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

Hafkamp, W.H.M.

Publication date
2008

5. Analyse

5.1. Inleiding

Binnen het onderzoek zijn twee aspecten van ICT-beveiliging nader bekeken: kwetsbaarheden- en incidentenresponse. Onderzocht is op welke wijze organisaties reageren op bepaalde aan ICT-beveiliging gerelateerde gebeurtenissen. Denk hierbij aan het wegnemen van kwetsbaarheden bij ICT-componenten of het verhelpen van de effecten van ICT-incidenten. Dit roept de vraag op wat organisaties (kunnen) doen om te voorkomen dat er kwetsbaarheden of incidenten ontstaan. Preventie dus. Een aspect hiervan is het gebruiken van veilige applicatiesoftware. In paragraaf 5.1.1 wordt hier nader op ingegaan. Ook kan de vraag worden gesteld wat organisaties leren van incidenten. Worden incidenten bijvoorbeeld systematisch geanalyseerd en worden maatregelen op basis van dit leerproces getroffen? In paragraaf 5.1.2 wordt ingezoomd op het PRISMA-model.

5.1.1. Levenscyclus

De levenscyclus van een computerapplicatie bestaat volgens het Amerikaanse NIST uit drie fasen [[FIPS80]: initiatie, ontwikkeling en productie. Na enige tijd van productie zal een uitbreiding of revisie van de applicatie nodig zijn en begint de cyclus opnieuw. Bij de initiatiefase worden de doelen en algemene eisen van de applicatie vastgesteld. De noodzakelijke beschikbaarheid, integriteit en/of vertrouwelijkheid van de applicatie en de applicatiegegevens leveren input voor het eisenpakket. Systeemplanners beschouwen gedurende deze fase alternatieve benaderingen voor een bedoeld systeem, veelal gebaseerd op haalbaarheidsstudies en kostenbatenoverzichten. In de eerste fase dienen ook beveiligingsaspecten te worden meegenomen onder meer in de kostenbatenanalyses. De ontwikkelfase bestaat uit definitie-, ontwikkel-, programmeer- en testactiviteiten. Gedurende elk stadium dient te worden besloten welke beveiligingscontrols toegepast moeten worden. De in de FIPS-standaard bedoelde basiscontrols tijdens ontwikkeling en programmering, hebben betrekking op gegevensvalidatie, verificatie van gebruikersidentiteit, autorisatie, logging, variatieverschillen en encryptie. Sommige van deze controls kunnen (deels) geïmplementeerd worden door de hardware of door het besturingssysteem. De selectie van de controls hangt niet alleen af van de gevoeligheid van de gegevens en het niveau van schade ontstaan door onjuiste handelingen maar hangt ook af van de aanwezigheid van kwetsbaarheden binnen de omgeving waarin de applicatie opereert. Relevant in dit kader is het initiatie uit 2004 genaamd Open Web Application Security Project (OWASP)[121]. OWASP is een vereniging die de OWASP open source gebruikersgemeenschap ondersteunt door het faciliteren van projecten, conferenties en dergelijke met als uiteindelijke doel organisaties te helpen bij het verbeteren van hun applicatiebeveiliging. Het OWASP initiatief levert richtlijnen en ontwikkelt hulpmiddelen voor het produceren van veilige softwarecode. OWASP produceert een top tien van meest kritische beveiligingstekortkomingen in webapplicaties. De eerste versie uit 2004 is in 2007 vervangen door een update [OWAS07]. Het laatste stadium van ontwikkelen betreft testen. Het testen en evalueren van beveiligingscomponenten is met name bedoeld om fouten en tekortkomingen te detecteren. Twee methoden worden nader toegelicht: statische en dynamische evaluatie.

[121] Zie http://www.owasp.org

Bij statische evaluatie worden technieken toegepast als penetratietesten en code reviews om zwakheden in de applicatie boven tafel te krijgen. Bij dynamische evaluatie wordt (een deel van de applicatie) uitgevoerd met testgegevens waarbij de resultaten van de uitvoering worden vergeleken met verwachte of bekende resultaten. Na een goeddoorlopen testfase wordt de applicatie in productie gebracht. Het waarborgen van de integriteit van gegevens in deze fase wordt onder meer gerealiseerd door verificatie van de inputgegevensinputverificatie en door gegevensbeheer, waaronder beheer van gebruikersautorisaties. Bij gegevensbeheer spelen verder aspecten als backup van gegevens en toepassinging van gegevensversleuteling.

Bij het uitvoeren van de gevalstudies is niet onderzocht hoe organisaties omgaan met de hiervoor beschreven softwarelevenscyclus. Wel is tijdens de bankengevalstudie onderzocht hoe er werd gescand op kwetsbaarheden en welke hulpmiddelen hierbij werden gebruikt. Uit de antwoorden blijkt dat er werd gescand op de aanwezigheid van kwetsbaarheden in de ICT-infrastructuurlaag van de banken en niet op de applicatielaag. Uit de antwoorden bleek tevens dat geen van de banken in 2003 beschikten over specifieks vulnerability scanners voor (web)applicaties. Hieruit kan worden geconcludeerd dat het structureel beoordelen van de beveiliging van software-applicaties door de ICT-beheerafdelingen in 2003 niet gebruikelijk was.

5.1.2. Leren van incidenten

In veiligheidsgerelateerd onderzoek worden vaak de termen incident, ongeluk en ‘near miss’ gebruikt. Van der Schaaf [SCHA92] legt in een simpel incident-oorzaakmodel de relaties tussen deze termen uit. Het model maakt duidelijk dat gevaarlijke situaties altijd voorafgegaan worden door een combinatie van technisch, menselijk en/of organisatorisch falen. Deze worden ook wel de bronoorzaken genoemd. Een technisch falen verwijst naar verkeerd of niet optimaal functionerende technische apparatuur, gebruikt tijdens of voorafgaand aan een incident. Het omvat onder meer storingen aan apparatuur, materiaaldefecten, ontwerpfouten, etc. Een menselijke fout verwijst naar fouten gemaakt door diegenen ‘at the sharp end of incident causation’, mensen die uiteindelijk het incident hebben getriggerd. Hierbij kan het gaan om interpretatiefouten, vergissingen of het niet opvolgen van bekende regels. Organisatorsche falen tenslotte verwijst naar fouten gemaakt door personen ‘at the blunt end of incident causation’, mensen die op zichzelf niet de directe oorzaak zijn van incidenten maar die andere fouten kunnen triggeren. Uit onderzoek van van Vuuren [VUUR98] blijkt dat organisatorisch falen de negatieve invloeden van de structuur, doelen en cultuur van de organisatie zelf op de veiligheid betreft. Voorbeelden zijn onjuistheden in de taakverdeling, prioriteiten van het management en de heersende veiligheidscultuur. Uit het onderzoek blijkt tevens dat bij de analyse van grote en spraakmakende ongevallen de nadruk ligt op technisch en menselijk falen. Klassieke voorbeelden zijn vlieg- en treinrampen waar meestal direct de piloot/machinist als schuldige wordt aangewezen wegens het niet opvolgen van een bekende procedure. Organisatorische aspecten worden zelden als bijdragende factor genoemd. Een belangrijke vooronderstelling is dat organisatorisch falen latent van aard is. Dat wil zeggen dat de gevolgen van organisatorisch falen niet onmiddellijk maar slechts na verloop van tijd en alleen onder de juiste omstandigheden tot uiting komen. Organisatorisch falen leidt tevens niet rechtstreeks tot incidenten maar creeert omstandigheden voor technisch en menselijk falen en is hierdoor moeilijker zichtbaar. Om een beeld te krijgen van de omvang van organisatorisch falen heeft Van Vuuren meerdere gevalstudies uitgevoerd in de staalindustrie en de medische sector. Van de 78

onderzochte incidenten in de staalindustrie bleek 36,9% een organisatorisch basisoorzaak te hebben. In de medische sector lag dit percentage op 35,8% (van 64 onderzochte incidenten). Zijn conclusie is dan ook dat organiatorisch falen een belangrijke bijdrage levert aan het ontstaan van incidenten.
Bij het onderzoek van van Vuuren is gebruik gemaakt van het in 1996 door onderzoekers van de Safety Management Group van de Technische Universiteit Eindhoven ontwikkelde PRISMA model. PRISMA staat voor Prevention and Recovery Information System for Monitoring and Analysis. Het model beoogt incidenten en procesafwijkingen op een systematische wijze te monitoren, analyseren en interpreteren met als uiteindelijke doel risico's te verminderen. PRISMA bestaat uit de volgende zeven stappen: (1) detectie van incidenten, (2) selectie, (3) beschrijvingen weergeven in een oorzakenboomdiagram, (4) classificatie, (5) statistische verwerking, (6) interpretatie en implementatie en (7) evaluatie.Het model wordt toegepast binnen de petrochemische industrie, de medische wereld, de luchtvaart, de telecommunicatie en bij kerncentrales. Uit onderzoek van Neys [NEYS03] blijkt dat de PRISMA methode ook binnen het ICT-domein inzetbaar is.

Wat betekent bovenstaande nu voor ICT-beveiliging en de wijze waarop organisaties reageren op aan ICT-beveiliging gerelateerde incidenten?. Uit het onderzoek is gebleken dat zowel de banken als de computer security incident response teams bij de universiteiten gebruik maken van vaste procedures voor het oplossen van incidenten. Herstel van de dienstverlening heeft hierbij prioriteit. Wanneer een incident niet direct kan worden afgehandeld, bijvoorbeeld omdat het in omvang escaleert of omdat bij het incident beveiligingsdisciplines van meerdere afdelingen betrokken zijn, wordt het incident tot probleem of calamiteit verheven. Het krijgt dan speciale status en aandacht van het senior management, zie bijvoorbeeld het onderzochte kastje-incident. Uit de interviews is gebleken dat problemen of calamiteiten achteraf worden geanalyseerd. De analyses leiden soms tot aanbevelingen aan het management voor het treffen van verbeteringsacties. Uit de gevalstudies is niet gebleken dat de banken of universiteiten een met PRISMA vergelijkbare methodiek gebruiken voor het gestructureerd monitoren, analyseren en interpreteren van incidenten met als doel het vaststellen van de basisoorzaken van de incidenten. Wel blijkt uit de interviews dat het verzamelen en analyseren van incidenten, inclusief aan ICT-beveiliging gerelateerde incidenten, bij de banken een meer structureel karakter heeft gekregen sinds de introductie van operationeel risicomanagement op grond van regelgeving vanuit de Bank for International Settlements.

5.2. Vergelijking van criteria en variabelen

5.2.1. Inleiding

Bij de analyses van de gevallen is voornamelijk gebruik gemaakt van de interviewverslagen. Door middel van trefwoorden en cijfergegevens zijn de onderzochte gevallen geordend. De ordening heeft plaatsgevonden op basis van de volgende trefwoorden:

- definitie;
- informatiebron;
- kwetsbaarhedenresponse;
- incidentenresponse;

- detectietechniek;
- ITIL change management.

Verder is geordend op de tijdens de interviews verstrekte aantallen en soorten incidenten.

De ordening is in eerste instantie separaat toegepast bij de organisaties die zijn onderzocht binnen de gevalstudie Banken. Vervolgens zijn de onderzoeksresultaten van de drie computer security incident responseteams geordend. In tweede instantie is geordend over deze twee gevalstudies heen. Daarbij is gekeken naar de elementen omvang van de organisatie en type dienstverlening en het effect hiervan op reactiesnelheid en materiekennis.

5.2.2. Eerste globale analyse

Definities
Uit de interviews met de banken bleek dat alle banken zich herkenden in de voorgestelde begrippenlijst. Verschillen zaten onder meer in de naamgeving van de incidentenresponseteams bij de banken. Met uitzondering van één bank hanteerden geen van de geïnterviewde banken een expliciet begrippenkader voor aan ICT-beveiliging gerelateerde incidenten, kwetsbaarheden of dreigingen. Van een categorisering van incidenten kan dan ook niet gesproken worden. Dit lag anders bij de onderzochte computer security incident responseteams. Surfnet-CERT en CERT-RU hanteerden een incidentenclassificatie, waarbij Surfnet-CERT uitgaat van een indeling van tien en CERT-RU van negen incidenttypen. De teams gebruiken soms verschillende termen voor soortgelijke incidententypen[122]. Verder blijkt dat Surfnet-CERT een verdere verfijning hanteert voor bepaalde typen incidenten. Waar bijvoorbeeld CERT-RU het begrip cracking hanteert voor elke vorm van ongeautoriseerde toegang maakt Surfnet-CERT een splitsing in root compromise en unauthorized use. Opvallend was verder dat CERT-RU een incidentencategorie schending van licenties hanteert. Deze incidentencategorie is niet aangetroffen bij de andere computer security incident responseteams.

Waarschuwingsdiensten
Van de onderzochte banken blijkt zeventig procent gebruik te maken van betaalde diensten voor het verkrijgen van kwetsbaarhedeninformatie. Het betreft de vier grootbanken plus drie overige banken. Enkele banken gaven tijdens de interviews aan dat, ondanks de filtering en analyse door de informatieleverancier, er nog steeds sprake was van aanzienlijke hoeveelheden berichten. De informatie werd ontvangen door medewerkers van de incident responseteams en/of door de verantwoordelijke operationele ICT-securitymanagers. Geen van de onderzochte computer security incident responseteams maakte gebruik van een betaalde informatiedienst. Zij verkregen informatie over kwetsbaarheden en incidenten voornamelijk van collegiale CSIRT's uit het FIRST-netwerk.

Detectietechniek
Uit het onderzoek kwam naar voren dat geen enkele bank over een volwaardige network intrusion detectieomgeving beschikt. Wel waren twee banken bezig met een pilotimplementatie. Daarentegen hanteerden alle banken een vorm van penetratietest en/of werd er regelmatig gescand door de ICT-afdeling op bekende kwetsbaarheden. De banken hanteerden hiervoor verschillende tools, zowel licentieproducten als freeware.

[122] Bijvoorbeeld social attacks versus abusive communication.

Gegevens over gebruikte detectietechnieken door computer security incident responseteams bij de hoger onderwijsinstellingen zijn niet beschikbaar.

Incidenten- en kwetsbaarhedenresponses
Zowel de grotere banken als de onderwijsinstellingen implementeren ITIL als best practise voor ICT-beheeractiviteiten. Wel blijkt dat bij kleinere ICT-organisaties er minder functionarissen een rol spelen bij de afhandelingsprocessen en er in geval van incidenten sneller overlegd wordt over zaken als mogelijke impact, prioriteit van afhandeling, etc. Bij één bank bijvoorbeeld werd door de ICT-securitymanager gezegd dat hij indien hij een change met spoed wilde laten implementeren (uitsluitend) overlegde met de systeembeheerder die aan het bureau tegenover hem zat.

Uit het onderzoek is verder gebleken dat drie van de tien banken beschikten over een permanent operationeel incidenten responseteam. Deze drie banken behoren tot de zogeheten grootbanken in Nederland. De incident responseteams bij de banken hebben een sterk adviserende taak. De andere banken gaven aan dat het adviseren over de afhandeling van incidenten of kwetsbaarheden een taak is van de verantwoordelijke ICT-beveiligingsfunctionaris.

5.2.3. Omvang van organisatie

Uit de gesprekken met contactpersonen bij de onderzochte organisaties is gebleken, dat de complexiteit van kwetsbaarheden- en incidentenresponsemanagement toeneemt, indien er sprake is van meerdere ICT-beheerafdelingen binnen een organisatie. Ook een variatie aan systeem- en netwerkconfiguraties draagt bij aan de complexiteit.

De onderzochte organisaties met ICT-beheerafdelingen die een omvang hebben van meer dan zeventig FTE's, hanteren allemaal een sterk op ITIL gebaseerd change managementproces. Er is sprake van vaste wijzigingsprocedures die integraal worden toegepast. Wijzigingen worden vaak tijdens onderhoudsperioden van enkele uren, meestal 's nachts, aangebracht, waarbij het uitgangspunt is dat de verstoring van de dienstverlening minimaal dient te zijn. Er is een officieel gremium die goedkeuring geeft aan de implementatie van de wijziging. Bij de beoordeling van een wijzigingsverzoek is de belangrijkste overweging dat de beschikbaarheid van de dienstverlening geen risico mag lopen. De beveiligingsfunctionaris in grote ICT-organisaties met complexe infrastructuren is niet structureel betrokken bij het change managementproces en heeft, naar eigen zeggen, beperkte invloed op dit proces.

De omvang van de organisatie heeft ook invloed op de organisatorische inrichting van het incidentenresponsemanagement. In alle onderzochte gevallen was er sprake van de aanwezigheid van een escalatiemechanisme waarbij het aantal betrokken functionarissen en afdelingen correspondeert met de ernst van de situatie.

Uit het onderzoek kwam naar voren dat het aantal medewerkers dat lid is van een computer security incident responseteam ligt tussen de vijf en tien medewerkers per organisatie. Lidmaatschap van een dergelijk team is een parttimetaak. Binnen de universiteiten hebben de computer security incident responseteams een sterk coördinerende rol bij de behandeling van alle aan ICT-beveiliging gerelateerde incidenten. Bij de meeste banken wordt de behandeling van majeure incidenten

gecoördineerd door ad-hoc samengestelde crisisteams die worden aangestuurd door een (senior) manager van de ICT-beheerafdeling.

5.2.4. Dienstverlening

Bij de analyse is verder nagegaan of het type dienstverlening bij enerzijds instellingen die financiële diensten aanbieden en anderzijds instellingen voor hoger onderwijs van invloed is op het aantal en soort incidenten en de incidentenafhandeling.

Voordat de omvang en soort incidenten is onderzocht, is gekeken welke definitie(s) worden gehanteerd voor het begrip ICT-beveiligingsincident. Een aantal universitaire CERT's hanteert een strikte incidentenclassificatie. Elke klasse[123] heeft een eigen omschrijving. De banken hanteren een veel minder strikte indeling. De door het wereldwijde Forum of Incident Response and Security Teams gehanteerde definitie wordt wel herkend en als bruikbaar beschouwd. Een aantal banken gaf aan dat fraudegerelateerde ICT-incidenten soms als ICT-beveiligingsincidenten en soms als fraude-incidenten worden geregistreerd. Als voorbeeld werd genoemd het registreren van phishing-incidenten.

Bij de analyse van de incidenten blijkt dat het overgrote deel, gemiddeld vijfenzeventig procent, bij de universiteiten te relateren is aan internetgebruik van medewerkers, studenten en overige gebruikers van de universitaire ICT-infrastructuur. Bij deze incidenten ging het voornamelijk om zaken als poortscans, spam, virussen en hacking. Bij de banken was het aantal opgegeven incidenten beduidend lager en betrof het veelal een ander type incidenten. Een opvallend deel van de door de banken opgegeven incidenten had betrekking op het kenmerk autorisatieschending en betrof de eigen medewerkers.
De oorzaak van het relatief beperkte aantal spam- en virusincidenten bij de banken ligt vermoedelijk in het feit dat het gebruik van Internet op de werkplek van bankmedewerkers ten tijde van het onderzoek (nog) beperkt was en er een strikter beleid werd gevoerd ten aanzien van toegang tot bepaalde delen van het Internet.

Uit bovenstaande kan worden afgeleid dat het aantal en het soort incidenten te relateren is aan de mogelijkheden voor het gebruik van het Internet door klanten van de ICT-organisatie. Een relatie tussen aantal en soort incidenten en het type dienstverlening van de organisatie, in casu onderwijsgerelateerde diensten en financiële diensten, is niet geconstateerd.

Uit de analyse blijkt verder dat de medewerkers van computer security incident responseteams bij de universiteiten een ander informatienetwerk hebben dan de beveiligingsfunctionarissen bij de banken. Er wordt tussen de onderzochte CSIRT's onderling, met als spil Surfnet-CERT, regelmatig informatie uitgewisseld over nieuw ontdekte kwetsbaarheden en dreigingen. Medewerkers van Surfnet-CERT krijgen hun informatie veelal vanuit het internationale FIRST-netwerk. Van de onderzochte banken was één bank lid van FIRST. De andere banken verkregen de informatie via abonnementen op (gratis) mailinglijsten, via leveranciers van hard- en softwareproducten en/of via betaalde informatiedienstaanbieders.

[123] Bijvoorbeeld spam.

5.2.5. Reactiesnelheid

Uit de analyse is gebleken dat de elementen complexiteit van de infrastructuur en omvang van de organisatie invloed hebben op de doorlooptijd van het aanbrengen van wijzigingen. Bij de ICT-organisaties waar de processen volgens ITIL zijn geïmplementeerd wordt een strikter change managementbeleid gevoerd dan bij organisaties waar dit niet het geval is. In beide situaties was er overigens geen sprake van een specifiek beleid voor security patching. De invloed van de ICT-beveiligingfunctionaris op het security patchproces in kleinere ICT-organisaties is groter dan in grotere organisaties. De beschikbaarheid van de dienstverlening conform de in een service level agreement vastgelegde afspraken vormt een kernaspect binnen change management. Hierdoor wordt er extra kritisch gekeken en terughoudend omgegaan met het aanbrengen van wijzigingen buiten de met de klant afgestemde onderhoudsperioden. Ook wordt er in ITIL-georiënteerde organisaties veel zorg besteed aan het beoordelen en testen van wijzigingen.

Uit de analyse kan worden afgeleid dat een generiek change management beleid bij grotere ICT-organisaties een negatief effect heeft op de snelheid van het implementeren van wijzigingen ten behoeve van ICT-beveiliging.

De omvang van de organisatie heeft een beperkte invloed op de reactiesnelheid bij incidentenresponse. Bij de analyse is bijvoorbeeld gebleken dat virusgerelateerde incidenten bij een aantal grote banken snel en effectief worden opgepakt. Ook de aanwezige interne calamiteitenorganisatie en -procedures lijken afdoende te werken. Echter als bij de beantwoording van incidenten naast de ICT-organisatie ook andere organisatiedisciplines[124] worden betrokken en het incident hierdoor niet als een zuiver ICT-incident wordt beschouwd, kan dit negatieve effecten hebben op de reactiesnelheid. Uit de gehouden interviews bleek dat de betrokken disciplines er soms strijdige doelstellingen op na houden. De ICT-afdeling wil bijvoorbeeld zo snel mogelijk de dienstverlening hervatten, de afdeling veiligheidszaken daarentegen wil een situatie bevriezen om eventueel aanwezig bewijsmateriaal veilig te stellen.

5.2.6. Materiekennis

Informatie over nieuw ontdekte kwetsbaarheden wordt binnen de ‘CSIRT gemeenschap’ via besloten e-mailinglijsten op een zeer snelle manier gedistribueerd. Financiële instellingen ontvangen kwetsbaarhedeninformatie onder meer via officiële publieke of betaalde mailinglijsten. Slechts een zeer beperkt deel van de beveiligingsfunctionarissen van de onderzochte banken had ten tijde van het onderzoek contacten met het externe CSIRT-netwerk. Binnen dit netwerk wordt uitgebreid informatie uitgewisseld over onder meer nieuw ontdekte kwetsbaarheden. In dit opzicht verkeren de beveiligingsfunctionarissen van de banken in een situatie waarbij sprake is van een tijdelijke informatieachterstand. Wel is het zo dat deze informatie met betrekking tot ontdekte kwetsbaarheden veelal erg prematuur is en soms speculatief van karakter. Ook was het treffen van voorzorgsmaatregelen direct na de bekendwording van een kwetsbaarheid[125] niet in alle gevallen mogelijk. Een informatieachterstand is daarom niet in alle gevallen relevant.

[124] Bijvoorbeeld de afdelingen veiligheidszaken, juridische zaken, communicatie, etc

[125] Zoals het aanbrengen van een workaround in afwachting van een beschikbare security patch.

5.2.7. Update

In het najaar van 2007 is aanvullend onderzoek gedaan om een actueel beeld te verkrijgen van kwetsbaarheden- en incidentenbeheersing bij onderzochte bancaire organisaties.
De wijze waarop kwetsbaarheden- en incidentenbeheersing is ingericht, verschilt niet fundamenteel van de situatie van vier jaar geleden. Patch management is nog steeds een probleem. De kennis over kwetsbaarheden en incidenten is wel toegenomen, mede door het aansluiten van enkele grote banken bij FIRST en het verstevigen van de contacten met GovCERT. Verder blijkt uit de reacties dat er tegenwoordig vooral wordt gescand op kwetsbaarheden in de applicatielaag en minder op kwetsbaarheden in de infrastructuur. Ook gaven enkele instellingen aan dat delen van het ICT-beheerproces zijn uitbesteed. Het is onduidelijk welke effecten de uitbesteding heeft op de kwaliteit van de kwetsbaarheden- en incidentenresponse van de organisatie. Nader onderzoek is gewenst.