voorkomen met een clear desk policy. De continuïteit van de stroomvoorziening en datacommunicatie vraagt aandacht. Tevens zijn richtlijnen nodig voor middelen als organizers, mobiele telefoons, diskettes, tapes en documentatie.
Computer- en netwerk-beheer	* Een goede organisatie van het IT-beheer kan de kans op fouten sterk verminderen. Dit vereist vastgelegde beheerprocedures, beheer van de technische beveiliging en verantwoordelijkheden voor dit beheer. Andere maatregelen zijn: antivirusmaatregelen, incidentafhandeling en -rapportage, beveiliging bij uitwisseling van gegevens met derden zoals e-mail, EDI. Een vaste methodiek, bijvoorbeeld ITIL Security Management, geeft steun.
Toegangsbeveiliging	* De toegang tot informatie en IT-middelen wordt op bedrijfsmatige overwegingen gebaseerd. Dit vraagt een autorisatieproces voor toegang tot informatie en IT-middelen. De uitgegeven autorisaties worden procesmatig onderhouden, bewaakt en eventueel weer ingetrokken.
Ontwikkeling en onderhoud van systemen	* Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden 'zeker' tot veilige systemen, die ook veilig blijven (change management).
Continuïteits-management	* Een calamiteit hoeft nog geen ramp te worden indien vooraf is nagedacht over de eisen aan continuïteit en er een proces is voor continuïteitsborging inclusief calamiteitenopvang, rampenplannen en (geoefende) uitwijk.
Toezicht	* Door middel van auditing en andere vormen van toezicht wordt inzicht gekregen in het halen van de doelstellingen uit het beleid en de realisatie van de afspraken. Ook aandacht voor de naleving van wettelijke en contractuele voorschriften, beveiligingscontrole op IT-systemen, IT-audit en interne controle.

De tien hoofdcategorieën voor informatiebeveiliging

In de Code zijn tien hoofdcategorieën vastgesteld als belangrijkste aandachtsgebieden voor beveiliging (zie tabel 1). Iedere categorie is op dezelfde wijze opgebouwd: er zijn doelstellingen geformuleerd en er is een basisset aan beveiligingsmaatregelen en activiteiten gedefinieerd waarmee die doelstellingen kunnen worden bereikt. Deze opzet wordt met het volgende voorbeeld geïllustreerd.

Voorbeeld: categorie 2, de 'organisatie van de beveiliging'. De *doelstelling* is een managementkader te realiseren voor informatiebeveiliging. Als *maatregelen* zijn bijvoorbeeld vereist: het vastleggen van verantwoordelijkheden en de coördinatie tussen de verantwoordelijken met invulling van duidelijke rapportagelijnen. *Activiteiten* zijn onder andere: het organiseren van de implementatie van het beleid, het toezicht op de veranderende risico's, het opstellen van de uitwijkplannen, het reageren op eventuele incidenten en het organiseren van externe onafhankelijke beoordeling van de beveiliging.

Waar te beginnen ...

Hoewel het aantal maatregelen in de Code op zich beperkt is, is toch aan een aantal maatregelen een hogere prioriteit gegeven. Een klein aantal maatregelen in de Code is onmisbaar omdat ze *essentieel* zijn (bijvoorbeeld vanwege wettelijke eisen) of *fundamenteel* voor informatiebeveiliging (bijvoorbeeld omdat deze maatregelen het managementraamwerk bieden voor beveiliging). Deze maatregelen zijn van toepassing op elke organisatie en omgeving (zie tabel 2). Ze vormen als het ware de sleutelmaatregelen voor succesvolle informatiebeveiliging. Tevens vormen deze maatregelen het startpunt voor bedrijven die nog niet zo ver zijn met informatiebeveiliging omdat deze maatregelen de basis vormen voor het management van informatiebeveiliging volgens de bekende managementcyclus: plan, do, check, act.

Werken met de Code

De Code vat de essentie van informatiebeveiliging samen in 8 essentiële maatregelen, 10 hoofdcategorieën, 36 doelstellingen en zo'n 125 maatregelen. De Code is daarmee een inzichtelijk hulpmiddel en vertrekpunt voor tal van activiteiten. Hieronder worden de belangrijkste genoemd.

Inrichting van de informatiebeveiliging
Als verzameling van 'best practices' is de Code een uitstekend vertrekpunt voor het (her)inrichten van de informatiebeveiliging binnen en tussen organisaties. De Code wordt hiervoor op maat van de organisatie gemaakt. Veelal worden in een Handboek Informatiebeveiliging de algemeen geformuleerde doelstellingen en maatregelen uit de Code gespecificeerd voor de organisatie en worden de interne procedures en verantwoordelijkheden beschreven. Eventueel worden onderwerpen die voor een organisatie niet van belang zijn weggelaten. De zo op maat gemaakte Code biedt het basisniveau aan beveiliging (baseline) voor de organisatie. Door aanvullend een eenvoudig schema voor risicoanalyse toe te passen, kan worden afgesproken voor wat voor soort informatie en systemen het basisniveau voldoende is, en in welke gevallen aanvullende, gespecialiseerde maatregelen nodig zijn.

Het proces zelf om tot inrichting van de informatiebeveiliging te komen is niet complex of moeilijk. Op ieder moment is inzicht in de vooruitgang van de organisatie te geven. De snelheid van implementatie hangt samen met de prioriteitstelling en het veranderingsvermogen van een organisatie. Afhankelijk van het vertrekpunt is een implementatietermijn van een half jaar tot twee jaar niet ongebruikelijk.

Inrichting IT-beheer
Aangezien veel organisaties het IT-beheer conform ITIL inrichten, is op Nederlands initiatief een ITIL-module ontwikkeld die de inrichting van security management binnen ITIL beschrijft. ITIL Security Management beschrijft het proces zelf en de relaties met andere processen waarbinnen de activiteiten plaatsvinden. Zo worden (beveiligings)incidenten afgehandeld door het proces Incident Management. Het proces Configuration en Asset Management geeft een goede kapstok voor een classificatiesysteem. Het proces Change Management geeft handvatten voor beheerste en gecontroleerde wijzigingen in de IT-infrastructuur. Hierbij kunnen eisen ten aanzien van het uitvoeren van risicoanalyses en het onderhouden van de baseline worden bewaakt. Dit zijn slechts enkele voorbeelden. In de module ITIL Security Management worden de doelstellingen en maatregelen uit de Code toegewezen aan de verschillende processen, onder regie van het proces Security Management. Tevens wordt aangegeven welke doelstellingen en maatregelen buiten de scope van ITIL vallen, maar natuurlijk wel moeten worden geregeld. Denk hierbij bijvoorbeeld aan fysieke beveiliging en omgang met het personeel.

Audits en benchmarking
Omdat de Code een neerslag is van wat grote en ervaren bedrijven op het gebied van informatiebeveiliging doen, kan de Code ook goed worden gebruikt als 'meetlat'.

Essentiële beveiligingsmaatregelen vanuit wettelijk oogpunt
* Voorkomen van onrechtmatig kopiëren van programmatuur of informatie.
* Veiligstellen van bedrijfskritische documenten/bestanden in verband met wettelijke eisen rond bijvoorbeeld bewaar- en bewijsplicht (grootboek).
* Bescherming van persoonsgegevens (privacy).
Essentiële maatregelen die de basis vormen voor beveiliging
* Doelstellingen voor beveiliging (beleidsdocument).
* Toewijzing van verantwoordelijkheden.
* Training en opleiding.
* Rapportage en afhandeling van beveiligingsincidenten.
* Continuïteitsplanning.

Tabel 2. Essentiële maatregelen.

Door middel van een audit met de Code als norm, wordt de organisatie de maat genomen. Uit de audit blijkt dan welke doelstellingen niet worden gehaald, of welke maatregelen ontbreken. Aangezien deze doelstellingen en maatregelen voor de meeste organisaties van toepassing zijn, heeft de organisatie hiermee een goed vertrekpunt voor het formuleren van verbeteringsactiviteiten, bijvoorbeeld in het jaarplan voor informatiebeveiliging.

Afspraken tussen partners
De Code wordt ook veel gebruikt als gemeenschappelijk referentiedocument tussen (handels)partners. Bij uitbesteding wordt voor de beveiligingsparagraaf van de service level agreement veelal gerefereerd aan de eis (aantoonbaar) te voldoen aan de Code. Ook in andere contracten met derden, zoals bij beheer door derden op afstand, softwareontwikkeling of inhuurcontracten, wordt de Code steeds vaker genoemd. En de Code wordt ook steeds vaker gebruikt voor het definiëren van algemene normen en richtlijnen voor specifieke situaties, zoals het omgaan met persoonsgegevens, websites, electronic commerce en, heel specifiek, het bieden van trust services op het Internet zoals Trusted Third Parties dat beogen.

Certificatie
Veel organisaties willen de kwaliteit en aandacht voor informatiebeveiliging zichtbaar maken. Dat is mogelijk door middel van een certificaat op basis van de Code voor Informatiebeveiliging. Zo'n certificaat kan aan klanten, afnemers, partners of andere derde partijen worden getoond om te laten zien dat de organisatie de informatiebeveiliging structureel beheerst en er ten minste een minimumpakket aan maatregelen is geïmplementeerd. Ook tussen bedrijfsonderdelen, die bijvoorbeeld een gemeenschappelijke IT-infrastructuur delen, is certificatie een eenvoudig maar krachtig managementinstrument. Voor veel organisaties zal een certificaat slechts de externe bekrachtiging zijn van wat ze zelf al weten: het huis is op orde. Voor organisaties die nog bezig zijn met de inrichting van hun informatiebeveiliging kan het certificaat een duidelijk en zichtbaar einddoel geven voor een verbeteringstraject. In Nederland zijn twee certificatieorganisaties erkend door de Raad voor Accreditatie. In Engeland zijn dat er inmiddels een stuk of tien. In veel landen is men reeds actief of bezig met het opzetten van certificatie, bijvoorbeeld in de Scandinavische landen, Australië, Zuid-Afrika en Zwitserland. Recent is certificatie ook weer op de Brusselse

agenda gekomen in de discussie over accreditatie van Trusted Third Parties. Overigens is certificatie geen nationale aangelegenheid: de certificaten zijn internationaal erkend en certificatieorganisaties die zijn geaccrediteerd door bijvoorbeeld de Raad voor Accreditatie certificeren ook internationaal.

Consistente aanpak
Uitgaande van de Code kan een uniforme aanpak worden bereikt van beveiligingsbeleid, inrichting van de organisatie inclusief het IT-beheer, het uitvoeren van audits tot en met certificatie. De bekende Deming-cyclus – *plan, do, check, act* – is hiermee ingevuld. Ofwel: een volledig instrumentarium voor het managen van informatiebeveiliging.

Wat is er nieuw of veranderd

De nieuwe Code is voor het grootste deel, misschien wel 95 procent, gelijk aan de oude versie. Dezelfde indeling in hoofdcategorieën is gevolgd, en alle doelstellingen in de vorige versie zijn gehandhaafd. Wel is het taalgebruik, zeker in de Nederlandse versie, weer bij de tijd gebracht. Ook is de soms wat eenzijdige aandacht voor centrale systemen rechtgetrokken.

De eerste opvallende wijziging is het vervangen van de tien oude sleutelmaatregelen door acht zogeheten 'essentiële maatregelen', die hierboven reeds besproken zijn. Dat is gedaan omdat de oude sleutelmaatregelen niet geheel evenwichtig waren. Zo komt een oude sleutelmaatregel als 'antivirusmaatregelen' niet meer voor als essentiële maatregel, omdat de toepasbaarheid afhankelijk is van de specifieke IT-omgeving. In bijvoorbeeld een mainframeomgeving is deze maatregel niet van toepassing. Door de essentiële maatregelen in twee soorten te splitsen is tevens duidelijk wat er moet 'van de wet', en wat essentieel is in de inrichting van een managementsysteem voor informatiebeveiliging.

Beveiliging vraagt steeds meer om proactief management.

De tweede opvallende wijziging, althans voor de Nederlandse lezer, is het toevoegen van een deel II bij de Code, geheten 'Specificatie van managementsystemen voor Informatiebeveiliging'. Dit deel is mede van belang voor certificatie. Naast een specificatie van eisen die aan de documentatie worden gesteld, beschrijft dit deel op meer stellende, normatieve wijze de doelstellingen en maatregelen uit deel I. De informele stijl van deel I is hier verlaten en in staccato worden alle mogelijke eisen samengevat. Voor de Nederlandse versie van de Code is dit deel nieuw. In Engeland bestond het al als bijlage. Interessant is dat in dit deel certificeringseisen, die destijds in een Brits/Nederlandse samenwerking met het voormalige ICIT zijn opgesteld, zijn overgenomen. De gelijkwaardigheid tussen certificaties in beide landen is hierdoor gewaarborgd.

Een derde wijziging is dat referenties naar specifiek Engelse situaties of wetgeving zijn verwijderd. In Engeland worden enkele bijlagen ontwikkeld die de specifieke Engelse situatie adresseren. Het ligt voor de hand dat in Nederland een soortgelijke bijlage wordt ontwikkeld waarin bijvoorbeeld aandacht is voor de nieuwe Wet bescherming persoonsgegevens, de Wet computercriminaliteit en de eisen die voortkomen uit de Arbo-wet.

Interessante discussies ontstonden altijd als aanhangers van risicoanalyse de aanhangers van de Code verketterden, en vice versa. De Code geeft immers een set van maatregelen die in vrijwel alle situaties, dus zonder uitgebreide risicoanalyse, zouden moeten worden geïmplementeerd. Dit weerspiegelt het karakter van een basisniveau aan beveiliging (baseline). In de Code wordt nu duidelijker aangegeven in wat voor situaties en bij welke maatregelen wél een risicoanalyse nodig is.

Andere opvallende wijzigingen zijn de meer technologieonafhankelijke taalkeuze, de verbeterde balans tussen de maatregelen ten gunste van beschikbaarheid, en het evenwicht in de beschrijvingen waarin oeverloze details zijn weggelaten, bijvoorbeeld over de kwaliteit van wachtwoorden.

Voorts komen bij de maatregelen onderwerpen naar voren die in de oude versie nog niet of nauwelijks aan de orde kwamen, waaronder:
* uitbesteding;
* gebruik van diensten van of relaties met derden (inhuur, softwareontwikkeling, standaardpakketten, insourcing);
* beheer op afstand;
* telewerken;
* laptops, organizers, mobiele telefoons;
* kantoorsystemen (agendabeheer, e-mail, teleconferencing, ...);
* electronic commerce;
* nieuwe media;
* aanbieden van diensten op en gebruik van externe publieke netwerken, zoals het Internet;
* gebruik van andere authenticatiemiddelen naast wachtwoorden, zoals tokens en certificaten;
* kwaadaardige software (uitbreiding);
* rechten en plichten van het personeel (geactualiseerde beschrijving);
* softwareontwikkeling en -onderhoud (geactualiseerd);
* business continuity management (meer aandacht voor het proces);
* en in het hoofdstuk over toezicht wordt de rol van de auditor wat positiever belicht.

Door de oude versie en de nieuwe versie van de Code naast elkaar te zetten, vallen direct de belangrijkste veranderingen in de IT-wereld van de afgelopen jaren op. Wat mij het meest opvalt is dat beveiliging steeds meer proactief management vraagt. Dat weerspiegelt zich bijvoorbeeld in de virusbestrijding, waarbij het accent steeds meer komt te liggen op 'early warning', bij intrusion detection, het actief analyseren van auditdata uit bijvoorbeeld logfiles, het volgen van nieuws over en reageren op beveiligingsincidenten en het bouwen aan informatiebeveiliging onder een architectuur.

Wat betekenen deze wijzigingen voor u

Zoals gezegd is de nieuwe versie eerder evolutie dan revolutie. Er is dan ook geen noodzaak tot acute wijzigingen. Als u de Code gebruikt voor de inrichting van uw informatiebeveiliging, dan kunt u overwegen de nieuwe onderwerpen bij de eerste revisie mee te nemen. Hetzelfde geldt voor de herziening van afspraken met partners. Gebruikers van ITIL Security Management hoeven niets te doen, want deze ITIL-module is reeds gebaseerd op de nieuwe Code. Auditors kunnen hun methodiek oplijnen met de nieuwe Code, zodat ook aandacht wordt besteed aan de nieuwe onderwerpen uit de Code. Certificatie, tot slot, zal de nieuwe versie als norm nemen. Sommige certificeerders zijn hier in 1999 reeds op vooruitgelopen. Te zijner tijd zal in het Nederlandse certificatieschema wellicht direct naar het nieuwe deel II kunnen worden verwezen.

Trends in informatiebeveiliging

Ter ondersteuning van het verschijnen van de nieuwe versie van de Code is een aantal onderzoeken uitgevoerd naar de huidige stand van de beveiliging. Dit betreft bijvoorbeeld onderzoeken van het Engelse Department of Trade and Industry en van KPMG. Sommige onderzoeksresultaten zijn vrij toegankelijk via het Internet; zie de referenties. Als de onderzoeken naast elkaar worden gezet, dan ontstaat bij mij het volgende beeld van een aantal opvallende trends:

- Veel organisaties hebben een inhaalslag uitgevoerd rond thema's als Business Continuity en Asset Management, als gevolg van de Jaar 2000-problematiek. De vraag is of organisaties de opgedane kennis en werkwijze in de eerste helft van dit jaar hebben kunnen borgen in de organisatie.
- Organisaties hebben steeds meer moeite de veiligheid van het snel groeiende aantal externe netwerkverbindingen te beheersen.
- De indruk bestaat dat informatiebeveiliging in nieuwe toepassingen, zoals electronic commerce, onvoldoende aandacht krijgt.
- Voor wat betreft virussen en andere kwaadaardige software is het algemene beeld dat de doos van Pandora nog maar op een kier staat.
- Het aantal organisaties met een security manager en een (IT-)security-managementproces is nog klein (14 procent), maar neemt wel snel toe. ITIL is de dominante structuur voor IT-beheer. Het gebruik van het in 1999 gepubliceerde ITIL Security Management komt in de statistieken nog niet voor.
- Slechts 37 procent van alle organisaties maakt structureel gebruik van risicoanalyse.
- In 14 procent van de bedrijven worden al penetratietests uitgevoerd. Bij 20 procent bestaan hiervoor plannen.
- 15 procent van de organisaties ziet certificatie als een mogelijk doel.
- Succesvolle informatiebeveiliging begint bij de top.
- Er is een verbetering te constateren in de wijze waarop organisaties met hun traditionele IT-risico's omgaan. In het bijzonder is er een verbetering te constateren in het werken vanuit beveiligingsbeleid en -plannen. Tevens is er verbetering in de afspraken over beveiliging in SLA's, bijvoorbeeld in uitbestedingssituaties. Ook het werken met de Code voor Informatiebeveiliging is de afgelopen jaren sterk toegenomen. Van de grote bedrijven gebruikt nu ongeveer een kwart de Code. Ten opzichte van de vorige meting twee jaar geleden is dat een toename van maar liefst 75 procent.

Referenties

Dit artikel maakt gebruik van de volgende bronnen:

- Code of Practice for Information Security Management (BS7799:1999) / Code voor Informatiebeveiliging (2000), uitgave Nederlands Normalisatie Instituut te Delft of Bestel@nni.nl
- P.L. Overbeek, E. Roos Lindgreen en M.E.M. Spruit, *Informatiebeveiliging onder controle*, Financial Times / Prentice Hall, Amsterdam 2000.
- *ITIL Security Management*, ITIL, 1999.
- P.L. Overbeek en W. Sipman, *Informatiebeveiliging, tweede druk*, Tutein Nolthenius, 1999.
- Websites: http://www.c-cure.org/; http://www.kpmg.nl/irm/

Dr. ir. P.L. Overbeek RE is werkzaam bij KPMG Information Risk Management. Hij is nauw betrokken bij zowel de Engelse als de Nederlandse versie van de Code.