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

Hafkamp, W.H.M.

Publication date
2008

4. Gevalstudies

In de periode februari 2003 tot en met oktober 2004 zijn drie gevalstudies uitgevoerd. Van februari tot en met mei 2003 heeft een onderzoek[71] plaatsgevonden naar kwetsbaarheden- en incidentenresponse bij tien Nederlandse banken, inclusief betalingsverkeeroperator Interpay[72], in het kader van een haalbaarheidsonderzoek naar samenwerking op het terrein van ICT-beveiliging tussen Nederlandse banken [HAKA03]. In dit hoofdstuk worden alleen de bevindingen gepubliceerd betreffende de organisatie en inrichting van kwetsbaarheden- en incidentmanagement bij de onderzochte banken. Aansluitend is van mei tot en met september 2003 een gevalstudie uitgevoerd naar de opzet en werking van computer security incident response bij de organisatie SURFnet en twee bij SURFnet aangesloten hoger onderwijsinstellingen. Tot slot is in de periode maart tot en met oktober 2004 de aanpak van cybercrime in Nederland onderzocht middels een gevalstudie bij het Team Digitale Expertise van het Korps Landelijke Politiediensten. In dit hoofdstuk worden de resultaten van de studies beschreven. Op verzoek zijn de gegevens van de banken geanonimiseerd en daarom niet te herleiden tot de deelnemende organisaties.

4.1. Interbancair onderzoek

4.1.1. Aanleiding

Ten tijde van het onderzoek vonden nog op ad-hocbasis gezamenlijke interbancaire maatregelen plaats, afhankelijk van de grootte van de dreiging of het type incident. Een haalbaarheidsstudie diende inzichtelijk te maken of een verdere samenwerking tussen Nederlandse banken op tactisch/operationeel niveau met betrekking tot aan ICT-beveiliging gerelateerde incidenten wenselijk en realiseerbaar was. De onderzochte samenwerking kreeg als werktitel: interbancair computer security ‘Information Sharing and Analysis Center (ISAC)[73]’[BAFS02].

Herstelsoftware of antivirussoftware-updates dienen snel, vaak binnen enkele uren, te worden aangebracht. Dit vereist een bepaald kennisniveau. Klanten van banken verwachten dat adequaat wordt gereageerd op incidenten en dat helder wordt gecommuniceerd over (mogelijke) dreigingen en oplossingen die voor hen relevant zijn.

Een interbancair computer security ISAC zou naar verwachting een aantal zaken verder bevorderen:

- het sneller onderkennen van nieuwe kwetsbaarheden en incidenten
- het effectief en efficiënt coördineren van informatie-uitwisseling en kwetsbaarhedenanalyses
- een gezamenlijk antwoord geven op initiatieven en voorstellen vanuit de overheid (loketfunctie).

[71] Het onderzoek is uitgevoerd door Wim Hafkamp (Rabobank) en Pierre Karsten (Interpay).

[72] Interpay Nederland en het Duitse Transaktionsinstitut fuer Zahlungsverkehrsdiensleistungen zijn op 21 september 2006 gefuseerd en bieden onder de naam Equens diensten voor verwerking van betalingsverkeer binnen Europa aan.

[73] Naam afgeleid van de in 1998 in de U.S.A. opgerichte Financial Sector Information Sharing and Analysis Center (zie http://www.fsisac.com)[ALLE02].

4.1.2. Doelgroep

Aan het onderzoek hebben (in alfabetische volgorde) meegewerkt: ABN AMRO Bank, Achmea Bank, Bank Nederlandse Gemeenten, Dexia Bank, Fortis Bank, F. van Lanschot, ING/Postbank, Interpay, Rabobank en SNS. Voorts zijn in het kader van het onderzoek oriënterende gesprekken gevoerd met De Nederlandsche Bank (DNB), het computer emergency response team van de rijksoverheid (GovCERT.nl), de Nederlandse vereniging van internet service providers (NLIP) en Microsoft Nederland.

De geïnterviewden zijn allen werkzaam binnen de ICT-(beveiligings)afdeling van de bank of hebben hiermee een nauwe relatie. Het onderzoek is uitgevoerd onder supervisie van de Nederlandse Vereniging van Banken (NVB).

4.1.3. Onderzoeksopzet

Op basis van deskresearch hebben de onderzoekers zich een globaal beeld verworven van het materiegebied. Vervolgens is een vragenlijst opgesteld ten behoeve van de interviews bij de tien banken. De vragen zijn voorafgaand aan de haalbaarheidsstudie getest in een proefinterview bij Rabobank en Interpay. Elk interview besloeg anderhalf tot twee uur. De inhoud van het interview werd kort toegelicht door de onderzoekers. In overleg met de Nederlandse Vereniging van Banken is een lijst gemaakt met contactpersonen bij de deelnemende organisaties. Voordat de vragenlijst werd doorgenomen werd gevraagd naar de functie van de geïnterviewde(n) en de organisatorische plaats van de functie binnen de organisatie. Van ieder interview is een gespreksverslag gemaakt dat binnen twee weken ter verifiëring werd toegestuurd aan de geïnterviewden. Sommige geïnterviewden stelden bedrijfsdocumenten ter beschikking ter ondersteuning van de gegeven antwoorden. Aan de geïnterviewden werd door de onderzoekers een garantie afgegeven dat de verstrekte informatie geanonimiseerd zou worden verwerkt in het eindverslag en dat de verstrekte schriftelijke en/of mondelinge gegevens vertrouwelijk zouden worden behandeld.

4.1.4. Bevindingen

4.1.4.1. Algemeen

Organisatie
Door de interviews is duidelijk geworden dat de organisatie van informatiebeveiliging binnen de diverse banken overeenkomsten vertoont. Zo is er sprake van een of meer functionarissen verantwoordelijk voor de taak van initiëren, beheren en onderhouden van het informatiebeveiligingsbeleid: de information security officer (ISO) functie. De situering van deze functie is echter niet eenduidig. Bij de meeste banken is ISO gepositioneerd binnen de ICT-organisatie. Ook een positie binnen de interne veiligheidsafdeling en binnen de auditafdeling kwamen voor. De information security officer vervult in alle gevallen een sleutelpositie als het gaat om het informeren van het verantwoordelijk (senior)lijnmanagement over belangrijke strategische/tactische aangelegenheden met betrekking tot informatiebeveiliging. Binnen de ICT-organisatie zijn daarnaast vaak meerdere ICT-securitymanagers actief. De ICT-securitymanager heeft een tactische/operationele taak. Hij vertaalt het algemene beleid naar concrete maatregelen, bijvoorbeeld maatregelen met betrekking tot de inrichting van firewalls,

virusscanning, etc. Ook bij de coördinatie en afhandeling van aan ICT-beveiliging gerelateerde incidenten is de securitymanager nauw betrokken.

Beleid
Het generieke informatiebeveiligingsbeleid is bij alle banken sterk gerelateerd aan de Nederlandse Code voor Informatiebeveiliging uit 2000 [NEN00]. De meeste banken hebben de code aangevuld met eigen bepalingen, bijvoorbeeld met betrekking tot logische toegangsbeveiliging.

De interviews laten zien dat diverse beheerprocessen binnen de ICT-afdelingen sterk leunen op de ITIL-principes. Het betreft vooral de processen incident-, problem- en change management. Het ITIL-proces configuration management is in veel gevallen wel ingevuld, maar niet altijd op detailniveau[74].

Definities
Ter hantering van een eenduidig begrippenkader hebben de onderzoekers gebruik gemaakt van een tabel met definities. Op de vraag of binnen de organisatie dezelfde definities worden gehanteerd, wordt in alle gevallen bevestigend geantwoord. Wel geven twee banken aan dat zij niet de term computer emergency response team hanteren maar een andere, soortgelijke term.
Ook geven enkele geïnterviewde banken aan dat het begrip 'IT' in 'IT security incident' enigszins misleidend is en binnen de eigen bank ruim wordt beschouwd, zodat ook fraudegerelateerde ICT-incidenten onder deze noemer vallen. Bij één bank is een verdere verdieping van het begrip ICT-beveiligingsincident aangebracht in 10 typologieën van ICT-beveiligingsincidenten (waaronder hacking, virus, diefstal, etc).

Tabel 7: definities gevalstudie banken

Definitie	**Omschrijving**	**Bron**
Vulnerability (kwetsbaarheid)	A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy	IETF: RFC2828, Internet Security Glossary, 2000
Threat (dreiging)	A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm	IETF: RFC2828, Internet Security Glossary, 2000
IT Security incident (ICT-beveiligingsincident)	An event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste or abuse; compromise of information; or loss or damage of property or information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software	FIRST: www.first.org, 2002
Calamiteit	Een gebeurtenis die een service of systeem zodanig verstoort dat veelal aanzienlijke	ITSMF: ICT Service Management 2002 v3.0

[74] Veelal bevat de database informatie over serienummer, modelnummer, tenaamstelling (eigenaar) en leverdatum.

	maatregelen moeten worden genomen om het originele werkingsniveau te herstellen	
Incidentenbeheer	Incidentmanagement heeft de reactieve taak (dreigende) storingen in ICT-diensten weg te nemen en ervoor te zorgen dat de gebruikers zo snel mogelijk weer aan het werk kunnen	ITSMF: ICT Service Management 2002 v3.0
(Computer emergency) response team	An organization whose function is to assist an information technology community or other defined constituency in preventing and handling security-related incidents. An individual response team also takes active steps to raise its constituents' level of awareness of computer security issues and to improve the security of its constituents' information technology resources	FIRST: www.first.org, 2002
Wijziging (Change)	Wijziging van/op een configuration item (CI)	ITSMF: ICT Service Management 2002 v3.0

4.1.4.2. Management van kwetsbaarheden

4.1.4.2.1 Alarmering

Externe berichtgeving
Alle geïnterviewde banken geven aan dat de ICT-securitymanagers en information security officers en systeembeheerders zich hebben geabonneerd op online beveiligingsnieuwsdiensten. Als voorbeelden worden genoemd de (gratis) berichtgeving van leveranciers van antivirussoftware en van ICT-securityportals op het Internet zoals www.security.nl, www.buqtrack.org en www.sans.org. Het gaat hierbij om generieke informatie over nieuw ontdekte kwetsbaarheden, virussen, trends, etc. Daarnaast maken zeven banken gebruik van een van onderstaande, betaalde informatiediensten met betrekking tot kwetsbaarheden:

- Exploits and Vulnerability Alert Service (EVAS) van de firma ITSec (5x)
- E-Security online van de firma Ernst & Young[75] (1x)
- DeepSight™ Alert Services van de firma Symantec (1x).

De leverancier van de betaalde informatiedienst stuurt met meestal dagelijks geselecteerde berichten over nieuw ontdekte kwetsbaarheden ten aanzien van infrastructurele componenten en besturingssystemen. De berichten worden door de leverancier voorzien van een prioriteit, conclusie en aanbeveling. Vaak wordt doorverwezen naar websites van leveranciers voor het downloaden van herstelsoftware.

De berichten over kwetsbaarheden worden in de meeste gevallen via e-mail gestuurd aan de ICT-beveiligingsafdeling binnen de bank. Deze analyseert de berichten en zorgt voor doorleiding naar de verantwoordelijke systeem- en netwerkbeheerders. Tijdens de interviews geven enkele banken expliciet aan, dat de externe berichtgeving vaak te

[75] Deze dienst is door Ernst & Young in 2004 verkocht aan de firma Computer Associates.

omvangrijk en niet bankapplicatie- of bankinfrastructuurspecifiek is. Hierdoor is men relatief veel tijd kwijt aan interpretatie en analyse van berichten. Dit geldt vooral voor de banken met grote, complexe, soms internationale ICT-infrastructuren. Bij de kleinere banken is vooral de relatief beperkte omvang van de ICT-beveiligingsafdeling bij de analyse van de berichten een knelpunt.

Scanners en detectoren
Naast externe berichtgeving ontvangen de ICT-beveiligingsafdelingen ook berichten over (potentiële) kwetsbaarheden en aanvallen van in de ICT-infrastructuur aanwezige beveiligingssystemen. De informatie is afkomstig van (loggings van) detectie- of scansoftware. Het gaat hierbij om gegevens afkomstig van virusscanners, vulnerabilityscanners, firewallsystemen, host-based intrusion detection- en network intrusion detectiesystemen. De gegevens worden weggeschreven naar een logbestand en/of real-time gemeld in de vorm van een console- of Short Message Service (SMS-) tekstbericht. Tabel 8 geeft een overzicht van de geïmplementeerde beveiligingsmaatregelen.

Tabel 8: geïmplementeerde beveiligingssystemen

Beveiligingssysteem	**Toepassing**	**Uitvoering**
Virusscanning Genoemde tools: - McAfee - Mailsweeper - Sophos	Dagelijkse scans bij alle banken. Er wordt gescand op de werkplekken, gateways en (mail)servers. Enkele banken maken gebruik van twee leveranciers van antivirus software	Uitvoering door systeembeheer. Opvolging bij detectie en besmetting door ICT-beveiligingsafdeling en/of virusspecialisten
Vulnerability scanning Genoemde tools: - Artemis - ISS - Qualys services - Nessus (freeware)	Alle banken scannen op kwetsbaarheden. Bij vier banken is sprake van periodieke scans. Bij de andere banken wordt niet structureel maar op basis van prioriteit/classificatie of 'op verzoek' gescand	Uitvoering en nadere analyse van de output wordt gedaan door de ICT-beveiligingsafdeling. De reactie op de resultaten, zoals het patchen van systemen, is een verantwoordelijkheid van de ICT-beheerafdeling
Intrusion detection Genoemde tools: - ISS - Snort (freeware)	Bij alle banken is een vorm van intrusion detection aanwezig op koppelvlakken met het Internet (firewall-functionaliteit). Intrusion detection *op het interne netwerk* wordt momenteel door één bank gedaan. Twee banken gaven aan dat zij bezig zijn met pilot-implementaties	Output gaat naar de netwerk(firewall)beheer en/of de ICT-beveiligingsafdeling

Penetratietesten
Alle banken laten periodiek de kwaliteit van de beveiliging van delen van de ICT-configuratie meten door middel van penetratietesten. De frequentie varieert van eenmaal per jaar tot elk kwartaal. De testen worden uitgevoerd door externe, gespecialiseerde bureaus. Vier banken laten daarnaast regelmatig penetratietesten uitvoeren door een eigen, interne afdeling.

4.1.4.2.2 Change management

Changeproces
Ook het wijzigingbeheer binnen de banken leunt sterk op de principes van ITIL. De functie van changemanager is ondergebracht binnen de ICT-beheerorganisatie. Twee banken geven aan dat het change management een deeltaak is. Bij alle banken werkt men met zogeheten change advisory boards (CAB's). De samenstelling van de CAB verschilt per bank. Een aantal banken geeft aan dat in de CAB zowel de beheer- als de gebruikersorganisatie vertegenwoordigd is. Changes worden vooral vanuit de beheerorganisatie geïnitieerd om tactisch/operationele redenen. Twee banken geven aan de securitymanager onderdeel is van de CAB. De vraag over de gemiddelde doorlooptijd[76] van een (spoed)wijziging wordt door vijf van de tien banken concreet beantwoord, zie tabel 9.

Tabel 9: gemiddelde doorlooptijd in aantallen werkdagen bij (spoed)wijzigingen

Bank	**Wijziging**	**Spoedwijziging**
A	5	2 – minder dan 24 uur[77]
B	10	2
C	10	tussen 2 – 4 uur
D	35	2 – minder dan 24 uur
E	3	binnen 2 uur
overige banken	onbekend	onbekend

Bij nadere analyse van de antwoorden blijkt dat vooral de banken met relatief kleine ICT-beheerorganisaties een kortere gemiddelde doorlooptijd hebben bij de implementatie van spoedwijzigingen. Op de vraag of het actualiseren van het virussignaturebestand onder het regiem van het changemanagentproces valt geven zes banken aan dat er wel sprake is van een test- en acceptatieprocedure, alvorens de actualisatie in productieomgeving wordt aangebracht, maar dat door de hoge aantallen updates van het bestand het 'normale' changeproces, inclusief CAB beoordeling, niet wordt gevolgd. De geïnterviewden van de overige banken moeten het antwoord schuldig blijven. Eén bank geeft aan dat uit oogpunt van snelheid en op grond van goede perfomance-ervaringen uit het verleden het aanbrengen van antivirusupdates op de Internetgateways geheel geautomatiseerd verloopt en niet wordt getest.

Security patchbeleid
Een aantal geïnterviewden geeft aan dat het aanbrengen van patches door de operationele ICT-beheerorganisatie meestal is bedoeld om functie- en of serviceverlies te voorkomen of de service te herstellen. Zo wordt bij geen of sterk verminderde beschikbaarheid van een kritische service een door de leverancier aangeleverde patch via een spoedwijziging binnen (zeer) korte termijn geïmplementeerd Een security patch vermindert of verwijdert een of meer kwetsbaarheden waarvan bekend is dat ze de kwaliteit van de beveiliging van de ICT-component aantasten. Twee van de tien banken geven aan dat men bezig is met het ontwikkelen van een integraal securitypatchbeleid gekoppeld aan een vulnerabilityscanproces. Een bank geeft aan dat de uitkomst van vulnerability scans niet

[76] Initiatie van de change tot en met de implementatie.
[77] in beide gevallen telefonisch accoord van CAB-leden; voor zeer urgente changes, uitgevoerd binnen maximaal 24 uur, dient de crisismanager accoord te geven.

per se leidt tot het aanbrengen van security patches, maar wel bijvoorbeeld tot het verhogen van de (virus)scanfrequentie. Enkele banken geven aan dat er terughoudend wordt omgesprongen met security patches. Er wordt soms gewacht totdat er een nieuw release- of servicepack beschikbaar komt, waar alle updates in zijn verwerkt. Argumenten voor deze terughoudendheid zijn: lage risico-inschatting, de wetenschap dat een patch een nieuw (performance) probleem kan introduceren, en het elkaar snel opvolgen van patches in een kort tijdsbestek.

Op de vraag hoeveel security patches de afgelopen zes maanden werden uitgevoerd, wordt door vier banken beantwoord: 10, 6, 1 (spoed), gemiddeld 1 per week. Hieruit blijkt een grote diversiteit met betrekking tot het aspect 'security patching'

4.1.4.3. Incident Management

Escalatieproces
Bij elke bank worden ICT-incidenten of -problemen vastgelegd in een database en voorzien van een uniek nummer. Twee banken geven expliciet aan dat aan ICT-beveiliging gerelateerde incidenten niet opgenomen worden in de reguliere ICT-incidentendatabase, maar separaat worden vastgelegd. De grotere banken hebben twee tot drie escalatieniveaus (servicedesk, eerste en/of tweede lijnssupport). Aan ICT-beveiliging gerelateerde incidenten worden doorgespeeld naar de verantwoordelijke ICT-beveiligingafdeling. Het herkennen en 'merken' van deze incidenten blijkt in de praktijk soms lastig. Vooral waar het incidenten betreft met (potentiële) fraudeaspecten, zoals pinfraudes en meldingen rondom hacking. Dergelijke incidenten worden door één bank gedefinieerd als restincidenten. Het routeren van incidentmeldingen gebeurt vaak op basis van professional judgement, al dan niet ondersteund door procedures vanuit een servicedesk. Bij één bank worden aan ICT-beveiliging gerelateerde incidenten gegroepeerd naar tien categorieën. Per categorie zijn escalatielijnen en –procedures opgesteld.

Interbancair zijn er door de Nederlandse Vereniging van Banken afspraken gemaakt over het melden van bepaalde soorten incidenten aan een centraal meldpunt. Ook is er een crisisdraaiboek opgesteld in geval van problemen met chartale en girale betalingsverkeerprocessen. In het draaiboek staan naast een aantal standaardprocedures de (privé) NAW-gegevens van de bij de aangesloten banken verantwoordelijke functionarissen. Er bestaan geen (formele) afspraken over het interbancair melden van aan ICT-beveiliging gerelateerde incidenten, zoals hackingaanvallen, virusbesmettingen, e.d.

Omvang
Op de vraag over de soort en het aantal incidenten waarmee de bank in 2002 werd geconfronteerd, wordt met enige terughoudendheid gereageerd. Ook zegt een aantal geïnterviewden niet te beschikken over organisatiebrede gegevens. Tabel 10 bevat de door zeven banken genoemde aantallen incidenten.

Tabel 10: Kwantificering beveiligingsincidenten banken

ICT beveiligingsincidenten 2002	**Aantal banken**
Onbekend	3
1-3	2

4-12	1
13-24	4
> 25	0

Van de in 2002 geregistreerde incidenten gaven twee banken aan dat in twee gevallen sprake was van een calamiteit. De vraag om de incidenten te rangschikken naar een van de vijf genoemde categorieën[78] blijkt lastig te beantwoorden. Een aantal geïnterviewden geeft aan niet of onvoldoende kwantitatief inzicht te hebben in deze materie. Vier geïnterviewden geven aan dat de incidenten die zich hebben voorgedaan binnen de organisatie zijn te relateren aan: dienstontzegging, ongeautoriseerde toegang, ongeautoriseerde wijziging van bevoegdheid of klantinformatie of aanwezigheid van een relevante kwetsbaarheid.

Calamiteitenorganisatie
Alle banken hebben binnen het aandachtsgebied ICT formele calamiteitenprocedures en calamiteitenteams ingesteld. De calamiteitenteams, soms opererend onder een andere naam, komen bijeen wanneer zich bepaalde majeure incidenten voordoen, bijvoorbeeld bij ernstige continuïteitsverstoring aan belangrijke ICT- en/of bedrijfsprocessen of bij ernstige imagoschade. Aan het hoofd van deze teams staat in de meeste gevallen de algemeen verantwoordelijke manager voor ICT-processen binnen de bank. Het calamiteitenteam bepaalt of er sprake is van een calamiteit en neemt besluiten gedurende en direct na de calamiteit.

Calamiteitenteams vormen vaak de laatste schakel in een incidentenescalatieproces. Een incident kan in aanvang worden gesignaleerd (en geregistreerd) door een eerstelijns helpdesk binnen de ICT-organisatie en uiteindelijk de status van calamiteit verkrijgen.

De binnen het onderzoek geraadpleegde beschreven ICT-calamiteitenprocedures hebben een sterke focus op beschikbaarheid, dat wil zeggen continuïteitsherstel van de dienstverlening. Hierbij is bijvoorbeeld te denken aan procedures voor uitwijk van ICT-processen. Uit de interviews en de bestudeerde procedures ontstaat het beeld dat de processen voor ICT-incidenten of -calamiteiten waarbij sprake is van integriteits- en vertrouwelijkheidsschending minder formeel zijn vastgesteld.

Computer emergency response teams
Drie grootbanken geven aan dat zij beschikken over een formeel computer emergency response team dat assisteert bij bepaalde typen incidenten. Voorbeelden van dergelijke incidenten zijn virusuitbraken, detectie van indringers, geconstateerde beveiligingslekken, etc. Het CERT vervult een faciliterende rol voor het eerder genoemde calamiteitenteam binnen de bank. Het lidmaatschap van een CERT is een deeltaak en wordt gevoerd naast de bestaande taak van die van beveiligingsspecialist. De CERT's bestaan uit 3 tot 15 leden. Bij één bank is sprake van een volledig mondiaal werkend CERT. De leden van de CERT's beschikken over grondige systeem- en/of netwerkkennis en hebben zich verder verdiept in de materie van technische systeem- en netwerkbeveiliging. De teams zijn 7 maal 24 uur per week inzetbaar.

[78] Categorieën: dienstontzegging, ongeautoriseerde toegang, ongeautoriseerde wijziging van bevoegdheid of klantinformatie, ongeautoriseerde verwijdering en aanwezig van een relevante kwetsbaarheid.

De CERT van één van de onderzochte banken is formeel lid van het wereldwijd opererende Forum van Incident Response and Security Teams (FIRST).

4.2. Computer security incident response teams

In de periode mei 2003 tot en met september 2003 is een onderzoek uitgevoerd naar de opzet en werking van drie Nederlandse computer security incident response teams. Alle onderzochte instellingen zijn nauw verbonden met het hoger onderwijs in Nederland. Het eerste onderzochte team maakt onderdeel uit van SURFnet bv, een instelling die diensten ontwikkelt en beheert ten behoeve van hoger onderwijs- en onderzoeksinstellingen in Nederland. De twee andere teams zijn onderdeel van de ICT-organisaties van respectievelijk de universiteiten van Nijmegen en Groningen.

4.2.1. CERT-NL

4.2.1.1. SURFnet

SURFnet is het Nederlandse computernetwerk voor hoger onderwijs en onderzoek[79]. Het netwerk bestaat sinds 1991. SURFnet verbindt de netwerken van HBO-instellingen universiteiten, onderzoekscentra, academische ziekenhuizen, wetenschappelijke bibliotheken en instellingen die vallen onder het ministerie van Onderwijs, Cultuur en Wetenschap. De infrastructuur die SURFnet gebruikt, bestaat uit zogeheten managed dark fiber. Dat wil zeggen dat er door een telecomprovider beheerde glasvezels wordt geleverd, waarop SURFnet zelf actieve apparatuur aansluit. Hierdoor kan SURFnet zelf bepalen welke bandbreedte gewenst danwel noodzakelijk is. De netwerkcapaciteit kan oplopen van 1 Gbit/s tot 10 Gbit/s. Tevens zijn er koppelingen met andere netwerken in de wereld. Zo zijn er hoogwaardige verbindingen met onderzoeks- en onderwijsnetwerken in Europa en in de Verenigde Staten. De SURFnetorganisatie maakt onderdeel uit van het wereldwijde Internet.

Ontstaansgeschiedenis

De stichting SURF[80] is midden jaren tachtig van de vorige eeuw opgericht met als hoofddoel het bevorderen van de samenwerking op ICT-gebied tussen Nederlandse instellingen voor hoger onderwijs en onderzoek. Een van de eerste activiteiten was het ontwikkelen van een landelijk ICT-netwerk. De stichting omvat drie aandachtsgebieden: wetenschappelijke informatievoorziening, organisatie en management en ICT in het onderwijs. De stichting SURF heeft twee werkmaatschappijen: SURFdiensten bv en SURFnet bv. SURFdiensten sluit licentieovereenkomsten met ICT-aanbieders waarin speciale educatieve regelingen worden vastgelegd. Hierdoor kan SURFdiensten exclusief voor studenten en medewerkers specifieke en/of voordelige ICT-producten aanbieden. SURFnet zorgt voor de ontwikkeling en het beheer en onderhoud van een geavanceerde communicatie-infrastructuur ten behoeve van de aangesloten instellingen. SURFnet streeft naar (het behoud van) een positie in de kopgroep van internationale researchnetwerken. Verder speelt SURFnet een belangrijke rol in nationale ICT-projecten, waaronder het GiGaPortproject. SURFnet bv kende ten tijde van het onderzoek

[79] Zie http://www.surfnet.nl

[80] SURF is een afkorting van Samenwerkingsverband Universitaire RekenFaciliteiten.

naast het secretariaat en de financiële administratie de afdelingen: accountadvisering, productmanagement, netwerkdiensten, innovatiemanagement, services & support en communicatie. Het computer emergency response team van SURFnet was ondergebracht bij de afdeling Services & support.

Omvang en strategie
Het SURFnet-netwerk bestaat fysiek uit een structuur van kabels die door schakelapparatuur aan elkaar gekoppeld zijn, waarvoor verschillende protocollen – waarvan het Internet Protocol (IP) de belangrijkste is – gelden die communicatie over het netwerk mogelijk maken. Naast de koppeling met andere nationale en internationale netwerken worden de lokale netwerken van de ruim 200 instellingen die zijn aangesloten door het SURFnet-netwerk met elkaar verbonden. Ongeveer 400.000 studenten en medewerkers maken vrijwel dagelijks gebruik van SURFnet.
SURFnet heeft een point of presence in Chicago (Nortwestern University) waarmee gekoppeld wordt met hoger onderwijs- en onderzoeksnetwerken in Noord-Amerika en het Verre Oosten. Tussen Amsterdam en Chicago is een lambdaverbinding gerealiseerd met een snelheid van 10Gbit/s[81]. Veel van de uitvoerende taken worden in opdracht van SURFnet bv uitgevoerd door beheerpartners. SARA reken- en netwerkdiensten bijvoorbeeld beheert het SURFnet IP-netwerk. Het Universitair Centrum voor Informatievoorziening van Radboud Universiteit Nijmegen voert het beheer van een aantal SURFnet diensten waaronder News, Listserv, Directory Services en WWW-hosting. Het Rekencentrum van de Katholieke Universiteit Brabant[82] verzorgt de PGP- en X509-PKI dienst. Andere partners zijn Ant Arbor, Info.nl en de Nederlandse UNIX-Gebruikers Vereniging.

4.2.1.2. CERT-NL

De effecten van de Morris-worm van ongeveer 25 jaar geleden en de daarmee gepaard gaande opkomst van incident response teams in vooral de Verenigde Staten waren de aanleiding om in 1991 tijdens een SURFnet relatiedag te besluiten tot oprichting van een computer emergency response team voor de SURFnet organisatie en haar klanten. Het team kreeg als naam CERT-NL[83].

SURFnet-CERT is het computer emergency response team van SURFnet, de Internet provider voor het hoger onderwijs en vele onderzoeksinstellingen in Nederland.
SURFnet-CERT onderzoekt en coördineert alle gevallen van beveiligingsinbreuken die afkomstig (lijken te) zijn van de SURFnetklanten of waarvan SURFnetklanten het slachtoffer zijn geworden.
SURFnet-CERT draagt verder zorg voor voorlichting aan de aangesloten instellingen op het gebied van beveiliging, zowel incidenteel bij calamiteiten als structureel; dit laatste bijvoorbeeld door het verspreiden van kennis over softwarebeveiligingslekken.
SURFnet-CERT is het oudste computer emergency response team van Nederland.
SURFnet-CERT is sinds 1992 full member van de organisatie FIRST.

[81] Dit type verbinding maakt het mogelijk om experimentele computerclusters, visualisatiestations (virtual reality) en distributed computingomgevingen te koppelen; status per 6 november 2003.
[82] Tegenwoordig Universiteit van Tilburg geheten.
[83] Per 1 januari 2004 is de naam CERT-NL formeel gewijzigd in SURFnet-CERT (zie:http://cert.surfnet.nl). De naamswijziging vond plaats na het onderzoek. In de verdere tekst is de afkorting CERT-NL vervangen door SURFnet-CERT.

De belangrijkste doelgroep van SURFnet-CERT zijn de (netwerk)beheerders van de bij SURFnet aangesloten instellingen. Ook studenten van de instellingen met beveiligingsproblemen behoren tot de doelgroep. Een belangrijke eis bij het al dan niet verlenen van coördinatie/advieswerkzaamheden door SURFnet-CERT is dat een klant, dat wil zeggen een aangesloten instelling, erbij betrokken moet zijn.

Organisatie CERT
Het zogeheten SURFnet-CERT Kernelteam bevat tien medewerkers, waarvan zes in dienst zijn van SURFnet en de andere vier afkomstig zijn van de bij SURFnet aangesloten instellingen. In juni 2002[84] waren dit medewerkers van respectievelijk de Universiteit van Amsterdam, Katholieke Universiteit Brabant, Technische Universiteit Delft en Universiteit Twente. SURFnet betaalt op jaarbasis de lumpsum voor de werkzaamheden van laatstgenoemde personen. De organisatorische aansturing van SURFnet-CERT gebeurt door een stuurgroep waarin alle SURFnetdirecteuren zitting hebben. De stuurgroep benoemt de leden van het Kernelteam. Elke bij SURFnet aangesloten instelling is verplicht een instellingscoördinator, de technical site co-ordinator, te benoemen. Deze coördinator dient zeven-maal-vierentwintig-uur per week bereikbaar te zijn voor SURFnet-CERT medewerkers. De instellingscoördinator fungeert tevens als eerste contactpersoon voor beveiligingsaangelegenheden namens de instelling, de zogeheten site security contact (SSC). Er worden geen specifieke kwaliteitseisen gesteld aan de SSC, dat wil zeggen een naam en contactgegevens volstaan. SURFnet-CERT beschikt daarnaast per instelling over een lijst met personen die verantwoordelijk zijn voor beveiligingsbeleidszaken en operationele beveiligingsactiviteiten[85].
Werkzaamheden voor SURFnet-CERT worden gecombineerd met andere taken. De tijd die door het Kernelteam effectief wordt besteed aan SURFnet-CERT taken wordt ingeschat op totaal tweeëneenhalf FTE. De medewerkers beschouwen hun taken voor SURFnet-CERT als een bijzondere en eervolle taak. Alle medewerkers draaien vrijwillig mee in een piketrooster, zodat SURFnet-CERT een zeven-maal-vierentwintig-uur-bereikbaarheid heeft. Het piket geldt voor één volle week.

De diensten van SURFnet-CERT ten behoeve van de aangesloten onderwijs- en onderzoeksinstellingen maken standaard onderdeel uit van de SURFnetdienstverlening. SURFnet-CERT promoot het gebruik van zogeheten computer security incident response team capabilities. Een aantal onderwijsinstellingen, waaronder Radboud Universiteit Nijmegen en Rijksuniversiteit Groningen, hebben de afgelopen jaren een dergelijke CSIRT ingericht. Bij de HBO-instellingen ligt het anders. HBO-instellingen kennen geen eigen incident response teams. Dit heeft vooral te maken met het grote aantal fusies tussen hogescholen van de afgelopen jaren en de daarmee gepaard gaande samenvoeging van automatiseringsafdelingen, aldus SURFnet-CERT.

Incidentenresponse
De hoofdtaak van SURFnet-CERT is incidentencoördinatie, waarbij de nadruk ligt op incident handling. Een groot deel van de gemelde incidenten wordt na registratie voor verdere afhandeling, meestal voorzien van een advies, doorgestuurd naar de site security contact van de betrokken instelling. Daarnaast wordt actief meegewerkt aan verdere standaardisatie inzake het thema incidentenresponse in internationale gremia als IETF,

[84] Presentatie door CERT-NL op de KWINT-Incident Response & Alarmering werkgroepvergadering d.d. 4 juni 2002.
[85] CERT-NL noemt dit site security entry points.

TERENA en FIRST. Preventie en het bevorderen van het beveiligingsbewustzijn zijn tevens belangrijke neventaken. Een voorbeeld hiervan is het opstellen van security bulletins voor de aangesloten instellingen. Binnen SURFnet-CERT verwacht men dat door toenemende capaciteitsproblemen de hoofdtaak van coördinatie in de nabije toekomst minder gaat worden en men zich meer zal gaan toeleggen op advisering en opleiding van incidentenresponseteams.

Incidentenclassificatie
SURFnet-CERT hanteert in zijn operationeel raamwerk de volgende definitie van een incident: *an event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property of information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.*

Bij SURFnet-CERT werden ultimo 2003 gemiddeld ongeveer veertig incidenten per maand gemeld en geregistreerd. Naast de incidentenmeldingen krijgt SURFnet-CERT dagelijks e-mails binnen met vragen over beveiliging. Ook deze worden geregistreerd. Op de website zijn jaarstatistieken te vinden met incidentenaantallen over de periode 1999-2001. Incidenten worden ondergebracht in tien categorieën plus een restcategorie. Op de vraag wat wordt verstaan onder een ernstig incident is het antwoord dat de impact voor de gebruiker bepaalt wat ernstig is. SURFnet-CERT-medewerkers beschouwen een geslaagde rootcompromise of een DOS-aanval over het algemeen als ernstig en bijvoorbeeld spam niet, tenzij een instelling op een spamblacklist is terechtgekomen.

Tabel 11: Overzicht geregistreerde incidenten SURFnet-CERT 1999-2001

Incident	**2001**	**2000**	**1999**
Abusive communication	10	16	9
Denial of service	32	30	22
Lan sniffing	3	3	2
Other	10	43	10
Probe	227	204	132
Root compromise	48	31	19
Spam	40	82	45
Trojan	2	4	18
Unauthorized use	24	26	11
Virus	18	5	0
Warez	8	6	2
Total	**413**	**450**	**321**

Aanmelden van incidenten
Het merendeel van de incidentenmeldingen wordt per e-mail in free-formattext of, in geval van poortscans, via een op http://cert-nl.surfnet.nl beschikbaar gesteld webformulier verzonden naar CERT-NL@SURFNET.NL. De identiteit van de melder wordt niet geverifieerd. SURFnet-CERT maakt bij zijn communicatie rondom incidenten gebruik van het i-map e-mailprotocol. Op de website staat een publieke PGP-sleutel die een incidentenmelder kan gebruiken om de vertrouwelijkheid van de incidentengegevens tijdens verzending te waarborgen.

Naast e-mail is er een speciaal telefoonnummer beschikbaar om incidenten met zeer hoge prioriteit aan te melden. Tijdens kantoortijd wordt geadviseerd om te bellen met de SURFnet-helpdesk.

Verwerken en behandelen van incidenten
Gebruikers kunnen door middel van het woord URGENT in het subjectveld de prioriteit van het incident aangeven. Het niveau van ondersteuning bij de afhandeling is afhankelijk van het type en de ernst van het gemelde incident. Er wordt gestreefd naar een responsetijd van maximaal vierentwintig uur.

Het operationeel raamwerk van SURFnet-CERT bevat een aflopende prioriteitenlijst met in totaal tien (Engelstalige) incidententypen:

- threats to the physical or mental safety of human beings;
- root or system-level attacks on any Server System, or any part of the backbone network infrastructure;
- root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose;
- any other type of compromise which leads or may lead to unauthorised access of systems;
- denial of service attacks on any of the above three items;
- any of the above at other sites, originating from the constituency of SURFnet-CERT.
- large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks;
- threats, harassment, and other criminal offenses involving individual user accounts.
- compromise of desktop systems;
- denial of service on individual user accounts, e.g. mailbombing.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent. These incidents will be assessed as to their relative severity at SURFnet-CERT's discretion.

Ieder gemeld incident wordt geregistreerd en gearchiveerd in een zelfontwikkeld programma genaamd REMEDY. Het programma heeft het karakter van een workflow engine en wordt naast incidentenregistratie ook gebruikt voor DNS-aanvragen en afhandeling van storingen. Elke registratie krijgt een uniek ticketnummer (CERT-NLxxx.xxx). De velden in het incidentrecord hebben betrekking op de incidentafhandeling zelf, zoals prioriteit, status, actor, trefwoorden of op de contactgegevens van de melder en het slachtoffer, waaronder het IP-adres. Ook kan in het record worden aangegeven of het IP-adres is geblokkeerd.

Veel van de gemelde incidenten worden na registratie met een kort advies via e-mail doorgestuurd naar de site security contact van de instelling waar het incident dient te worden afgehandeld.

Sluiten van een incident
Het incident wordt afgesloten nadat de site security contact per e-mail de status van het incident heeft teruggemeld aan de dienstdoende SURFnet-CERT medewerker en deze vervolgens de afsluiting meldt aan de aanmelder. Ongeveer eenderde van alle gemelde en geregistreerde incidenten blijft langer dan een week open staan. De afhandeling van

incidenten, in het bijzonder het terugkoppelen naar aanmelders, is handwerk en vergt veel tijd, als het incidenten betreft waar meerdere partijen bij zijn betrokken. Dit is onder meer het geval bij incidenten met het predikaat portscan.

(externe) Contacten
SURFnet-CERT gebruikt een aantal mailinglijsten voor communicatie naar contactpersonen binnen het domein van SURFnet en overige in beveiliging geïnteresseerde personen.

Tabel 12: mailinglijsten SURFnet-CERT

Mailinglijst	**Doelgroep**
CERT-NL-BULLETINS@NIC.SURFNET.NL	Lijst ten behoeve van individuen die geen relatie hebben met de site security contacts en kennis willen nemen van SURFnet-CERT-adviezen
CERT-NL-SEP-BULLETINS@NIC.SURFNET.NL	Lijst ten behoeve van instellingen zonder security entry point
CERT-NL-SEP@NIC.SURNET.NL	Lijst ten behoeve van discussies tussen security entry points, site security contacts en SURFnet-CERT

Naast de communicatie via mailinglijsten onderhoudt SURFnet-CERT periodieke contacten met andere instanties waaronder het Korps Landelijke Politiediensten, GOVCERT en internationale fora als IETF, FIRST en TERENA. De contacten binnen deze gremia zijn sterk persoonsgerelateerd. SURFnet-CERT hanteert een ‘Disclosure Policy’ voor de communicatie of publicatie van bij SURFnet-CERT geregistreerde incidenten of kwetsbaarheden.

SURFnet-CERT’s disclosure policy
Het geheimhoudingsbeleid heeft als uitgangspunt dat SURFnet-CERT elke informatie zal delen indien dit anderen zal helpen bij het voorkomen of verhelpen van beveiligingsincidenten. SURFnet-CERT zal toepasselijke maatregelen treffen om de identiteit van leden van haar doelgroep of van anderen te beschermen.
De volgende indeling wordt gehanteerd bij het ontsluiten van informatie:

Gebruiker(s) privé-informatie: informatie over een bepaalde (groep) gebruiker(s) die om juridische, contractuele of ethische redenen als vertrouwelijk moet worden beschouwd. Deze informatie zal niet in identificeerbare vorm buiten SURFnet-CERT worden vrijgegeven.

Indringer(s)informatie: idem als gebruiker privé informatie. De informatie zal echter wel worden gedeeld met systeembeheerders en andere CSIRTs ingeval van incident tracking.

Gebruiker(s)organisatie-informatie: deze informatie wordt beschouwd als technische informatie die alleen met toestemming wordt vrijgegeven.

Kwetsbaarhedeninformatie:	technische informatie over kwetsbaarheden of aanvallen, inclusief herstelsoftware en workarounds. Kwetsbaarhedeninformatie wordt vrijelijk gedistribueerd. Wel zal alles in het werk worden gesteld om de betreffende leverancier te informeren voordat het algemene publiek wordt geïnformeerd.
'Beschamende' informatie:	betreft de verklaring dat een incident heeft plaatsgevonden inclusief informatie over omvang en ernst. Deze verklaring wordt pas afgegeven, nadat de gebruiker(s)organisatie toestemming heeft gegeven.
Statistische informatie:	'beschamende' informatie waarbij de identificerende gegevens zijn verwijderd.

Vertrouwelijke informatie over gebruikers of indringers wordt op basis van 'need to know' gedeeld met gebruikers binnen de doelgroep van SURFnet-CERT. Een gebruiker wordt bijvoorbeeld geïnformeerd, wanneer wordt vermoed dat het identificatienummer van de gebruiker is gecompromitteerd. Ook wordt volledige medewerking aan justitie verleend ingeval van justitieel onderzoek.

4.2.2. CERT-RU

4.2.2.1. Katholieke Universiteit Nijmegen

De Radboud Universiteit Nijmegen (RU), voorheen Katholieke Universiteit Nijmegen[86] , biedt op het landgoed Heyendael te Nijmegen ruim zestig opleidingen aan, verdeeld over acht faculteiten[87]. Naast de faculteiten en onderzoeksinstituten kent de universiteit een aantal facilitaire diensten en bedrijven die onderwijs en onderzoek aan de universiteit ondersteunen. Deze zijn ondergebracht in een cluster Ondersteuning en een cluster Facilitair. Binnen het cluster Facilitair bevindt zich onder andere het Universitair Centrum Informatievoorziening (UCI). Het UCI is onder meer verantwoordelijk voor netwerkdiensten en het beheer van de centrale netwerkinfrastructuur en een aantal centrale computersystemen. Tevens biedt het UCI cursussen op het gebied van PC- en netwerkapplicaties. Er wordt gerapporteerd aan het College van Bestuur van de Universiteit.

De universiteit telde tijdens het onderzoek ruim 16.500 studenten. Bij de RU werken voorts ongeveer 4000 medewerkers. Daarnaast zijn er ca. 8000 medewerkers werkzaam bij het Universitair Medisch Centrum Nijmegen Stichting Radboud. De universiteit kent het zogeheten integraalmanagement(IM)principe. Faculteiten en clusters bij de RU zijn zelf verantwoordelijk voor hun faciliteitenbeheer, waaronder dat van de ICT-middelen,

[86] De naamswijziging vond plaats na het onderzoek namelijk in september 2004; In de verdere tekst is de afkorting KUN vervangen door RU.
[87] Zie www.ru.nl.

en voeren dit via de zogeheten computer ondersteuningsgroepen (COG's). Er is met uitzondering van concernbrede toepassingen en diensten geen gedwongen winkelnering bij het UCI. Dit impliceert een grote verscheidenheid aan hard- en software en een relatief laag niveau van standaardisatie. Het College van Bestuur stuurt vooral op het realiseren van doelstelling en resultaten bij het UCI.

4.2.2.2. Organisatie CERT

CERT-RU, voor de naamswijziging van de universiteit CERT-KUN geheten, is op 29 november 2001[88] officieel geïnstalleerd door het College van Bestuur van de universiteit. Een toenemende belangstelling voor informatiebeveiliging en een toenemend aantal incidenten, mede als gevolg van het open netwerk en de aanwezigheid van privacygevoelige informatie, waren de belangrijkste redenen voor het oprichten van een eigen computer emergency response team. De RU volgt qua beveiliging een driesporenbeleid te weten het ontwikkelen van beleid, het treffen van preventieve maatregelen en het opzetten van een coördinatiepunt voor incidenten (in casu CERT-RU) als vangnet.

CERT-RU is primair ingesteld voor het coördineren van het voorkomen en oplossen van incidenten op het gebied van computer- en netwerkbeveiliging[89]. Een incident wordt gedefinieerd als *een gebeurtenis of het constateren van een gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, betrouwbaarheid of beschikbaarheid van gegevens in elektronische informatiesystemen binnen de RU of in informatiesystemen buiten de RU die met systemen binnen de RU gegevens uitwisselen*[90]. Een andere taak van CERT-RU is de voorlichting over incidenten en actuele bedreigingen. De voorlichting houdt in het binnen de RU onder de aandacht brengen van actuele kwetsbaarheden en de oplossingen daarvoor, en het waarschuwen voor trends in incidenten, bijvoorbeeld het risico van beschikbaarheidsaanvallen, actuele portscans, besmettelijke virussen, etc. Hiertoe is een specifieke distributielijst opgesteld, CERTRUadvisory@nic.surfnet.nl, waarop alle bekende formele beveiligingscontactpersonen, de zogeheten domain security contacts, van de RU en overige geïnteresseerden zijn geabonneerd. Bronnen van informatie zijn naast vrije nieuwsgaring door de CERT-RU-leden zelf, vooral het Upstream CERT[91] en de adviezen van een aantal voor de RU relevante software- en hardwareleveranciers. Een derde taak van CERT-RU betreft de advisering met betrekking tot het interne ICT-beveiligingsbeleid.

De doelgroep van CERT-RU bestaat uit universitaire medewerkers, studenten, leveranciers, e.a., in feite iedereen die betrokken is bij incidenten waarbij de RU betrokken is als veroorzaker of als benadeelde. Het CERT-RU werkt hierdoor voor de hele universiteit.

---

[88] Uit het KUN-themakatern 'ICT-beveiliging KUN' van december 2001. De oorspronkelijke naam CERT-KUN is in september 2004 gewijzigd in CERT-RU.

[89] Uit het Operational Framework voor het CERT-KUN, versie 1.0, d.d. 26 november 2001.

[90] Beveiligingstaken als vulnerability scanning en intrusion detection vallen buiten de scope van CERT-RU.

[91] Het Upstream CERT was in september 2003 CERT-NL (SURFnet-CERT).

CERT-RU is organisatorisch verankerd binnen het UCI. Met betrekking tot incidentenafhandeling ziet het een onafhankelijke rol weggelegd voor zichzelf. Over incidenten wordt gerapporteerd aan het verantwoordelijk lijnmanagement. In het uiterste geval wordt het incident als escalatie rechtstreeks doorgespeeld aan het hoogste orgaan, het CvB.
Binnen elk IM-beheerdomein wordt een contactpersoon voor CERT-RU aangesteld, de zogeheten domein security contact (DSC).

CERT-RU bestaat uit negen mensen. Zij vervullen een parttime taak. De totale tijdsbesteding aan CERT-activiteiten per jaar wordt geschat op 0,5 FTE. Men hanteert een zeven-maal-vierentwintig-uur-rooster. Eens in de negen weken heeft elk lid officieel dienst. Het dienstdoende CERT-lid kan daarnaast voor ondersteuning een beroep doen op de andere CERT-leden, wanneer die aanwezig zijn. Ieder CERT-lid heeft inzage in de gemelde en vastgelegde incidenten en alle communicatie daarover. Leden worden geselecteerd door CERT-RU zelf. De faculteiten wordt vervolgens gevraagd om de desbetreffende kandidaat voor te dragen, waarna benoeming plaatsvindt door de directeur UCI. Binnen CERT-RU streeft men naar een evenwichtige vertegenwoordiging van de diverse integraalmanagementeenheden. Naast het genoemde principe van brede vertegenwoordiging gelden de volgende criteria bij indiensttreding:

- werkzaam zijn bij Radboud Universiteit Nijmegen
- het beschikken over bewezen kennis/ervaring op gebied van beveiliging
- diversiteit/spreiding van specialismen binnen het team (netwerk, OS, virus, etc.).

De werkzaamheden vinden plaats op vrijwillige basis. CERT-leden krijgen aan het einde van het jaar meestal een vergoeding.

4.2.2.3. Incidentenresponse

De hoofdtaak coördinatie van het voorkomen en oplossen van aan ICT-beveiliging gerelateerde incidenten betekent in de praktijk het onderhouden van een meldpunt voor incidenten, het opstellen en uitvoeren van incidentenafhandelingsprocedures en zonodig het verstrekken van gegevens aan partijen binnen de RU die tot repressie willen overgaan. Incidenten kunnen in principe door elke persoon die valt onder de gedefinieerde doelgroep worden aangemeld bij CERT-RU. Binnen de RU wordt echter aangemoedigd dat melding plaatsvindt via de decentrale computerondersteuningsgroepen die doormelden naar CERT-RU, tenzij lokale afhandeling triviaal is. Het CERT-RU handelt in beginsel alle communicatie af via de DSC, tenzij een dergelijke afhandeling in strijd is met de privacy van een individuele melder. Buiten de RU wordt het upstream-CERT gebruikt als primaire communicatiepartner. CERT-RU hanteert het vangnetprincipe. De meeste incidenten worden door de computerondersteuningsgroepen zelf opgelost. De CERT-RU-organisatie en -procedures staan beschreven in een openbaar toegankelijk operational framework [OPF01]. Daarnaast zijn er drie vertrouwelijke documenten waarin procedures staan beschreven voor respectievelijk de CERT-RU-helpdesk, de CERT-RU-medewerker en de DSC.

Definities

CERT-RU hanteert een classificatie van soorten incidenten[92]:

Tabel 13: incidentklassen CERT-RU

Incident	Omschrijving	Symptomen
Cracking	Hierbij is sprake van ongeautoriseerde toegang tot een systeem	Wijziging in logs en bestanden en het algemeen functioneren Ook checksums kunnen wijzigen en er kan activiteit op een ongebruikelijke tijd worden geconstateerd
DoS attack	Aanvallen op een systeem of service met als doel dat systeem of die service uit te schakelen of lam te leggen, meestal door excessief gebruik (= misbruik) te maken van op zichzelf legitieme functionaliteit	Systeem of service is voor de buitenwereld niet meer te bereiken terwijl de netwerkverbinding intact is en het systeem op zichzelf functioneert; het heeft het alleen te druk met de afhandeling van een excessieve vraag of aanbod
Poortscans	Van een systeem wordt bekeken wat voor (netwerk) services geleverd worden. Een poortscan wordt vaak gevolgd door een crack of een D.o.S.-attack, het wordt soms gebruikt om te kijken welke mogelijk (onbeveiligde) ingangen er zijn	Een firewall detecteert simpele vormen van dergelijke scans en zal deze melden via zijn logboek of interface
Virussen	Programma's die als doel hebben individuele systemen (meestal PC's of Mac's) te verstoren of misbruiken. Door de sterke besmettelijkheid van sommige virussen treden sneeuwbal effecten op die grote aantallen systemen beroeren; zelfs D.o.S. effecten kunnen optreden, b.v. door de enorme hoeveelheid resulterend E-mail verkeer	Vreemd gedrag van PC's en/of applicaties (berucht zijn WORD, EXCEL en OUTLOOK), verdwijnen of defect raken van gebruikersbestanden en programmatuur, het ontvangen van vreemde mailtjes
Spamming	Ongewenste mail, vaak overdadige mail vaak met als doel reclame te maken	Gebruiker ontvangt mail van een onbekende waar hij niet om gevraagd heeft. Vaak is de verzender niet te achterhalen
Mail-relay	Platform om ongewenste mail door te sturen	Via een open mail-relay kan men mails versturen afkomstig van een extern domein en bedoeld voor een (ander) extern domein. Men fungeert dus in wezen als onbetaald postkantoor voor derden. In de regel weet de

[92] Uit Procedures voor incidentafhandeling versie 1.0 d.d. 26 november 2001, deel 3: Procedure voor de Domain Security Contacts binnen de RU.

		beheerder van een systeem niet dat hij mail-relay is, tenzij hij bewust deze service host wat echter niet tot de 'Best Internet Practice' behoort. Een beheerder zal meestal niets merken van de 'service'die hij verleent maar zal vaak door derden hierop gewezen worden
Social attacks	Onheuse benaderingen zoals beledigingen, bedreigingen en ongewenste seksuele benaderingen	Gebruiker ontvangt mail of leest op een website social attacks. Hierin wordt hij beledigd, bedreigd en/of lastig gevallen
Schending van licenties/ copyright	Het ongeoorloofd aanbieden van bestanden en programma's. Het ongeoorloofde schuilt vaak in licentiebeheer of in illegaliteit van bestanden	Een Internetter kan dit soort bestanden opzoeken op verschillende sites
Overige		Het is onmogelijk ieder mogelijk beveiligingsincident bij voorbaat in te delen in een bepaalde, vooraf goed gedefinieerde, categorie. Vandaar deze restcategorie

Aanmelden van incidenten
Aanmelding en vastlegging gebeurt op pragmatische wijze[93]. Door het grote aantal in te vullen velden per incidentrecord heeft CERT-RU besloten beveiligingsincidenten op een andere manier te archiveren. De meeste incidenten, meer dan negentig procent, worden gemeld via de functionele mailbox van CERT-RU, cert@ru.nl. Andere kanalen zijn met name telefoon en fax.

CERT-RU hanteert twee urgentieniveaus van communicatie:

Standaard Communicatie met het CERT-RU via e-mail, of in bijzondere gevallen per fax, verdient in het algemeen de voorkeur. Op deze berichten zal steeds binnen 24 uur worden gereageerd.

Urgent Meldingen telefonisch via de UCI Helpdesk. De medewerkers van de UCI Helpdesk zijn geïnstrueerd in het aannemen van gesprekken voor het CERT-RU en het doorgeleiden van urgente meldingen naar het dienstdoende lid van het CERT-RU (de CERT-RU medewerker van dienst).

Incidenten kunnen desgewenst versleuteld per e-mail worden aangemeld. Hierbij wordt gebruikt gemaakt van PGP-versleuteling. Openingstijden, telefoonnummer, e-

[93] Binnen UCI zijn beheerprocessen, waaronder incident management, sterk gestandaardiseerd op basis van de ITIL-methodiek. Voor de vastlegging van incidenten wordt een separate tool gebruikt. Door de grote aantal in te vullen velden per incidentrecord heeft CERT-RU besloten incidenten op een andere manier te archiveren.

mailadressen en public PGP-key zijn opgenomen in een bijlage bij het operationeel raamwerk.

Verwerken en behandelen van incidenten
De meeste incidenten worden binnen één week afgehandeld en afgesloten. Complexe incidenten, veelal incidenten waar andere, externe partijen bij betrokken zijn, kunnen soms maanden open staan. Dit komt echter zelden voor. Er blijven soms incidenten openstaan, omdat er te laat een terugmelding komt van de contactpersoon binnen de IM-eenheid dat het probleem is opgelost. CERT-RU geeft uitsluitend adviezen. Er vindt geen controle op de uitvoering van de adviezen plaats. Ook worden aangedragen adviezen, bijvoorbeeld de installatie van security patches, niet door CERT-RU getest.

Registratie van incidenten vindt plaats binnen het e-mailsysteem. Van incidenten die niet via e-mail binnenkomen, wordt ten behoeve van registratie een e-mail aangemaakt. In het mailsysteem, gebaseerd op het IMAP-protocol, wordt per incident een map aangemaakt met een uniek, opvolgend incidentnummer. Uitsluitend CERT-leden hebben lees- en schrijfrechten op deze mappen. Alle e-mails met betrekking tot een bepaald incident worden in de desbetreffende map geplaatst. Na verloop van tijd worden de mappen gearchiveerd. Daarnaast wordt een EXCEL-spreadsheet gehanteerd waarbij per rij het incident nader wordt omschreven zoals incidentnummer, categorie, korte omschrijving, datum aanmelding, naam betrokken CERT-RU-lid, naam contactpersoon, organisatieonderdeel en status. De spreadsheet wordt bij iedere dienst overgedragen aan het dienstdoende CERT-lid. De spreadsheet wordt met name gebruikt als raadpleegdocument door CERT-leden bij nieuwe incidentenmeldingen en als bron voor de managementrapportage.

CERT-RU-leden maken gebruik van standaard netwerk- en besturingssysteemsoftware[94] om bijvoorbeeld IP-adressen te traceren of systeemlogs te analyseren. Vaak is men aangewezen op de door de beheerder verstrekte (log)informatie. Er wordt geen gebruik gemaakt van specialistische forensische hulpmiddelen.
Het scannen op kwetsbaarheden en intrusion detection gebeurt niet centraal vanuit CERT-RU. Wel vinden deze activiteiten individueel plaats door CERT-leden binnen hun organisatorische entiteit.

Incidentenstatistieken
Per maand worden vijftig tot zestig incidenten door CERT-RU behandeld. Het werkelijk aantal incidenten waar de RU als organisatie mee te maken krijgt, is vele malen groter doordat veel incidenten door de COG's zelf worden afgehandeld. Tachtig procent van de incidenten van CERT-RU heeft te maken met virussen, inclusief wormen, en spam. Ook het aantal portscans scoort hoog.

4.2.2.4. (Externe) Contacten

CERT-RU hanteert een drietal beleidslijnen ten behoeve van communicatie Allereerst is er de security policy, die er op is gericht om te voorkomen dat CERT-RU nalatigheid kan worden verweten. Het beleid is opgesplitst in twee delen. Het ene (interne) deel betreft de manier waarop CERT-RU de communicatie en opslag van gegevens beveiligt. In dit deel gelden de volgende uitgangspunten: beveiliging is geregeld volgens 'best current

[94] Genoemd werden de programma's 'PING' en 'TRACEROUTE'.

practices', incidentenrapportages worden geanonimiseerd en er is beperkte toegang tot incidentengegevens. Het andere (externe) deel betreft de manier waarop CERT-RU omgaat met informatie, in het bijzonder incidenteninformatie, die het van buiten krijgt. Het CERT-RU-profiel dat hierbij wordt gehanteerd is conform de IETF RFC 2350. Uitgangpunten zijn:

- alle binnenkomende informatie wordt vertrouwelijk behandeld
- zeer gevoelige informatie wordt uitsluitend versleuteld gecommuniceerd
- CERT-RU gebruikt verstrekte informatie alleen op need-to-knowbasis en in principe in geanonimiseerde vorm
- als een informatieverstrekker aanvullende beperkingen verbindt aan het verspreiden van de bewuste informatie zal CERT-RU dit respecteren
- CERT-RU doet geen aangifte van incidenten bij justitie, tenzij de wet aangifte vereist
- CERT-RU werkt op verzoek van justitie mee in officiële onderzoeken: een bevel ter zake van de rechter-commissaris is daarbij voorwaarde.

Het persbeleid van CERT-RU komt er kort gezegd op neer, dat de persvoorlichter van de RU, dienst Communicatie en Marketing alle vragen over CERT-werkzaamheden die worden gesteld door de pers, beantwoordt.

CERT-RU hanteert tenslotte een gedragscode voor zijn medewerkers. In algemene zin geldt dat een CERT-RU-medewerker spreekt namens CERT-RU en zich daarbij te allen tijde geduldig, waardig en beheerst gedraagt.

Het Upstream-CERT is het CERT van de internetserviceprovider van de RU[95]. Dit is de standaard externe bron en bestemming van incidentengerelateerde informatie voor het CERT-RU. De binnen de RU bestaande SSC-functie van SURFnet-CERT maakt integraal onderdeel uit van CERT-RU. Een andere veel gebruikte bron van informatie is het CERT Coordination Center van de Carnegy Mellon University, Pittsburgh U.S.A. en tegenwoordig ook GOVCERT.NL.

Daarnaast is er tweemaal per jaar een overleg met andere universitaire CERT's in Nederland. De contacten met organisaties als TERENA beperken zich tot het deelnemen aan cursussen door CERT-RU leden.

4.2.3. CERT-RUG

4.2.3.1. RijksUniversiteit Groningen

De Rijksuniversiteit Groningen is georganiseerd in tien faculteiten. De RUG is een grote universiteit met meer dan 20.000 studenten (september 2003). Naast de faculteiten kent de RUG een aantal centrale diensten zoals het Bureau, het Facilitair Bedrijf en het Rekencentrum

Het Rekencentrum (Zernikeborg) is een centrum voor informatietechnologie dat hoogwaardige ICT-diensten aanbiedt, primair aan de Rijksuniversiteit Groningen, secundair aan onderwijsinstellingen en derden in de noordelijke regio. Het

[95] Dit was ten tijde van het onderzoek SURFnet-CERT.

dienstenpakket bestaat onder meer uit het beheer en de ontwikkeling van het universitaire computernetwerk RUGnet, koppeling met het Internet, het beschikbaar stellen van centraal opgestelde computers voor wetenschappelijke en studiedoeleinden, eerste- en tweedelijnsondersteuning bij computerproblemen en het verzorgen van computercursussen.

In oktober 2000 is de functie van securitymanager ontstaan binnen het rekencentrum. Deze functie is geplaatst binnen de afdeling communicatie en relatiemanagement (CRM). Een toenemende belangstelling voor beveiliging lag aan deze nieuwe functie ten grondslag. Een van de eerste acties van de securitymanager was het initiëren van een tweetal nota's: visie op ICT-security en acceptable use policy.

Begin 2002 heeft de securitymanager een op e-mail gebaseerde communicatiestructuur binnen de RUG geïmplementeerd ten behoeve van het melden en afhandelen van beveiligingsincidenten en het distribueren van informatie en adviezen met betrekking tot ICT-beveiliging. Ook is in dat jaar de securitykerngroep in het leven geroepen. Deze groep vormt tezamen met de communicatiestructuur het hart van CERT-RUG[96].

Doelgroep zijn enerzijds (alle) systeembeheerders binnen de RUG en anderzijds de contactpersonen voor beveiliging bij de faculteiten/afdelingen.

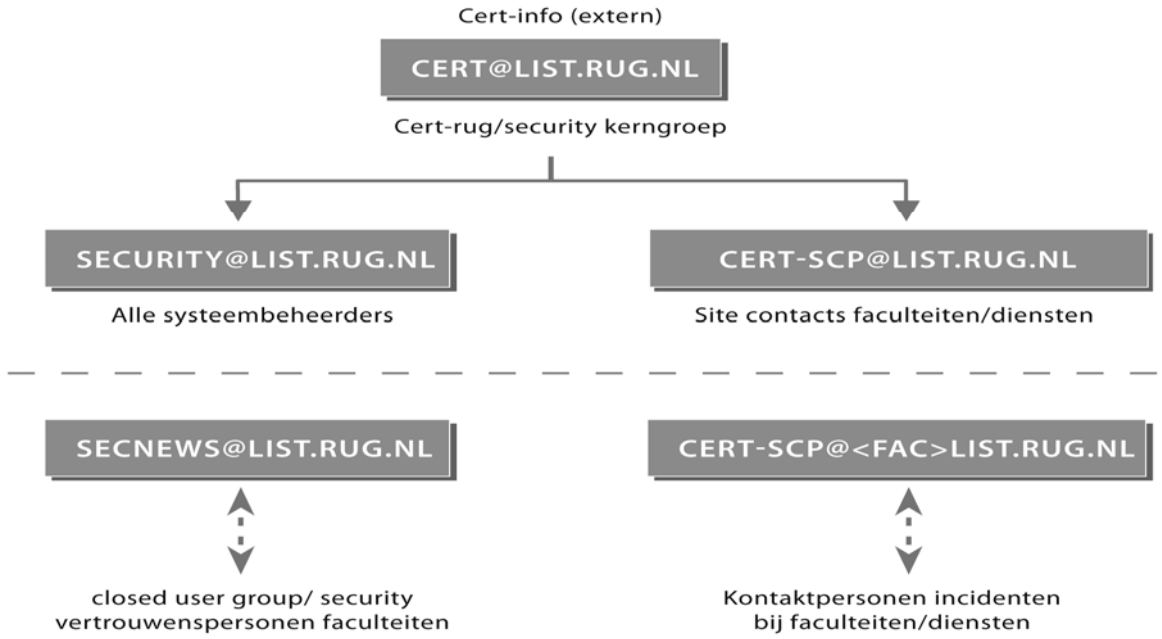
4.2.3.2. Organisatie CERT-RUG

CERT-RUG wordt primair ingevuld door de securitykerngroep. Deze bestaat uit vijf ervaren medewerkers/managers werkzaam bij het Rekencentrum, inclusief de securitymanager. De leden zijn onder meer werkzaam bij de afdelingen Netwerkdienst, Systeembeheer en Lanbeheer van het Rekencentrum. Een van de leden is als eerste aanspreekpunt verantwoordelijk voor de juiste afhandeling van de binnengekomen e-mail op de functionele mailbox. Er bestaat geen formeel consignatierooster. De leden vervangen elkaar in geval van ziekte, vakantie e.d. Mede door de brede vertegenwoordiging van disciplines is de securitykerngroep in staat de afhandeling van diverse soorten incidenten te coördineren of zelf uit te voeren.

De securitykerngroep valt formeel onder verantwoordelijkheid van de directie van het Rekencentrum.

Naast de kerngroep bestaat er ook nog een virtueel platform, SECNEWS genaamd, van gespecialiseerde en vertrouwde systeembeheerders waar incidenten en beveiligingsvraagstukken worden uitgewisseld. Leden van deze zogeheten closed user group worden aan de securitymanager voorgedragen door de voor ICT binnen de faculteit verantwoordelijke managers. Figuur 17 geeft een overzicht van de communicatiestructuur voor ICT-beveiliging binnen de universiteit.

[96] De naam CERT-RUG is geen officiële benaming en wordt ook niet gehanteerd binnen de diverse procedures en raanwerkdocumenten.



Figuur 17: ICT-beveiligingscommunicatiestructuur Rijksuniversiteit Groningen

4.2.3.3. *Incidenten Response*

CERT-RUG heeft geen operationeel raamwerk met beveiligingsprocedures. Wel is er een document dat de beveiligingscommunicatiestructuur beschrijft, een gedragscode voor alle ICT gebruikers[97] en er zijn 'adviezen en aanwijzingen'[98]. Een belangrijke taak van CERT-RUG is het operationaliseren en exploiteren van de communicatiestructuur en het coördineren van de afhandeling van gemelde incidenten.

Een aan ICT-beveiliging gerelateerd incident wordt door de securitymanager gedefinieerd als *'alles wat de integriteit van de systemen aantast'*. CERT-RUG hanteert geen incidentenclassificatie.

Aanmelden van incidenten
Incidenten bij faculteiten of afdelingen worden meestal via e-mail gemeld aan een per faculteit opgestelde functionele mailbox: CERT-SCP@<FAC>.RUG.NL Aan deze lijst dienen de e-mailadressen van minimaal twee personen te worden gekoppeld. Voor incidenten op universiteitsniveau is de functionele maibox CERT@list.rug.nl ingericht. Alle leden van de securitykerngroep zijn met hun e-mailadres aan deze lijst gekoppeld. Zij krijgen dus gelijktijdig de melding gedistribueerd. Ook is genoemd adres het contactadres voor een aantal externe CERT's, waaronder SURFnet-CERT. Daarnaast kan rechtstreeks worden gebeld naar de securitymanager of een ander lid van de securitykerngroep en kan via de helpdesk van het rekencentrum een incident bij de securitymanager worden gemeld. Buiten kantoortijd is er een algemeen alarmtelefoonnummer van het Rekencentrum. Bij incidenten zal in eerste instantie de directeur van het rekencentrum worden benaderd die vervolgens de securitymanager inschakelt. Bij het melden van incident via e-mail kan gebruik worden gemaakt van PGP-versleuteling.

[97] Acceptable Use Policy geheten.
[98] Bijvoorbeeld adviezen over de geldigheidstermijn van passwords, aanwijzingen ten aanzien van het gebruik van draadloze communicatie tussen computers en de installatie van personal firewalls.

Registreren en behandelen van incidenten
Er zijn geen formele procedures voor afhandeling, prioritering en vastlegging van aan ICT-beveiliging gerelateerde incidenten. Gezien het geringe aantal (serieuze) incidenten wordt dit niet noodzakelijk geacht. Binnengekomen en afgehandelde incidenten worden door de securitymanager binnen zijn eigen e-mailomgeving opgeslagen.

De normale procedure van CERT-RUG bij de afhandeling van beveiligingsincidenten is het waarschuwen van de gebruiker en in tweede instantie het overdragen van het incident via een proces-verbaal aan de directie van de afdeling/faculteit. De directie kan vervolgens als disciplinaire maatregel op grond van de Acceptable Use Policy [AURG01] de gebruiker uitsluiten van verdere dienstverlening.

Aan de hand van checksumcontrole of PGP-controle wordt de authenticiteit en integriteit van binnengekomen waarschuwingen en/of patches gecontroleerd. De betrouwbaarheid van de patch zelf wordt niet getest door de securitykerngroep.

Begin 2003 is een zogeheten rapid deployment force ('crashteam') opgericht binnen de afdeling systemen van het Rekencentrum. De leden zijn vrijgesteld om op aanvraag te worden ingezet bij incidenten. Zij beschikken over tools voor forensisch onderzoek en intrusion detection. Het team wordt bij incidenten aangestuurd door de het hoofd systeembeheer tevens lid van de securitykerngroep.

De securitykerngroep stelt op verzoek hulpmiddelen ter beschikking ten behoeve van vulnerability scanning (NESSUS) en integriteitscontrole[99].

Incidentenstatistieken
Op jaarbasis is er sprake van gemiddeld twaalf serieuze beveiligingsincidenten die door CERT-RUG worden behandeld. Het betreft onder meer hackingincidenten en spamincidenten. Bij deze incidenten kan de RUG het doelwit zijn, maar ook worden gebruikt als uitvalbasis voor ongewenste activiteiten. Naast deze incidenten krijgt CERT-RUG ook veel meldingen met betrekking tot detectie van virussen en schendingen van de gedragscode, de zogeheten abuse-meldingen. De virusincidenten zijn volgens de securitymanager door up-to-datescanners en soms aanvullende maatregelen, zoals het herconfigureren van firewalls, goed onder controle te houden.

4.2.3.4. (Externe) contacten

SURFnet-CERT en TERENA vormen voor CERT-RUG het belangrijkste externe netwerk. CERT-RUG is als derde organisatie in Nederland door TERENA geaccrediteerd voor de zogeheten level 2-status.

De universiteit zal ondanks het ontbreken van formele procedures bij een serieus beveiligingsincident in principe altijd aangifte doen bij justitie, aldus de securitymanager. De securitykerngroep speelt een beslissende rol bij het besluit om aangifte te doen.

[99] Respectievelijk de open source software NESSUS en het zelfgebouwde STEALTH (SSH-Based Trust Enhancement Acquired through a Locally Trusted Host).

4.3. GovCERT

Een aantal jaren geleden is GovCERT, het computer emergency responseteam voor Nederlandse overheden, opgericht. Het team vervult niet alleen de rol van incidentencoördinator ten behoeve van overheidsinstellingen, maar is ook verantwoordelijk voor de operationalisering van de waarschuwingsdienst. Een gevalstudie zoals uitgevoerd bij de CERT's van enkele hoger onderwijsinstellingen en SURFnet behoorde helaas niet tot de mogelijkheden. De directeur van GovCERT was in maart 2004 bereid om de organisatie van GovCERT en de werking van de waarschuwingsdienst schriftelijk nader toe te lichten. Hieronder volgt een samenvatting van deze toelichting.

4.3.1. Inleiding

GovCERT is in juni 2002[100] ontstaan uit een van de ICT-programma's van het ICT-Uitvoeringsorgaan[101] van de rijksoverheid en is een initiatief van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. Naast een negental ministeries participeren in het eerste kwartaal van 2004 ook de Belastingdienst, het Centraal Bureau voor Statistiek, KNMI en andere zogeheten zelfstandige bestuursorganen in GovCERT.NL. De organisatie heeft als belangrijkste taak om de overheid te ondersteunen op het gebied van preventie en afhandeling van aan ICT-beveiliging gerelateerde incidenten, zoals computervirussen, hackeractiviteiten en fouten in applicaties en hardware. GovCERT is voor de overheid het centrale meld- en coördinatiepunt voor relevante beveiligingsincidenten[102].

4.3.2. Organisatie GovCERT

Het team bestaat in 2004 uit vijftien personen en is zevenmaal-vierentwintig-uur beschikbaar. De medewerkers werken in actieve dienst tussen 09:00 en 23:00 uur. Daarnaast is een medewerker op toerbeurt oproepbaar tussen elf uur 's avonds en negen uur in de ochtend. GovCERT faciliteert voorts een operationeel incidentresponseteamoverleg, waarbij vertegenwoordigers van diverse overheidsinstellingen en het bedrijfsleven[103] recente incidenten, kwetsbaarheden en trends bespreken.

4.3.3. Waarschuwingsdienst

Sedert 13 februari 2003 is vanuit GovCERT.NL in opdracht van het Ministerie van Economische Zaken een waarschuwingsdienst operationeel. Het doel van de Waarschuwingsdienst[104] is de burger en ondernemers behorend tot het kleinbedrijf in Nederland ook te laten profiteren van de maatregelen die de rijksoverheid voor zichzelf

[100] GovCERT heette tot 13 februari 2003 nog CERT-RO. Voor deze naamswijziging is gekozen omdat het werkterrein breder werd dan uitsluitend de *rijks*overheid en om de internationale positie te benadrukken. Een andere reden voor deze naamswijziging was dat buitenlandse CERT's de naam CERT-RO associeerden met de nationale CERT van Roemenie.
[101] Zie http://www.ictu.nl.
[102] Zie http://www.govcert.nl.
[103] Het betreft voornamelijk vertegenwoordigers van Nederlandse Internetserviceproviders en banken.
[104] Uit 'algemene voorwaarden' van de Waarschuwingsdienst.

heeft genomen om incidenten te signaleren en zo mogelijk te voorkomen. Op de website wordt uitdrukkelijk gesteld dat zij geen helpdeskfunctie vervult voor persoonlijke vragen en/of incidentenmeldingen. Via de website kan men zich abonneren op berichten van de waarschuwingsdienst. Daarbij kan worden gekozen voor een e-mail- of SMS-berichtendienst. Een jaar na de officiële opening hadden zich al zesendertigduizend abonnees ingeschreven voor de dienst E-mail Alert en waren er tweehonderdnegenendertig waarschuwingen geplaatst op de website.

Informatie ten behoeve van de waarschuwingsdienst wordt gehaald uit publiekelijk beschikbare mailinglijsten en -websites en (besloten) mailinglijsten van anti-virusprogrammaleveranciers, FIRST, Trusted Introducer, e.a. Verder zijn er contacten met de Nederlandse politie- en inlichtingendienst en met buitenlandse computer security incident responseteams.
Binnenkomende berichten worden volgens een vaste intakeprocedure gecontroleerd op berichtauthenticiteit. Allereerst wordt bepaald of het bericht binnenkomt van een vertrouwde bron uit de bronnenlijst. Bij de bepaling van de authenticiteit wordt verder gebruik gemaakt van DNS-queries, nslookups en traceroutes, het bekijken van de header van een e-mailbericht of bij telefoon de stemherkenning. Bij gebruikmaking van PGP of PKI wordt de authenticiteit vastgesteld door middel van een cryptografische sleutel.

Alle berichten van de waarschuwingsdienst worden volgens de in figuur 18 weergegeven vaste opmaak verstuurd.

```
  ##########################################
 ##    Waarschuwingsdienst  - ALERT    ##
 ##########################################

Programma   : [xxx]
Versie      : [xxx]
Besturingssysteem: [xxx]

Samenvatting
[xxx]

Gevolgen
[xxx]

Mogelijke oplossingen
[xxx]

Hyperlinks
[xxx]
---------------------------------------------------------------
Disclaimer
[xxx]
```

Figuur 18: structuur van een GovCERT E-mail Alert

GovCERT hanteert een zogeheten mediamix filterprocedure voor bepaling van de impact van binnengekomen berichten en besluitvorming ten behoeve van escalatie.

4.3.3.1. Mediamix filter

De classificatie van informatie uit de bronnen voor de Waarschuwingsdienst vindt plaats op basis van een tweetal schalen: kans x objectieve impact en kans x subjectieve impact.

Horizontaal: 1. De kans dat een gebruiker te maken krijgt met het probleem.
2. De impact van het in aanraking komen met het probleem wat betreft de technische en economische schade.

Verticaal: 1. De kans dat een gebruiker een gevoel van onveiligheid krijgt.
2. De (verwachte) mate van publieke aandacht dat het probleem krijgt.

Samen bepalen deze factoren het risico: laag, midden of hoog.

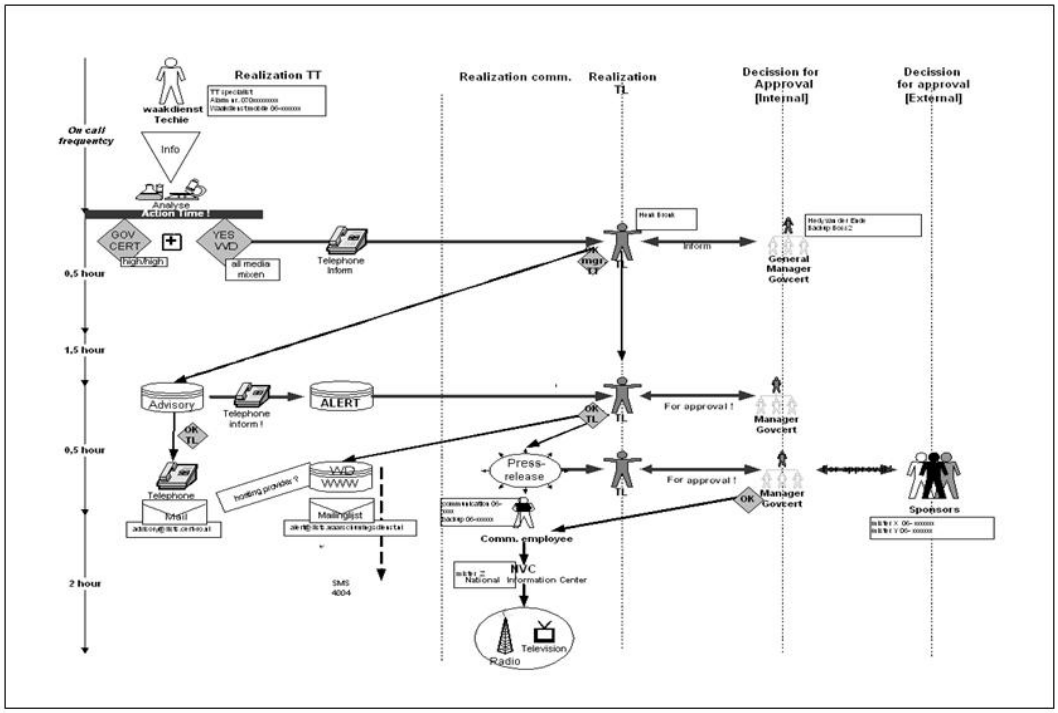
Tabel 14: mediamix filter GovCERT

Classificatie		**Kans x objectieve impact**		
		Laag	*Midden*	*Hoog*
Kans	*Laag*	kanalenmix 1	kanalenmix 1	kanalenmix 2
x	*Midden*	kanalenmix 1	kanalenmix 2	kanalenmix 3
subjectieve impact	*Hoog*	kanalenmix 2	kanalenmix 3	kanalenmix 4

Mix 1 = Website
Mix 2 = Website, e-mail
Mix 3 = Website, e-mail, pers
Mix 4 = Website, e-mail, pers, radio/tv.

4.3.3.2. Escalatieprocedure

GovCERT hanteert een escalatieprocedure voor het vaststellen van het communicatiekanaal ten behoeve van de verspreiding van waarschuwingen, waarbij standaard(goedkeurings)procedures worden gevolgd voor het opschalen van waarschuwingen aan de diverse media, zie figuur 19.



Figuur 19: de escalatieprocedure bij GovCERT

4.4. Korps Landelijke Politiediensten

In de periode maart tot en met oktober 2004 is onderzoek gedaan bij het Team Digitale Recherche van het Korps Landelijke Politiediensten (KLPD) te Driebergen. Een belangrijke reden voor onderzoek bij de politie was het feit dat politie en justitie meestal de laatste schakel vormen binnen de totale keten van afhandeling van ernstige aan ICT-beveiliging gerelateerde incidenten[105]. Het onderzoek spitste zich toe op de wijze waarop KLPD-onderzoeksprocessen verlopen. Ook is gekeken naar het gebruik van hulpmiddelen en de interactie tussen de politie als opsporingsinstantie en slachtoffers van cybercrime. Hiertoe is het zogeheten kastje-incident[106] nader geanalyseerd.

4.4.1. Inleiding

In 2003 heeft de Dienst Nationale Recherche van het Korps Landelijke Politiediensten een verkennende analyse binnen de Nederlandse politiekorpsen uitgevoerd naar de aard en omvang van cybercrime in Nederland [WERF03]. Doelstelling van deze analyse was het in kaart brengen van de mate waarin geselecteerde verschijningsvormen van cybercrime voorkomen bij de digitale specialistische opsporingsinstanties in Nederland, de manier waarop deze vormen van cybercrime worden uitgevoerd en mogelijke ontwikkelingen rond bepaalde criminaliteitsvormen. De analyse van de registraties van

[105] Voor zover het incidenten betreft met (mogelijk) strafrechtelijke componenten.
[106] Dit misdrijf heeft zich in 2003 voorgedaan bij een grote financiële instelling in Nederland.

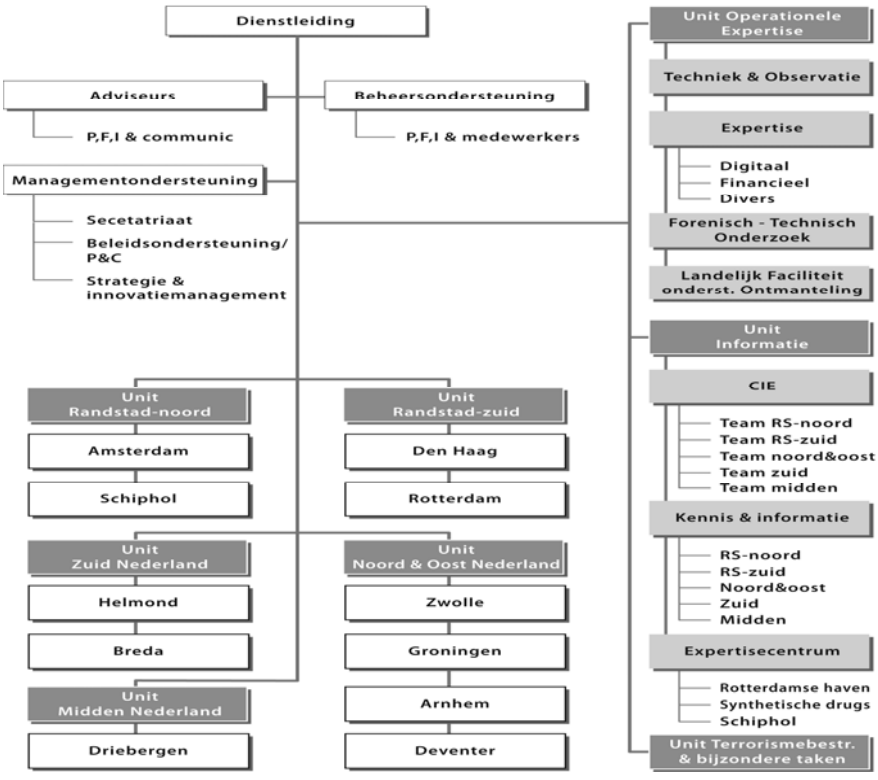
de digitale rechercheteams in Nederland en de registraties van gesprekspartners uit het bedrijfsleven heeft echter de onderzoeksvragen niet concreet kunnen beantwoorden. De hoofdreden is dat betrouwbare registraties vanuit opsporing en bedrijfsleven ontbreken. Wel is op basis van interviews en documenten geconcludeerd dat digitale technieken in toenemende mate worden ingezet bij het uitvoeren van criminele activiteiten.

4.4.2. Team Digitale Recherche

4.4.2.1. Organisatie

Het KLPD vormt samen met de vijfentwintig regionale politiekorpsen de Nederlandse politie. Het KLPD werkt op nationaal en internationaal niveau en heeft zelfstandige, ondersteunende en coördinerende taken [KLPD03].
In specifieke situaties ondersteunt het KLPD de regionale korpsen en/of coördineert gezamenlijke activiteiten. Daarbij kan het gaan om de inzet van materieel, technologie en gespecialiseerde professionals bij massamanifestaties, grootschalige evenementen en rampen. Daarnaast levert het KLPD recherche-expertise, misdaadanalyse en logistieke diensten. Het KLPD heeft twaalf uitvoerende diensten. Deze diensten verrichten de kernactiviteiten van het korps zoals de Dienst Verkeerspolitie, de Dienst Spoorwegpolitie en de Dienst Nationale Recherche (zie figuur 20). Er zijn vier ondersteunende diensten voor de bedrijfsvoering en verder vier stafbureaus. Er werken ongeveer vijfenveertighonderd mensen bij het KLPD.

Het onderzoek is uitgevoerd binnen het Team Digitale Expertise (TDE) van de Unit Operationele Expertise, onderdeel van de Dienst Nationale Recherche van het KLPD.



Figuur 20: organogram dienst Nationale Recherche (maart 2004)

De organisatie van de Unit Operationele Expertise bestaat uit een unithoofd, een afdeling Techniek & Observatie (60 FTE's) met observatierechercheurs en vakspecialisten, een team Digitaal (20 FTE's) met digitaal rechercheurs, internetrechecheurs en R&D-specialisten, een team Financiële expertise (14 FTE's) en een team Diverse expertise (14 FTE's) met juristen, onderzoekers, cultureel antropologen, e.a. Daarnaast is aan de Operationele unit specifieke expertise toegevoegd voor de ondersteuning van het ontmantelen van XTC-labs.

4.4.2.2. Definitie van cybercrime

In 2002 is binnen het KLPD een onderzoek uitgevoerd naar een praktijkgerichte definitie van de criminaliteitsproblematiek die wordt aangeduid als cybercrime [MOWE02]. Hierbij stonden de volgende vragen centraal:

- wat is een goede Nederlandse vertaling van de term cybercrime?
- hoe kan cybercrime omschreven worden?
- welke criteria zijn leidend in de begripsafbakening?
- aan welke verschijningsvormen denkt men bij cybercrime?.

Op basis van raadpleging van diverse deskundigen en Europese publicaties is binnen de KLPD de volgende definitie ontstaan: *cybercrime omvat elke strafbare en strafwaardige gedraging, voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.*

Voor het categoriseren van delicten die tot cybercrime gerekend kunnen worden, is gebruik gemaakt van een indeling van de Engelse National High Tech Crime Unit (NHTCU)[107], waarbij onderscheid wordt gemaakt tussen enerzijds 'oude versus nieuwe misdrijven' en anderzijds 'oude versus nieuwe hulpmiddelen'. Het onderscheid tussen oude en nieuwe misdrijven heeft vooral betrekking op het aspect *doelwit* van het delict, terwijl de *instrumenten* met behulp waarvan delicten worden gepleegd de onderscheidende factor zijn tussen oude en nieuwe hulpmiddelen.

Tabel 15: oude versus nieuwe misdrijven [SMIT02]

	Hulpmiddelen		
Misdrijven		Oud	Nieuw
	Oud	1. Diefstal van geheugenchips d.m.v. braak	2. Oplichting van consumenten door een nepwebsite
	Nieuw	3. Ontregelen van digitale meetapparatuur	4. Hacking

De delicten die onder kwadrant twee, drie en vier geschaard kunnen worden, vallen volgens de auteurs onder de noemer cybercrime. In kwadrant drie gaat het vooral om *de wijze waarop* geautomatiseerde werken worden ingezet bij het plegen van strafbaar of strafwaardig gedrag. Het onderscheid tussen kwadrant twee en kwadrant vier wordt aangeduid met cybercrime in brede zin respectievelijk cybercrime in enge zin. De auteurs

[107] NHTCU is in januari 2006 ondergebracht bij de National Crime Squad, een landelijk opererende Britse politie-eenheid dat onderzoek doet naar specifieke, ernstige misdrijven.

stellen dat het kenmerkende van de gedragingen in kwadrant twee is, dat ze worden uitgevoerd *met behulp van* een computer(systeem). Computertechnologie ondersteunt dus de uitvoering van het delict. Een ander voorbeeld dat wordt genoemd, is het verspreiden van kinderpornografisch beeldmateriaal via het Internet. Delicten waarbij een computer het *doel* is van de criminele gedraging worden door de auteurs aangeduid met cybercrime in enge zin.

Tabel 16: overzichtstabel met voorbeelden van verschijningsvormen van cybercrime

Cybercrime	
Verschijningsvormen waarbij de computer als middel wordt gebruikt bij de uitvoering van strafbare of strafwaardige gedragingen	*Verschijningsvormen waarbij de computer tevens het doel is van de strafbare of strafwaardige gedragingen: cybercrime in enge zin*
Bedrijfsspionage	Hacking (computervredebreuk)
Diefstal van gegevens	Defacing
Witwassen	(D)DOS-aanval
(virtuele) Kinderpornografie	Verspreiding malicious code
Discriminatie	Softwarepiraterij
Oplichting via Internet	Skimming
Heling	Manipulering (tampering) van gegevens
Terrorisme	Chipspiraterij
Illegaal gokken	Spoofing

4.4.2.3. Aangifteproces

Het aangifte- en opsporingsproces van het KLPD wordt conform de methoden Aanpak Bedrijfsvoering Informatiehuishouding en Opleiding (ABRIO)[108] en Ordening Methodiek Processen (OMP)[109] vormgegeven en uitgevoerd.

Regulier aangifte- en opsporingsproces
Het primaire rechercheproces van het KLPD vindt op verschillende niveaus plaats. De operationele 'blauwe' diensten, zoals Spoorweg- Water- en Verkeerspolitie, hebben met betrekking tot hun eigen taakveld een eerstelijnslijnsverzorging van het rechercheproces. In dat proces worden aangiften opgenomen en eventueel onderzoeken uitgevoerd. Het betreft hier dan relatief eenvoudige onderzoeken zoals de inbraak in de woning aan boord van een schip of de diefstal van goederen uit een benzinestation langs de autosnelweg.

Zware georganiseerde criminaliteit
De Dienst Nationale Recherche (DNR) is belast met de bestrijding van zware georganiseerde criminaliteit in binnen- en buitenland en enkele specifiek benoemde aandachtsgebieden. Ze wordt in deze aanpak en uitvoering van onderzoeken aangestuurd door het Landelijk Parket van het Openbaar Ministerie. Er worden bij de DNR geen directe aangiften opgenomen en onderzocht.

High tech crime

[108] ABRIO heeft als doel verbetering te brengen in de werkprocessen bij politie en openbaar ministerie.
[109] OMP is een bruikbare methodiek voor de beschrijving van bedrijfsprocessen en de daaruit voortkomende producten.

Voordat de politie in actie komt bij een geval van cybercrime of high tech crime[110] dient aangifte te worden gedaan bij de regiopolitie. Vervolgens worden deze aangiften op basis van weegcriteria en prioriteitsstelling van de betreffende politieregio beoordeeld met als belangrijkste doel het bepalen of een nader onderzoek wordt ingesteld. De regiopolitie maakt daarbij meestal gebruik van de ondersteuning van medewerkers van een (inter)regionaal bureau digitale expertise. In bijzondere gevallen levert het Team Digitale Expertise (TDE) van de DNR ondersteuning. Het TDE voert niet zelfstandig cybercrimeonderzoeken uit. Het ondersteunt met zijn expertise primair de DNR in de onderzoeken van de specifieke aandachtsgebieden van deze organisatie.

Art. 161 Sv bepaalt dat iedereen[111] die kennis draagt van een begaan strafbaar feit is bevoegd daarvan aangifte te doen of een klacht in te dienen. Opsporingsambtenaren zijn verplicht de aangifte in ontvangst te nemen. Bij sommige misdrijven is er een verplichting tot het doen van aangifte. Een belangrijk criterium is dat er sprake dient te zijn van een strafrechtelijk misdrijf of strafrechtelijke overtreding. Bij het opstellen van een procesverbaal tijdens of na de aangifte zal de opsporingsambtenaar duidelijk moeten aangeven welke artikelen uit het strafrecht van toepassing zijn. Bij cybercrime in enge zin levert dat soms problemen op, omdat de opsporingsambtenaar niet altijd de feiten kan vertalen naar de juiste artikelen uit het strafrecht. Een goed voorbeeld zijn de zogeheten phishingincidenten, waarbij de georganiseerde criminaliteit via nep-emails en nagebootste websites identiteitsgegevens en creditcardnummers van klanten van banken proberen te ontfutselen. Veelal is hier sprake van poging tot oplichting danwel poging tot diefstal. De aangifte van een phishingincident door een Nederlandse financiële instelling leverde in 2004 bijvoorbeeld enige problemen op omdat de regiopolitieambtenaar het incident in aanvang verwarde met een poging tot computervredebreuk (hacking).

Meestal wordt door een slachtoffer aangifte gedaan bij het politiebureau in de regio waar het strafbare feit is gepleegd of waar het slachtoffer woonachtig of werkzaam is.

4.4.2.4. Onderzoeksproces

Binnen KLPD/DNR is vanaf het jaar 2000 gewerkt aan de ontwikkeling van een methodiek voor de uniforme beschrijving van de werkprocessen bij de politie en het Openbaar Ministerie. Dit heeft geresulteerd in een aantal documenten onder de noemer 'Ordening Methodiek Processen' (OMP). Hoewel de TDE medewerkers bekend zijn met de uitgangspunten van OMP hanteren zij tijdens onderzoek geen vaste onderzoeksaanpak, *'elke zaak is uniek'* wordt gezegd. Wel wordt er bij bepaalde typen misdrijven een 'standaard'checklijst gehanteerd tijdens het onderzoek. Een voorbeeld is het misdrijf 'hacking':

Bij hacken en cracken heeft iemand de bedoeling, zonder dat hij toestemming van de eigenaar heeft, in een geautomatiseerd werk binnen te dringen zoals omschreven in artikel 138a lid 1 WvSr. Het kan zijn dat de dader, nadat hij is binnengedrongen, nog

[110] Internationaal wordt in plaats van cybercrime soms de term high tech crime gebezigd voor 'misdaden met behulp van (of gericht tegen) informatie- en communicatietechnologie'. Men onderscheidt twee hoofdcategorieën: vormen van criminaliteit, die gericht zijn tegen computersystemen en/of communicatienetwerken, de eerder genoemde cybercrime in enge zin en klassieke criminaliteit gepleegd met behulp van ICT. In het kader van het onderzoek wordt de term cybercrime gehanteerd.

[111] Dit is dus niet beperkt tot een slachtoffer van een strafbaar feit.

andere handelingen verricht, zoals bijvoorbeeld het overnemen en voor zichzelf of een ander vastleggen van gegevens. In dat geval is sprake van een misdrijf op grond van artikel 138a lid2 WvSr. Een hacker kan echter ook opzettelijk dan wel door schuld een geautomatiseerd werk vernielen. In dat geval kan tevens strafbaarheid op grond van de artikelen 161sexies en 161septies WvSr bestaan. Het is ook mogelijk dat nadat is binnengedrongen opzettelijk gegevens worden vernield. Deze situatie is zelfs expliciet strafbaar gesteld in artikel 350a lid 2 WvSr. Als na het binnendringen in een geautomatiseerd werk door schuld gegevens worden vernield, dan kan artikel 350b van WvSr toepassing zijn [GEES03][112].

Er worden binnen het Team Digitale Expertise drie verschijningsvormen onderkend:

Fysieke inbraak Bij deze vorm van inbraak heeft een hacker fysieke toegang tot een systeem en kan hij via een console toegang krijgen of een hard disk met gegevens uit een systeem halen.

Lokale inbraak Bij deze inbraak heeft een hacker al gebruikersrechten op een systeem. Via een exploit of het afkijken van een wachtwoord kan een hacker zijn gebruikersrechten uitbreiden.

Inbraak op afstand Een hacker heeft bij deze inbraak geen gebruikersrechten op een systeem. Door middel van een of meerdere exploits kan een hacker zichzelf toch toegang verschaffen tot een systeem.

Voor het aantonen van hacking/cracking zijn de volgende gegevens nodig:

- source-IP-adres(sen)
- destination-IP-adres
- tijdstip van aanval
- output van meerdere datapakketten, met informatie over de diverse lagen van het OSI model
- overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing
- overzicht van het gebruikersbeheer op het systeem, zodat inzichtelijk is welke gebruikers op het systeem actief zijn, en welke rechten deze users hebben.
- audit logs.

Een van de eerst activiteiten bij onderzoek is het inventariseren van bewijsmateriaal. Vroeger ging men uit van het standpunt dat ‘alles wat maar enigszins digitaal’ was in beslag genomen diende te worden. In verband met de enorme toename van digitale gegevens op personal computers en op servers, wordt er tegenwoordig ter plaatse gerichter gezocht en worden gegevens vervolgens veilig gesteld. In sommige gevallen maakt de TDE-specialist gebruik van een mobiele flightcase waarbij grote aantallen gegevens, tot een maximum van drie gigabyte, ten behoeve van nader forensisch onderzoek worden gekopieerd.

[112] Citaat uit de GovCERT-handleiding ‘Van herkenning tot aangifte’ (juli 2003), waar ook medewerkers van het TDE een bijdrage aan hebben geleverd.

Bij forensisch onderzoek worden meestal meerdere typen onderzoek onderscheiden, bijvoorbeeld inhoudelijk onderzoek (onderzoek naar gegevens), communicatieonderzoek (wie communiceert met wie) en tijdlijnenonderzoek (op welke tijdstippen zijn welke handelingen verricht). Ten behoeve van bewijsgaring maken de TDE-specialisten gebruik van verschillende hulpmiddelen. Voor het kopiëren en veiligstellen[113] van bewijsmateriaal en analyse van de data wordt meestal gebruik gemaakt van de softwaretools Forensisch Toolkit (FTK) van de firma Accessdata en Encase van de firma Guidance Software. Om eventuele wijzigingen in de imagekopie onmogelijk te maken, wordt tussen de te onderzoeken computer en de schijf waarop de image wordt geplaatst een zogeheten read-only hardwaredevice geplaatst die ervoor zorgt dat er geen (onbewuste) schrijfacties kunnen plaatsvinden naar het onderzoeksobject. Voor onderzoek op Unix machines wordt vaak gebruik gemaakt van RDD[114], dit is een variant op de standaard Unix-DD-tool ontwikkeld door het Nederlands Forensisch Instituut (NFI) uit Rijswijk. In het kader van een opsporingsonderzoek naar feiten, gepleegd via het Internet, of naar personen die via het Internet communiceren stuit men soms op computers die in openbare gelegenheden staan zoals Internetcafés, belhuizen of bibliotheken. De digitale sporen die na gebruik op de computer achterblijven kunnen voor de opsporing van belang zijn. Medewerking van de systeembeheerder van dergelijke openbare gelegenheden is niet altijd mogelijk of gewenst. Daarom wordt gekeken naar een nieuwe variant op Encase, Field Intelligence Model (FIM) genaamd, waarmee via een netwerkverbinding op afstand kopieën of previews van de harde schijf en/of het RAM-geheugen kunnen worden gemaakt. Hiertoe dient op de te onderzoeken computer eerst een klein programma te worden geïnstalleerd. Het gebruik van FIM roept echter een aantal juridische vraagstukken op met betrekking tot de doorzoekingsbevoegdheden, zoals opgenomen in het wetboek van strafvordering.
Voordat een nieuw onderzoekstool wordt ingezet, wordt de technische bruikbaarheid en integriteit beoordeeld door het NFI.

Naast direct bewijsmateriaal, zoals gegevens uit logbestanden, kan soms indirect bewijsmateriaal van belang zijn. Voorbeelden zijn fysieke toegangsregistraties of cameraopnamen bij gebouwen. Het rond krijgen van een zaak is dan ook vaak een combinatie van tactisch rechercheren door onder meer het vormen van een beeld van de dader, het ondervragen van verdachte(n), etc. en het verkrijgen van feitenmateriaal aan de hand van digitaal en/of Internetrechercheren.

Voor onderzoek van grote aantallen gegevensbestanden is door specialisten van het TDE een zogeheten digitale wasstraat ontwikkeld. Het belangrijkste doel hiervan is het veilig stellen van gegevens en het ordenen van de te onderzoeken bestandstypen[115]. Verder worden gezipte files geheel geautomatiseerd uitgepakt, niet-relevante systeembestanden verwijderd en diverse controles automatisch uitgevoerd, bijvoorbeeld de eventuele aanwezigheid van kinderpornoplaatjes.

Naast het bewijsmateriaal wordt de bewijsvergaring uit het oogpunt van mogelijke contra-expertise zorgvuldig vastgelegd. In een aantal gevallen worden de zoekopdrachten en overige handelingen geautomatiseerd opgeslagen. Bij Internetrechercheren worden de

[113] Het veiligstellen gebeurt middels het plaatsen van een hash over de onderzoeksgegevens (per bestand, per schijf of beide) waarbij elke wijziging in de data zichtbaar wordt bij de hashcontrole achteraf.
[114] De 'R' verwijst naar de naam van de auteur (Raoul).
[115] Bijvoorbeeld alle email-bestanden, alle worddocumenten, etc.

onderzoekshandelingen van de TDE-specialist standaard automatisch vastgelegd in een de zogeheten tapfile.

Het belangrijkste eindproduct van een opsporings- en vervolgingsonderzoek is het procesverbaal[116], waarin het bewijs is verwerkt[117] of waarbij wordt verwezen naar bijgevoegd bewijsmateriaal op foto, DVD, etc.

4.4.3. Cybercrimecasus

In het kader van de derde gevalstudie is het eerdergenoemde kastje-incident bij de organisatie BANK[118] uit 2003 nader onderzocht. Bij dit onderzoek zijn relevante documenten geanalyseerd en zijn interviews gehouden met medewerkers en het hoofd Special Investigations van BANK en een medewerker van het Bureau Digitale Expertise van de politie Amsterdam-Amstelland.

De eerste melding
Op 4 juli 2003 meldt een beleidsmedewerker van BANK aan de ICT-helpdesk dat zijn PC niet meer werkt. Na enkele uren komt een helpdeskmedewerker langs en constateert een vreemd hangend kastje, met 'enige uitstekende draden' gekoppeld aan de achterkant van de PC. Het toetsenbordsnoer is losgeschoten. De medewerker sluit de snoeren weer aan, koppelt het kastje af en neemt het mee naar de helpdesk. Daar vertrouwt men het niet helemaal en informeert de afdeling Information Risk Management. Deze afdeling schakelt vervolgens de interne afdeling Special Investigations in. Deze afdeling coördineert integriteits- en fraudeonderzoeken binnen BANK. Special Investigations vermoedt na een korte analyse een fraudeaanval of poging daartoe.

Onderzoek door Special Investigations
Special Investigations (SI) doet na deze conclusie vervolgens onderzoek ter plaatse, reconstrueert de situatie en maakt foto's van de omgeving en het kastje. De SI-medewerker trekt na onderzoek ter plaatse de conclusie dat er mede door de ligging van het gebouw wellicht sprake is van een remotebediening van het kastje. Men vermoedt dat het kastje in staat is gegevens, zoals userids en wachtwoorden en wellicht (betaal)transacties, op afstand af te luisteren en/of te manipuleren.

Special Investigations doet vervolgens binnen enkele uren aangifte en overhandigt het kastje voor nader onderzoek aan de politie Amsterdam-Amstelland. De politie deelt mede dat het kastje dezelfde dag nog naar het Nederlands Forensisch Instituut zal worden gestuurd ten behoeve van nader onderzoek.
Special Investigations plaatst een aantal camera's bij de bewuste werkplek in de hoop terugkerende daders op videobeeld vast te leggen[119]. De min of meer ongebruikelijk snelle reactie van handelen, vooral de snelle aangifte, is mede ingegeven door het feit dat

[116] Als voorbeeld wordt een geanonimiseerd procesverbaal uit 2000 aangeleverd waarin aangifte van en onderzoek naar een DDOS-anval is beschreven.
[117] Bijvoorbeeld een quote uit een logbestand.
[118] Op verzoek van de organisatie, een grote Nedelandse financiële instelling, wordt hier een gefingeerde naam gebruikt.
[119] Men verwachtte dat de dader(s) terug zouden keren, omdat het kastje niet (goed) was aangesloten door loshangende kabels.

de politie van Amsterdam twee maanden eerder BANK had getipt dat de organisatie mogelijk slachtoffer zou worden van interne fraude.

Special Investigations legt een zwijgplicht op aan de helpdesk- en beleidsmedewerker en informeert verder een beperkt aantal zogeheten 'key-players' bij grote fraude-onderzoeken. Hiertoe behoren onder meer de managers van respectievelijk de afdelingen Internal Audit en Legal & Compliance.

In de eerste dagen na 4 juli formuleerde Special Investigations drie kernvragen:

- wat kon het kastje allemaal en hoe werkte het?
- welke autorisaties had de medewerker bij wie het kastje was gevonden?
- welke bedrijfskritische applicaties waren mogelijk betrokken?.

Bij BANK leefde men in de veronderstelling dat het NFI snel antwoord zou geven op de eerste vraag. Na vier weken was er echter nog steeds geen antwoord vanuit het Openbaar Ministerie (OM) en het NFI. Bij de evaluatie een half jaar later bleek dat het OM geen prioriteit gaf aan deze zaak en dat het NFI wachtte op toestemming van de Officier van Justitie (OvJ) om analyses en een DNA-sporenonderzoek uit te voeren op het kastje.

Het periodiek bekijken van de video-opnamen door BANK leverde na ongeveer twee weken resultaat op, doordat men drie verdachten signaleerde. De bewaking van BANK herkende een van de verdachten, een ingehuurde medewerker. Ook de politie herkende een verdachte. De derde verdachte was niet bekend. De verdachten hielden echter hun mond over de werking van het kastje en of er daadwerkelijk fraude was gepleegd. De derde verdachte werd na ongeveer twee maanden aangehouden.

Escalatie
Eind juli kwam wederom een melding binnen van de politie, dat 'er iets ging gebeuren' bij BANK, soortgelijk aan het incident van 4 juli. Special Investigations besloot daarop het escalatieconsigne binnen de organisatie af te geven. Diverse directeuren werden op de hoogte gebracht. Doordat een aantal directeuren de eigen crisisorganisatie activeerde, was er binnen enkele uren sprake van een ware BANK-brede crisissituatie. Omdat er nog geen duidelijke antwoorden waren op de drie kernvragen van het incident van 4 juli en de kans aanwezig was dat er wederom fraude met betalingsverkeersapplicaties werd gepleegd werd een aantal interne betalingsverkeersapplicaties stopgezet en besloten in alle gebouwen van BANK fysiek te speuren naar ongebruikelijke voorwerpen bij computerapparatuur. Ook besloot men om collegabanken, de Nederlandse Vereniging van Banken en de toezichthouder, De Nederlandsche Bank, te informeren over de situatie.

Na overleg met collega's bij andere financiële instellingen besloot het hoofd SI van BANK een commercieel ICT-forensisch onderzoeksbureau in te schakelen om uitsluitsel te geven over de werking van het eerder gevonden kastje. Dit bureau gaf aan de hand van de foto-informatie van BANK binnen een week uitsluitsel over de mogelijke werking van een dergelijk apparaat. Het rapport werd via de toezichthouder naar alle banken in Nederland gestuurd.

Omdat de verdachten niets los lieten, heeft Special Investigations uiteindelijk de conclusie getrokken dat er geen georganiseerde criminaliteit achter het incident van 4 juli

zat en dat de tweede melding door de politie loos alarm was. Men heeft tot op heden geen bewijs kunnen vinden dat met het kastje daadwerkelijk fraude is geplaagd. Wel is met hulp van het rapport van het onderzoeksbureau de indruk overgebleven dat het amateuristisch ogende apparaatje had kunnen werken.

Lessons learned
Het kastje-incident is uiteindelijk bij BANK geëscaleerd tot een majeure crisis met interbancaire consequenties. Het hoofd SI zegt dat het onderzoek en de crisis zelf veel tijd en geld hebben gekost. Bij het interne onderzoek zijn naar schatting tussen de vijftig en honderd medewerkers betrokken geweest. Special Investigations heeft een evaluatierapport opgesteld voor de Raad van Bestuur van BANK en hierin staan de volgende verbeterpunten beschreven:

- de ICT-organisatie, vooral ook de helpdesk, dient beter te worden geïnstrueerd over het behandelen van incidenten[120]
- bij overdracht van voorwerpen aan justitie dienen betere afspraken te worden gemaakt over doorlooptijd, toegankelijkheid tot het politieonderzoek en teruggave van overhandigde voorwerpen
- de fysieke toegangsbeveiliging dient te worden verbeterd
- voor het nemen van eventuele arbeidsrechtelijke stappen is het niet nodig om te wachten op de uitslag van het politie-onderzoek
- bevorder de bewustwording binnen BANK, dat er sprake is van een integraal beveiligingsprobleem binnen de organisatie (IT, fysiek, etc.)
- houd een crisisorganisatie klein en verbeter de interne communicatie.

4.4.4. Evaluatie

Op basis van de uitgevoerde gevalstudie bij de KLPD en het onderzoek bij het Bureau Digitale Expertise van de politie Amsterdam-Amstelland is vastgesteld dat de expertise met betrekking tot misdrijven waarbij informatietechnologie-elementen een rol spelen, niet breed aanwezig is binnen de politieregio's, maar vooral geconcentreerd is bij (kleine) teams speciaal opgeleide rechercheurs of buitengewone opsporingsambtenaren. De druk op deze teams is groot, doordat bij veel opsporingsonderzoeken een beroep op hen wordt gedaan.

KLPD hanteert een complexe definitie van cybercrime en maakt hierbij onderscheid tussen een aantal verschijningsvormen. Hoewel het aantal misdrijven waarbij de computer het doelwit is de afgelopen jaren is toegenomen, wordt de huidige capaciteit, meer dan tachtig procent, nauwelijks besteed aan directe bestrijding van cybercrime maar vooral aan onderzoeken waarbij de computer als middel wordt gebruikt bij de uitvoering van strafbare gedragingen.

Het verzamelen en veiligstellen van bewijsmateriaal is een kernactiviteit binnen elk ondersteunend onderzoek. Ook bij cybercrime in enge zin wordt vaak gebruik gemaakt van een combinatie van tactisch rechercheren en digitaal en/of Internetrechercheren om een zaak rond te krijgen. Zowel de Internet- als de digitaalrechercheur maakt tijdens opsporingsonderzoek gebruik van standaardhandelingen om bewijs te verzamelen of

[120] Onder meer dienen er een instructies te komen dat de helpdeskmedewerker geen 'ogenschijnlijk vreemde voorwerpen gekoppeld aan ICT apparatuur' mag aanraken danwel verwijderen.

veilig te stellen. De meest gebruikte tools voor forensisch onderzoek van computergegevensbestanden zijn Encase en FTK.
Het kastje-incident demonstreert het belang van een integrale beveiligingsaanpak bij grote organisaties. Verkokering van beveiligingsdiciplines, zoals gescheiden afdelingen voor fraudebestrijding, ICT beveiliging en fysieke beveiliging, leidt tot verbrokkeling van de aanwezige kennis en kunde met betrekking tot de bestrijding van beveiligingsincidenten, en tot verzwakking van de communicatie en het coördinerend vermogen. Het gevolg is dat de effectieve afhandeling van een incident gevaar loopt en bewijsmateriaal verloren gaat.