Standaarden en richtlijnen

In november 1994 is de 'Code voor Informatiebeveiliging, een leidraad voor beleid en implementatie' (hierna genoemd de Code) verschenen. Dit document, uitgegeven door het Nederlands Normalisatie Instituut, is een vertaling - en gedeeltelijke aanpassing aan de Nederlandse situatie - van deel 1 van de Britse standaard BS 7799. In de lente van 1999 wordt een revisie van BS 7799 part 1 gelanceerd, welke volgens het NNI tevens zal leiden tot revisie van de Code. Reden om de wijzigingen nader te beschouwen.

Inleiding

BS 7799 is ontwikkeld door het Department of Trade and Industry en wordt uitgegeven door het British Standards Institute. Oorspronkelijk bestond BS 7799 uit slechts één document maar bij het beschikbaar komen van Part 2 werd het oorspronkelijke document bekend onder de naam BS 7799 Part 1.

BS 7799 Part 2 is niet verkrijgbaar in een Nederlandse versie. Dat deel beschrijft het certificatieschema - onder de naam c-cure - zoals in Engeland in 1998 ingevoerd is en geeft aan hoe een organisatie kan kiezen - op basis van risico analyse - welke van de in BS 7799 Part 1 genoemde maatregelen relevant zijn. Het in Nederland door ICIT ontwikkelde certificatieschema maakt geen expliciet deel uit van de Code.

Revisie van BS 7799 Part 1

In 1998 is een project gestart om BS 7799 Part 1 (de gevolgen voor Part 2 worden separaat onderzocht) aan te passen aan de huidige stand van zaken. Een *Draft for Public Comment* is in september 1998 vrijgegeven (het document is voor £ 14,- te bestellen bij BSI); de sluitingsdatum voor het opgeven van wijzigingen was gesteld op 30 november 1998. Zoals hierboven genoemd is vrijgave van de gereviseerde versie voorzien in de lente van 1999.

Revisie noodzakelijk?

Sinds 1994 hebben de ontwikkelingen van informatietechnologie niet stilgestaan. Duidelijke trends waren en zijn het toenemend gebruik van publieke netwerken (vooral Internet) en het feit dat informatie op steeds meer plaatsen voorhanden komt.

Niet langer is de PC immers onze enige client maar we communiceren nu ook met PDA's, GSM telefoons en per voice-mail; er zijn dus ook steeds meer systemen te beveiligen.

Een ander niet onbelangrijk aspect is dat we de laatste jaren steeds meer samenwerkingen aangaan met externe partners zoals consultants, detacherings-bureau's; we besteden steeds meer uit.

Langzamerhand begon BS 7799 en dus ook de Code op de genoemde gebieden gedateerd te raken en werd het dus tijd voor een update.

Vergelijking van Draft en Code

Hoewel BS 7799 goed bruikbaar is in Nederland, is in veel gevallen de Code te prevaleren. De Code is beter leesbaar en veel begrippen rond informatiebeveiliging behoren in het Engels niet tot ieders idioom. Zolang echter de Code nog niet geënt is op de nieuwe versie van BS 7799, is de analyse relevant welke verschillen bestaan tussen de twee documenten.

Samenvatting

Samengevat (hierna worden enkele wijzigingen uitgewerkt) zijn de volgende belangrijkste wijzigingen aangebracht:

- Twee sleutelmaatregelen zijn komen te vervallen; het totaal aantal maatregelen is nu **121**.
- Beveiliging richting derden, bij uitbesteding en bij telewerken krijgt extra aandacht.

- Het belang van risicomanagement wordt meer expliciet vermeld.
- Het begrip ‘computersysteem’ wordt ruimer geïnterpreteerd.
- De maatregel ‘viruscontrole’ wordt uitgebreid naar alle kwaadaardige software.
- Electronic commerce wordt meegenomen inclusief relevante begrippen als non-repudiation.
- Publiek toegankelijke systemen (zoals websites) worden behandeld.
- Encryptie systemen en sleutelmanagement krijgen meer aandacht.
- Wijzigingsbeheer wordt meer expliciet vermeld.
- De tekst m.b.t. het onderwerp continuïteitsplanning, is vrijwel geheel herschreven.
- De problematiek rond het vergaren van bewijslast wordt toegelicht.

> And you all know, security
> Is mortals’ chiefest enemy.
> Shakespeare - Macbeth Act III

De belangrijkste wijzigingen

Hieronder passeren de meest belangrijke verschillen de revue.

Vervallen van sleutelmaatregelen

Meest belangrijke wijziging in de Draft is het vervallen van twee sleutelmaatregelen (welke eerder als essentieel en fundamenteel gezien werden), te weten:

6.3.1 Viruscontrole
10.2.1 De naleving van het beveiligingsbeleid

Hoogstwaarschijnlijk heeft aan het vervallen van de laatstgenoemde maatregel ten grondslag gelegen dat als sleutelmaatregel het belang van het beleidsdocument voor informatiebeveiliging al onderkend wordt en dat naleving in dat geval verondersteld mag worden.

Outsourcing

Een geheel nieuwe paragraaf m.b.t. outsourcing is toegevoegd.

Doelstelling is het handhaven van informatiebeveiliging ondanks het uitbesteden van de verantwoordelijkheid voor de verwerking aan een andere organisatie.

De punten ter opname in een uitbestedingscontract worden genoemd zoals het vastleggen van de beschikbaarheid bij calamiteiten en de eisen te stellen aan fysieke en logische beveiliging.

Kwaadaardige software

De term ‘viruscontrole’ is algemener gemaakt en omvat nu alle kwaadaardige software (‘malicious software’). De richtlijnen zijn gemoderniseerd en beschrijven nu ook email attachments en de gevaren bij het verkrijgen van bestanden uit externe netwerken. Tevens wordt benadrukt het op de hoogte zijn (door vakbladen e.d. te raadplegen) van de verschillen tussen virussen en de zogenaamde ‘hoaxes’ (nep-virussen). Ook het ongewenst propageren van valse informatie (rond nep-virussen) komt aan de orde.

Publieke netwerken

Ten aanzien van publiekelijk toegankelijke systemen (bijvoorbeeld websites) worden richtlijnen gegeven m.b.t. het handhaven van verplichtingen in wetgeving en het schaden van het belang van de organisatie.

Het belang van digitale handtekeningen wordt aangegeven en een viertal punten met betrekking tot de verwerking van invoer vanuit publieke netwerken wordt gegeven (compleetheid, snelheid, beveiliging tijdens transport en het beveiligen van toegang van het publieke systeem naar daaraan gekoppelde systemen).

De paragraaf rond gegevens-encryptie is uitgebreid met enige informatie rond de gangbare ‘geheime sleutel’ en ‘publieke sleutel’ technieken. Enkele voor- en nadelen worden opgesomd, alsmede de rol van een Certification Authority. Termen zoals non-repudiation worden nu toegelicht.

Mobiele computers; telewerken
Een geheel nieuwe paragraaf wordt gewijd aan mobiele computers en telewerkers. De risico's van dergelijke apparatuur door het gebruik in openbare ruimtes en met betrekking tot ontvreemding worden geschetst.

Gewezen wordt op de noodzaak tot het creëren van bewustzijn van deze risico's bij de gebruikers van dit soort apparatuur. Als nieuw beleid dient neergelegd te worden de regels met betrekking tot zenden/ontvangen van gegevens en het maken van back-ups.

Tevens wordt de koppeling tussen deze externe systemen en de kantoorsystemen besproken.

Continuïteitsplanning
Het herschreven hoofdstuk m.b.t. continuïteitsplanning gaat nu dieper in op het feit dat onderkennen van de risico's de eerste stap is en dat continuïteitsplanning niet alleen herstel omvat maar ook minimalisering van de gevolgen. Tevens wordt continuïteitsplanning nu meer beschreven redenerend vanuit de bedrijfsprocessen dan alleen vanuit de IT voorzieningen en de inhoud, het up-to-date houden van een continuïteitsplan en het testen krijgt meer aandacht.

Benodigde aanpassingen aan de Code voor Informatiebeveiliging

Navraag bij het NNI leerde dat men voornemens is, na formalisering van de revisie van BS 7799 Part 1, een vertaling/aanpassing voor Nederland uit te voeren.

Dit zal vermoedelijk resulteren in Versie 2 van de Code voor Informatiebeveiliging.

Dit impliceert aanpassing van het ICIT certificatieschema, alsmede aanpassing van electronische vragenlijsten zoals SecurityPAC van CPA en de Riskette van Coseco. Ook blijft het vraagstuk open welke maatregelen te treffen zijn bij reeds gecertificeerde instanties of voor organisaties die met certificatie trajecten bezig zijn.

Openstaande punten

Hoewel deze revisie van BS 7799 Part 1 het document aanpast aan de stand van zaken zijn toch nog duidelijke omissies aanwezig.

Elke organisatie welke een beveiligingsbeleid wenst te formuleren wordt met dit document in de juiste richting gestuurd maar de desbetreffende paragraaf is nog steeds vrij beknopt. BS 7799 en de Code zijn beide documenten die de lezer vooral aangeven wat er moet gebeuren maar hoe blijft veelal in het duister.

Helaas wordt het proces van het selecteren van de juiste maatregelen slechts aangestipt en niet meer dan dat. Gemist wordt nog steeds de integratie met een product zoals CRAMM of andere kwantitatieve of kwalitatieve risico-analyse methodes.

De leesbaarheid van het document laat te wensen over; zo wordt informatieve tekst afgewisseld met te implementeren maatregelen, soms zelfs in dezelfde alinea. Checklists op basis van de Code (een door het NGI opgestart project) kunnen dit laatste probleem wellicht wegnemen.

Ernst J. Oud is senior consultant bij Getronics Business Continuity BV. Op basis van de Code voor Informatiebeveiliging implementeert hij bij organisaties een integraal informatie-beveiligingsplan gebruikmakend van de projectmethode Integrated Security Methodology (ISM). Een meer gedetailleerd overzicht van de revisie van BS 7799 is te vinden op *http://www.euronet.nl/users/ernstoud/pdf/bs_7799.pdf*