oktober 2010 nummer 6

INFORMATIEBEVEILIGING

Zwichten voor autoriteit

‘Gescoopt’ Risico Management

Rekenen aan Malware

ACTA en netneutraliteit

PvIB
Platform voor InformatieBeveiliging

ib

De internationale normcommissie voor IT-beveiligingstechnieken

De ISO/IEC 27000-serie

Auteur: Jan Rietveld > Jan Rietveld is secretaris van de NEN-commissie IT-beveiligingstechnieken en is bereikbaar via jan.rietveld@nen.nl.

Dit artikel gaat over de normen in de 270xx-serie van de internationale normcommissie JTC 1/SC 27 'IT Security techniques'. Het sluit aan bij het meer algemene artikel over JTC 1/SC 27 dat is verschenen in IB-magazine 7 van november 2009.

Binnen de normcommissie JTC 1/SC 27 'IT Security techniques' werken de werkgroepen 1 en 4 aan de normen in de 270xx-serie. WG 1 richt zich op de normen bedoeld voor het managen van informatiebeveiliging, informatiebeveiliging op beheerniveau (governance niveau) en WG 4 op normen die organisaties helpen bij het implementeren van '270xx-serie'-normen, 'Security controls and services'. De belangrijkste norm in de serie is ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging - Eisen'. Het zogenaamde Information Security Management System (ISMS) waartegen gecertificeerd kan worden. De ontwikkelingen volgen elkaar snel op en daardoor zijn verschillende normen in de revisie, zoals de 27000, de 27001, de 27002 en de 27005.

Vijf normtypen binnen de 270xx-serie

De normen in de 270xx-serie kunnen in vijf groepen worden verdeeld. Hieronder worden deze besproken waarbij soms aandacht wordt gegeven aan een individuele norm als daar aanleiding voor is.

Groep 1: overzicht en woordenlijst (Vocabulary standard)

In deze categorie valt alleen de norm ISO/IEC 27000:2009 'Information security management systems - Overview and vocabulary'. ISO/IEC 27000 is de basis voor de 270xx-serie en geeft een overzicht van de normen in de 270xx-serie en hoe deze zich tot elkaar verhouden. Ondanks dat deze norm pas vorig jaar is verschenen, wordt al aan een revisie gewerkt. Dit komt door de vele (snelle) ontwikkelingen rond informatiebeveiliging wat zich vertaalt in nieuwe normen en revisies van bestaande normen in de 270XX-serie. Het is gewenst het woordgebruik in de verschillende 270xx-normen te harmoniseren en een consistent woordgebruik te bevorderen. ISO/IEC 27000 moet hier richting aan geven. Verder maken de ontwikkelingen het nodig bepaalde tekstdelen te actualiseren. Gezien de dynamiek en ontwikkelingen rond informatiebeveiliging is het de verwachting dat de 27000 de komende jaren vaker moet worden aangepast. Er zijn dan ook voorstellen om de norm om te zetten naar een Standing Document waardoor het aanpassen eenvoudiger wordt.

Een van de commentaren op de huidige 270xx-serie is dat zij erg heterogeen is zonder duidelijke basis of leidende principes. De normen zijn op basis van behoefte ontstaan. Geprobeerd wordt in de herziene 27000 een duidelijk en eenduidig raamwerk op te nemen dat als basis kan dienen voor de hele 270xx-serie.

ISO/IEC 27000 is gratis te downloaden. Zie de informatie aan het einde van dit artikel.

Groep 2: normen met eisen (Requirements standards)

In deze categorie valt de belangrijkste norm van de serie, ISO/IEC 27001 'Managementsystemen voor informatiebeveiliging - Eisen'. Deze norm is in 2005 gepubliceerd en wordt op het moment herzien. Er zijn tientallen commentaren voor verbeteringen en aanpassingen binnengekomen. Zo ligt er een voorstel om in de norm duidelijk aan te geven wat de relatie is met het Capability Maturity Model (CMM) en dat de norm alleen van belang is voor organisaties die minimaal CMM niveau 3 hebben bereikt. Bepaalde termen moeten duidelijker worden gedefinieerd en sommige termen worden uit deze norm verwijderd om te worden opgenomen in de 27000. Verder wordt nader gekeken naar het gebruik van de termen 'asset' en 'information asset' en naar de termen 'risk evaluation criteria' en 'risk acceptance criteria' die tot verwarring kunnen leiden. Geconstateerde onduidelijkheden worden weggewerkt en er wordt geprobeerd het taal- en woordgebruik te harmoniseren met NEN-EN-ISO 9000 'Kwaliteitsmanagementsystemen -Grondbeginselen en verklarende woordenlijst' en NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen'. Verder liggen er voorstellen om de tekst duidelijker en eenduidiger te maken en verdubbelingen en overbodige toevoegingen te verwijderen. Dit natuurlijk naast het corrigeren van typos. In oktober 2010 wordt in Berlijn vergaderd over de nieuwe versie van deze norm. Het streven is dat de nieuwe versie in 2011 verschijnt.

Zoals misschien bekend, is de 27001 een managementsysteemnorm. In het Engels wordt gesproken van Management System Standard (MSS). Bekende MSS-normen zijn NEN-EN-ISO 9001 'Kwaliteitsmanagementsystemen - Eisen' en NEN-EN-ISO 22000 'Eisen aan een organisatie in de voedselketen'. ISO werkt aan een systeem om alle MSS-normen beter op elkaar af te stemmen door ze op dezelfde wijze te structureren, daar waar mogelijk gelijke tekst te gebruiken en door het gebruik van dezelfde terminologie en definities. De termen moeten aansluiten bij NEN-EN-ISO 19011 'Richtlijnen voor het uitvoeren van kwaliteits- en/of milieumanagementsysteemaudits' en NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen'. Door de MSS-normen te harmoniseren moet een geïntegreerd gebruik ervan worden geoptimaliseerd. De nieuwe structuur heeft als titel meegekregen High Level Structure (HLS).
Voor bedrijven is deze harmonisatie van belang om meer efficiënt en effectief te kunnen werken. Door met de ISO/IEC 27001 aan te sluiten bij de HLS wordt de kwaliteit ervan verhoogd en sluit hij beter aan bij andere managementnormen waardoor bijvoorbeeld

het gecombineerd auditen op de 9001 en 27001 eenvoudiger wordt.
De markt vraagt om geïntegreerde management systemen. De NEN-commissie Informatie- en archiefmanagement kijkt al naar het gezamenlijk toepassen van de MSS-normen NEN-ISO/IEC 27001, NEN-EN-ISO 9001 en ISO NEN-ISO 15489-1 'Informatie- en archiefmanagement - Deel 1: Algemeen'. Binnenkort verschijnt een Nederlandse Praktijk Richtlijn (NPR) waarin beschreven wordt hoe deze drie normen samen toegepast kunnen worden, NPR 2083 'De geïntegreerde toepassing van ISO- en ISO/IEC-normen in de informatiehuishouding'.

ISO/IEC 27006 'Requirements for bodies providing audit and certification of information security management systems' is de norm waarmee organisaties kunnen worden geaccrediteerd zodat ze tegen de 27001 mogen certificeren. De 27006 is gebaseerd op en in lijn met ISO 17021-1 die beschrijft waar certificerende instellingen aan moeten voldoen. Van ISO 17021 is een revisie verschenen en ISO/IEC 27006 moet in overeenstemming worden gebracht met deze nieuwe versie. Echter, hoewel de verantwoordelijke ISO-experts voor een revisie zijn, hebben de normalisatie-instituten van de verschillende landen hier nog geen eenduidig besluit over genomen. Of er een revisie komt wordt waarschijnlijk tijdens de eerder genoemde vergadering in oktober in Berlijn besloten.

Groep 3: richtlijnen (guidelines standards)

Het betreft hier richtlijnen voor het toepassen van de eisen uit de voorgaande groep. Op het moment zijn er acht normdocumenten die onder deze categorie vallen waarvan NEN-ISO/IEC 27002 'Code voor informatiebeveiliging' de bekendste is. Ook deze norm wordt herzien. Er zijn ruim 700 commentaren binnengekomen waarvan meer dan 600 inhoudelijk van karakter. Gepland is dat de nieuwe versie eind 2012 verschijnt.

ISO/IEC 27005 'Information security risk management' wordt ook herzien. Gekozen is voor een korte revisieronde waarin de norm wordt aangepast aan NEN-ISO 31000 'Risicomanagement - Principes en richtlijnen' en aan Guide 73 'Risicomanagement - Verklarende woordenlijst'. Er staan geen grote technische aanpassingen op stapel.

De andere normdocumenten zijn:
NEN-ISO/IEC 27003 'Information security management system implementation guidance', een richtlijn die de 27001 ondersteunt.
NEN-ISO/IEC 27004 'Information security management - Measurement', bedoeld om het effect te meten van de implementatie van de 27001.
Deze beide normen zijn gepubliceerd. Daarnaast zijn nog vier normen in ontwikkeling:
ISO/IEC 27007 'Guidelines for information security management systems auditing', gepland voor eind 2011.
ISO/IEC 27008 'Guidance for auditors on information security management systems controls', gepland voor mei 2012.
ISO/IEC 27013 'Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001', gepland voor eind 2012.
ISO/IEC 27014 'Information security governance framework', gepland voor eind 2012.

Groep 4: sector specifieke eisen en richtlijnen (sector-specific requirements/ guidelines standards)

De hiervoor genoemde normen zijn algemeen toepasbaar. Echter, er zijn normen die zich specifiek richten op informatiebeveiliging binnen een bepaalde sector. Initiatieven voor deze sector specifieke normen zijn soms genomen binnen de normcommissie Informatiebeveiliging en hebben een nummer in de 270xx-serie. Hieronder een overzicht:

ISO/IEC 27010 'Information security management for inter-sector and inter-organisational communications' voor communicatie en samenwerking tussen de publieke en/of private sector. De norm is in ontwikkeling en wordt waarschijnlijk afgerond in november 2012.
NEN-ISO/IEC 27011 'Information security management guidelines for telecommunications organizations based on ISO/IEC 27002'. Deze is reeds gepubliceerd en in 2011 wordt gekeken of hij herzien moet worden.
ISO/IEC 27015 'Information security management guidelines for financial and insurance services'. Deze norm wordt ontwikkeld in samenwerking met de ISO-commissie Financiële diensten (ISO/TC 68). Verwacht wordt dat hij eind 2012 wordt gepubliceerd.

Een sector specifieke richtlijn kan ook zijn oorsprong hebben binnen een sector specifieke ISO-commissie. Echter, bij deze normen is vaak gebruik gemaakt van normen uit de 270xx-serie. Een overzicht:
NEN-EN-ISO 27799 'Informatiebeveiligingsmanagement in de gezondheidszorg volgens ISO/IEC 27002'. Deze norm is ontwikkeld door ISO/TC 215 'Health informatics'. De revisie van NEN 7510 die voorjaar 2011 verschijnt, is gebaseerd op de 27799 en de 27002.

Verder kan genoemd worden NEN-ISO/TR 13569 'Financiële diensten - Leidraad voor de beveiliging van informatie. Deze TR (Technical Report, dus géén norm) is door ÍSO/TC 68 gemaakt.

Groep 5: maatregel-specifieke richtlijnen (control-specific guideline standards)

Op het moment wordt in deze serie aan zes normen gewerkt. Ter informatie, een norm kan uit verschillende delen bestaan. NEN-ISO/IEC 27033 'Network security' is hier een voorbeeld van. Deel 1, 'Overview and concepts' is verschenen. Er zijn drie delen in ontwikkeling. Deel 2,'Guidelines for the design and implementation of network security', deel 3, 'Reference networking scenarios - Threats, design techniques and control issues' en deel 4, 'Securing communications between networks using security gateways - Threats, design techniques and control issues'. Besloten is deze norm met nog drie delen uit te bereiden, voor 'Virtual private networks'. Voor 'IP convergence' en een voor 'Wireless networks'. De komende maanden worden de eerste voorstellen voor deze drie nieuwe delen doorgenomen door de nationale normcommissies.
In de laatste ontwikkelfase is ISO/IEC 27031 'Guidelines for ICT readiness for business continuity'. Verder wordt gewerkt aan ISO/IEC 27034 'Application security', een norm in vijf delen. Verwacht wordt dat deel 1, 'Overview and concepts' eind 2011 wordt gepubliceerd, de vier andere delen in 2013. ISO/IEC 27035 'Information security incident management' wordt ook eind 2011 verwacht.
Tot slot, er wordt onderzocht of er behoefte is aan een norm voor 'ICT Supply chain security'.

Mogelijke toekomstige onderwerpen in de 270xx-serie

Er wordt natuurlijk nagedacht over hoe de 27001 verder te ondersteunen en kracht bij te zetten. Zo wordt er gesproken over een norm voor 'Monitoring and review' van interne procedures, voor 'Continual improvements' en voor een management review norm. Verder wordt gedacht aan een norm voor informatiebeveiliging van het midden- en kleinbedrijf (MKB) en 'home users' op basis van de 27001: hoe kan een MKB-bedrijf een ISMS opzetten en onderhouden? Er is nog geen concreet voorstel maar er is de intentie om er aan te gaan werken.

Tot slot

De commissie 'IT beveiligingstechnieken' van het Nederlands Normalisatie-instituut (NEN) werkt mee aan de normen van JTC 1/SC 27. Heeft u suggesties voor aanvullingen en/of

De internationale normcommissie voor IT-beveiligingstechnieken

commentaar inzake een van de genoemde normen? Neemt u dan contact op met de secretaris van de commissie.

Ter informatie

Voor informatie over de NEN-commissie kunt u contact opnemen met de secretaris van de commissie: Jan Rietveld, e-mail: jan.rietveld@NEN.nl, telefoonnummer (0156) 26 90 376.

Informatie over de documenten van de normcommissie vindt u via Technical Committees op de ISO-website: www.iso.org.

Informatie over de NEN-commissie vindt u op www.nen.nl/IT-beveiligingstechnieken.

Sommige 'ISO/IEC JTC 1/SC 27'-normen zijn kosteloos beschikbaar via: http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.

Geprinte versies van deze normen kunt u via NEN.nl bestellen.

Het artikel uit IB-magazine 7 (novembernummer van 2009) is te downloaden als PDF op de website van PvIB: https://www.pvib.nl/download/?id=13614545&download=1.

Overzicht van de normen die verschenen zijn en die in ontwikkeling zijn.

ISO/IEC	Publicatie-jaar	Titel	Status
27000	2009	Overview and vocabulary	Gepubliceerd
27001	2005	Requirements	Gepubliceerd
27002	2005	Code of practice for information security management	Gepubliceerd
27003	2010	Information security management system implementation guidance	Gepubliceerd
27004	2009	Information security management - Measurement	Gepubliceerd
27005	2008	Information security risk management	Gepubliceerd
27006	2007	Requirements for bodies providing audit and certification of information security management	Gepubliceerd
27007		Guidelines for information security management systems auditing	In ontwikkeling
27008		Guidelines for auditors on information security management systems controls	In ontwikkeling
27010		Information security management for intersector and inter-organisational communications	In ontwikkeling
27011	2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Gepubliceerd
27013		Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001	In ontwikkeling
27014		Information security governance framework	In ontwikkeling
27015		Information security management guidelines for financial and insurance services	In ontwikkeling
27031		Guidelines for ICT readiness for business continuity	In ontwikkeling
27032		Guidelines for cybersecurity	In ontwikkeling
27033-1	2009	Network security - Part 1: Overview and concepts	Gepubliceerd
27033-2		Network security - Part 2: Guidelines for the design and implementation of network security	In ontwikkeling
27033-3		Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues	In ontwikkeling
27033-4		Securing communications between networks using security gateways - Threats, design techniques and control issues	In ontwikkeling
27033-5		Network security - Part 5: Securing communications across networks using Virtual private Network (VPNs) - Threats, design techniques and control issues	In ontwikkeling
27033-6		Network security - Part 6: IP convergence	In ontwikkeling
27033-7		Network security -Part 7: Wireless	In ontwikkeling
27034-1		Application security - Part 1: Overview and concepts	In ontwikkeling
27034-2		Application security - Part 2: Organization normative framework	In ontwikkeling
27034-3		Application security - Part 3: Application security management process	In ontwikkeling
27034-4		Application security - Part 4: Application security validation	In ontwikkeling
27034-5		Application security - Part 5: Protocols and application security controls data structure	In ontwikkeling
27035		Information security incident management	In ontwikkeling
27036		Guidelines for security of outsourcing	In ontwikkeling
27037		Guidelines for identification, collection and/or acquisition and preservation of digital evidence	In ontwikkeling
27038		Specification for digital redaction	In ontwikkeling