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

Hafkamp, W.H.M.

Publication date
2008

6. Conclusie

In het onderzoek is nagegaan of organisaties adequaat reageren op informatie met betrekking tot nieuw ontdekte kwetsbaarheden of incidenten door gebruik te maken van gestandaardiseerde ICT-beheerprocessen.

Als eerste is onderzocht wat organisaties verstaan onder aan ICT-beveiliging gerelateerde kwetsbaarheden en incidenten. Het gebruik van dezelfde precisie en gedetailleerdheid bij het beschrijven en indelen van incidenten is van belang om de ernst en scope vast te kunnen stellen en geeft daarnaast een beter inzicht in de (pogingen tot) het treffen van maatregelen en de daarbij behorende inspanning en kosten. Uit de gevalstudies is gebleken dat een en ander in de praktijk nog geen gemeengoed is.

Voorafgaand aan de uitvoering van de gevalstudies werd al snel duidelijk dat ITIL dé standaard is bij het inrichten van ICT-beheerprocessen. Voor het onderzoek was het van belang om vast te stellen welke ITIL-processen essentieel zijn bij kwetsbaarheden- en incidentenresponse. Uit het onderzoek is gebleken dat het hierbij gaat om de processen incident management en change management. Daarbij is gebleken dat vooral de afhandeling van externe kwetsbaarhedeninformatie onvoldoende is geborgd in de ITIL-beheerprocessen van de onderzochte organisaties.

Een derde aspect dat is onderzocht, is hoe organisaties omgaan met het afhandelen van incidenten. Gebleken is dat er zich binnen de onderzochte organisaties meerdere incidenten hebben voorgedaan, gerelateerd aan ICT-beveiliging. Deze incidenten konden alle worden opgelost en hebben vrijwel nergens geleid tot een calamiteit.
Wel is gebleken dat de doorlooptijd van afhandeling van incidenten beduidend langer werd als ook disciplines van buiten de ICT-organisatie worden betrokken bij de afhandeling. In een enkele situatie liep de doorlooptijd op tot enige maanden.

In de afgelopen jaren hebben veel organisaties een aparte organisatie ingericht voor het coördineren en afhandelen van aan ICT-beveiliging gerelateerde incidenten. Deze teams, aangeduid als computer security incident responseteams, zijn vaak samengesteld uit ICT-specialisten met diepgaande kennis op een of meer ICT-gebieden. In een gevalstudie is onderzocht hoe de teams zijn samengesteld, wat het doel is en hoe de teams werken. Bij de beoordeling van de gevalstudies bleek dat de inzet van deze teams bij banken nog geen gemeengoed is. Bij incidenten valt men terug op de aanwezige ICT-beveiligingfunctionaris(sen) of, in geval van ernstige incidenten, maakt men gebruik van generieke calamiteitenteams.

De afhandeling van incidenten waarbij een of meer strafrechtelijke componenten een rol spelen, vereist meestal een sporenonderzoek. Een gevalstudie bij het Korps Landelijke Politiediensten heeft duidelijk gemaakt dat het verzamelen en bewaren van bewijsmateriaal, het gebruik van speciale onderzoekstools en het vastleggen van onderzoekshandelingen van groot belang is, indien van een incident aangifte wordt gedaan bij politie en justitie.

De centrale onderzoeksvraag luidt*: Hoe reageren organisaties met op ITIL-gebaseerde ICT-beheerprocessen op kwetsbaarheden- en incidenteninformatie?* Uit het onderzoek kan worden geconcludeerd dat binnen de bancaire sector in Nederland de analyse en afhandeling van informatie met betrekking tot kwetsbaarheden verbeterd kan worden.

Ook de analyse en afhandeling van incidenten kan effectiever als het gaat om incidenten die niet uitsluitend binnen de scope van de ICT-organisatie kunnen worden opgelost.

Ofschoon het onderzoek zich heeft gericht op de bancaire sector, is de stelling verdedigbaar dat de conclusies een bredere geldigheid kennen. De redenen hiervoor zijn:

- onderzochte ICT-beheerprocessen zijn generiek en niet specifiek voor de bancaire sector
- in de bancaire sector is ICT een wezenlijk onderdeel van het primaire proces en is de noodzaak om risico's te beheersen zeer hoog, hoger dan in veel andere sectoren.

In de paragrafen 6.1 tot en met 6.4 wordt nader ingegaan op de vier onderzoeks-deelvragen.

6.1. Definities & taxonomieën

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

Incident
In de literatuur is een relatief grote variëteit aan definities en classificaties met betrekking tot aan ICT-beveiliging gerelateerde incidenten terug te vinden.

ITIL Security Management [CAOP99] beschrijft informatiebeveiligingsincidenten als gebeurtenissen die schade kunnen veroorzaken aan de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerking. Hierbij kan het gaan om opzettelijke activiteiten of 'ongelukken'. Het begrip incident dient hierbij zeer ruim te worden beschouwd, namelijk *elke* gebeurtenis die niet behoort tot de standaardwerking van een systeem.

FIRST[126], het wereldwijde forum van incident response en securityteams definieert een informatiebeveiligingsincident als een gebeurtenis met daadwerkelijk of potentieel nadelige effecten op computer- of netwerkhandelingen, die resulteert in:

- fraude, verspilling of misbruik
- het in opspraak brengen van informatie
- verlies of schade aan eigendom of informatie.

Het binnendringen van computersystemen, exploitatie van technische onvolkomenheden en introductie van computervirussen of andere kwaadaardige software zijn volgens FIRST voorbeelden van beveiligingsincidenten.

Het CERT/CC kiest voor een andere benadering. Het beschrijft een beveiligingsincident als een activiteit die een expliciet of impliciet (informatie)beveiligingsbeleid schendt. Hoewel deze definitie vanwege haar praktische werking voordelen biedt boven de door FIRST gehanteerde definitie, kleeft er ook een bezwaar aan. Er wordt immers verondersteld dat organisaties een uniform beveiligingsbeleid hanteren. Om aan dit

[126] Zie http://www.first.org.

bezwaar tegemoet te komen heeft het CERT/CC op zijn website activiteiten gekarakteriseerd die wereldwijd zijn erkend als schendingen van security policies. Deze activiteiten zijn:

- pogingen (succesvol en niet-succesvol) ongeautoriseerd toegang te krijgen tot een systeem of de gegevens daarvan
- niet-gewenste verstoring of dienstontzegging
- ongeautoriseerd gebruik van een verwerkingssysteem of van opgeslagen gegevens
- wijzigingen van hardware-, firmware- of softwarekarakteristieken zonder kennis van de eigenaar, diens instructie of toestemming.

De in 2004 gepubliceerde norm NPR-ISO/IEC TR 18044 (information security incident management) maakt onderscheid tussen een information security *event* en information security *incident*. Een information security event is hierbij een geïdentificeerde gebeurtenis op een systeem, dienst of netwerk, waarbij indicaties aanwezig zijn van een mogelijke inbreuk op een informatiebeveiligingsbeleid of indicaries van een tekortkoming aan beschermingsmaatregelen. Een information security incident wordt gedefinieerd als een of meerdere ongewenste of onverwachte information security events die een significante waarschijnlijkheid hebben op het compromitteren van business operations of die de informatiebeveiliging bedreigen.

Uit de gevalstudies bij de banken kwam geen sterk beeld naar voren van het gebruik van definities bij aan ICT-beveiliging gerelateerde incidenten danwel het hanteren van categorieën of klassen van incidenten. Tijdens de interviews werd door geïnterviewden een aantal voorbeelden gegeven van incidenten in een poging het begrip ICT-beveiligingsincident nader te omschrijven. Het voorstel om de FIRST definitie te hanteren tijdens het verdere onderzoek werd door alle onderzochte organisaties aanvaard. De meeste banken hanteerden geen *formele* classificering van aan ICT-beveiliging gerelateerde incidenten. Slechts bij één bank werd een ICT-beveiligingsincident opgesplitst in tien subcategorieën.

Twee van de drie onderzochte universitaire computer security incident responseteams categoriseerden aangemelde incidenten. Hierbij werden deels dezelfde klassenindeling en definities gebruikt. Voorbeelden zijn de klassen spam en poortscan.

Kwetsbaarheid
De term kwetsbaarheid blijkt minder vaak voor te komen in de literatuur dan de term incident. ITIL Security Management uit 1999 benoemt de term vulnerability bijvoorbeeld niet. De ITIL Glossary[127] geeft een generieke, niet-ICT-specifieke definitie *een kwetsbaarheid is een zwakte die kan worden benut door een dreiging*. Hierbij worden enkele voorbeelden gegeven zoals een wachtwoord dat nooit is veranderd of een tapijt dat is gemaakt van brandbaar materiaal.
De definitie van kwetsbaarheid in de Internet Security Glossary (IETF RFC2828) spitst zich toe op de ICT-omgeving. Hier wordt de term kwetsbaarheid omschreven als een fout of zwakte in een (computer)systeemontwerp of -implementatie of -operatie die kan worden gebruikt om het beveiligingsbeleid van het systeem te schenden. Hier geldt hetzelfde bezwaar als bij de incidentdefinitie van CERT/CC, namelijk dat als zeker wordt

[127] Zie http://www.best-management-practise.com/glossary/itil_glossary.htm

verondersteld dat er een systeembeveiligingsbeleid aanwezig is. In geen van de gevalstudies is een voorkeur voor een bepaalde kwetsbaarheidsdefinitie gebleken.

Uit de interviews is naar voren gekomen dat de definities van incident en kwetsbaarheid bij de banken in de praktijk weinig aandacht krijgen. Bij de onderzochte computer security incident responseteams was meer aandacht voor het eenduidig beschrijven en indelen van incidenten en kwetsbaarheden. Frequente uitwisseling van informatie over incidenten en kwetsbaarheden tussen de computer security incident response teams en het (extern) publiceren van statistieken over incidenten en kwetsbaarheden zijn mogelijke motieven.

6.2. De impact van ITIL

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

6.2.1. Literatuuronderzoek

Een aantal ITIL-beheerprocessen hebben een nauwe relatie met kwetsbaarheden- en incidentenresponse. Uit het literatuuronderzoek is bij vijf processen een directe relatie geconstateerd.

Information Technology Service Continuity Management
Met het ITIL ITSCM-proces als opvolger van de ITIL module Contingency Planning is het accent ten aanzien continuïteitsbeheer verlegd van correctief naar preventief handelen. Het bepalen van de impact op de bedrijfsprocessen, het vaststellen van de ICT-risico's en vervolgens de te voeren strategie leveren een groot scala aan preventieve maatregelen en herstelmaatregelen op. Met name in de beschrijving van de herstelactiviteiten binnen ITSCM krijgt uitwijk een prominente plaats. Er worden diverse uitwijkvarianten beschreven binnen ITSCM, variërend van 'cold standby' voor organisaties die tweeënzeventig uur of langer kunnen functioneren zonder herinrichting van alle ICT-faciliteiten tot en met 'hot standby' voor organisaties waarbij uitwijk en direct herstel van ICT faciliteiten na een calamiteit noodzakelijk is. Uitwijken en herstel van ICT-dienstverlening is voornamelijk geschikt bij infrastructurele incidenten in grote rekencentra [GOGH01]. Voor bepaalde typen van calamiteiten zoals beschikbaarheidaanvallen via het Internet of grootschalige soft- of hardwarefouten is uitwijk echter geen optie. Na een herstart op de uitwijklocatie is de kans immers groot dat zich daar een herhaling van de calamiteit voordoet.

Availability management
Het zichtbaar maken en kwantificeren van beschikbaarheidseisen is een belangrijke toegevoegde waarde van availability management. Uiteraard heeft dit gevolgen voor de keuze van ICT-componenten. Hierbij is te denken aan aspecten als het dubbel uitvoeren van onderdelen van de ICT-infrastructuur en de inzet van fault-tolerant[128] systemen.

[128] Fault-tolerant = een computer of netwerk blijft functioneren wanneer een component faalt.

Availability management kan echter ook een rol spelen binnen een incidentenresponse proces. Zo geven de beschikbaarheideisen een belangrijke aanwijzing welke incidenten als eerste in behandeling dienen te worden genomen. Ook in een situatie van uitwijk of herstel kunnen de eisen ten aanzien van beschikbaarheid een prioriterende werking hebben.

Security management
Tot het verschijnen van het boek ITIL Security Management [CAOP99] was beveiliging binnen ITIL vooral gericht op het waarborgen van de beschikbaarheid van de ICT-dienstverlening. De elementen integriteit en vertrouwelijkheid (of exclusiviteit) kwamen nauwelijks aan bod [BREM98]. Een aparte module over security management binnen de ITIL-reeks was noodzakelijk omdat binnen de ICT-beheerorganisatie beveiliging steeds meer als een afgebakend proces wordt beschouwd met eigen verantwoordelijkheden en eigen verantwoordelijken. ITIL Security Management heeft een nauwe relatie met een aantal andere ITIL-processen. Toepassing van de module wordt daarom alleen als zinvol beschouwd, als organisaties ook de ITIL-processen Service Delivery en Service Support hebben ingericht [SPRU00]. ITIL Security Management besteedt relatief weinig aandacht aan onderwerpen als incidentenresponse. Het boek verwijst hiervoor bijvoorbeeld naar het ITIL-proces Incident Management. Sommige incidenten vergen echter een specifieke aanpak, zoals het veiligstellen van bewijsmateriaal[129]. Dit komt onvoldoende aanbod in de module. Ook wordt de specifieke rol van de beveiligingfunctionaris met betrekking tot kwetsbaarheden- en incidentenresponse niet genoemd.

Problem management
Pro-active problem management richt zich zowel op het analyseren en rangschikken van incidenten in een bepaalde periode (trendanalyse), alsmede op het identificeren van mogelijke zwakke plekken in de infrastructuur. Doel van dit alles is het voorkomen van nieuwe incidenten. In die zin kan problem management binnen de ICT-beheerorganisatie een belangrijke rol spelen bij het interpreteren en prioriteren van externe berichtgeving over kwetsbaarheden en nieuwe aanvalstechnieken. Ook kan de problem manager een impuls geven aan de opvolging van gevonden lekken of zwakke plekken, bijvoorbeeld na het uitvoeren van infrastructurele vulnerability scans. Wel dient een aantal randvoorwaarden aanwezig te zijn. Zo dient de problem manager kennis te hebben van de beveiliging van besturingssystemen van de aanwezige systemen om de berichtgeving op waarde te kunnen schatten. Ook dient de problem manager te beschikken over voldoende draagvlak en bevoegdheid binnen de beheerorganisatie om prioriteit aan de door hem beoordeelde meldingen te geven en opvolging af te dwingen.

Change management
Standaardisatie is een belangrijk uitgangspunt binnen ITIL Change Management. De diverse activiteiten volgen een vast stramien van processtappen. Standaardisatie werkt over het algemeen genomen efficiëntie- en effectiviteitverhogend. Rorive geeft aan dat ITIL-processen uitstekend werken voor het invullen of ondersteunen van security patchmanagement processen [RORI04].
Echter er zijn ook nadelen. Standaardisatie kan een negatief effect hebben op de doorlooptijd van een wijziging. Een incidentenresponseteam wordt soms beperkt in zijn mogelijkheden om tijdig repressieve maatregelen te treffen teneinde het incident te verhelpen of verdere escalatie te voorkomen [HAFK02]. Zeker bij incidenten met een

[129] Bijvoorbeeld autorisatie- en loggingbestanden.

hoge (potentiële) impact op de ICT-dienstverlening, bijvoorbeeld een beschikbaarheidaanval, een door het detectiesysteem ontdekte indringer of een virusuitbraak, dient de gewenste responsetijd eerder in uren dan in dagen te worden uitgedrukt. Gestandaardiseerde, op ITIL-gebaseerde, change management- en configuration managementprocessen zijn meestal niet ingesteld op dergelijke spoedeisende situaties. Het gevolg kan zijn dat bij het beantwoorden van dergelijke incidenten de ITIL Change Management processtappen worden genegeerd of dat er speciale 'bypasses' worden toegepast, zoals het implementeren van updates zonder het uitvoeren van de voorgeschreven testen.

6.2.2. Gevalstudies

Uit de gevalstudie bij Nederlandse banken bleek dat met name de ITIL Service Support processen incident management en change management bepalend zijn bij het beantwoorden van aan ICT-beveiliging gerelateerde kwetsbaarheden en incidenten. Door de inrichting van een centrale helpdeskorganisatie als eerstelijns ondersteuning bij incidenten en problemen en het hanteren van standaardprocedures voor de afhandeling van incidenten en het aanbrengen van systeemwijzigingen zijn de processen voor kwetsbaarheden- en incidentenafhandeling bij de ICT-organisaties van de onderzochte banken in een specifiek keurslijf gegoten.

Bij de meeste onderzochte banken is er verder sprake van geformaliseerde interne ICT-dienstverlening. Dat wil zeggen ICT-activiteiten werden intern doorbelast en er werd gewerkt met formele afspraken in de vorm van service level agreements. Bij deze organisaties speelden ook de processen service level management en availability management een rol. In de service level agreements tussen de ICT-organisatie en de gebruikersorganisaties werden onder meer afspraken gemaakt over de beschikbaarheid van de systemen en applicaties en de datums en tijdstippen waarop onderhoud gepleegd mag worden.

Dit beeld wordt bevestigd bij het kwetsbaarhedenbeheerproces. In vrijwel alle gevallen werd volgens het vigerende change managementproces een standaardwijzigingsverzoek ingediend door systeembeheer, enige tijd nadat de leverancier een nieuwe security patch heeft uitgebracht. Pas bij een situatie van acute dreiging, bijvoorbeeld nadat zich op een systeem- of netwerkcomponent een aan de kwetsbaarheid gerelateerd incident had voorgedaan of de kwetsbaarheid veel media-aandacht had gehad, kreeg de wijziging een hogere prioriteit.

6.3. Calamiteiten

Deelvraag 3: *Hoe verlopen incidentenafhandelingsprocessen binnen organisaties?*

Alle onderzochte banken beschikten over formele calamiteitenplannen en calamiteitenteams. Ook de onderzochte universitaire incidentenresponseteams hadden vergelijkbare escalatieprocedures. Uit de gevalstudies bleek dat een incident zelden heeft geleid tot een calamiteitsituatie. De calamiteitenprocedures bleken in dergelijke situaties goed te werken.

Veel incidenten konden zonder al te veel problemen zelfstandig door de ICT-beheerorganisatie worden opgelost. Een goed voorbeeld zijn geïsoleerde virusincidenten[130]. Dergelijke incidenten worden volgens vaste procedures beantwoord. De afhandeling van complexe incidenten waarbij ook niet-ICT-disciplines betrokken zijn, zoals juridische zaken, veiligheidszaken en communicatie vormden soms wel een probleem. Een inbraak op een computersysteem (hacking) is een voorbeeld van een dergelijk complex incident. De betrokken afdelingen hadden soms tegenstrijdige visies op de afhandeling van het incident. Bij een nader onderzocht incident bleek bijvoorbeeld dat de afdeling belast met fraudeonderzoek de getroffen omgeving wilde bevriezen in het kader van sporenonderzoek en bewijsverzameling. De ICT-afdeling wilde echter zo snel mogelijk herstel van de beschikbaarheid van de betrokken ICT-componenten teneinde de dienstverlening te herstellen.

6.4. De rol van CSIRT's

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

De onderzochte computer security incidentenresponseteams blijken een centrale rol te spelen bij het beantwoorden van aan ICT-beveiliging gerelateerde incidenten. Mede door de grote aantallen gemelde incidenten hebben deze teams veelal een (semi-) permanent operationeel karakter. Hierdoor is niet alleen de bekendheid van deze teams groot bij de ICT-gebruikersgemeenschap, maar zijn de teams ook in staat snel incidenten te prioriteren en de coördinatie en verdere afhandeling van deze incidenten te verzorgen. Ook speelt het al eerder genoemde externe CSIRT-netwerk een belangrijke rol. Het netwerk vervult een belangrijke rol waar het gaat om kennisvergaring rondom nieuwe kwetsbaarheden en biedt de CSIRT-medewerkers mogelijkheden om adviezen en ervaringen met betrekking tot incidenten en kwetsbaarheden te delen.

Bij de banken zijn dergelijke operationele teams nog geen gemeengoed. Incidenten worden hoofdzakelijk volgens het reguliere (ITIL) incidentenmanagementproces aan een beheerder of afdeling toegewezen door een incident- of probleemcoördinator. Bij (dreigende) calamiteiten wordt ad hoc een calamiteitenteam samengesteld, veelal bestaande uit managers van de beheerorganisatie aangevuld met diverse specialisten. Beide elementen beïnvloeden in negatieve zin de doorlooptijd van afhandeling van een incident.

[130] Dat wil zeggen dat één werkplek is besmet met een computervirus.