Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

Publication date
2008

1. Inleiding

De beveiliging van een computersysteem vergelijken met een vergiet is een te gunstige vergelijking. Immers, bij een vergiet is de plaats van elk gaatje te berekenen wanneer je er enkele hebt gevonden. Bij een computersysteem is dit echter niet mogelijk.

Prof. dr. I.S. Herschberg (1928-1998)

1.1. Management van informatiebeveiliging

De belangstelling voor ICT-beveiliging is de afgelopen tien jaren sterk gegroeid. Dit blijkt onder meer uit het toenemende aantal professionals voor informatiebeveiliging. Het Nederlandse Genootschap voor Informatiebeveiligers telde bij de start op 9 september 1999 honderdtachtig leden. Medio 2007 ligt het aantal ruim boven de duizend. Het belangrijkste doel van de vereniging is het ondersteunen van in Nederland gevestigde werknemers of zelfstandigen die zich beroepsmatig bezighouden met het beveiligen van informatie. Ook kan de belangstelling worden afgeleid uit het stijgende aantal internationale standaarden voor ICT-beveiligingstechnieken en management van informatiebeveiliging van onder meer de International Organization for Standardization (ISO) en de Internet Engineering Task Force (IETF). Publicaties van beveiligingonderzoeksinstituten, zoals de Computer Crime and Security Survey van het Amerikaanse Computer Security Institute in samenwerking met het Computer Intrusion Squad van het San Francisco Federal Bureau of Investigation [GORD06] en mediaberichten over virus- en hackersincidenten hebben de aandacht voor het vakgebied ICT-beveiliging verder gestimuleerd.

1.1.1. Information security governance

Vanaf eind jaren negentig zijn diverse normenkaders, standaarden en concepten ontwikkeld voor het ontwikkelen, implementeren en beheren van aan ICT-beveiliging gerelateerde activiteiten. Von Solms [SOLM00] spreekt van drie golven in de historie van informatiebeveiliging. Tijdens de eerste golf lag de nadruk bij informatiebeveiliging op technische aspecten, met name het invullen van ingebouwde beveiligingsmaatregelen van (centrale) computers: toegangscontrolelijsten, userids en wachtwoorden. De tweede golf werd gedomineerd door gedistribueerde computeractiviteiten en de opkomst van het internet. Typerend voor deze fase is de toenemende aandacht van het management voor informatiebeveiliging. Dit resulteerde onder meer in de aanstelling van specifieke functionarissen voor informatiebeveiliging. De derde golf ontstond kort voor de eeuwwisseling. Dat was het begin van een tijdperk met veel aandacht voor governance en standaardisatie, ofwel institutionalisering van informatiebeveiliging. Zo gaf in 2001 het IT Governance Institute (ITGI) een publicatie uit over IT security governance. In de tweede herziene versie worden kennis over het informatiebezit en de bescherming van informatie aangemerkt als sleutelelementen bij het inrichten van IT security governance [ITGI06]. Het instituut, opgericht in 1998, vindt dat IT governance en daaraan gekoppeld IT security governance een verantwoordelijkheid is van de hoogste leiding van een organisatie. De vijf ICT-aandachtsgebieden volgens ITGI zijn: afstemming tussen ICT-

en bedrijfsstrategie, leveren van toegevoegde waarde, risicobeheersing, capaciteitsbeheer en monitoring van resultaten.

Een invloedrijk initiatief uit de jaren tachtig betrof het ontwikkelen van een model voor een effectief en efficiënt gebruik van ICT-middelen bij ministeries en publieke overheidsinstellingen in Engeland. De opdrachtgever, het Britse overheidsagentschap voor centrale computers en telecommunicatie, streefde hierbij naar een leveranciersonafhankelijke benadering. Het resulteerde in een zogeheten Information Technology Infrastructure Library (ITIL), een verzameling taken, procedures, controlelijsten en verantwoordelijkheden verzameld uit de praktijk van een aantal ICT-organisaties. ITIL werd in een groot aantal landen een de facto standaard voor het inrichten van IT service managementprocessen.

In 1996 werd door de Amerikaanse Information Systems Audit and Control foundation een raamwerk voor ICT-governance ontwikkeld, de zogeheten Control Objectives for Information and related Technology (COBIT). Het raamwerk benadrukt het belang van de plan-do-check-act cyclus voor elke ICT-dienstverlening. ICT-processen worden in het raamwerk gedefinieerd in vier domeinen die overeenkomen met de levenscyclus van een informatiesysteem: plan and organise, acquire and implement, deliver and support en tenslotte monitor and evaluate [GULD01]. Het COBIT proces DS5 ensure systems security bijvoorbeeld maakt onderdeel uit van het domein deliver en support. Het IT Governance Institute heeft in 2007 een analyse uitgevoerd naar de relatie tussen COBIT 4.0 en ITIL [ITGI07]. Het instituut concludeert dat alle ITIL service delivery en ITIL service support processen binnen COBIT een tegenhanger hebben. Sommige COBIT processen worden echter niet geadresseerd binnen ITIL, bijvoorbeeld het COBIT proces P07 Manage IT human resources.Verder wordt vastgesteld dat de kracht van ITIL, in tegenstelling tot COBIT, is gelegen in de praktische beschrijving van operationele ICT-processen en de brede acceptatie van ITIL als best practise voor IT service management.

In Nederland heeft met name de door het Nederlands Normalisatie-instituut uitgegeven Code voor Informatiebeveiliging [NEN00] bij veel organisaties als basis gediend voor information security governance. De code onderscheidt drie kwaliteitskenmerken.

Vertrouwelijkheid:	waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe geautoriseerd zijn.
Integriteit:	waarborgen van de juistheid en de volledigheid van informatie en de verwerking daarvan.
Beschikbaarheid:	waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

De standaard is in 2005 geactualiseerd [NEN05]. Informatiebeveiliging wordt hierin gedefinieerd als ‘de bescherming van informatie tegen een groot aantal bedreigingen met als doel het waarborgen van bedrijfscontinuïteit, het minimaliseren van bedrijfsrisico’s en het maximaliseren van investeringsrevenuen en bedrijfskansen’ In 2004 is door de standaardisatie-organisaties ISO en IEC besloten om bestaande en nieuwe standaarden voor het managen van informatiebeveiliging uit te geven in een 2700x-reeks. Om deze reden is de uitgegeven standaard ISO/IEC 17799-2005 in 2007 omgenummerd naar

ISO/IEC 27002. De in 2005 gepubliceerde standaard beschrijft een procesmodel voor een information security management systeem. In de standaard worden generieke eisen beschreven voor het managementsysteem waaronder het identificeren, analyseren en evalueren van risico's en het selecteren en implementeren van beveiligingscontrols. Het model verwijst hierbij naar de controls uit de ISO/IEC 17799-2005/27002-2007.

Zowel in de 2000-versie als in de geactualiseerde versie van 2005 van de NEN-norm worden meer dan honderd maatregelen beschreven binnen de categorieën beleid, organisatie, personeel, fysieke beveiliging, beheer van communicatie- en bedieningsprocessen, toegangsbeveiliging, ontwikkeling en onderhoud van systemen, continuïteitsmanagement en naleving. Eerst in 2005 is de code uitgebreid met een hoofdstuk over incident management. De internationale code is een afgeleide van de Britse norm BS7799:1999 part 1, die tot stand is gekomen onder verantwoordelijkheid van het British Standards Institute. De Nederlandse rijksoverheid heeft sinds 1994 haar eigen normenkader, het zogeheten Besluit voorschrift informatiebeveiliging rijksdienst [VIR94]. Het besluit van de ministerraad bestaat uit zes bepalingen waarin de zorgplicht voor het vaststellen en implementeren van informatiebeveiligingsmaatregelen wordt beschreven. Het voorschrift geldt voor alle ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.

1.1.2. Risicobeheersing

Nieuwe wetgeving, zoals de Amerikaanse Sarbanes-Oxley Act uit 2002, en sectorspecifieke regelgeving, onder meer het Basel II- raamwerk voor financiële instellingen, hebben de afgelopen jaren een impuls gegeven aan het onderwerp risicomanagement. Organisaties die te maken hebben met deze wet- of regelgeving dienen aantoonbaar 'in control' te zijn en zicht te hebben op diverse soorten risico's, waaronder de risico's met betrekking tot de informatievoorziening. Bedrijfsprocessen zonder adequate informatievoorziening zijn nauwelijks meer voorstelbaar [OVRS05]. De ICT-systemen en -processen die deze informatie leveren, dienen zodanig te worden ingericht en beveiligd dat de gewenste beschikbaarheid, integriteit en vertrouwelijkheid van de informatie worden gerealiseerd. Informatiebeveiliging is een onderdeel van risicomanagement in brede zin en maakt deel uit van de interne beheersing van een organisatie [FRLH06].

In 1994 heeft het Committee of Sponsoring Organizations of the Treadway Commission (COSO), een raamwerk (Internal Control – Integrated Framework) uitgevaardigd om organisaties te helpen met het beoordelen en verbeteren van de interne beheersingssystemen. Het COSO model heeft niet zozeer betrekking op informatietechnologie, als wel op interne beheersing in brede zin. Interne beheersing bestaat volgens dit model uit vijf componenten: beheersingsomgeving, risicoanalyse, beheersingsmaatregelen, informatie en communicatie en monitoring. In 2004 heeft COSO een aanvullend raamwerk voor het identificeren, analyseren en beheersen van risico's gepubliceerd [COSO04]. Het raamwerk, Enterprise Risk Management – Integrated Framework, beschouwt het terrein van ondernemingsrisicomanagement en definieert dit als volgt:

Ondernemingsrisicomanagement is een proces dat bewerkstelligd wordt door het bestuur van de onderneming, het management en ander personeel en wordt toegepast bij het formuleren van de strategie en binnen de gehele onderneming, ontworpen om potentiële gebeurtenissen die invloed zouden kunnen hebben op de onderneming te identificeren en om risico's te

managen zodat deze binnen de risico-acceptatiegraad vallen, om een redelijke zekerheid te bieden ten aanzien van het behalen van de ondernemingsdoelstellingen.

Wetgeving of (inter)nationale, sectorspecifieke regelgeving incorporeert ICT-beveiliging soms in een breder operationeel risicobeheersingskader. Dit geldt bijvoorbeeld voor wet- en regelgeving voor de financiële sector.

Een operationeel risico wordt door de Bank for International Settlements [BIS03] gedefinieerd als 'de mogelijkheid op het lijden van verlies door inadequate of falende processen, mensen en systemen, of door externe gebeurtenissen'. Een integrale benadering van operationele risico's is nodig in verband met de verplichte allocatie van kapitaal om mogelijke financiële schade door incidenten op te vangen. Ook De Nederlandsche Bank vereist in artikel 53 van haar Regeling Organisatie en Beheersing[1] [ROB01] een systematische aanpak van operationele risico's: 'Elke instelling beschikt over een informatiesysteem dat toereikend is voor de systematische meting, bewaking en documentatie van alle operationele risico's, zowel op instellingsniveau als op het niveau van de onderscheiden bedrijfsonderdelen. De operationele risico's die de instelling loopt, dienen tijdig te worden gerapporteerd onder vermelding van geconstateerde (dreigende) calamiteiten en verliezen.'

Operationele risicobeheersing behelst meer dan het waarborgen van de kwaliteit van informatie alleen. Ook beveiliging van personen en andere 'business assets' behoren tot de scope van operationele risicobeheersing. *Informatie*risicobeheersing heeft uitsluitend betrekking op het waarborgen van de (bedrijfs)informatie.

Het uitvoeren van risicoanalyses, een belangrijk onderdeel van risicobeheersing, betreft het systematisch identificeren en analyseren van relevante risico's waaraan de organisatie is blootgesteld. Er zijn grofweg twee benaderingen: een kwantitatieve en een kwalitatieve benadering. Bij de kwantitatieve benadering worden risico's uitgedrukt in de vorm van schadebedragen. Bij het berekenen hiervan wordt gebruik gemaakt van rekenkundige formules. Het International Information Systems Security Certification Consortium[2] hanteert als voorbeeld in zijn opleiding voor Certified Information Systems Security Professional (CISSP) vier formules.

Tabel 1: kwantitatieve risicoanalyseformules volgens het ISC[2]

Concept	**Product**
Exposure factor	Percentage van het bezittingenverlies veroorzaakt door de dreiging
Single loss expectancy	Waarde van de bezitting vermenigvuldigd met de exposure factor
Annualized rate of occurence	Aantal malen dat de dreiging zich manifesteert per jaar
Annualized loss expectancy	Single loss expectancy vermenigvuldigd met de annualized rate of occurrence

[1] De Regeling Organisatie en Beheer is niet meer als separate regeling van toepassing voor Nederlandse financiële instellingen. De kernprincipes uit de regeling zijn opgenomen in een algemene maatregel van bestuur onder de Wet op het financieel toezicht (Wft), die op 1 januari 2007 is ingegaan.
[2] Zie http://www.isc2.org

Met andere woorden de 'annualized loss expectancy' is het verwachte verlies op jaarbasis van een organisatie door één dreiging. Voor het geautomatiseerd uitvoeren van kwantitatieve risicoanalyses zijn diverse hulpmiddelen verkrijgbaar. Enkele overheidsinstellingen in Nederland gebruiken het hulpmiddel CRAMM (UK Government Risk Analysis and Management Method). Het is in de jaren negentig ontwikkeld door het toenmalige Britse overheidsagentschap voor telecommunicatie en wordt vooral bij grotere overheidsinstellingen en bedrijven binnen en buiten Engeland gebruikt voor het uitvoeren van beveiligingsrisicoanalyses.

Het internationale Information Security Forum[3] daarentegen kiest voor een meer kwalitatieve benadering van risico's. Het heeft hiertoe de methodiek Fundamental Information Risk Management (FIRM) ontwikkeld. De methodiek is bedoeld om de effectiviteit van de informatierisicobeheersing op een praktische en structurele manier te monitoren. Een belangrijk element binnen FIRM is de zogeheten Information Risk Scorecard waarbij per 'information resource' relevante aspecten worden vastgesteld.

Criticality:	wat is de maximumschade die de business kan lijden als sleutelinformatie verwerkt, opgeslagen of getransporteerd door de 'information resource' per ongeluk of opzettelijk wordt ontsloten, gewijzigd of gedurende uren, dagen of zelfs weken niet beschikbaar is?
Vulnerability:	wat is de status van in totaal zeventien control areas[4]?; zijn er speciale omstandigheden zoals een bepaalde entiteit die regelmatig aan verandering onderhevig is?
Level of threat:	een inschatting van het aantal en de soorten incidenten die hebben plaatsgevonden in de laatste twaalf maanden.
Business:	wat voor impact hadden de incidenten, die hebben plaatsgevonden in de laatste twaalf maanden (van financiële schade tot reputatieschade)?
Strengthening Controls:	zijn er activiteiten op het versterken van de zeventien control areas geïnitieerd, gepland of afgerond gedurende de rapportageperiode?
Accountability:	de eigenaar van de 'information resource' dient te worden bepaald.

1.2. Trends in aanvallen

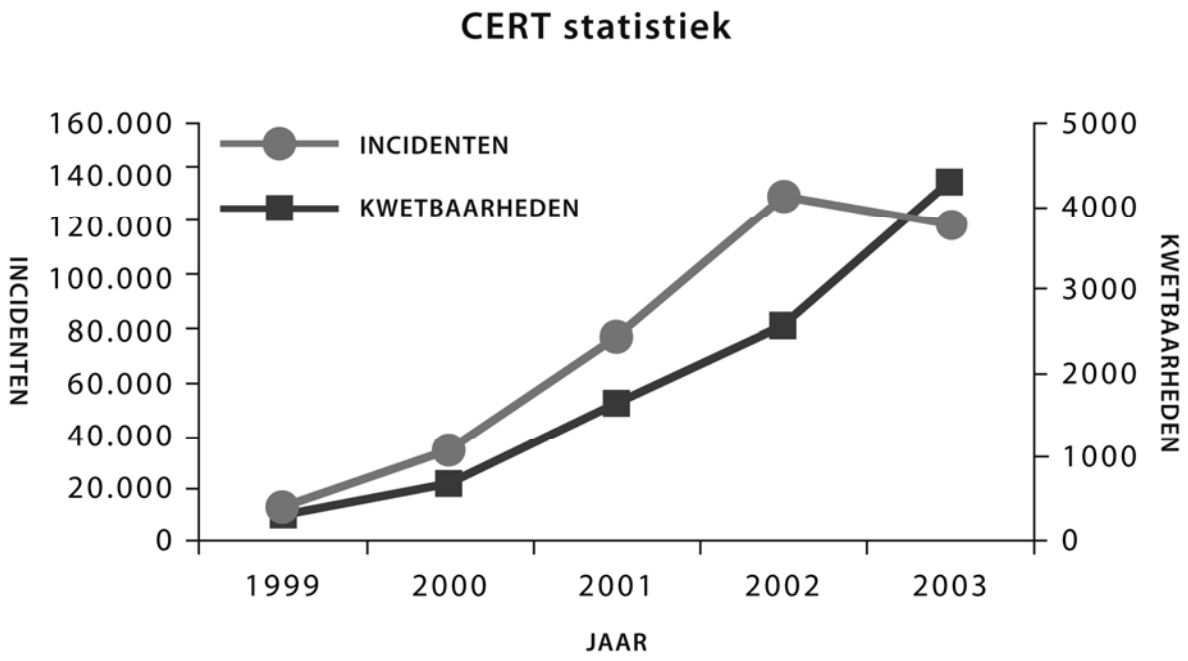
Informatiebeveiliging en incidenten worden vaak in één adem genoemd. In de naweeën van grote wereldwijde computervirusincidenten en beschikbaarheidsaanvallen op aan het Internet verbonden webservers, is gebleken dat veel organisaties die actief aanwezig zijn

[3] Het Information Security Forum (www.securityforum.org) is een internationale vereniging met ongeveer 250 leden. De leden zijn (zeer) grote organisaties afkomstig uit de profit- en non-profitsector. Het delen van informatiebeveiligingskennis en -ervaring en het ontwikkelen van standaarden en hulpmiddelen op dit terrein zijn de belangrijkste doelstellingen van de vereniging.

[4] Voorbeelden van control areas zijn: beleid en standaarden, bewustzijn, fysieke beveiliging en wijzigingsmanagement.

op het Internet ondanks forse beveiligingsmaatregelen kwetsbaar zijn en getroffen worden door incidenten [STTN01]. Als de geregistreerde incidenten nader worden geanalyseerd, zijn hieruit een aantal kenmerken te halen. Het CERT® Coordination Center (CERT/CC) heeft de afgelopen jaren uitgebreid onderzoek gedaan naar de omvang en aard van deze incidenten.

1.2.1. Kwetsbaarheden- en incidententrends



Figuur 1: overzicht[5] van door CERT/CC geregistreerde kwetsbaarheden en incidenten

Figuur 1 geeft een overzicht van de bij CERT/CC gemelde, aan het Internet gerelateerde incidenten in de periode 1998 tot en met 2003. Howard heeft in de periode 1989 tot en met 1995 onderzoek gedaan naar in totaal 4567 bij CERT/CC gemelde en geregistreerde incidenten. Het onderzoek wordt beschouwd als het eerste grootschalige onderzoek naar aan ICT-beveiliging gerelateerde incidenten. Van de onderzochte incidenten bleken er 268 valse alarmmeldingen. De resterende 4299 incidenten zijn uiteindelijk nader geanalyseerd. Uit de zeer gedetailleerde analyse zijn de volgende aspecten naar voren gekomen:

Incidententypen
Ruim tachtig procent van de onderzochte incidenten had betrekking op ‘ongeautoriseerde toegang’, waaronder het verkrijgen van toegang tot useraccounts met privileges, waardoor indringers controle krijgen over een besturingssysteem (root break-ins). Het overige percentage van de incidenten, gemeld bij CERT/CC, werd geclassificeerd als

[5] Het CERT® Coordination Center publiceert vanaf 1 januari 2004 geen rapportages meer over ontvangen incidenten. De argumentatie hiervoor is dat het wijdverspreide gebruik van geautomatiseerde aanvalsmiddelen jegens internetgekoppelde systemen ervoor zorgt dat het tellen van gemelde incidenten weinig extra informatie oplevert met betrekking tot onderzoek naar de scope en impact van aanvallen.

'ongeautoriseerd gebruik'. Het betrof onder meer beschikbaarheidsaanvallen, verminking van informatie en ontsluiting van informatie.

Tools en vulnerabilities
Bij ongeveer achthonderd incidenten werd melding gemaakt van het gebruik van een hulpmiddel. Het ging hierbij vooral om kwaadaardige softwareprogramma's, zoals trojan horses en sniffers ter verkrijging van privileges of toegang op systeemniveau. De onderzochte CERT/CC-incidentrecords bevatten toen nog zeer weinig referenties naar autonome programma's zoals virussen. Bijna de helft van alle incidenten benoemden specifieke kwetsbaarheden, met name problemen met wachtwoorden. Voorbeelden zijn het kopiëren van wachtwoordbestanden, het geautomatiseerd kraken van wachtwoorden en misbruik van zwakke wachtwoorden.

Bovenstaande percentages en aantallen zijn gedateerd en niet meer bruikbaar voor actuele analyses. Beschikbaarheidsaanvallen, virusuitbraken en aanvallen gericht op (identiteits)fraude van de afgelopen tien jaar geven bij nieuw onderzoek ongetwijfeld een ander statistisch trendbeeld. CERT®/CC heeft in 2002 op zijn website een overzicht [CERT02] gepubliceerd van een drietal trends in aanvalstechnieken.

Trend 1 *Automatisering van aanvalshulpmiddelen:*
Het niveau van automatisering in aanvalsmiddelen zal verder toenemen. Geautomatiseerde aanvallen kennen over het algemeen vier fasen:
1. scannen op potentiële slachtoffers
2. compromitteren van kwetsbare systemen
3. propageren van de aanval[6]
4. gecoördineerd beheer van aanvalshulpmiddelen ten behoeve van beschikbaarheidsaanvallen, scannen en compromitteren van kwetsbare systemen.

Trend 2 *Toenemende geavanceerdheid van aanvalshulpmiddelen:*
'Handtekeningen' van aanvalsmiddelen zijn moeilijker te analyseren en te detecteren door bijvoorbeeld antivirusprogrammatuur. Karakteristiek voor deze trend zijn het antiforensische karakter, het dynamische gedrag en de modulariteit van de aanvalsmiddelen. Dit alles leidt ertoe dat het steeds moeilijker wordt om aanvallen te onderscheiden van legitiem netwerkverkeer.

Trend 3 *Snellere ontdekking van kwetsbaarheden:*
Het aantal nieuw ontdekte kwetsbaarheden gerapporteerd aan CERT/CC verdubbelt zich ieder jaar. Het is voor beheerders een moeilijke taak om bij te blijven met patches. Bovendien worden ieder jaar nieuwe klassen kwetsbaarheden ontdekt. Reviews van bestaande softwarecode leidden soms tot de ontdekking van deze nieuwe kwetsbaarheden in honderden verschillende softwareproducten. Indringers zijn vaak in staat om deze exemplaren sneller te ontdekken dan leveranciers in staat zijn ze te corrigeren. Vanwege deze trend tot geautomatiseerde ontdekking van

[6] De opstellers vermelden dat tools als Code Red en Nimda zichzelf binnen 18 uur propageerden tot een stadium van 'wereldwijde verzadiging'.

nieuwe kwetsbaarheden wordt de zogeheten time-to-patch in toenemende mate kleiner.

1.2.2. Taxonomie van computer- en netwerkaanvallen

Howards heeft met zijn analyse van incidenten een belangrijke impuls gegeven aan het ontwikkelen van methodes voor het analyseren en categoriseren van computer- en netwerkaanvallen. De hieruit ontstane taxonomieën zijn vooral nuttig voor beveiligingsspecialisten die zich bezighouden met het behandelen van incidenten en kwetsbaarheden. Een aansprekend voorbeeld is het Common Vulnerabilities and Exposures (CVE) project[7] met als belangrijkste doelstelling het leveren van algemene definities voor kwetsbaarheden. De CVE-database is een de facto standaard voor het classificeren van kwetsbaarheden. Een taxonomie is van belang bij de uitwisseling van informatie tussen teams van ICT-beveiligingsspecialisten. Zij levert immers een gemeenschappelijk classificatieschema en verbetert daarnaast de taalconsistentie bij het beschrijven van aanvallen en kwetsbaarheden.

Met enige regelmaat worden nieuwe taxonomieën gepresenteerd. Een recent voorbeeld is een taxonomie van Hansman en Hunt uit 2005 [HAHU05], waarbij gebruik wordt gemaakt van het concept van dimensies. Een dimensie kan meerdere niveaus omvatten. De dimensies leveren gezamenlijk een meer holistische kijk op een aanval. De taxonomie gebruikt vier dimensies.

Attack vector: de eerste of basisdimensie wordt gebruikt om de aanval te categoriseren in een aanvalsklasse die is gebaseerd op de aanvalsvector.
Voorbeeld notering: Network attacks (level 1) > wireless attacks (level 2) > WEP cracking (level 3).

Target: de tweede dimensie betreft het doel van de aanval. Als een aanval meerdere doelen heeft, bevat deze dimensie meerdere ‘entries’.
Voorbeeld notering: Software (level 1) > Operating system (level 3) > Unix family (level 4) > Linux (level 4) > Redhat Linux 7.0 > etc.

Vulnerabilities and exploits: deze dimensie betreft de kwetsbaarheden en programma’s die de aanvaller gebruikt. Hierbij wordt verwezen naar het CVE-project. Als de kwetsbaarheid of het programma (nog) niet is opgenomen in de CVE-database dan wordt voorgesteld om de indeling van Howard te volgen, te weten (a) kwetsbaarheid in implementatie, (b) kwetsbaarheid in ontwikkeling, (c) kwetsbaarheid in configuratie.

Payloads: de laatste dimensie beschrijft de ‘payload’ van de aanval. De payload kan een andere aanval op zichzelf zijn. De dimensie heeft vijf categorieën: (a) eerste dimensie aanval payload, (b) corruptie van informatie, (c) onthulling van informatie, (d) diefstal van service, (e) subversie.

[7] Zie http://cve.mitre.org.

Het eerste majeure aan het Internet gerelateerde incident, de zogeheten 'Morris-worm', zou volgens deze taxonomie de volgende notitie hebben gekregen:

aanval:	morris-worm.
Eerste dimensie:	network-aware-worm.
Tweede dimensie:	BSD 4 Sun 3 & Vax variants.
Derde dimensie:	implementation design.
Vierde dimensie:	theft of service & subversion.

1.2.3. Computercriminaliteit

Aan ICT-beveiliging gerelateerde incidenten *met strafbare kenmerken* worden in de literatuur vaak aangeduid als cybercrime. Het blad The New Forensics [ANAS03] typeert cybercrime als een voortdurende wedstrijd tussen de moderne crimineel die gebruik maakt van moderne technieken om bijvoorbeeld bedrijfsgeheimen te ontfutselen of te frauderen, en forensisch onderzoekers die op zoek zijn naar digitale sporen om de modus operandi te bepalen en de dader te traceren.

Het Nederlandse rechercherapport Cybercrime van het Korps Landelijke Politiediensten (KLPD) onderscheidt twee verschijningsvormen van cybercrime. De eerste vorm is die waarbij de computer als *middel* wordt gebruikt bij de uitvoering van strafbare of strafwaardige gedragingen, zoals (virtuele) kinderpornografie en witwassen. De tweede verschijningsvorm is die waarbij de computer ook het *doel* is van de strafbare of strafwaardige gedragingen: cybercrime in enge zin, zoals beschikbaarheidsaanvallen en computervredebreuk (hacking).

Het onderzoek schetst een theoretisch beeld van de omvang en ontwikkeling van cybercrime in Nederland en geeft aanbevelingen voor de bestrijding [AMSR02]. 'Meer blauw in cyberspace' is een van de aanbevelingen in het rapport.

In 2003 is door het Korps Landelijke Politiediensten [VLE03] een onderzoek naar cybercrime gehouden waarvoor tweeënveertig bedrijven, instanties en instellingen in Nederland werden benaderd. De survey was gebaseerd op een Amerikaans/Australisch model voor cybercrimeonderzoek. Van de tweeënveertig aangeschreven instellingen reageerden er slechts slechts negen..

Concrete landelijke cijfers over de omvang van cybercrime in Nederland zijn niet te geven, omdat niet altijd aangifte wordt gedaan en medewerking aan onderzoek gering is. Doordat politiekorpsen aangiften op verschillende manieren registreren, ontbreekt bovendien een geconsolideerd totaaloverzicht op het gebied van computercriminaliteit in Nederland, aldus het Landelijk Parket van het Openbaar Ministerie [DIJK03].

Samenvattend luidt de conclusie dat de trends in aanvallen het belang van een adequate ICT-beveiliging bevestigen, waarbij het een belangrijk vraagstuk is te weten hoe organisaties omgaan met incidenten en kwetsbaarheden. ICT-beveiliging is hierbij niet een op zichzelf staande activiteit maar integraal onderdeel van een generiek risicomanagementproces.

1.3. Problemen bij de afhandeling van kwetsbaarheden- en incidenteninformatie

1.3.1. Probleemomschrijving

De beheersing van *kwetsbaarheden* wordt gekenmerkt door een grote, meestal ongestructureerde, stroom aan meldingen over nieuw ontdekte kwetsbaarheden of programma's die bekende kwetsbaarheden misbruiken. Ter illustratie: het computer emergency response team van de Nederlandse overheid alleen al stelde in 2006 zeshonderdenvier adviezen op [GOVC07]. Een gemiddelde dus van twaalf per week. Daarnaast gaf het team via de website http://www.waarschuwingsdienst.nl in 2006 honderdentweeentwintig waarschuwingen af. Als wordt uitgegaan van een veelheid aan informatiestromen is het evident dat organisaties worden geconfronteerd met vele duizenden, misschien zelfs tienduizenden, meldingen per jaar. Dit leidt ons tot een eerste probleem.

Probleem 1:

ICT-organisaties lijken niet in staat om de constante stroom aan kwetsbaarheedeninformatie tijdig te analyseren en te beantwoorden.

Het beeld met betrekking tot beheersing van *incidenten* is minder duidelijk. Uit onwetendheid of imago-overwegingen zijn organisaties meestal terughoudend met het vrijgeven van (statistische) informatie over incidenten waarmee zij te maken hadden. APACS, de Britse Payments Association, registreerde in Engeland in september 2006 1513 unieke phishingaanvallen op Britse banken. De totale schade door phishingaanvallen op banken in de Verenigde Staten wordt geschat op 2 miljard dollar. Engelse banken hebben in 2006 33,5 miljoen pond sterling aan schade geleden door fraude bij internetbankieren. In 2004 was het bedrag nog aanzienlijk lager, namelijk 12,2 miljoen pond sterling [HOL07]. Ook de Anti-Phishing Working Group[8] schetst een beeld van de omvang van aan Internet gerelateerde fraude-aanvallen. Zo waren er eind 2006 wereldwijd bijna dertigduizend phishingsites actief, waarvan de meeste gericht waren op banken. Het CSI/FBI 2006 beveiligingsonderzoek uit de Verenigde Staten geeft aan dat virusaanvallen tot de meeste schade heeft geleid bij organisaties.

Uit onderzoek [ARKI02] blijkt dat beveiligingsincidenten, als zij optreden, organisaties voor grote problemen kunnen stellen. Incidenten die gerelateerd zijn aan feiten die in het Wetboek van Strafrecht zijn gesteld, en daarmee vallen onder de noemer cybercrime, kunnen organisaties voor extra probemen stellen. Bij deze categorie incidenten gaat het er immers om niet alleen de schade van het incident te beperken (repressie) of te herstellen (correctie) maar ook om maatregelen te treffen in het kader van opsporing en strafvervolging.

[8] De Anti-Phishing Working Group is een internationale vereniging van ruim zeshonderd vooraanstaande organisaties uit de financiële wereld, internet service providers, de online retailbranche en enkele opsporingsinstanties met als doel het elimineren van identiteitsdiefstal en –fraude, zie http://www.antiphishing.org.

Probleem 2:

Incidentenresponseprocessen binnen organisaties werken niet optimaal bij de afhandeling van computercriminaliteit.

De twee hiervoor genoemde problemen lijken samen te hangen met een drietal organisatorische aspecten:

- tijdprobleem bij de afhandeling van kwetsbaarhedeninformatie
- versnippering van beveiligingstaken
- gebrek aan kennis.

Deze aspecten worden hierna behandeld.

1.3.2. Het tijdlek in het ICT-beveiligingsproces

Het (bijna) publiceren over nieuwe gaten in besturingssystemen of over kwaadaardige programma's die hier misbruik van maken, leidt vooralsnog niet tot een betere bescherming van kwetsbare ICT-infrastructuren [JONG02].

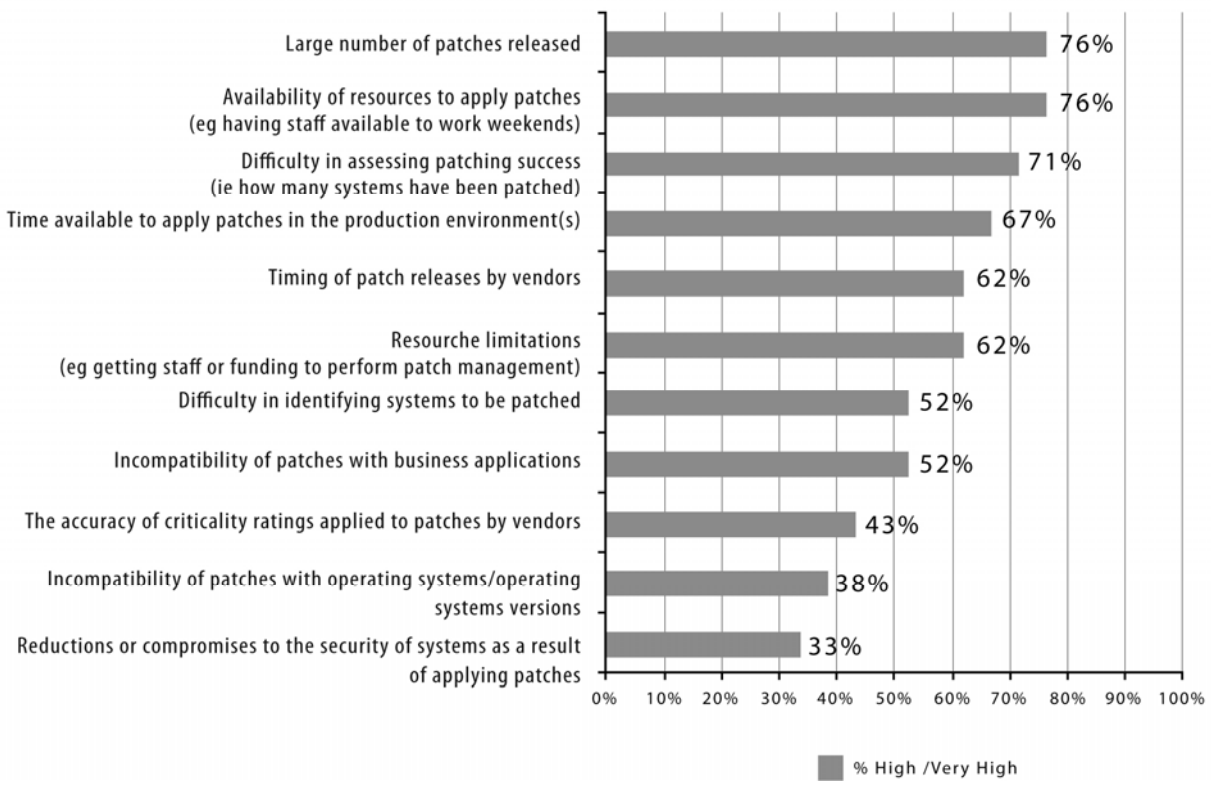
De ICT-beheerders krijgen teveel aan informatie en hebben te weinig tijd om hierop adequaat te reageren, zou kort samengevat de conclusie kunnen zijn. ICT-organisaties die niet beschikken over een eigen team van ICT-beveiligingsspecialisten, verkrijgen hun informatie over nieuw ontdekte kwetsbaarheden of kwaadaardige codes veelal van publieke mailinglijsten, productleveranciers of commerciële informatiedienstverleners. De aspecten analyseren en filteren zijn volgens onderzoeksbureau Gartner [HEIS04] de belangrijkste verschillen tussen deze bronnen.

Analyseren: leverancierneutrale productspecialisten *analyseren* de meldingen en geven een omschrijving van het probleem, inclusief een inschatting van de gevoeligheid en aanbevelingen voor een adequate response.

Filteren: met name de commerciële informatiedienstverleners bieden via het world wide web de mogelijkheid om de stroom aan berichten te *filteren* op basis van de behoeften en de noodzaak van de klant.

Naast het probleem van het aantal berichten speelt ook het aspect van adequate afhandeling van de berichten binnen de bestaande beheerprocessen [FELL04]. Grotere ondernemingen hebben hun ICT-organisatie en -processen veelal ingericht volgens de ITIL methodologie. Hierdoor verlopen de meeste beheerprocessen, waaronder wijzigingenbeheer, volgens een vast patroon. De ICT-systeembeheerder is hierdoor minder flexibel in zijn activiteiten en gebonden aan vaste wijzigingsprocedures, wat weer een nadeel kan zijn bij het pro-actief en snel wegnemen van nieuw ontdekte kwetsbaarheden op computersystemen [POAG04]. Figuur 2 geeft enkele resultaten weer van een onderzoek naar de problematiek van 'patch management' van de bij de ISF aangesloten organisaties[9] . Voor kwetsbaarhedenbeheer, en dan vooral responsetijden op gepubliceerde patches, zijn in de literatuur geen harde normen gevonden. In de praktijk worden informele normen gehanteerd, zoals bijvoorbeeld het streven om urgente patches binnen een dag te installeren.

[9] Met toestemming van het ISF verkregen resultaten van ISF's Special Interest Group 'Patch Management', London 30 november 2004.



Figuur 2: ISF onderzoek Patch Management 2004

Zo geeft zevenenzestig procent van de respondenten aan dat het aspect ‘timing of patch releases’ een hoog tot zeer hoog probleem is. Zesenzeventig procent beschouwt het grote aantal vrijgegeven patches als een probleem en eenenzeventig procent van de respondenten zegt dat het tijdsaspect bij het implementeren van patches in de productieomgeving een issue is. Uit het onderzoek blijkt verder dat een beperkt aantal respondenten gebruik maakt van geautomatiseerde patch management tools. Tweeëntwintig procent van de respondenten spreekt van ‘geforceerde’ implementatie (in casu automatische installatie). Er wordt hierbij relatief vaak gebruik gemaakt van zelfontwikkelde tools (vijfenzeventig procent).

Het onderzoek bevestigt het beeld dat organisaties problemen hebben met het gestructureerd implementeren van beveiligingsherstelsoftware (security patches). Microsoft, een van de belangrijkste spelers op het gebied van kantoorautomatisering, heeft enige jaren geleden besloten om het aantal patchreleases drastisch te beperken. Sinds november 2004 worden patches in principe standaard eenmaal per maand op een dinsdag naar buiten gebracht. De donderdag hieraan voorafgaand wordt bondig een waarschuwing afgegeven met naam en aanduiding van het gevaar en enige algemene informatie over de patch [RIPP04]. Ofschoon er indicaties zijn dat tekortkomingen in patchmanagement in een aantal gevallen de oorzaak zijn van daadwerkelijke incidenten - waaronder inbraken, diefstal en denial-of-service – bestaan hierover geen betrouwbare cijfers.

1.3.3. Versnippering van beveiligingstaken

Het tijdsaspect is niet het enige probleem. Beveiliging in grotere ondernemingen omvat vaak meerdere disciplines. Zo wordt bij banken onder meer onderscheid gemaakt tussen beveiliging van personen, beveiliging van (gelds)waarden, beveiliging van gebouwen en beveiliging van informatie. Vanwege de specifieke taakstelling en het vereiste kennisniveau is het beheersen van deze disciplines traditioneel belegd bij verschillende afdelingen. Zo is er meestal sprake van een separate afdeling die verantwoordelijk is voor het beheer van de gebouwen en de portefeuille fysieke beveiliging en bewaking in beheer heeft. Beveiliging van waarden is tegenwoordig vaak uitbesteed aan gespecialiseerde bedrijven en informatiebeveiliging is meestal ondergebracht bij de voor ICT verantwoordelijke afdeling binnen het bedrijf.
Andere disciplines die te maken hebben met het onderwerp beveiliging zijn de interne accountantsdienst, de afdelingen risicomanagement en juridische zaken en afdelingen die zich bezig houden met fraude-onderzoek.

Door deze versnippering van beveiligingsverantwoordelijkheden en -kennis kunnen er problemen ontstaan met de coördinatie en tijdige beantwoording van incidenten die meerdere beveiligingsdisciplines raken. ‘Phishing’ is een voorbeeld van een dergelijke incidentencategorie. Bij ‘Phishing’ [HAFK04] maken veelal in het buitenland gevestigde criminelen gebruik van misleidende trucs om via het Internet identiteitsgegevens van klanten, waaronder pincodes en creditcardgegevens, te achterhalen met als doel deze gegevens te gebruiken voor het plegen van fraude. Bij het behandelen van een geconstateerd phishingincident is ICT-kennis nodig om te achterhalen welke spoofing-technieken zijn gebruikt en waar de Internet hostingprovider zich bevindt[10]. Voor het laten verwijderen van de website is vaak juridische ondersteuning nodig en voor het achterhalen van de dader(s) is kennis van fraude-onderzoeksmethoden noodzakelijk. Ook is kennis van en toegang tot de organisatie van politie en justitie van belang, bijvoorbeeld voor het doen van aangifte in het kader van opsporing en vervolging.

1.3.4. Gebrek aan kennis

Het afhandelen van incidenten met strafrechtelijke componenten vereist naast een adequate organisatie een zorgvuldige aanpak. Voor het opsporen en eventueel laten vervolgen zijn een correcte bewijsvergaring en bewijsbewaring noodzakelijk. Hiervoor is kennis op het gebied van forensisch ICT-onderzoek nodig. De onderzoeker dient tijdens het onderzoek bovendien te beschikken over specifieke hulpmiddelen. Vaak ontstaat er een spanningsveld tussen de bij het incident betrokken disciplines. Zo zal vanuit forensisch perspectief een onderzoeker aanwezig bewijsmateriaal, afkomstig van bijvoorbeeld logbestanden, nader willen analyseren, wat veelal een situatie van ‘bevriezing’ met zich meebrengt [MAPR01]. De ICT-beheerafdeling zal echter zo snel mogelijk de gevolgen van een incident willen wegnemen met als doel het herstellen van de beschikbaarheid van de dienstverlening.

Om kennis te bundelen en coördinatie te bevorderen hebben een aantal organisaties de afgelopen jaren een zogeheten computer security incident response team (CSIRT) opgericht. Primaire doel van dergelijke teams is het bieden van vooral technische kennis

[10] Bijvoorbeeld middels het gebruik van ‘whois-databases’ voor het verkrijgen van registratie-informatie van het te onderzoeken IP-adres.

en ondersteuning aan de ICT-beheerorganisatie om de gevolgen van een aan ICT-beveiliging gerelateerd incident te beperken.

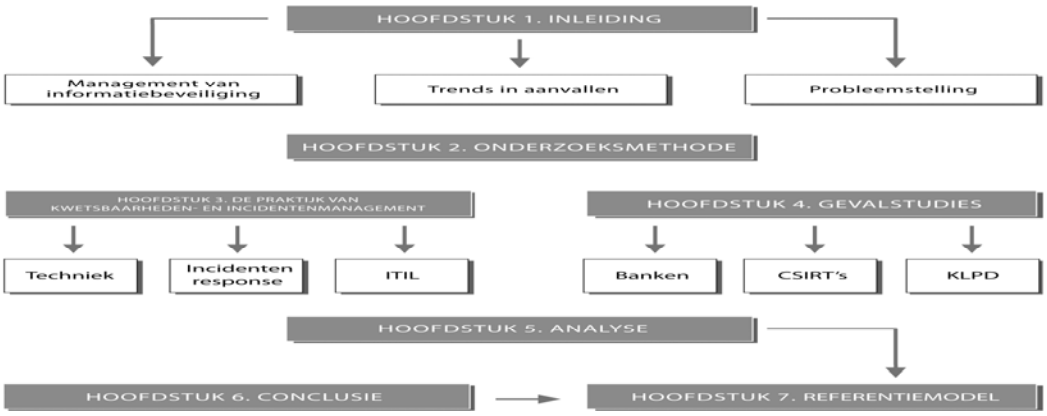
1.4. Structuur

Dit boek beschrijft het onderzoek naar kwetsbaarheden- en incidenteninformatie[11] binnen complexe, informatieverwerkende ICT beheerorganisaties. De problematiek wordt vanuit twee gezichtspunten benaderd:

1. generieke technologische ontwikkelingen op het gebied van detectie van indringersactiviteiten en van kwetsbaarheden, én
2. de inrichting van ICT-beheerprocessen.

Centraal in het onderzoek staat de wijze waarop ICT-organisaties hun beheerprocessen hebben ingericht om kwetsbaarheden- en incidenteninformatie te verzamelen, te analyseren en te beantwoorden.

Het onderzoek is in 2002 gestart en omvat naast een literatuuronderzoek drie gevalstudies in Nederland. Het resultaat van het onderzoek is beschreven in zeven hoofdstukken, zie figuur 3. Hoofdstuk 1 geeft een inleiding in het managen van informatiebeveiliging, de relatie tussen informatiebeveiliging en risicomanagement en aanvalstrends. In hoofdstuk 2 worden enkele hypothesen, de probleembeschrijving en onderzoeksdoelstelling en -methode nader uiteengezet. Onder de titel ‘De praktijk van kwetsbaarheden- en incidentenresponsemanagement’ worden in hoofdstuk 3 een aantal technische en organisatorische praktijkimplementaties met betrekking tot kwetsbaarheden- en incidentenresponse beschreven. De drie uitgevoerde gevalstudies zijn in hoofdstuk 4 nader uitgewerkt. Hoofdstuk 5 en 6 bevatten achtereenvolgens de analyse en conclusie, gebaseerd op de beschouwde praktijkimplementaties (hoofdstuk 3) en de uitgevoerde gevalstudies (hoofdstuk 4). Hoofdstuk 7 tenslotte omvat een procesmodel voor kwetsbaarheden- en incidentenresponse, die is opgesteld naar aanleiding van de bevindingen en conclusies uit het onderzoek.



Figuur 3: de structuur van het proefschrift

[11] Onder incidenten en kwetsbaarheden worden in dit boek verstaan aan ICT-beveiliging gerelateerde incidenten en kwetsbaarheden, tenzij dit anders wordt vermeld.