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

Hafkamp, W.H.M.

Publication date
2008

2. Onderzoeksmethode

In deze paragraaf worden de onderzoeksvraag, de onderzoeksmethode en de verwachte onderzoeksresultaten nader uiteengezet.

2.1. Onderzoeksvraag

Dit onderzoek richt zich op de hypothese dat de huidige mechanismen voor het omgaan met kwetsbaarheden en incidenten niet optimaal functioneren binnen ICT-beheerorganisaties. Onduidelijk is echter of er een samenhang is – en zo ja welke – met de wijze waarop ICT-beheer is ingericht. Als beschreven in hoofdstuk 1 wordt in veel gevallen de de facto standaard ITIL gebruikt.

De centrale onderzoeksvraag luidt:

Hoe reageren organisaties met op ITIL-gebaseerde ICT-beheerprocessen op kwetsbaarheden- en incidenteninformatie?

De onderzoeksvraag wordt vanuit verschillende invalshoeken beantwoord door middel van vier deelvragen.

2.1.1. Definities

De ICT-wereld in zijn algemeenheid en ICT-beveiliging in het bijzonder kennen veel termen, afkortingen en definities. Verschillen in definities met betrekking tot begrippen als ‘incident’ en ‘kwetsbaarheid’ kunnen leiden tot interpretatiefouten bij de analyse. Ook wordt het uitwisselen van informatie tussen organisaties moeilijker, als er niet sprake is van een gezamenlijk begrippenkader. De eerste deelvraag betreft dan ook het aspect ‘definities’.

Deelvraag 1:	*Hoe kunnen ICT-beveiligingsincident en ICT-beveiligingskwetsbaarheid worden gedefinieerd?*

Toelichting Tijdens het onderzoek zal onder meer nagegaan worden of organisaties beide begrippen hanteren en hoe ze van elkaar worden onderscheiden. Verder wordt onderzocht wat organisaties verstaan onder de term ‘cybercrime’.

2.1.2. ITIL-beheerprocessen

Op het Europese continent hebben veel organisaties hun ICT-beheerprocessen ingericht volgens ITIL of een soortgelijke methodiek. ITIL gaat uit van een procesmatige benadering van ICT-beheer. Dit komt vooral tot uitdrukking in het cyclische karakter: plannen, implementeren, evalueren, onderhouden. De service support set en de service delivery set zijn de belangrijkste verzamelingen van beschreven ITIL-processen. De service delivery set maakt onder andere onderscheid in de processen service level management, availability management, IT service continuity management en

performance and capacity management. De service support set richt zich meer op het beheer van de ICT-middelen zelf. In deze set zijn beschreven de processen configuration and asset management, incident management, problem management, change management en release management. Een relatief jonge ITIL-loot is het proces security management dat relaties heeft naar én de service support én de service deliveryprocessen. Hoofddoel van de ITIL-module security management is enerzijds het realiseren van de service level agreementeisen ten aanzien van informatiebeveiliging en anderzijds het realiseren van een zeker basisbeveiligingsniveau [OVER00]. Het proces security management heeft raakvlakken met vrijwel alle hierboven genoemde ITIL-processen.

Deelvraag 2:	*Welke ITIL-beheerprocessen spelen een bepalende rol bij het reageren op incidenten en kwetsbaarheden?*

Toelichting Bij het onderzoeken van deze deelvraag wordt onderzocht welke ITIL service delivery- en service supportprocessen een bepalende rol spelen en hoe deze processen in grote lijnen verlopen.

2.1.3. ICT-calamiteiten

Uit continuïteitsoogpunt beschikken tegenwoordig veel ICT-organisaties over calamiteitenplannen, -procedures en -teams. Het voornaamste doel hiervan is om de ICT-dienstverlening zo snel mogelijk te herstellen na een omvangrijk incident. Een nevendoelstelling is het beperken van verdere schade. Aspecten als communicatie en besluitvorming zijn belangrijke ingrediënten binnen een calamiteitenbeheerproces.

Deelvraag 3:	*Hoe verlopen incidentenafhandelingsprocessen binnen organisaties?*

Toelichting Door een gevalstudie wordt onderzocht of organisaties voor afhandeling van ernstige incidenten beschikken over een calamiteitenprocedure en –organisatie. Ook wordt in dit kader onderzocht welke elementen van belang zijn bij een forensisch ICT-onderzoek.

2.1.4. Computer emergency response teams

De term computer emergency response team (CERT) is in 1988 ontstaan, nadat de Morris-worm een explosie van kopieën van zichzelf verspreidde naar andere op het Internet aangesloten computers [KOSS00]. Het programma resulteerde in een ‘computer shutdown’ van ongeveer tien procent van alle, wereldwijd op het Internet aangesloten computers. Dit eerste majeure computerbeveiligingsincident leidde tot de oprichting van het Computer Emergency Response Team Coordination Center © (CERT/CC)) door het toenmalige Amerikaanse Defense Advanced Research Projects Agency.

Het CERT/CC wordt beheerd door het Sofware Engineering Institute van Carnegy Mellon University in Pittsburgh Amerika. Dit instituut is een door de federale overheid gesubsidieerd onderzoekscentrum en wordt onder meer gesponsord door het Amerikaanse Department of Defense.
Al snel volgden andere landen het voorbeeld. In Nederland werd in juli 1991 CERT-NL als overkoepelend incident response team voor SURFnet en de daarop aangesloten

netwerken opgericht. Andere landen met actieve 'nationale' teams – niet in alle gevallen nationaal in de zin van door of ten behoeve van de nationale overheid ingesteld maar wel in de zin van de eigen natie als aandachtsgebied beschouwend - zijn onder meer Italië, Canada, Australië en Slovenië. De teams zijn veelal samengesteld uit expertteams werkzaam binnen de rekencentra die de academische netwerken beheren. Deze netwerken waren van oudsher via het Internet aan elkaar gekoppeld.

Deelvraag 4: *Wat is het doel en de werking van computer emergency response teams?*

Toelichting Bij het onderzoek naar opzet en werking van het computer emergency response team wordt onder meer gekeken naar de aanwezigheid van een zogeheten operationeel raamwerk en naar de organisatorische inrichting en positionering van het team.

2.2. Onderzoeksmodel

Het onderzoek omvat zowel een literatuurstudie als een aantal vergelijkende gevalstudies. Begin 2001 is gestart met een literatuurstudie naar een aantal technische ontwikkelingen rondom ICT-beveiliging. In de loop van dat jaar is de studie uitgebreid met een onderzoek naar de ITIL-methodiek en naar cybercrime en computer security incident response teams. In het eerste kwartaal 2003 is gestart met de uitvoering van een aantal kortdurende gevalstudies bij Nederlandse banken en aansluitend bij enkele Nederlandse computer security incident response teams. In 2004 tenslotte is een gevalstudie uitgevoerd bij het Korps Landelijke Politiediensten. De totale doorlooptijd van de gevalstudies bedroeg ongeveer negen maanden.
Duidelijk is dat het onderzoeksobject een beperkte, doch cruciale, deelverzameling vormt van de onderewrepen die wel worden samengevat onder de noemer 'informatiebeveiliging'[OVRS05].

2.3. Empirisch onderzoek

2.3.1. Vergelijkende gevalstudies

Binnen het onderzoek is gekozen voor het uitvoeren van drie gevalstudies. De eerste gevalstudie betrof een onderzoek bij tien Nederlandse banken naar de globale opzet van hun aan ICT-beveiliging gerelateerde kwetsbaarheden- en incidentenmanagementprocessen. De keuze voor een onderzoek bij banken lag voor de hand omdat financiële instellingen de afgelopen tien jaren een grote mate van automatisering hebben doorgemaakt en veiligheid traditioneel hoog in het vaandel hebben staan. De banken waren bereid mee te werken aan het onderzoek, indien de gegevens zouden worden geanonimiseerd en tijdens het onderzoek de haalbaarheid naar interbancaire samenwerking op één of meer aspecten van kwetsbaarheden- en incidentenmanagement zou worden meegenomen. Bij de tweede gevalstudie is gekeken naar de inrichting en werkwijze van computer security incident responseteams in Nederland. Tijdens deze gevalstudie zijn het team van SURFnet en aansluitend twee universitaire teams van respectievelijk de universiteiten van Nijmegen en Groningen onderzocht. Om te weten te komen wat er allemaal speelt bij het onderwerp cybercrime, is gekozen voor een derde gevalstudie, te weten bij de groep digitale recherche van het Korps Landelijke Politiediensten in Driebergen. Een onderdeel van deze studie betrof een

onderzoek naar de aanpak en coördinatie van een groot incident, het zogeheten kastje-incident in 2003 bij een bank in Nederland. De bank heeft hiervan destijds aangifte gedaan bij het Bureau Digitale Expertise van de politie Amsterdam-Amstelland.

Validiteit
Tijdens het onderzoek is gewerkt met een vooraf samengestelde vaste set van omschrijvingen, termen en afkortingen. Bij het operationaliseren van de begrippen is besloten om een keuze te maken uit bestaande, aan het onderzoeksonderwerp gerelateerde object- en procesdefinities, en niet zelf begrippen te definiëren om zoveel mogelijk aan te sluiten bij de onderzoeksobjecten.

Om de interne validiteit van de meervoudige gevalstudie te waarborgen werden zogeheten member checks toegepast. Gespreksverslagen en overige vastleggingen werden voorgelegd aan betrokkenen om vast te stellen of de interpretaties zoals die de onderzoeker(s) voor ogen stonden, herkenbaar waren. Op deze wijze was het mogelijk om fouten in de gegevens of interpretaties zichtbaar te krijgen en te corrigeren.

Documentenstudie
Bij de onderzochte gevallen is gebruik gemaakt van divers documentatiemateriaal, onder meer (jaar)verslagen, beleidsstukken, organisatieschema's, (incident)procedures en trendrapportages.

Interviews
Naast het verzamelen en bestuderen van documentatie zijn ook zogeheten informanteninterviews gehouden[12]. In overleg met de contactpersonen is bij de diverse gevalstudies bepaald welke informanten werden geïnterviewd. Het uitgangpunt was dat bij alle te onderzoeken gevallen één of meer interviews werden afgenomen bij gelijksoortige informanten. Hierbij ging het onder meer om de security manager van de ICT-afdeling(en) bij banken, de coördinator bij de computer security incident response teams en de digitaal rechercheur binnen de politieorganisatie.

Eigen waarneming
Bij twee gevalstudies is verder gebruik gemaakt van eigen waarneming ter ondersteuning van de interviews en de documentenstudie. Per gevalstudie zijn minimaal één tot maximaal acht dagdelen, verspreid over een periode van drie maanden, gebruikt voor eigen waarneming.

2.3.2. Gevalstudie banken

De vragenlijsten bij de interbancaire gevalstudie bestonden uit vier blokken met in totaal dertien hoofdvragen en meerdere subvragen. Het onderzoek omvatte zowel gesloten als open vragen. Het eerste blok vragen (A) betrof de wijze van beantwoording van incidenten en kwetsbaarheden. De overige drie blokken met vragen (B-D) hadden betrekking op een mogelijke samenwerking tussen de deelnemende banken. De vragen, antwoorden en resultaten van het onderzoeksdeel betreffende de mogelijke interbancaire samenwerking zijn in dit proefschrift niet opgenomen.

[12] Bij de uitvoering van de gevalstudies zijn enkele standaardvragenlijsten en -checklijsten gehanteerd (zie bijlage 1).

2.3.3. Gevalstudie computer security incident response teams

Ook bij het onderzoek naar de drie computer security incident response teams binnen het hoger onderwijs is gebruik gemaakt van een vragenlijst. Bij het verzamelen van informatie zijn naast de interviews documenten geraadpleegd zoals werkprocedures, jaarverslagen en publicaties. De vragen hadden betrekking op de onderwerpen historie, activiteiten, organisatie, procedures, hulpmiddelen en interne en externe kontakten.

2.3.4. Gevalstudie korps landelijke politiediensten

Bij de interviews met de politiemedewerkers[13] en interviews met medewerkers van de afdeling veiligheidszaken bij een Nederlandse bank is gebruik gemaakt van een tweetal vragenlijsten met in totaal zestien vragen. De vragen hadden voornamelijk betrekking op de wijze waarop het interne incidentenafhandelingsproces geschiedt, zoals het proces van aangifte en de wijze van verzamelen en analyseren van bewijsmateriaal.

Bij elk van de gevalstudies is gebruik gemaakt van op maat gemaakte vragenlijsten, zie hiervoor de bijlage.

2.4. Onderzoeksresultaten

Binnen de context van dit onderzoek wordt ICT-beveiliging beschouwd als het geheel aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van bedrijfsinformatie te waarborgen. De maatregelen kunnen preventief, detectief of repressief van aard zijn. Het onderzoek naar kwetsbaarhedenresponsemanagement beoogt een bijdrage te leveren aan het verbeteren van bestaande, aan ITIL gerelateerde, processen voor het afhandelen van kwetsbaarheden- en incidenteninformatie binnen een ICT-beheerorganisatie. Maatregelen in dit kader zijn vooral bedoeld om kwetsbaarheden en incidenten te voorkomen danwel tijdig te signaleren. Het onderzoek naar incidentenresponsemanagement kijkt met name naar de repressieve kant van security management. Met andere woorden welke maatregelen heeft een organisatie getroffen om een geconstateerd incident zo efficiënt en effectief mogelijk op te lossen.

Uit de onderzoeksresultaten worden twee vereenvoudigde referentiemodellen ontwikkeld, een voor de beantwoording van kwetsbaarheden en een voor de beantwoording van incidenten. In het eerste model wordt per processtap aangegeven welk ITIL-proces van toepassing is. Ook wordt een indicatie gegeven van de gemiddelde tijdseenheid per processtap. Deze tijdseenheden zijn niet normatief maar indicatief en kunnen worden beschouwd als ‘best practise’. De waarden zijn in juni 2006 bij enkele leden van het internationale beveiligingsforum I-4 getoetst. Het model voor de beantwoording van incidenten geeft aan hoe de eerste analysefase van incidentenberichten kan worden verbeterd. In dit model wordt weergegeven hoe de relatie is tussen de ICT-helpdesk, het computer security incident response team en de ICT-(systeem)beheerorganisatie bij de afhandeling van incidenten. Tevens worden ten behoeve van systeembeheerders enkele vuistregels gegeven voor forensisch ICT-onderzoek.

[13] Internet- en digitaalrechercheurs werkzaam bij het Team Digitale Expertise en Bureau Digitale Expertise van respectievelijk het Korps Landelijke Politiediensten en de Politie Amsterdam-Amstelland.

De onderzoeksresultaten zijn een hulpmiddel voor grotere ICT-organisaties die hun beheerprocessen hebben ingericht volgens de principes van ITIL service delivery en ITIL service support. Het referentiemodel voor de afhandeling van kwetsbaarheden is met name bedoeld voor ICT-beveiligingsfunctionarissen, problem managers en change managers die betrokken zijn bij de afhandeling van kwetsbaarheden. Het referentiemodel voor de analyse van incidenten is vooral een hulpmiddel voor de eerstelijnsondersteuning van de ICT-beheerorganisatie, meestal een centrale helpdesk.

In dit onderzoek is voor zover bekend voor het eerst aandacht besteed aan kwetsbaarheden- en incidentenbeheersing binnen grote organisaties met meer of minder gestandaardiseerde ICT-beheerprocessen. De wetenschappelijke bijdrage van dit proefschrift bestaat derhalve uit een verhoogd of zelfs nieuw inzicht in deze samenhang. Door het proces van kwetsbaarhedenafhandeling en incidentenbeheersing effectiever te maken kunnen de ontwikkelde referentiemodellen daarnaast bijdragen aan een samenleving die minder gevoelig is voor kwetsbaarheden en minder schade ondervindt van incidenten.