BEST PRACTICE

BASISKENNIS INFORMATIE-BEVEILIGING

OP BASIS VAN ISO27001 EN ISO27002

2de herziene druk

Hans Baars | Jule Hintzbergen
Kees Hintzbergen | Andre Smulders

Van Haren PUBLISHING

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002
Tweede herziene druk

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over Best Practices, methodes en standaarden op het gebied van de volgende domeinen:

- IT en IT-management;
- Enterprise-architectuur;
- Projectmanagement, en
- Businessmanagement.

Deze uitgaven zijn beschikbaar in meerdere talen en maken deel uit van toonaangevende series, zoals *Best Practice, The Open Group series, Project management* en *PM series.*

Op de website van Van Haren Publishing is in de **Knowledge Base** een groot aanbod te vinden van whitepapers, templates, gratis e-books, docentenmateriaal etc. Ga naar www.vanharen.net.

Van Haren Publishing is tevens de uitgever voor toonaangevende instellingen en bedrijven, onder andere: Agile Consortium, ASL BiSL Foundation, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen per domein zijn:

IT en IT-management
ABC of ICT™
ASL®
CATS CM®
CMMI®
COBIT®
e-CF
ISO 17799
ISO 20000
ISO 27001/27002
ISPL
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA

Architecture (Enterprise en IT)
ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Business Management
BABOK® Guide
BiSL®
BRMBOK™
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
Novius B&IP
OPBOK
SAP
SixSigma
SOX
SqEME®

Project-, Programma- en Risicomanagement
A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
PRINCE2®

Voor een compleet overzicht van alle uitgaven, ga naar onze website: www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Basiskennis informatiebeveiliging

op basis van ISO27001 en ISO27002

2de herziene druk

Hans Baars
Jule Hintzbergen
Kees Hintzbergen
André Smulders

Van Haren PUBLISHING

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Colofon

Titel:	Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002 - Tweede herziene druk
Auteurs:	Hans Baars, Jule Hintzbergen, Kees Hintzbergen, André Smulders
Reviewers van de Engelstalige versie:	Norman Crocker (Cronos Consulting) Steven Doan (Schlumberger, USA) James McGovern (The Hartford) Prof. Pauline C. Reich (Waseda University School of Law) Bernard Roussely (Cyberens Technologies & Services) Tarot Wake (Invictus Security) John van Huijgevoort (NL versie)
Tekstredactie:	Harry Ousen
Uitgever:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Hard copy:	978 94 018 0013 6
ISBN eBoek:	978 94 018 0543 8
Druk:	Tweede druk, eerste oplage, december 2015 Tweede druk, tweede oplage, oktober 2016
Redactie en zetwerk:	CO2 Premedia, Amersfoort
Copyright:	© Van Haren Publishing, 2010, 2015

Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net.

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, of op welke wijze ook, zonder voorafgaande schriftelijke toestemming van de uitgever.

Trademarks:
COBIT® is a Registered Trade Mark of the Information Systems Audit and Control Association (ISACA) / IT Governance Institute (ITGI).
ITIL® is a Registered Trade Mark of AXELOS.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Woord vooraf

Het woord beveiliging (security) heeft voor veel mensen een negatieve connotatie. Beveiliging wordt immers alleen toegepast als daar een reden voor is, namelijk wanneer er risico's bestaan dat dingen niet zullen gaan zoals ze moeten gaan. Afgaand op de vele berichten in de media, lijkt het wel of de informatiebeveiliging het grootste punt van zorg is. Iedereen kent de berichten waar aandacht wordt besteed aan ICT-beveiligingslekken, hacking, enz. Ook nieuwe onderwerpen als Cloud computing, Internet of Things en Big data brengen nieuwe risico's met zich mee die ook de pers halen. Onze maatschappij gaat meer en meer naar een informatiegestuurde maatschappij en daarmee nemen beveiligings- en privacy risico's toe als er niet goed vanaf het begin wordt nagedacht over beveiliging.

In dit boek worden veel onderwerpen over informatiebeveiliging op een zo eenvoudig mogelijke manier besproken, want informatiebeveiliging is ieders verantwoordelijkheid, hoewel veel mensen zich dat vaak niet realiseren. Ook wordt duidelijk gemaakt dat informatiebeveiliging niet nieuw is, de bron ervan ligt al vele eeuwen achter ons. Bovendien wordt de laatste jaren bij fysieke beveiliging steeds meer ICT-technologie toegepast. Voorbeelden zijn fysieke toegangscontrolesystemen en (IP-)camerasystemen.

Het boek is bedoeld voor iedereen die iets met informatiebeveiliging te maken heeft en voor diegenen die gewoon wat meer kennis over dit onderwerp willen opdoen. En bovenal is het boek bedoeld als studieboek voor het examen *Information Security Foundation based on ISO/IEC 27002* (ISFS) van EXIN. Achterin het boek is dan ook een voorbeeldexamen van ISFS opgenomen zodat ook de lezer de kennis die opgedaan wordt met het doornemen van dit boek direct zelf kan toetsen.

Eind 2009 verscheen de eerste druk van de Engelstalige versie van het boek, de eerste druk van de Nederlandse vertaling verscheen in 2011. In deze tweede druk is een groot aantal verbeteringen doorgevoerd, met name gerelateerd aan de herzieningen en uitbreidingen van de ISO/IEC 27002 norm.
Behalve aan de fysieke beveiligingsmaatregelen en de technische IT-aspecten wordt dus ook aandacht besteed aan organisatorische beveiligingsmaatregelen en de

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

communicatie- en operationele procedures die noodzakelijk zijn voor een effectief risicomanagement binnen een organisatie.
Aangezien de oorspronkelijke Engelstalige uitgave de bron is voor deze uitgave, wordt ingegaan op de internationale wet- en regelgeving, en niet alleen op de wetgeving in Nederland en België.

De organisatie van Informatiebeveiliging Professionals in Nederland (PvIB) beveelt dit boek aan als een goede start in de wereld van informatiebeveiliging.

De auteurs
December 2015

.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Dankwoord

Voor deze Nederlandse vertaling van de tweede druk van ons boek Information Security Foundation willen we een speciale dank laten uitgaan naar onze uitgever Van Haren Publishing vanwege de nimmer aflatende ondersteuning die we van hen ontvangen alsmede voor alle werkzaamheden die zij uitvoeren om ervoor te zorgen dat ook deze uitgave weer bij de lezers terecht komt in de kwaliteit die wij voor ogen hebben.

Ook willen we van harte onze dank uitspreken aan Gerard Heimans van de Informatiebeveiligingsdienst voor gemeenten (IBD) die ons geholpen heeft met de vertaling van het Engels naar het Nederlands van delen van dit boek. Door zijn inbreng hebben we kunnen besparen op tijd en is de vertaling nog scherper neergezet.

Als laatste willen we John van Huijgenvoort van Capgemini bedanken voor het reviewen van de Nederlandse vertaling. Door zijn inbreng hebben we de kwaliteit die wij voor ogen hebben nog een slag hoger kunnen leggen.

De auteurs
Najaar 2015

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Inhoudsopgave

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

1 Introductie

Dit boek is bedoeld voor iedereen in een organisatie die basiskennis van informatiebeveiliging wil opdoen. Kennis over informatiebeveiliging is belangrijk voor iedere medewerker in een organisatie. Het maakt geen verschil of je in een commerciële of een niet-commerciële organisatie werkt. De risico's zijn voor iedere organisatie gelijk.

Alle medewerkers moeten weten waarom zij in hun dagelijkse werkzaamheden beveiligingsvoorschriften moeten naleven. Lijnmanagers moeten kennis hebben van informatiebeveiliging omdat zij daarvoor binnen hun afdeling verantwoordelijk zijn. Deze basiskennis is ook belangrijk voor alle directieleden en zelfstandigen zonder personeel. Ook zij zijn verantwoordelijk voor het beschermen van de eigendommen en informatie die zij bezitten. En natuurlijk geldt ook dat een bepaald gevoel van bewustwording belangrijk is voor de thuissituatie. En vanzelfsprekend is deze basiskennis onontbeerlijk als je besluit van informatiebeveiliging, IT of procesmanagement je beroep te maken.

Iedereen heeft te maken met informatiebeveiliging, al is het maar met de beveiligingsmaatregelen die de organisatie waarin je werkt, genomen heeft. Deze beveiligingsmaatregelen zijn soms afgedwongen door wet- en regelgeving. Soms worden ze geïmplementeerd op basis van intern beleid. Neem als voorbeeld het gebruik van een wachtwoord op de computer. Vaak beschouwen we beveiligingsmaatregelen als lastig en overbodig. Ze kosten tijd en het is lang niet altijd duidelijk waartegen ze ons beschermen.

In informatiebeveiliging is het de truc om de gulden middenweg te vinden tussen een aantal aspecten:

- De kwaliteitseisen die een organisatie stelt aan zijn informatie;
- De risico's die geassocieerd worden met die kwaliteitseisen;
- De beveiligingsmaatregelen die genomen worden om die risico's af te dekken;
- Wanneer en op welke manier incidenten buiten de organisatie gerapporteerd worden.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

1.1 WAT IS KWALITEIT?

Kwaliteit is een maat voor overeenkomst tussen prestatie en verwachting. In het algemeen wordt met kwaliteit aangegeven of eigenschappen van een product of dienst overeenkomen met wat ervan verwacht wordt.

Eerst zul je als organisatie moeten bepalen wat je onder kwaliteit verstaat. Op het eenvoudigste niveau dient kwaliteit twee vragen te beantwoorden: 'wat wordt er gevraagd?' en 'hoe doen we het?'.

Vanzelfsprekend ligt de basis van kwaliteit altijd in het gebied van de werkprocessen. Aan de hand van kwaliteitsaspecten, zoals beschreven in de ISO9000, en procesbeschrijvingen volgens het Total Quality Management (TQM), specificeren, meten, verbeteren kwaliteitsprofessionals de processen, en indien nodig herontwerpen zij processen om er zeker van te zijn dat organisaties krijgen wat ze willen.

1.2 WAAR ZIJN WE NU?

Er zijn net zoveel definities voor het woord kwaliteit als er kwaliteitsconsultants zijn, maar algemeen aanvaarde omschrijvingen zijn[1]:

- Voldoen aan eisen ('Conformance to requirements') – Philip Crosby.
- Passend binnen het gewenste gebruik ('Fitness for use') – Joseph Juran.
- De eisen die een bedrijf stelt aan zijn de kwaliteit van zijn producten. Die kunnen beschreven, maar ook onbeschreven zijn. - ISO8402:1994.
- Kwaliteitsmodellen voor bedrijven, inclusief de Deming-prijs, het EFQM excellence model en de Baldrige prijs.

Het primaire doel van dit boek is om studenten voor te bereiden op het examen EXIN Information Security Foundation based on ISO/IEC27002. Het boek is gebaseerd op de internationale standaard NEN-ISO/IEC27002, ook bekend als de *Code voor Informatiebeveiliging.*

Docenten kunnen de informatie in dit boek gebruiken om de kennis van hun studenten te toetsen. Aan het eind van ieder hoofdstuk is een case opgenomen. Iedere case gaat in op de onderwerpen die in het desbetreffend hoofdstuk zijn behandeld en geven veel vrijheid in de wijze waarop de vragen beantwoord kunnen worden. Voorbeelden van recente incidenten zijn 'vertaald' naar de casestudie en verduidelijken de teksten in het boek.

1 http://syque.com/articles/what_is_quality/what_is_quality_1.htm

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

De case start op een basisniveau en naar gelang we verder komen in het boek, groeit het niveau. De case is gebaseerd op boekhandel Springbooks. In het begin telt Springbooks enkele medewerkers en heeft ze beperkte informatiebeveiligingsrisico's. Per hoofdstuk zien we de boekhandel groeien en aan het eind is het een grote organisatie met 120 winkels en haar internetwinkel kent een uitgebreid assortiment. De risico's en dreigingen nemen met de groei van de winkelketen ook toe.

Dit boek is bedoeld om de verschillen tussen risico's en kwetsbaarheden uit te leggen en de beveiligingsmaatregelen die kunnen helpen om deze risico's en kwetsbaarheden zo veel mogelijk in te perken.

Door het algemene karakter van dit boek is het ook goed bruikbaar als materiaal voor een bewustwordingstraining of als naslagwerk tijdens een bewustwordingscampagne.

Dit boek is in eerste instantie gericht op profit- en non-profitorganisaties. Het is echter ook goed toepasbaar in de huiselijke situatie en voor kleine bedrijven (MKB) die geen eigen beveiligingsmedewerkers in dienst hebben. In het MKB is beveiliging meestal een (bij)taak voor een enkele medewerker.

Na het lezen van dit boek heb je algemene kennis opgedaan over de onderwerpen waar informatiebeveiliging over gaat. Je weet ook waarom die onderwerpen belangrijk zijn en heb je kennis van de meest algemene concepten die gebruikt worden binnen de informatiebeveiliging.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

2 Case: Springbooks – een internationale boekhandel

2.1 INTRODUCTIE

Om de theorie in dit boek te begrijpen, vertalen we die theorie naar de dagelijkse praktijk. We gebruiken daarvoor een case die gaat over boekhandel Springbooks. Deze case wordt in een aantal hoofdstukken gebruikt, en daarbij worden vragen gesteld die gerelateerd zijn aan de onderwerpen die in het hoofdstuk zijn behandeld.

Figuur 2.1 De hoofdvestiging van Springbooks in Londen

In dit hoofdstuk beschrijven we de oprichting van de boekwinkel, de historie en groei die de boekwinkel doormaakte naar een internationaal bedrijf. Een organisatie die met haar tijd mee gaat en ook via internet boeken verkoopt. We hebben in deze case gekozen voor een fictief Engels bedrijf vanwege de bijzondere verhouding die het heeft met Europa, die ook zijn weerslag vindt in de organisatie van het bedrijf.
Springbooks werd opgericht in 1901. Gedurende haar groei tot een internationale organisatie, met vestigingen door heel Europa, moest zij zich constant aanpassen aan de veranderende omstandigheden. De belangrijkste en grootste veranderingen vonden plaats in de afgelopen 50 jaar, in de manier waarop met informatie wordt omgegaan. Iedereen zal begrijpen dat er grote verschillen zijn in de wijze waarop de processen gecontroleerd werden tijdens de oprichting in 1901, tot de eerste computers hun intrede deden in de jaren ’60 en ’70 van de vorige eeuw tot aan nu waar organisaties enorm afhankelijk zijn van geautomatiseerde systemen. ICT is een van de belangrijkste gereedschappen geworden voor Springbooks.

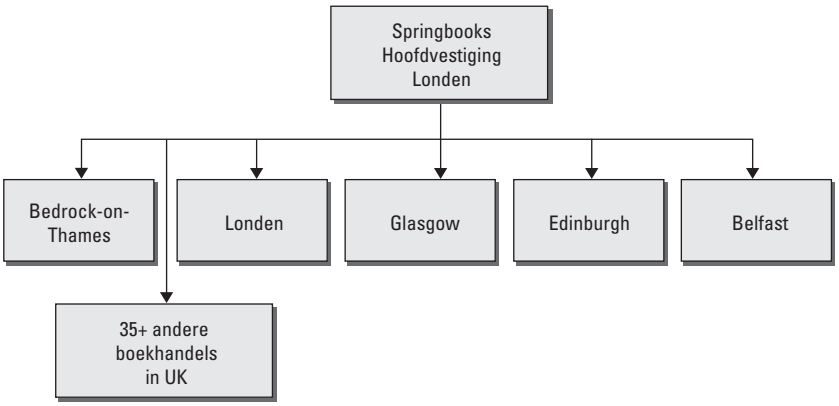
Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

2.2 SPRINGBOOKS

Springbooks Ltd. is een Europees opererende boekhandel. SB is een organisatie bestaande uit 120 boekhandels. De meeste daarvan opereren op franchisebasis. 50 Boekwinkels zijn eigendom van SB zelf.

Figuur 2.2 Organisatieplaatje Springbooks 1901-1931

SB werd opgericht in 1901 in Bedrock-on-Thames, UK. Henry Spring opende in dat jaar een kleine boekwinkel, niet wetende dat zijn kinderen een mega-winkelketen zouden gaan beheren.



Figuur 2.3 Organisatie van Springbooks in 1938

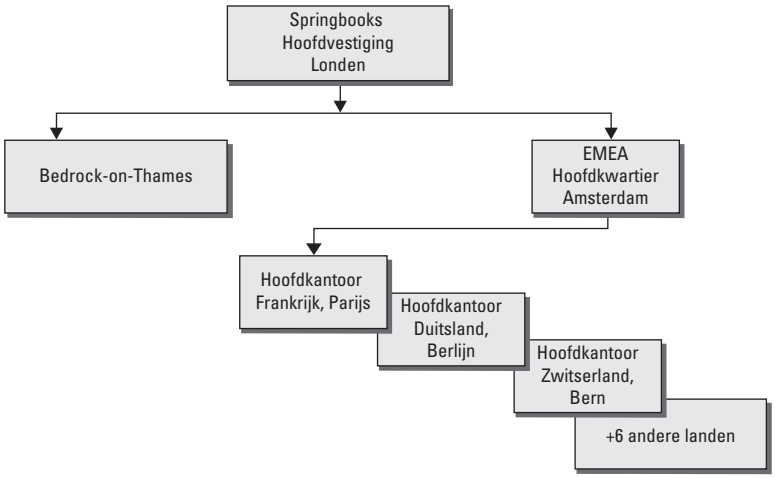
In 1938 was het bedrijf al uitgegroeid tot 40 winkels in alle belangrijke steden in het Verenigd Koninkrijk. Onmiddellijk na het einde van de Tweede Wereldoorlog opende SB boekwinkels in Amsterdam, Kopenhagen, Stockholm, Bonn, Berlijn en Parijs.

Tegenwoordig heeft SB winkels in een groot aantal steden van Europa. De Raad van Bestuur is gevestigd in het hoofdkantoor te Londen. Het Europese hoofdkantoor is gevestigd in Amsterdam.

Ieder land heeft een centraal kantoor dat in de hiërarchie onder het hoofdkantoor te Amsterdam staat.

Amsterdam is verantwoording schuldig aan het hoofdkantoor te Londen. Hiermee is een goed georganiseerde organisatie ontstaan. Alle boekwinkels zijn verantwoording schuldig aan het landelijke centrale kantoor. De landelijke kantoren op hun beurt dragen zorg voor de bevoorrading van de winkels en regelen het leveren van internetbestellingen en

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net



Figuur 2.4 Organisatie van Springbooks in 1946-2015

de uitwisseling van internationaal verkochte boeken tussen de verschillende centrale vestigingen.

In 2000 werden plannen gemaakt om in 2010 'overzee' te gaan naar de Verenigde Staten, Canada, Australië en Nieuw Zeeland. De bankcrisis aan het eind van 2008 zorgde er echter voor dat men deze plannen tijdelijk moest opschorten, tot aan het voorjaar van 2015, toen de plannen weer opgepakt werden.

De bankcrisis had een serieus effect op de waarde van de aandelen van SB. Wanneer mensen moeten bezuinigen, doen ze dat het eerst op boeken, tijdschriften en kranten. Deze zaken vormen de kernactiviteiten van SB. Het gevolg was dan ook dat de waarde van aandelen SB zakte en het beter werd geacht om tijdelijk niet te investeren in nieuwe markten. De zoektocht naar nieuwe markten heeft echter wel geleid tot nieuwe plannen.

De Raad van Bestuur was erg ouderwets in zijn ideeën over hoe een bedrijf geleid moet worden. Internet, nee, dat was niet de manier om handel te drijven. Een onafhankelijk consultancybureau bracht echter het advies uit dat het beter was dat SB een on-line-winkel zou lanceren, waarin meer werd verkocht dan alleen boeken en tijdschriften. Er is nu een internetwinkel op het gebied van reizen, waarbij meteen reisboeken en -gidsen worden aangeboden. En op de wat langere termijn zullen ook consumentenelektronica, fotoapparatuur en andere consumentengoederen aangeboden gaan worden.

Organisatie
Londen UK:
In het Londense hoofdkantoor is de Raad van Bestuur gevestigd en de eindverantwoordelijke Chief Information Officer (CIO), Chief Financial Officer (CFO), Chief Procurement Officer (CPO) and Chief Executive Officer (CEO).

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Ieder land heeft een centraal kantoor dat verantwoordelijk is voor de verkopen in dat land. In de Europese vestigingen is de 'land'-directeur verantwoording schuldig aan de regionale directeur te Amsterdam.

Bedrock-on-Thames UK:
De UK directeur is verantwoordelijk voor de Engelse boekwinkels. Er is ook een UK-CIO, CEO, CFO en een Local Information Security Officer (LISO).

Amsterdam:
EU-directeur (EU met uitzondering van UK).

EU CIO, CEO, CFO, CPO, LISO en de Corporate Information Security Officer (CISO).

Springbooks heeft een informatiebeveiligingsorganisatie die deels gecentraliseerd is. Het overkoepelende beveiligingsbeleid wordt voorgeschreven vanuit de Londense vestiging. ISO27001 en ISO27002 zijn de standaarden die in alle landen worden toegepast.

In Londen is de Chief Information Security Manager eindverantwoordelijk voor de informatiebeveiliging in de organisatie. Hij zorgt ervoor dat informatiebeveiliging deel uitmaakt van de dagelijkse werkprocessen van alle SB-medewerkers.

De LISO's zijn er verantwoordelijk voor dat het bedrijf het beveiligingsbeleid uitdraagt binnen de landelijke organisatie en dat aan landelijke wet- en regelgeving wordt voldaan.

De LISO is ook verantwoordelijk voor de fysieke beveiliging van de SB-winkels en voor de bedrijfshulpverlening in de SB-winkels.

Iedere winkel kent een informatiebeveiligingsmedewerker. Dit is een medewerker met een opleiding op het gebied van informatiebeveiliging en bedrijfshulpverlening. Deze medewerker is verantwoordelijk voor de informatiebeveiliging in die winkel.

IT is centraal georganiseerd. Een Wide Area Network (WAN) verbindt alle winkels met elkaar. Het Springbooks WAN is een computernetwerk dat ervoor zorgt dat alle winkels met elkaar kunnen communiceren en dat ze van de centrale computervoorzieningen, zoals voorraadbeheer, gebruik kunnen maken. Dit is een verschil met het Local Area Network (LAN), waarop alle computers in een boekwinkel (binnen één enkel pand) zijn aangesloten.

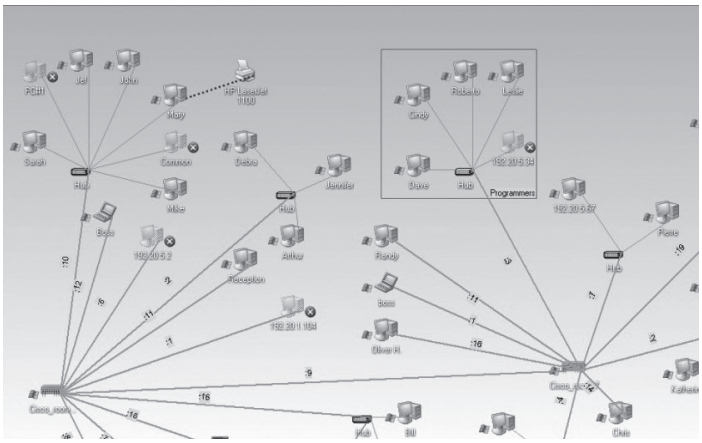
Alle kassa's zijn aangesloten op het WAN. Ieder verkocht boek wordt aan de kassa gescand en de verkoop wordt onmiddellijk in de centrale database geregistreerd. Dit maakt het mogelijk om op ieder gewenst moment een overzicht te hebben van de actuele voorraad. Het bevoorraden van de winkels gebeurt op basis van de actuele verkoopcijfers.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Zodoende kan SB ervoor zorgen dat goedlopende boeken altijd op voorraad zijn, en dat ze minder goed verkopende boeken snel kunnen leveren.

Iedere medewerker heeft zijn eigen gebruikersnaam om in te loggen op het kassasysteem. Ieder verkocht boek wordt gekoppeld aan de verkoopmedewerker. In dezelfde database is veel klantinformatie aanwezig, zoals namen, adressen en creditcardinformatie.

Omdat in deze database klantinformatie is opgeslagen, is het zeer belangrijk dat men voldoet aan de nationale privacywetgeving, maar ook aan de interne beveiligingseisen. Onverwachte en ongeautoriseerde openbaarmaking van de vertrouwelijke informatie kan grote consequenties hebben voor het vertrouwen dat de klanten in Springbooks hebben.



Figuur 2.5 De WAN dataverbindingen tussen de boekwinkels van Springbooks

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net

3 Termen en definities

Een van de grote veranderingen in de 2013-versie ten opzichte van de 2005-versie van de ISO/IEC 27001 is dat alle termen en definities eruit gehaald zijn. In 2014 is een nieuwe ISO/IEC 27000:2014 gepubliceerd waarin de termen en definities zijn ondergebracht die voor de hele 27000-serie van toepassing zijn.

Onderstaande definities worden uitgelegd in de ISO/IEC 27000:2014. Vaak verwijzen die termen en definities weer naar een andere norm waarop deze term of definitie gebaseerd is. Het doel is om daarmee een eenheid in het gebruik van termen en definities te creëren, waarmee voorkomen wordt dat een bepaalde term in de ene standaard een andere betekenis heeft dan in een andere standaard.

In dit hoofdstuk beschrijven we in het kort enkele belangrijke termen en definities met betrekking tot informatiebeveiliging. In Bijlage A is een uitgebreidere woordenlijst opgenomen.

Voor we de termen en definities bespreken die relevant zijn voor dit boek, geven we eerst een korte toelichting op de laatste ontwikkelingen op het gebied van ISO-standaarden. In 2012 verscheen de Annex SL, *Proposals for management system standards*. Dit document geeft richting aan hoe een ISO-managementstandaard ingericht moet worden. De Annex SL stelt eisen aan de hoofdstukindeling van een managementstandaard en de inhoud waaraan die hoofdstukken moeten voldoen. Hierdoor worden in de komende tijd alle managementstandaarden gelijkvorming ingericht. Hierdoor zit er een groot verschil in de opbouw van de 2005-versie en de 2013-versie van de ISO/IEC 27001.

3.1 DEFINITIES

Aanval
Een poging om ongeautoriseerd toegang te krijgen tot bedrijfsinformatie. Die informatie te lezen, te stelen, te wijzigen, onbruikbaar te maken, of ongeoorloofd gebruik van die bedrijfsinformatie te maken.

Copyright protected. Use is for Single Users only via a VHP Approved License.
For information and printed versions please see www.vanharen.net