Op veel deelgebieden binnen de informatiebeveiliging zijn er zowel nationaal als internationaal beveiligingstandaarden aanwezig of in ontwikkeling. We kennen inmiddels de Code of Practice, CvI en VIR, en sinds 1999 Common Criteria en ITIL Security Management. De grote, brede standaarden vinden slechts aarzelend ingang, maar dat zou met ITIL wel eens kunnen gaan veranderen. Wat het detailniveau betreft, wemelt het van de veelgebruikte standaarden, onder andere door het succes van netwerken en Internet. We hebben ze zo goed en zo kwaad als het kan voor u op een rij gezet.

GEEN SECURITY ZONDER IJKING
EEN BIJNA UITPUTTEND OVERZICHT

Door: Saïd EI Aoufi en Paul Peursum

Standaardisatie biedt vele voordelen, zowel voor leveranciers als voor afnemers van producten. Er is een grote markt voor producten die gebaseerd zijn op standaarden, omdat deze producten breder toepasbaar zijn en eenvoudiger in te passen in andere producten. Immers, met
behulp van standaardisatie kunnen ongelijksoortige systemen met elkaar worden gekoppeld, denk maar aan systemen in een netwerkomgeving.
In dit artikel besteden we allereerst aandacht aan nationale en internationale organisaties voor standaardisatie en normalisatie. Vervolgens geven we een overzicht van een aantal bekende gebruikte standaarden.

1 NATIONALE EN INTERNATIONALE ORGANISATIES

Nationaal, Europees en internationaal is een aantal organisaties actief op het gebied van standaardisatie en normalisatie. Ondersteund door nationale normalisatie-instituten als het Nederlands Normalisatie Instituut (NNI) nemen veel bedrijven in Nederland deel aan het standaardisatiewerk. Duizenden experts uit de hele wereld zijn lid van nationale en internationale standaardisatiecommissies en -werkgroepen. Per jaar neemt de
productie van normen voorlopig alleen maar toe.

Standaardisatie in Nederland

Het Nederlands Normalisatie-instituut (NNI) te Delft is de nationale normalisatie-instelling voor Nederland. Het Nederlands Elektrotechnisch Comité (NEC) is voor Nederland verantwoordelijk voor normalisatie op het gebied van elektrotechniek, informatietechnologie en telecommunicatie.

Europese standaardisatie

Aan de Europese standaardisatie wordt gewerkt door de Europese normalisatie organisaties Comité Européen de Normalisation (CEN), Comité Européen de Normalisation Electrotechnique (CENELEC) en de European Telecommunication Standards Institute (ETSI). Deze drie organisaties zijn de drie officiële, formele normalisatie-instituten in Europa. Specifiek voor de standaardisatie van Open Systemen bestaat er nog een vierde organisatie in Europa: de European Workshop for Open Systems (EWOS).

Internationale standaardisatie

Internationaal bestaan er de volgende instituten op het gebied van standaardisatie en normalisatie: de International Organization for Standardization (ISO), de International Electrotechnical Commission (IEC) , de American National Standards Institute (ANSI).
Ander voorbeelden van bekende normeringinstituten zijn: de Comité Consultatief International Télégraphique et Téléphonique (CCITT), de National Institute of Standards and Technology (NIST), de United Nations (UN), het Institute of Electrical and Electronics Engineers (IEEE).

2 BEKENDE 'BREDE' STANDAARDEN

Hieronder geven we enkele bekende en veel gebruikte standaarden op nationaal, Europees en internationaal niveau die op meer algemeen niveau binnen informatie-beveiliging worden gebruikt. Merk op dat dit geen complete opsomming is, er zijn in de markt nog veel meer standaarden te vinden.

Code of Practice (BS7799)

Sinds enige tijd bestaat er een praktijkgerichte houvast voor het opzetten, invoeren en evalueren van informatiebeveiligingsmaatregelen. Deze leidraad heet de British Standard 7799 'Code of Practice for Information Security Management'. Het document is in het Nederlands vertaald. De vertaling staat bekend onder de naam 'Code voor Informatiebeveiliging'.

BS7799 beschrijft maatregelen voor informatiebeveiliging die zich bij tal van organisaties in de praktijk hebben bewezen. De doelstelling van BS7799 is tweevoudig, namelijk:
1 - het beschikbaar stellen van 'best practices' op het gebied van informatiebeveiliging; en
2 - het bevorderen van vertrouwen tussen de organisaties.
Om er zeker van te zijn dat blijvend aan de afspraken op basis van BS 7799 tegemoet wordt gekomen, kunnen
organisaties een bewijs van hun handelspartner verlangen. Dat bewijs is een erkend certificaat door een onafhankelijke certificatie-instelling waarop vermeld staat dat aan BS 7799 wordt voldaan. In Nederland wordt het certificatietraject uitgevoerd door KEMA en KPMG.

De BS7799 is inmiddels ook als internationale norm

Kan ITIL Security Management beveiliging op vele agenda's krijgen ?

bekend: ISO 17799.

Code voor Informatiebeveiliging (ook wel aangeduid als CvI of zelfs als 'de Code') is een uitgave van het Nederlands Normalisatie-instituut (NNI) in samenwerking met het Ministerie van Economische Zaken.
Meer informatie: Nederlandse Normalisatie-instituut (tegenwoordig NEN), telefoon: 015-2690 390, Internet: www.nen.nl.

Voorschrift Informatiebeveiliging Rijksdienst (VIR)

Het VIR biedt een kader op strategische niveau voor invoering van informatiebeveiliging langs de managementcyclus van beleid, planning, uitvoering en controle. VIR wordt binnen de rijksoverheid of daarbuiten gebruikt. De uitwerking van het VIR heeft plaatsgevonden in het 'Handboek Informatiebeveiliging Rijksdienst' dat ter ondersteuning van de inspanningen binnen de rijksdienst wordt aangereikt. Informatie is te verkrijgen bij het ACIB, dat valt onder de afdeling Infrastructuur en Continuïteit van de Directie Informatievoorziening Openbare Sector van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
Meer info: Advies- en Coördinatiepunt Informatiebeveiliging (ACIB), tel.: 070-302 6763, Internet: www.minbzk.nl/acib of e-mail: acib@minbzk.nl

Memorandum van De Nederlandsche Bank

Voluit 'Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen' geheten, is toegezonden aan alle banken in Nederland. De achtergrond van het memorandum is dat DNB als toezichthoudende instantie meer expliciet wenst te worden geïnformeerd over de wijze waarop
banken omgaan met betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. In het memorandum worden verantwoordelijkheden hieromtrent geformuleerd en worden aandachtspunten inzake beveiliging en interne controle gegeven.
Meer info: De Nederlandsche Bank, tel.: 020-524 9II1, Internet: www.dnb.nl

COBIT

Control Objectives for Information and related Technology (COBIT) voorziet een raamwerk van IT-controleobjectieven die men kan invoeren en beheren binnen een onderneming om de levering van betrouwbare informatie te verzekeren. Het omvat algemeen toepasbare en aanvaarde internationale standaarden voor goed IT-management en controle. De principes kunnen toegepast worden op elk platform en binnen elke bedrijfsomgeving. Voor meer informatie moet men bij Isaca zijn:
ISACA, 3701 Algonquin Road, Suite 1010, Rolling Meadows, Illinois 60008 USA, tel.: +1 847 253 1545, Internet: www.isaca.org/cobit.htm

ITIL

ITIL staat voor Information Technology Infrastructure Library. ITIL is een procesgerichte benadering voor IT-beheer. Beveiligingsmanagement is sinds vorig jaar één van de processen van ITIL. Het ITIL-proces Security Management geeft de structurele inpassing van beveiliging in de beheerorganisatie. Security Management is mede gebaseerd op de Code voor Informatiebeveiliging. Het doel van dit proces is tweeledig: het realiseren van de beveiligingseisen in de verschillende Service Level Agreements en het realiseren van een basisniveau aan beveiliging. ITIL wordt vooral in Engeland en Nederland bij vele organisaties geïmplementeerd.

3 EDI-STANDAARDISATIE

Electronic Data Interchange (EDI) standaarden hebben onder andere betrekking op: communicatiemodellen, gegevens uitwisseling (berichten, begrippen, classificatie- en codestelsels) en communicatietechnologie. De Verenigde Naties (VN) zijn actief op het gebied van standaardisatie van EDI. Een EDI-standaard op beveiligingsgebied is Edifact (EDI For Administration, Commerce and Transport). Op basis hiervan is een groot aantal berichten opgesteld. In directories zijn verzamelingen van berichten opgenomen met alle dataelementen, segmenten, codes en gebruiksaanwijzingen. Meer info: http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/index.asp.

4 TEST- EN EVALUATIESTANDAARDEN

Op de markt zijn er specifieke standaarden voor het testen en evalueren van producten. De bekendste standaarden hiervoor zijn TCSEC, ITSEC en Common Criteria.

TCSEC

Voor 1985 was IT-beveiliging voornamelijk een ambachtelijke zaak. Hierin kwam verandering toen de Amerikaanse overheid in 1985 de Trusted Computer Systems Securiry Evaluation Criteria (DOD 5200.28-STD), vanwege de kleur van de kaft ook wel het Orange Book genoemd, publiceerde. Dit document gaf een aantal niveaus van beveiliging en de criteria waaraan een
systeem moest voldoen om beveiliging volgens dit niveau te bieden. Deze niveaus (C1, C2, B1, B2, B3, A1) gaven exact aan wat voor functionaliteit het systeem moest bezitten en hoe dat gecontroleerd moest worden. De Amerikaanse overheid gebruikte het Orange Book om de beveiligingseisen in de overheid vast te leggen.

ITSEC

De Europese overheid presenteerde Europese beveiligingsevaluatiecriteria: de ITSEC (Information Technology Security Evaluation Criteria), samengesteld door Engeland, Frankrijk, Duitsland en Nederland. Deze standaard zou ten eerste elk land de vrijheid geven beveiligingsevaluaties van producten onder eigen beheer uit te voeren en anderzijds voldoende richtlijnen geven om certificaten uitgegeven in het ene land ook in het andere land te erkennen (wederzijdse erkenning).

Common Criteria

Op initiatief van in eerste instantie de Europese Commissie en de landen betrokken bij de TCSEC, FC (Federal Criteria, een NIST-product dat niet is gepubliceerd), CTCPEC (een Canadese standaard) en de ITSEC zijn er beveiligingsevalutiecriteria geproduceerd, genaamd de Common Criteria (CC). Doel van de Common Criteria is hierbij duidelijk om enerzijds de grenzen te verleggen en anderzijds de beste kanten van het Orange Book, FC, CTCPEC en ITSEC te combineren. Randvoorwaarde is dat de Common Criteria wederzijdse erkenning van resultaten mogelijk moet maken. Informatie onder andere bij www.sevenlocks.com/papers/PapersEvaluati.htm.

5 ISO EN ANSI

De International Standardization Institute (ISO) heeft een ontwerp gemaakt van een netwerk voor het aan elkaar koppelen van producten van verschillende leveranciers. Dit netwerk wordt het Open Systems Interconnection (OSI)-referentiemodel genoemd. Voor beveiliging is de beveiligingsarchitectuur (OSI-Security Architecrure) ontwikkeld. Hierin wordt onderscheid gemaakt naar beveiligingsdiensten (security services) en beveiligingstechnieken (Security mechanisms or techniques) en de plaats binnen de zeven lagen waar de beveiliging aangeboden wordt.

De afgelopen jaren is standaardisatie voortdurend een onderwerp van discussie geweest.

ISO-standaarden

Er zijn door de jaren heen verschillende ISO-standaarden ontwikkeld. Voorbeelden zijn:

- ISO 8730, geeft aan hoe banken hun onderling verkeer kunnen beschermen;
- ISO 8732, geeft aan hoe het sleutelmanagement geregeld dient te worden te behoeve van de berichruitwisseling;
- ISO 10202, behandelt de beveiligingsaspecten van betaaltransacties, waarbij gebruik gemaakt wordt van IC-kaarten, of meer specifiek smartcards.

Inlichtingen via: www.iso.ch

ANSI-standaarden

American National Standards Institute (ANSI) kent op het gebied van beveiliging ook een reeks standaarden. Voorbeelden hiervan zijn:

- X3.92: Data Encryption Algorithm;
- X3.105: Information System-Data Link Encryption;
- X3.106: Information System- Data Link Encryption Modes of Operation.

Kijk voor meer informatie bij: web.ansi.org

6 CRYPTOGRAFIE EN PROTOCOLLEN

Er zijn inmiddels al vele cryptografische algoritmen in vele toepassingen 'standaard' opgenomen. Voorbeelden van dergelijke algoritmen zijn:

Data Encryption Standard (DES)

DES is een symmetrische algoritme en wordt wereldwijd toegepast, vooral in de bankwereld. De algoritme werkt op blokken van 64 bits en gebruikt een sleutel van 56 bits. DES wordt, mede door zijn snelheid, breed gebruikt voor de beveiligde opslag en transport van data.

International Data Encryption Algorithm (IDEA)

IDEA is een symmetrische algoritme die net als DES wereldwijd wordt gebruikt. De algoritme werkt op blokken van 64 bits en gebruikt een sleutel van 128 bits. Een
belangrijke toepassing van IDEA is het e-mailpakket PGP.

Rivest Shamir AdIeman (RSA)

RSA is de meest gebruikte asymmetrische algoritme, veelal gebruikt voor het zetten van digitale handtekeningen en sleuteltransport.

Digital Signature Standard (DSS)

DSS wordt gebruikt voor het zetten van digitale handtekeningen.

Message Digest algoritmen (MDx) en Secure Hashing Algorithm (SHA)

MD2, MD4, MD5 zijn Hashing-algoritmen die alle resulteren in een 128-bit hash en daarvan afgeleid de SHA met een 160-bit hash.

Met betrekking tot cryptografische protocollen noemen we de volgende:

Secure Shell (SSH)

Dit protocol wordt voor telnet- en ftp-sessies gebruikt.

Secure Sockets Layer (SSL)

Protocol om een beveiligde verbinding tot stand te brengen. Zie: www.netscape.com

Secure HTTP (S-HTTP)

Protocol om een beveiligde verbinding tot stand te brengen.

Het voornaamste verschil tussen SSL en S-HTTP is dat bij SSL een veilige verbinding tot stand wordt gebracht, waarover dan pagina's worden opgehaald, en bij S-HTTP zijn de verzoeken en de antwoorden elk afzonderlijk
versleuteld.

IP Security protocol (IPSec)

IPSec zorgt ervoor dat bij de 'low level' IP-pakketten die tussen systemen worden uitgewisseld via een onveilig netwerk de beveiligingsdoelen vertrouwelijkheid, authenticiteit en integriteit wordt gewaarborgd.

Public Key Cryptograhpic Standards (PKCS)

Dit zijn Public Key Encryption Standaarden van RSA Data Security.

Sites die een goed overzicht geven van de genoemde cryptografische protocollen zijn:
www.rsasecurity.com (protocollen in het algemeen);
www.ipsec.com (voor IPSec);
www.ssh.org (voor SSH).

Secure Electronic Transactions (SET)

De SET-specificatie, vrijgegeven in juni 1996, gebruikt encryptietechnieken voor het veiligstellen van de privacy en voor het aan kopers- en aanbiederszijde garanderen van de juiste identiteit.

IEEE 802.11

Protocol standaard voor draadloze (wireless) LAN-producten.

Point-to-Point Tunneling Protocol (PPTP)

PPTP wordt gebruikt voor het creëren van VPN Internetcommunicatie en werkt op de IP-laag.

Secure MIME (S/MIME)

S/MIME zorgt voor een veilige transport, opslag van 'gevoelige' data op applicatielaag.

X.500-standaarden

X.500 is een verzameling van ISO/ITU-T standaarden. Deze standaarden beschrijven de verschillende modellen en protocollen die nodig zijn om een directory service te maken. De in 1988 voor het eerst uitgegeven X.500-standaard omvat verschillende onderdelen. Een bekend
onderdeel is de X.509, het Authentication Framework, dat beschrijft hoe de directory gebruikt kan worden voor het verifiëren van de identiteit van partners in het netwerk.

7 TOT BESLUIT

De afgelopen jaren is standaardisatie voortdurend een onderwerp van discussie geweest. Standaardisatie biedt voor verschillende groepen voordelen. De gebruikers kunnen gezamenlijk een nieuwe technologie benutten als dit gebruik uitwisselbaar is en de leveranciers kunnen hun producten makkelijker op de markt afzetten als er standaardisatie is gebruikt. Belangrijk is dat de
Nederlandse bedrijven in moeten spelen op wat internationaal op het gebied van standaardisatie gebeurt. Zij zullen de internationale ontwikkelingen nauwkeurig moeten volgen en zo op de hoogte zijn van de nieuwe trends.

De auteurs

Drs. ing. Saïd EI Aoufi is consultant bij MetaPoint BV en ing. Paul Peursum is Managing ICT Architect bij More-Secure Consultants BV.

Dit artikel is eerder verschenen in Informatiebeveiliging Praktijkjournaal (huisorgaan van het GVIB), jaargang 3, nummer 2, maart 2000, Ten Hagen Stam Uitgevers.

Contact:

More-Secure B.V.
Da Costalaan 14
3768 GH SOEST
T: +31 (0)35-6018457 | M : +31 (0)6-5357 9338
E: info@more-secure.nl | W: www.more-secure.nl