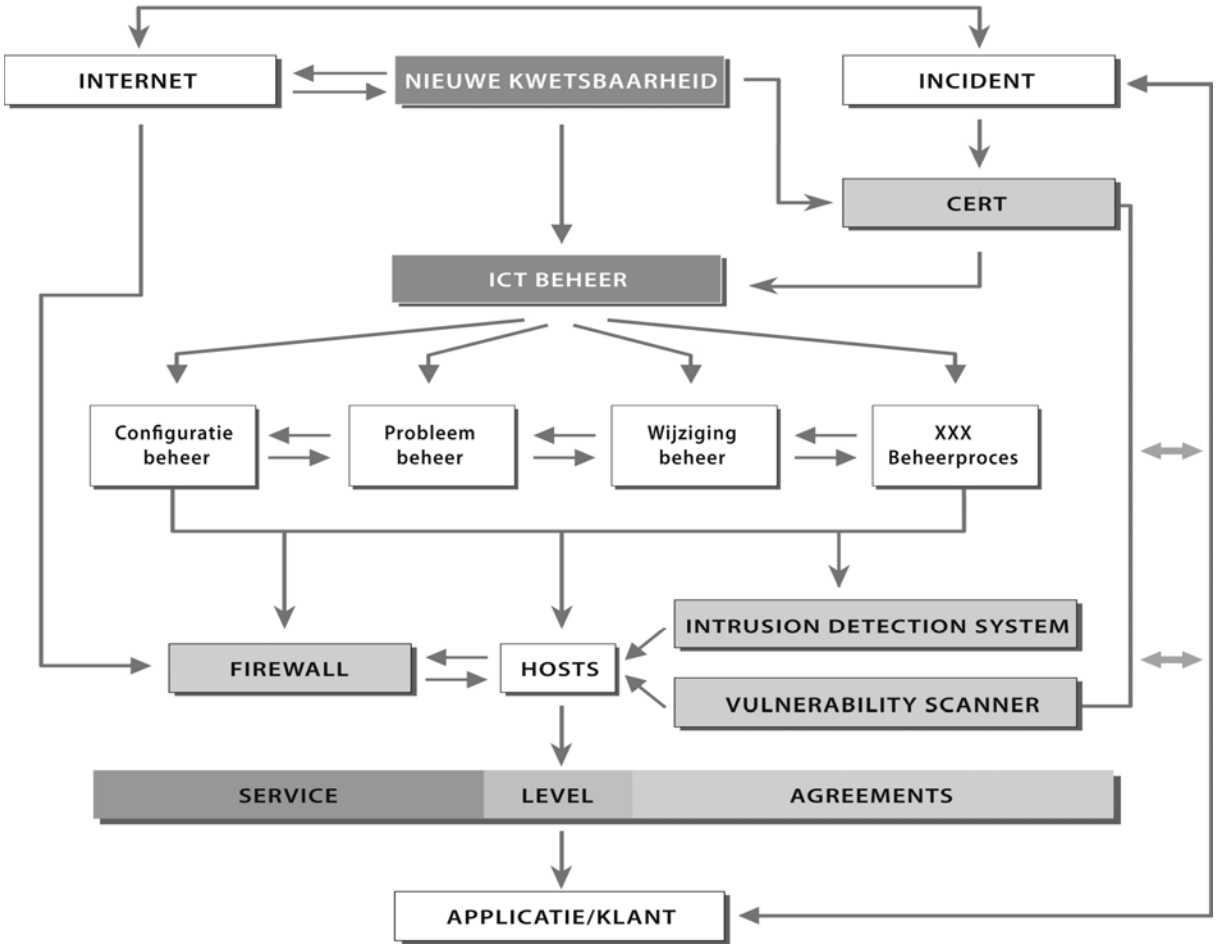
# Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

**Publication date**
2008

# 3. De praktijk van kwetsbaarheden- en incidentenmanagement

Grote aantallen ICT-componenten, complexe beheerprocessen en hoge tijdsdruk zijn de belangrijkste aandachtspunten bij het beantwoorden van incidenten en kwetsbaarheden bij grotere organisaties. Figuur 4 geeft de samenhang weer tussen de belangrijkste technische en organisatorische aspecten bij kwetsbaarheden- en incidentenresponse.




Figuur 4: samenhang tussen kwetsbaarheden en -incidentencomponenten

Multinationals en grote informatieverwerkende organisaties beschikken over het algemeen genomen over complexe technische infrastructuren met diverse soorten computernetwerken en –systemen, waarbij het aantal in beheer zijnde ICT-configuratie items kan oplopen tot enkele honderdduizenden. Ter illustratie: de centrale ICT-organisatie van Rabobank Nederland beheerde in het derde kwartaal van 2006 honderdzevenenvijftigduizend desktopinstallaties en eenentwintigduizend servergebaseerde software-installaties. Om de infrastructuur effectief en efficiënt te beheren, maken ICT-beheerafdelingen gebruik van gestandaardiseerde processen voor het afhandelen van incidenten, het implementeren van wijzigingen, het uitvoeren van onderhoud, etc.

Naast de omvang en diversiteit van de ICT-infrastructuur geeft ook het element tijdsduur soms een extra dimensie, omdat bepaalde kwetsbaarheden en gevolgen van incidenten door de ICT-organisatie binnen een zeer korte tijdsperiode, soms binnen vierentwintig uur, dienen te worden verholpen.

In deze paragraaf worden een aantal in de praktijk voorkomende, aan het onderwerp gerelateerde processen, technieken en organisatievormen behandeld.

Allereerst wordt stilgestaan bij een aantal technologische ontwikkelingen die van belang zijn voor het onderzoek. De introductie van bijvoorbeeld application proxy firewalls heeft gezorgd voor een verbeterde toegangscontrole en -scheiding tussen het Internet en het interne bedrijfsnetwerk. Ook maken intrusion detection systems het tegenwoordig mogelijk om (bijna) realtime-inbreuken en/of indringers op het interne netwerk te detecteren en eventueel te blokkeren, en ook kan met hulp van vulnerability scanners de eigen infrastructuur systematisch worden onderzocht op de aanwezigheid van kwetsbaarheden.

Vervolgens wordt de Information Technology Infrastructure Library (ITIL) methodiek nader beschouwd. In een aantal Europese landen hebben grotere organisaties hun ICT beheerprocessen vanaf 1990 gestandaardiseerd volgens deze methodiek. ITIL beschrijft de elementen, stappen en onderlinge relaties van de meest voorkomende ICT-beheerprocessen [ITSM04]. Het ‘hart’ van ITIL wordt gevormd door een tiental processen behorende tot de service support en service delivery set. Incident management, configuration management, change management, maar ook capacity management, availability management en security management zijn voorbeelden van genoemde processen. Dit hoofdstuk gaat op een aantal van deze ITIL-processen nader in.

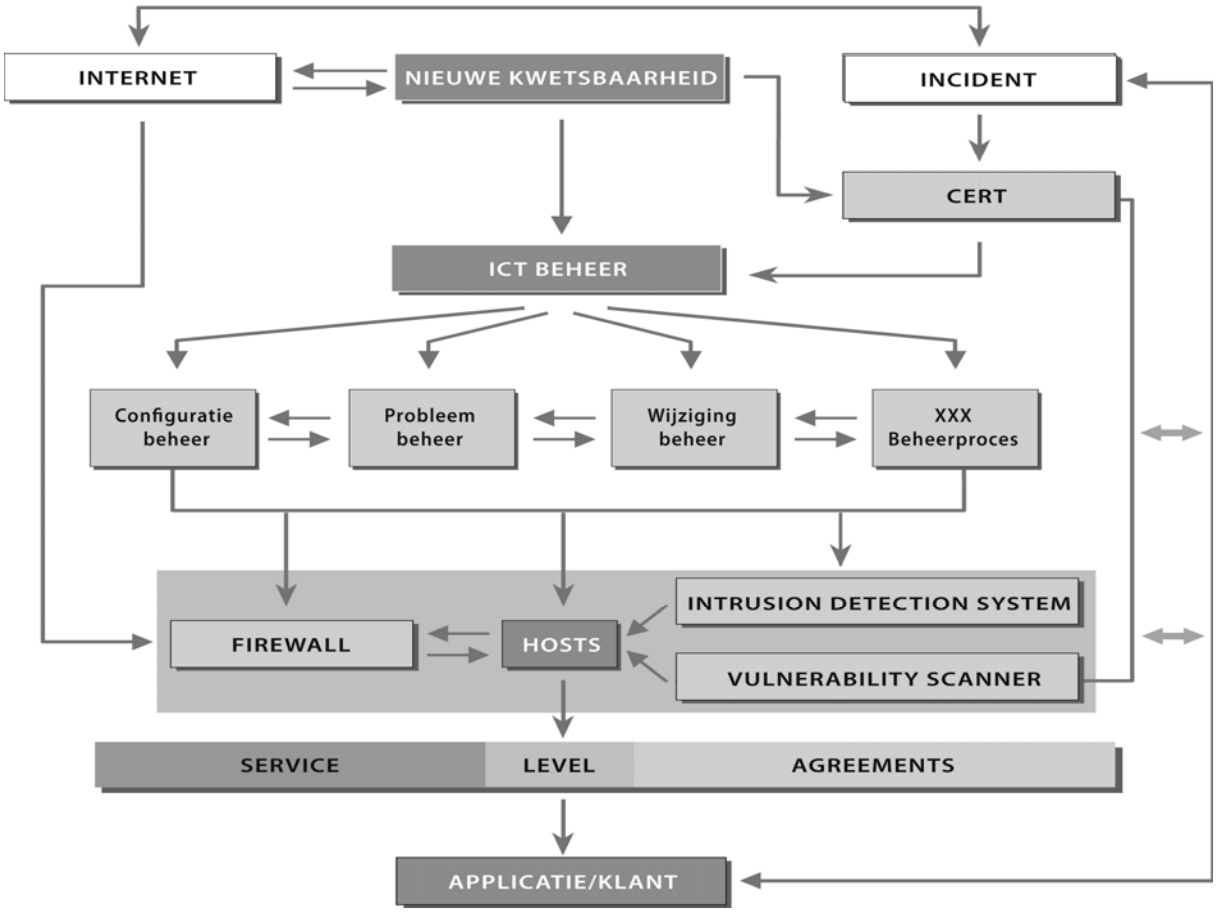
Tenslotte wordt in dit hoofdstuk aandacht besteed aan ontwikkelingen met betrekking tot computer security incident response teams en managed security service providers.

## *3.1. Technologische ontwikkelingen*

De opkomst van nieuwe hard- en softwarebeveiliging in de jaren negentig, waaronder firewalls, vulnerability scanners en intrusion detection systems, heeft een belangrijke bijdrage geleverd aan het verbeteren van de kwaliteit van kwetsbaarheden- en incidentenresponse. Deze technieken hebben tot doel enerzijds het voorkomen van incidenten en anderzijds het tijdig detecteren van kwetsbaarheden of incidenten zodat de organisatie maatregelen kan nemen om (verdere) schade te voorkomen. In navolgende paragrafen worden de technieken op hoofdlijnen besproken.

### *3.1.1. Firewalls*

Directe verbindingen tussen bedrijfsnetwerken en het internet maken het voor een indringer een stuk eenvoudiger om op afstand te zoeken naar systemen met kwetsbaarheden. Firewalls, geplaatst op de koppelvlakken tussen het eigen netwerk en het Internet, dienen deze bedreiging te adresseren, zie figuur 5.




Figuur 5: firewalls en intrusion detection systems

In een gesloten netwerk worden daarnaast soms firewalls geplaatst op de koppelvlakken tussen *interne* bedrijfsnetwerken met verschillende niveaus van beveiliging.

RFC 2828 van de IETF definieert een firewall als een *'Internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall)'*.

De naam 'firewall' heeft zich ontwikkeld tot een verzamelterm voor computerapparatuur en -software die toegang tot het interne netwerk controleren. Firewalls vormen een essentiële beheersingsmaatregel voor kwetsbaarheden- en incidentenbeheersing. Hieronder worden een drietal veel voorkomende technologieën op hoofdlijnen uiteengezet: packet filter, stateful inspection en application proxy firewalls.

#### *3.1.1.1. Packet filter firewalls*

Packet filter firewalls zijn in essentie routers [TANN03]), uitgebreid met toegangscontrolefuncties voor netwerkadressen en communicatiesessies. Packet filter firewalls, soms ook screening routers genoemd, opereren op laag 3 van het Open Systems Interconnection (OSI) model[14] [MICH96].

[14] Zie bijlage 2 voor een uitwerking van het OSI-lagenmodel.

De toegangscontrolefunctionaliteit van de packet filter firewall bestaat uit het genereren en handhaven van een set van regels op basis waarvan netwerkpakketten door de firewall worden doorgelaten of geweigerd. Elk netwerkpakket omvat een:

*Bronadres:* netwerk adres van het computersysteem waarvandaan het pakket initieel is verzonden.

*Bestemmingsadres:* netwerkadres van het computersysteem waar het pakket heen moet.

*Soort verkeer:* het netwerkprotocol dat wordt gebruikt om te communiceren tussen bron- en bestemmingsadres.

*Karakteristieken:* karakteristieken van de OSI-laag-4 communicatiesessie, zoals de bestemmingspoort van de sessie.

Op basis van de inhoud van een netwerkpakket en de ingestelde regels wordt het pakket doorgelaten of geweigerd. De firewall werkt hierdoor dus als een filter. Regels kunnen zowel worden ingesteld voor binnenkomend als uitgaand netwerkverkeer. De firewallbeheerder configureert in de firewall de adressen en poorten die dienen te worden geweigerd danwel te worden doorgelaten.

Packet filter firewalls behoren tot de eerste generatie firewalls en zorgen voor een goedkope en nuttige grensvlakbeveiliging [CHBR03]. Het gebruik van een dergelijke firewall heeft voor- en nadelen.

De belangrijkste *voordelen* van een packet filter firewall zijn *snelheid* en *flexibele inzetbaarheid*.

Packet filter firewalls zijn snel omdat ze enkel OSI-laag-3 pakketten analyseren en niet de protocolgegevens van de bovenliggende OSI-lagen.

Een packet filter firewall is bovendien flexibel inzetbaar. Aangezien de huidige netwerkprotocollen OSI-laag-3 en lager ondersteunen, is de packet filter firewall in te zetten in verschillende soorten netwerkinfrastructuren. Flexibel inzetbaar betekent ook dat de gebruiker geen wijzigingen behoeft aan te brengen in de client of server om te kunnen communiceren. Omdat packet filter firewalls ook denial-of-service aanvallen kunnen tegenhouden, worden ze vaak ingezet op de grensvlakken tussen het Internet en het eigen bedrijfsnetwerk.

*Beperkte aanvalsherkenning*, *ontbreken van gebruikersauthenticatieschema's* en *beperkt configuratiebeheer* zijn de belangrijkste *nadelen* van packet filter firewalls.

Een packet filter firewall is niet in staat een aanval tegen te houden die gebruik maakt van applicatiespecifieke kwetsbaarheden omdat het alleen OSI-laag-3 pakketjes onderzoekt. De firewall kan hierdoor niet bepaalde, ongewenste applicatiecommando's blokkeren [TANN03].

Verder ondersteunt vrijwel geen enkele packet filter firewall zogeheten gebruikersauthenticatie schema's. Gebruikers kunnen dus uitsluitend op basis van een netwerkadres worden tegengehouden.

Packet filter firewalls herkennen ook geen aanvallen waarbij gebruik wordt gemaakt van bepaalde zwakheden in de TCP/IP-specificatie en protocolstack, zoals het wijzigen of spoofen van een network layer address

Door het geringe aantal variabelen dat wordt gebruikt binnen de packet filter firewall rules is de kans op verkeerde of geen filtering door foutieve configuratie aanwezig.

#### *3.1.1.2. Stateful inspection firewalls*

Stateful inspection firewalls zijn packet filters die enige kennis omvatten van de netwerklagen boven OSI-laag-3. Deze firewalls accomoderen bepaalde aspecten van het TCP/IP-protocol. Wanneer de TCP-applicatie een sessie aangaat met een ander systeem dan wordt ook op het op bronsysteem een poort gecreëerd om data terug te ontvangen van het bestemmingssysteem. Op grond van TCP-protocolafspraken dient het nummer van de poort van het bronsysteem groter dan 1023 en kleiner dan 16384 te zijn en van het bestemmingssysteem een lager dan 1024 genummerde poort, bijvoorbeeld poort 25 voor het e-mailprotocol SMTP. Het openzetten van poorten voor terug te ontvangen data levert uiteraard een risico op. Stateful inspection firewalls lossen dit probleem op door het opzetten van een state table waarin een overzicht wordt bijgehouden van uitgaande TCP-connecties met de corresponderende poortnummers van het bronsysteem. De tabel wordt gecontroleerd wanneer pakketten arriveren bij de firewall. Indien een van het bestemmingssysteem terugontvangen pakket overeenstemt met in de tabel opgenomen gegevens, wordt het pakket doorgelaten.

Stateful inspection firewalls delen de sterkten en zwakten van packet filter firewalls maar kunnen als *veiliger* worden beschouwd, omdat ze *bepaalde contextinformatie van communicatiesessies meenemen* bij het besluit om netwerkpakketten toe te laten of te weigeren. Omdat de bovenste (applicatie)lagen van het OSI model niet of niet grondig onderzocht worden, kunnen pakketten waarin kwaadaardige software is verborgen nog steeds de firewall passeren.

#### *3.1.1.3. Application proxy firewalls*

Application proxy firewalls combineren de toegangscontrole op de onderste OSI-lagen met een applicatielaag functionaliteit. Dit type firewalls onderzoekt alle netwerklagen door het inbrengen van extensieve contextinformatie in het firewallbeslisproces. De sessie wordt door de firewall gedeeld in de vorm van een client/servercommunicatie, waardoor twee verbindingen ontstaan: één van de client naar de firewall en één van de firewall naar de server. De aanwezige proxy server software maakt de firewall tot een proxy server. Proxies ontvangen verzoeken van de client en maken vervolgens verbinding met de gewenste server namens de client door het kopiëren van het packet met uitzondering van de brongegevens. Hierdoor wordt directe toegang tot services op het interne bedrijfsnetwerk en omgekeerd voorkomen. Daarbij kan de firewall de inhoud van de sessie doorzoeken (screenen), voorzien in gebruikersauthenticatie en ervoor zorgen dat alleen een specifieke dienst wordt gebruikt.

De belangrijkste *voordelen* van een application proxy firewall zijn *accuraatheid* en de mogelijkheid van *gebruikersauthenticatie.*

De loggings van application proxy firewalls bevatten veel meer informatie over pakketten, omdat het totale pakket wordt onderzocht. De meest firewalls van dit type ondersteunen verschillende vormen van gebruikersauthenticatie, zoals userid en wachtwoord of certificaten.

De belangrijkste *nadelen* van een application proxy firewall zijn lange *verwerkingstijd* en beperkte *ondersteuning bij nieuwe applicaties*.

Het kost een application proxy firewall relatief veel tijd om een volledig pakket te lezen en te interpreteren. Dit type firewall is daarom minder geschikt voor intensieve, realtime-applicaties. Daarnaast is er een beperking in de ondersteuning van nieuwe netwerkapplicaties en -protocollen aangezien voor elk nieuw protocol een nieuwe proxy moet worden geschreven en geïmplementeerd. Vaak worden daarom alleen de gangbare protocollen ondersteund.

#### *3.1.1.4. Firewallarchitecturen*

Bij bedrijfsnetwerken bestaan firewalls vaak niet uit één enkele computer maar uit een bepaald aantal onderling gerelateerde en geschakelde firewallcomponenten, waardoor een hybride omgeving ontstaat[15]. Een van de veiligste firewallimplementaties vandaag de dag is de screened subnet firewall met een zogeheten demilitarized zone (DMZ). Deze omvat twee pakketfilterrouters en een bastion host. De router in het interne netwerk controleert de uitgaande pakketten en de router in het externe netwerk de inkomende pakketten. De pakketten die de eerste hindernis hebben genomen, gaan voor nader onderzoek naar de application gateway (bastion host). De reden voor het gebruik van twee pakketfilters op verschillende Local Area Networks is dat er geen pakketten in of uit mogen zonder dat ze de application gateway zijn gepasseerd [TANN03]. Kortom er is geen omweg. Dit type firewallarchitectuur ondersteunt dus zowel pakketfiltering alsmede proxydiensten en creëert een klein netwerk tussen het externe netwerk en het eigen, vertrouwde bedrijfsnetwerk. Binnen dit kleine netwerk, afgekort als DMZ, bevindt zich meestal de bastion host en publieke webdiensten van het bedrijf. De buitenste router biedt hierdoor bescherming tegen externe aanvallen, terwijl de binnenste router toegang tot het bedrijfsnetwerk beheert via de DMZ door routering naar de bastion host. De bastion host bevat de diverse proxies[16].

#### *3.1.1.5. Firewallbeheer*

Naast de inrichting dient de ICT-beheerafdeling ook zorg te besteden aan het beheer van de firewall(s). Een bekende methode om in te breken in een firewall is het binnendringen in de bronnen die benodigd zijn voor beheer op afstand, zoals toegang verkrijgen via de systeemconsole of de grafische managementinterface. Door het toepassen van encryptie

[15] Combinatie van verschillende firewallfuncties zoals packet filtering en application gateway.

[16] Een proxyserver is een server die zich bevindt tussen de computer van een gebruiker en de computer waarop de door de gebruiker gewenste informatie staat (het Engelse woord proxy betekent ‘tussenpersoon’). Wil iemand op een computer waarop een proxyserver is ingesteld een andere computer bereiken, dan gebeurt dit niet rechtstreeks, maar via deze proxyserver (bron: http://nl.wikipedia.org)

zoals SSL[17], sterke authenticatie en het beperken van toegestane IP adresreeksen kan de veiligheid bij firewallbeheer worden verbeterd en dit type aanval worden voorkomen.

Een andere factor bij een succesvol firewallbeheer is platformconsistentie. Het Amerikaanse National Institute of Technology adviseert om firewallplatformen te implementeren op systemen met een besturingssysteem dat is 'gestript en gehard' [WACP02]. Om installatiefouten te voorkomen of onnodig kwetsbaarheden (mee) te installeren dienen firewalls niet te worden geplaatst op systemen met verschillende installatieopties en dienen alle onnodige besturingssysteemfuncties te worden verwijderd voorafgaand aan de firewallimplementatie.

Na de enorme opmars van firewalls ongeveer vijftien jaar geleden kwam het besef dat firewalls alleen niet voldoende bescherming bieden tegen aanvallen. Immers veel bedrijven hebben naast internetconnecties andere toegangsmogelijkheden tot het interne netwerk, bijvoorbeeld via dial-in modems, die de firewall omzeilen. Daarnaast is het zo dat firewalls 'acteren' op een bepaalde laag van de protocolstack. Dat betekent dat ze niet kijken naar hogere lagen. Als er uitsluitend gefilterd wordt op poortnummers op de transportlaag van het OSI-model, worden mogelijke problemen op bijvoorbeeld het niveau van het e-mail protocol niet gesignaleerd [SING03]. Ook bieden firewalls geen oplossing tegen menselijke fouten, zoals het uitvoeren van gevaarlijke instructies vanuit e-mail. Firewalls geven verder geen bescherming tegen bepaalde aanvallen van binnenuit, uitgevoerd door ontevreden medewerkers [SCHE00].

Dit alles heeft geleid tot een nieuwe generatie van beveiligingsdetectietechnieken, waaronder zogeheten vulnerability scanners en intrusion detection systems, waarbij aanvallen of kwetsbaarheden in het eigen netwerk (bijna) realtime kunnen worden gedetecteerd, zie de paragrafen 3.1.2.1. en 3.1.3.

### *3.1.2. Management van ICT-beveiligingskwetsbaarheden*

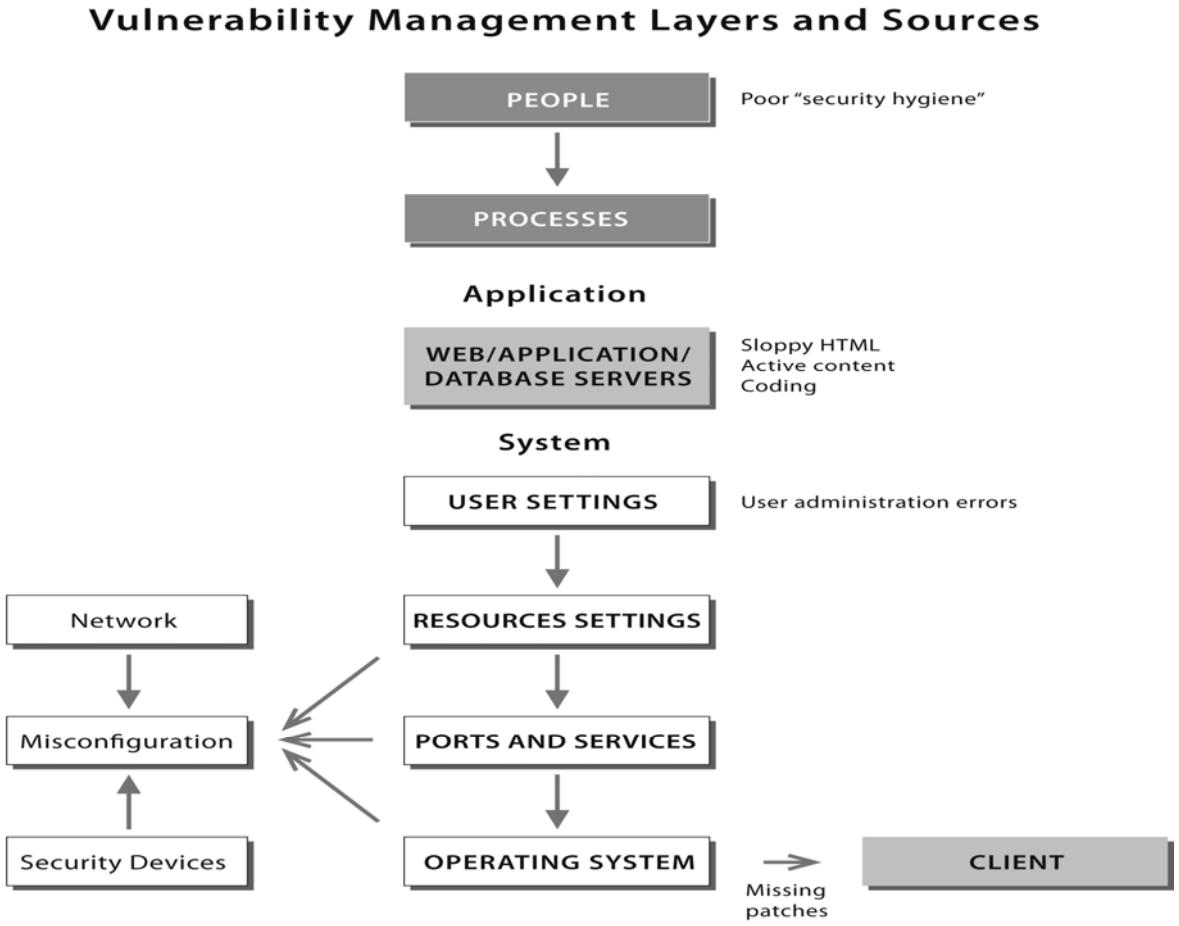
Een kwetsbaarheid (vulnerability) wordt in dit onderzoek gedefinieerd als *een fout of zwakte in een (computer)systeemontwerp of -implementatie of -operatie die kan worden gebruikt om het beveiligingsbeleid van het systeem te schenden*.
Deze kwetsbaarheden kunnen door een aanvaller worden gebruikt om binnen te dringen in een computernetwerk of -systeem om gegevens te wijzigen, te ontsluiten of om de beschikbaarheid van een systeem of dienst aan te tasten. Voorbeelden van dergelijke kwetsbaarheden zijn:

- aanwezige 'achterdeurtjes' in een softwareprogramma[18]
- configuratiefouten bij installatie
- programmeerfouten.

Kwetsbaarheden kunnen soms op afstand worden misbruikt. Leveranciers van vulnerability scanproducten melden vanaf medio 2003 een sterke toename van op afstand te misbruiken kwetsbaarheden [SIST03]. De zwaarte van een kwetsbaarheid is meestal een combinatie van enerzijds de mogelijkheid om op afstand, meestal het Internet,

[17] Secure Socket Layer (SSL) is een veel gebruikt encryptieprotocol voor het versleutelen van Hyper Text Transport Protocol (HTTP) gegevens.
[18] bijvoorbeeld voor testen of foutherstel.

gebruik te maken van de kwetsbaarheid en anderzijds de eenvoud door het gebruikmaken van een exploit[19]. Dit laatste is voornamelijk het geval wanneer de exploit in het openbaar gepubliceerd is en deze eenvoudig van het Internet kan worden gedownload. Zwakheden kunnen in principe in elke laag van het OSI-model voorkomen. ICT-kwetsbaarhedenbeheer richt zich de laatste jaren vooral op het opsporen en elimineren van zwakheden in de applicatieomgeving. Zoals uit figuur 6 blijkt, kan hierbij onderscheid worden gemaakt tussen mens, proces, applicatie en systeem.




Figuur 6: voorbeelden van 'vulnerability managementlagen' [Gartner, NICO03]

Het inventariseren van aanwezige ICT componenten, het structureel identificeren en opsporen van kwetsbaarheden en het verwijderen van deze kwetsbaarheden zijn basale kenmerken van kwetsbaarhedenmanagement [MEBH05]. Het aantal kwetsbaarheden en programma's dat hiervan gebruikmaakt, is in aantal de afgelopen jaren sterk gestegen[20]. Kwetsbaarhedenmanagement kan dan ook worden beschouwd als een belangrijke beveiligingsuitdaging voor de komende jaren voor elke ICT-organisatie. Daarbij gaat het niet alleen om een adequaat proces van detecteren en analyseren maar ook om het tijdig wegnemen van kwetsbaarheden, bijvoorbeeld door het aanbrengen van geteste beveiligingsherstelsoftware (security patching). Bij het beheren van

[19] Een exploit is een programma dat of techniek die een kwetsbaarheid in software gebruikt voor het doorbreken van de beveiliging van een computersysteem of anderszins een systeem aanvalt.
[20] Zie statistieken op http://www.cert.org.

kwetsbaarhedenresponseprocessen in grotere organisaties zijn vaak meerdere ICT-medewerkers betrokken. Bijvoorbeeld de afdeling ICT-beveiliging voor het uitvoeren van scans en het analyseren van externe informatie over kwetsbaarheden. Daarnaast de changemanager die een ICT-wijziging initieert om een geconstateerde kwetsbaarheid weg te nemen, en de systeem- of netwerkbeheerder die zorgt voor het testen en implementeren van de wijziging.

Taken van de beveiligingsmanager in dit kader hebben veelal betrekking op de beoordeling van externe berichtgeving over nieuwe kwetsbaarheden, initiatie en coördinatie van vulnerability scanactiviteiten en doorleiding van informatie over kwetsbaarheden naar ICT-beheerders binnen de organisatie[21].

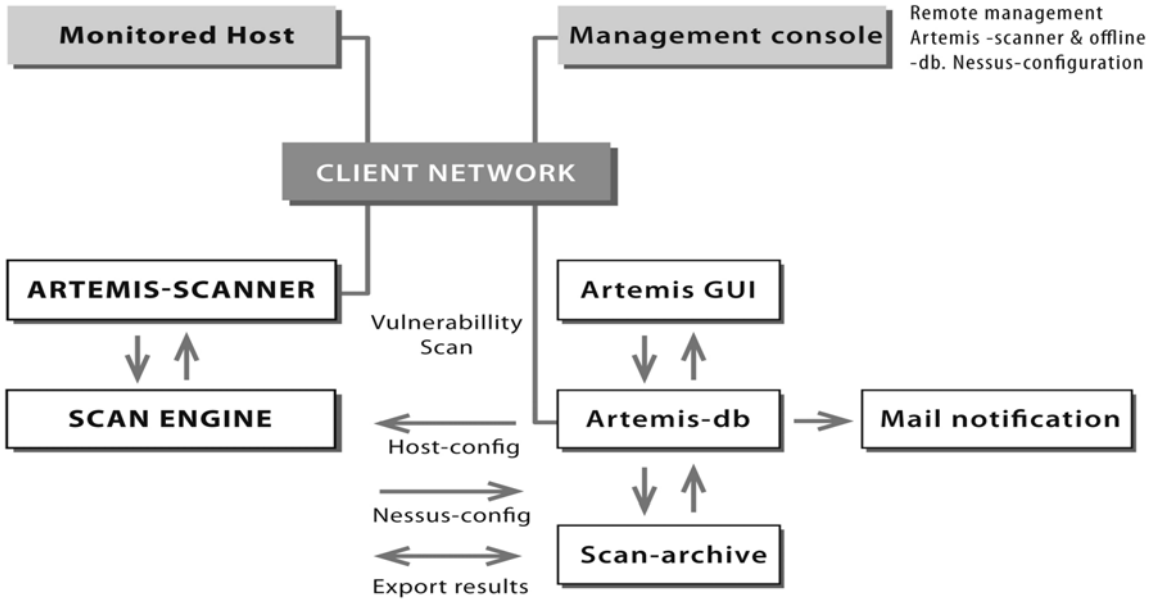
#### *3.1.2.1. Vulnerability scanning*

Bij vulnerability scanning worden ICT-netwerkcomponenten, -systemen en/of -applicaties periodiek doorgelicht (gescand) op de aanwezigheid van kwetsbaarheden. Vulnerability scanning wordt daarom gerekend tot de groep van proactieve beschermingsmaatregelen tegen systeeminbraken [VEEL04]. Een nieuwe ontwikkeling is het scannen op kwetsbaarheden gedurende softwareontwikkelingsfasen. Gartner schat dat, wanneer vijftig procent van de bij ingekochte of zelfontwikkelde aanwezige softwarekwetsbaarheden wordt verwijderd vóór het in productie nemen van de software, de totale kosten voor configuratiebeheer en incidentenresponse kan worden teruggebracht tot vijfenzeventig procent [PESC03]. De huidige softwaretestprogramma's kunnen worden beschouwd als eerstegeneratietechnologie. Ook Microsoft is middels haar in 2000 geïnitieerde Secure Windows Initiative begonnen met het gebruik van vulnerability scanning bij de ontwikkeling van Windows Server besturingssysteemsoftware.

Een belangrijke voorwaarde voor maar tevens een nadeel van periodiek scannen is dat het te scannen systeem online moet zijn. Een systeem dat kwetsbaarheden bevat, bijvoorbeeld een laptop met een verouderd besturingssysteem, die alleen overdag aan het lokale netwerk gekoppeld is, zal niet worden gescand door een scanner die alleen 's nachts actief is. Eventueel op de laptop aanwezige kwetsbaarheden vormen op deze manier een risico voor andere netwerkcomponenten.

Bij vulnerability scanning kan gebruik worden gemaakt van local scanners of remote scanners. Een local scanner is een softwareprogramma dat draait op de computer zelf. De scanner kan handmatig worden geactiveerd door een run-commando van de systeembeheerder of periodiek aan de hand van een scheduler. Local scanners zijn gebonden aan het besturingssysteem van de te scannen computer. Een van de eerste local scanners is het in 1995 door Dan Farmer en Dr. Wietse Venema ontwikkelde programma security analysis tool for auditing networks (S.A.T.A.N.) voor (hoofdzakelijk) Unix-systemen.
Een remote scanner scant een reeks computersystemen op afstand via het lokale netwerk door het testen van de beveiliging van het doelsysteem middels het uitproberen van aanvalsscripts of het zoeken naar de aanwezigheid van bepaalde kenmerken van kwetsbaarheden, de zogeheten signatures[22]. Figuur 7 geeft een schematisch overzicht van een remote vulnerability scanner (Artemis) implementatie die is gebaseerd op de open standaard Nessus.

[21] Deze taak wordt soms samengevat onder de naam vulnerability tracking and tracing.
[22] Dit stelselmatig onderzoeken wordt vaak ook aangeduid met de term probing.




Figuur 7: voorbeeld van een remote vulnerability scannerimplementatie

Het inrichten van een remote scanomgeving vergt de nodige fine tuning, omdat er rekening dient te worden gehouden met aspecten als netwerkbelasting, systeemperformance en de eventuele blokkerende werking van firewalls binnen het te scannen netwerksegment. Remote scanners genereren relatief veel valse alarmen (false negatives). Dit komt voornamelijk doordat bepaalde (combinaties van) kenmerken van een systeemconfiguratie al kunnen leiden tot een melding door de scanner.

#### *3.1.2.2. Penetratietesten*

Penetratietesten (ethical hacking) is het testen van de kwaliteit van de beveiliging van ICT-netwerken, -systemen en/of -applicaties door externe, ingehuurde specialisten. Soms bieden leveranciers van deze diensten een keuzepakket aan waarbij de klant kan kiezen tussen een blackbox- of een whiteboxtest. In de eerste variant krijgt de leverancier van de dienst geen enkele informatie en heeft hij ook geen toegang tot het doelnetwerk of -systeem. In de andere variant krijgt de leverancier een standaardtoegang tot een netwerk of systeem en wordt vanuit die situatie gezocht naar zwakke plekken of wordt getracht hogere (systeem)rechten te verkrijgen. Bij een penetratietest worden meestal meerdere soorten vulnerability scan tools gebruikt.

### *3.1.3. Intrusion detection*

Daar waar firewalls vooral bedoeld zijn om indringing van buitenaf te voorkomen, worden intrusion detection systems (IDS) vooral ingezet om aanvallen binnen het eigen netwerk te signaleren. Volgens IETF RFC282 is een security intrusion *een gebeurtenis of combinatie van gebeurtenissen die uitmondt of uitmonden in een incident waarbij een indringer toegang tot een systeem verkrijgt of tracht te verkrijgen waartoe hij niet is geautoriseerd*. Wang spreekt van een serie gerelateerde activiteiten waarbij sprake is van een kwaadaardige tegenstander [WANR03]. Uit de definities kan worden afgeleid dat het gaat om opzettelijk en ongeautoriseerd handelen waarbij het verkrijgen van toegang tot een systeem of netwerk het hoofddoel is. Intrusion detection systems worden ingezet om

dergelijke gebeurtenissen te detecteren en hierover waarschuwingen af te geven, zodat de organisatie maatregelen kan treffen om verdere schade door indringers te voorkomen.

Intrusion detection systems maken gebruik van loggegevens. De onderzoekers Lee en Stolfo [LEST00] stellen bij elk IDS ontwerp de premisse dat wanneer auditmechanismen zijn geactiveerd, evident bewijs van illegitieme- en indringersactiviteiten zich manifesteren in loggegevens. Vanwege de grote hoeveelheid aan loggegevens zijn efficiënte en intelligente data-analysetechnieken en hulpmiddelen noodzakelijk om gedrag van systeemactiviteiten te herkennen.

Bij intrusion detection systems worden vaak vier kenmerken onderscheiden:

1. anomaly detection
2. misuse detection
3. host-based
4. network-based.

Deze kenmerken worden in volgende paragrafen kort behandeld. Vervolgens zal worden stilgestaan bij de belangrijkste systeemresponseopties en implementatiekwesties.

#### *3.1.3.1. Anomaly detection model*

Ruim twintig jaar geleden verschenen de eerste modellen voor realtime intrusion detection gebaseerd op abnormaal gedrag. Het intrusion detection expert system uit 1987 van Dorothy Denning [DENN87] omvat zes componenten.

| | |
|---|---|
| *Subjects:* | activiteit initiatoren op een doelsysteem (meestal gebruikers). |
| *Objects:* | bronnen,beheerd door commando's, apparaten, etc. |
| *Audit records:* | loggegevens, gegenereerd door een doelsysteem. |
| *Profiles:* | structuren die het gedrag van eerder genoemde subjects karakteriseren. |
| *Anomaly records:* | (log)gegevens, gegenereerd wanneer abnormaal gedrag wordt gedetecteerd. |
| *Activity rules:* | regels die de te nemen acties beschrijven bij enige conditie. |

Het model kan worden beschouwd als een op regels gestuurd patroonvergelijkingssysteem. Elke keer dat een logbestand wordt gegenereerd, wordt er vergeleken met de aanwezige gedragsprofielen die dan de (eventuele) vervolgactie bepalen.
Bij een anomaly detection model wordt dus gekeken naar (statistische) afwijkingen van 'normaal' gebruik van het netwerk of systeem dat wordt bewaakt. Hiertoe wordt een profiel opgesteld en beheerd dat bestaat uit een aantal patronen met specifieke gebeurtenissen of karakteristieken binnen een bepaalde tijdseenheid. Voorbeelden zijn geheugengebruik, processorgebruik of bepaalde typen netwerkpakketten. Aldus wordt een basisniveau van normaal gebruik gedefinieerd. Het anomaly detection system vergelijkt gebeurtenissen of karakteristieken met het normale profiel en slaat alarm bij bepaalde afwijkingen. Het grootste voordeel van dit model is de mogelijkheid tot het identificeren van de nieuwste aanvallen. Intrusion detection systems, gebaseerd op dit model, genereren echter veel valse alarmen, omdat ook een situatie van tijdelijke afwijkingen van normaal gebruik door het systeem als een aanval wordt beschouwd.

#### *3.1.3.2. Misuse detection model*

Het misuse detection model, ook wel signature-based intrusion detection model genaamd, maakt gebruik van een kennisdatabase met aanvalspatronen of –karakteristieken. Host logbestanden of netwerkpakketten worden continu vergeleken met de in de database aanwezige verzameling van aanvalskenmerken (signatures). Bij een 'hit' slaat het systeem alarm.
Voordeel van dit model is de hoge accuraatheid bij het identificeren van aanvallen. Intrusion detection systems die zijn gebaseerd op dit model, genereren over het algemeen lage aantallen valse alarmen. Het model levert in de praktijk soms netwerkperformanceverlies op en vereist daarnaast goed capaciteitsbeheer omdat gegevens over langere perioden moeten worden vastgehouden. Uit de praktijk is gebleken dat de zogeheten langzame aanvallen, dat wil zeggen aanvallen die verspreid over meerdere weken plaats vinden, niet altijd worden herkend [KRVI01]. Een ander probleem is dat zeer recente aanvalstechnieken soms niet kunnen worden gedetecteerd, omdat de kenmerken nog niet zijn opgenomen in de database.

#### *3.1.3.3. Host-based versus Network-based Intrusion Detection*

In de jaren tachtig werd het doorzoeken van logbestanden op ongebruikelijke of verdachte, aan beveiliging gerelateerde systeemactiviteiten gemeengoed. Vaak ging het hierbij om het handmatig doorlopen van logbestanden van toegangscontrole- en autorisatiesystemen [AMOR99]. De huidige generatie host-based intrusion detection systems (HIDS) maakt gebruik van software die permanent specifieke loggings monitort, zoals syslogs (Unix) en speciale auditlogs. Zodra er een wijziging van een bestand wordt geconstateerd in de loggegevens, wordt deze activiteit getoetst aan het ingestelde beveiligingsbeleid en wordt al dan niet een alarm gegenereerd.

Host-based intrusion detection systems vinden hun basis in de analyse van zogeheten 'audit trails'. Auditmechanismen dienen een aantal doelen. Een interpretatiedocument van de Amerikaanse Trusted Computer System Evaluation Criteria ('Orange Book') uit 1987 [NCSC87] beschrijft vijf primaire technische en adminstratieve doelen:

| | |
|---|---|
| *Toegang tot en gebruik van bestanden:* | het openen, sluiten, lezen en uitvoeren van (specifieke) bestanden behoort tot deze categorie. |
| *Ontdekking van omzeilen van de beveiliging:* | een mislukte poging tot het openen van een bestand kan het bewijs zijn dat iemand een beveiliging probeert te omzeilen. |
| *Ongebruikelijke privileges:* | het gebruik van een systeemprivilege op een ongebruikelijk tijdstip of gelijktijdig door meerdere gebruikers waar enkelvoudig gebruik normaal is, kan wijzen op onterechte privileges. |
| *Afschrikkende werking:* | een auditmechanisme als bewakingsmiddel heeft een afschrikwekkende werking, als (potentiële) indringers op de hoogte zijn van het bestaan hiervan. |

| | |
|---|---|
| *Gebruikersvertrouwen:* | gebruikers voelen zich veiliger in hun computeromgeving, als zij weten dat er hulpmiddelen voor auditonderzoek worden gebruikt. |

Typische 'auditable events'[23] zijn:

- gebruik van identificatie- en authenticatiemiddelen zoals wachtwoordbestanden
- creëren of verwijderen van objecten, bijvoorbeeld bestanden
- systeemadministratieve handelingen.

Een sterke eigenschap van een host-based intrusion detection system is dat daadwerkelijk indringersactiviteiten op een gegevensbestand, bijvoorbeeld het verwijderen of wijzigen van een useridentificatie, bijna realtime kunnen worden gedetecteerd. Dit in tegenstelling tot network-based intrusion detection systems die enkel *verdacht* netwerkverkeer kunnen detecteren. Naast het monitoren van bestandsactiviteiten kunnen HIDS ook andere belangrijke systeemcomponenten in de gaten houden zoals het gebruik van schijfruimte. Het detectiesysteem behoeft vaak geen additionele hardware en kan worden geïnstalleerd op bestaande ICT-configuraties als file- of webservers. Dit maakt host-based intrusion detection systems qua investering aantrekkelijker dan network-based intrusion detection systems.
Host-based intrusion detection systems gebruiken audit trails als belangrijkste informatiebron. Om alle data te kunnen monitoren is soms extra (extern) computergeheugen noodzakelijk. Aangezien HIDS gebruik maken van processorcapaciteit en andere computerbronnen kan dit de performance van het systeem beïnvloeden.

Network-based intrusion detection systems (NIDS) detecteren aanvallen door middel van analyse van netwerkpakketstromen. Bij NIDS worden meerdere sensoren op verschillende plekken in het netwerk geplaatst. Deze sensoren voeren analyses uit op het netwerkverkeer en melden (potentiële) aanvallen aan een centrale managementconsole. De aanvalsherkenning bij abnormal behaviour profiling bestaat meestal uit het herkennen van een patroon van ongewenste of ongebruikelijke aan elkaar gerelateerde activiteiten of een verdachte karakterset. Bij normal behaviour profiling wordt echter gebruik gemaakt van patronen met normaal netwerkverkeer.

#### *3.1.3.4. Response-opties*

Na het analyseren van de verzamelde event information kan een IDS een responseactiviteit genereren. De responseactiviteiten kunnen worden verdeeld in twee categorieën: actieve en passieve responses.

*Actieve responses*
Actieve IDS-responses zijn (deels) geautomatiseerde acties van een IDS op basis van bepaalde detecties. Rebecca Gurley Base onderscheidt drie vormen van actieve responses [BASE00]:

[23] Gebeurtenissen en activiteiten op een computersysteem die worden beschouwd als beveiligingskritisch en waardevol voor vastlegging.

- verzamelen van aanvullende informatie
- wijzigen van de omgeving (bijvoorbeeld blokkeren van een netwerk IP-adres)
- actie, in de vorm van een tegenaanval, ondernemen jegens de aanvaller.

De responsevormen kunnen los van elkaar en in combinatie worden uitgevoerd.

De eerste variant, het verzamelen van aanvullende informatie, wordt aanbevolen bij de bescherming van kritische systemen of wanneer het beleid is bij serieuze aanvallen juridische stappen tegen de aanvaller(s) te ondernemen. Voor het verzamelen van de informatie kan gebruik worden gemaakt van speciale servers zoals honeypots of decoys [STOL89].

Het wijzigen van de omgeving is de 'meest ingetogen' variant van de drie actieve IDS-responses. Sommige systemen omvatten karakteristieken van expertsystemen, die settings aanpassen of extra detectieregels toevoegen op basis van bepaalde aanvalsvormen. Bij deze actieve responsevariant wordt dan ook gesproken van self-healing systems.

Het terugtraceren van de aanvalsroute tot de aanvalsbron en vervolgens de aanvalscomputer of het aangetroffen netwerk onklaar maken, wordt beschouwd als de meest agressieve variant van actieve beantwoording van aanvallen. Aan deze variant zijn significante risico's verbonden. Het kan bijvoorbeeld leiden tot het vernielen van eigendommen of diensten van onschuldigen. Bijvoorbeeld in het geval van een thuiscomputer die is geïnfecteerd, wordt misbruikt voor het uitvoeren van een denial-of-service-aanval zonder dat de eigenaar van de computer hier weet van heeft. In de meeste rechtssystemen wordt een 'tegenaanval' als een onrechtmatige daad beschouwd, wat strafrechtelijke en/of privaatrechtelijke tot gevolg kan hebben. Ook kan een tegenaanval escaleren tot nog meer activiteiten door de aanvaller of medeaanvallers.

*Passieve responses*
Deze vorm van response heeft als belangrijkste eigenschap het informerende karakter, zodat een IDS-beheerder een vervolgactie kan nemen. De twee belangrijkste verschijningsvormen zijn:

1. directe alarmering[24]
2. vastlegging en archivering.

#### *3.1.3.5. Implementatiekwesties*

Bij het selecteren van het type IDS spelen vaak meerdere criteria een bepalende rol.

Tabel 2: IDS-selectiecriteria

| Criterium | Omschrijving |
|---|---|
| Accuraatheid | Wanneer een IDS een activiteit incorrect identificeert als een aanval of een aanval incorrect identificeert als legitieme activiteit is er sprake van inaccuraatheid |
| Performance | De performance van een IDS is het niveau waarop audit events worden verzameld, opgeslagen en verwerkt. Er is sprake van |

[24] Meestal een bericht naar een centrale IDS-managementconsole met nadere informatie over het aangevallen IP-adres en het gebruikte aanvalshulpmiddel.

| | |
|---|---|
| | slechte performance, indien de detectie niet real-time danwel near-time geschiedt |
| Fouttolerantie | De IDS moet bestand zijn tegen aanvallen zelf. Dit is vooral van belang omdat een IDS-omgeving mogelijk draait bovenop een besturingssysteem dat kwetsbaarheden bevat |
| Tijdigheid | De IDS dient de resultaten van de interne data-analyse zo snel mogelijk over te brengen naar de gebruiker om (verdere) schade te voorkomen |
| Data | Het aantal en type te analyseren data[25] beïnvloedt mogelijk de performance en/of accuraatheid |

Naast efficiencyoverwegingen zijn er ook ander factoren die bepalend kunnen zijn voor welke IDS-omgeving het meest geschikt is voor een organisatie. Als er bijvoorbeeld sprake is van een netwerk waarover veel vercijferde informatie wordt verstuurd, dan zal een host-based IDS-architectuur geschikter zijn dan een architectuur waarin wordt gewerkt met network-based IDS-implementaties omdat een IDS geen vercijferde data kan analyseren.

*Conclusie*
Uit een in 2001 gehouden vergelijkend onderzoek tussen anomaly en misuse detection models [BICV01] wordt geconcludeerd dat geen van de twee benaderingen alle typen indringersactiviteiten kan detecteren. Een combinatie van beide modellen wordt daarom geadviseerd voor ICT-omgevingen waar beveiliging zeer belangrijk is.

Een onderzoek van de Amerikaanse Carnegie Mellon University naar de stand van zaken met betrekking tot IDS-technologieën [CMUS00] schetst de uitdagingen en problematiek van de huidige generatie intrusion detection systems. Naast de eerder bij de selectiecriteria genoemde aspecten zien de onderzoekers ook risico's door verkeerde, geautomatiseerde IDS-responseactiviteiten, gebrek aan algemeen geaccepteerde intrusion detection terminologie en -concepten en onacceptabel hoge 'valse signalen'[26].
Aansluitend op dit onderzoek schrijft John McHugh in zijn paper Intrusion and intrusion detection [HUGH01] dat op twee terreinen meer onderzoekswerk noodzakelijk is:

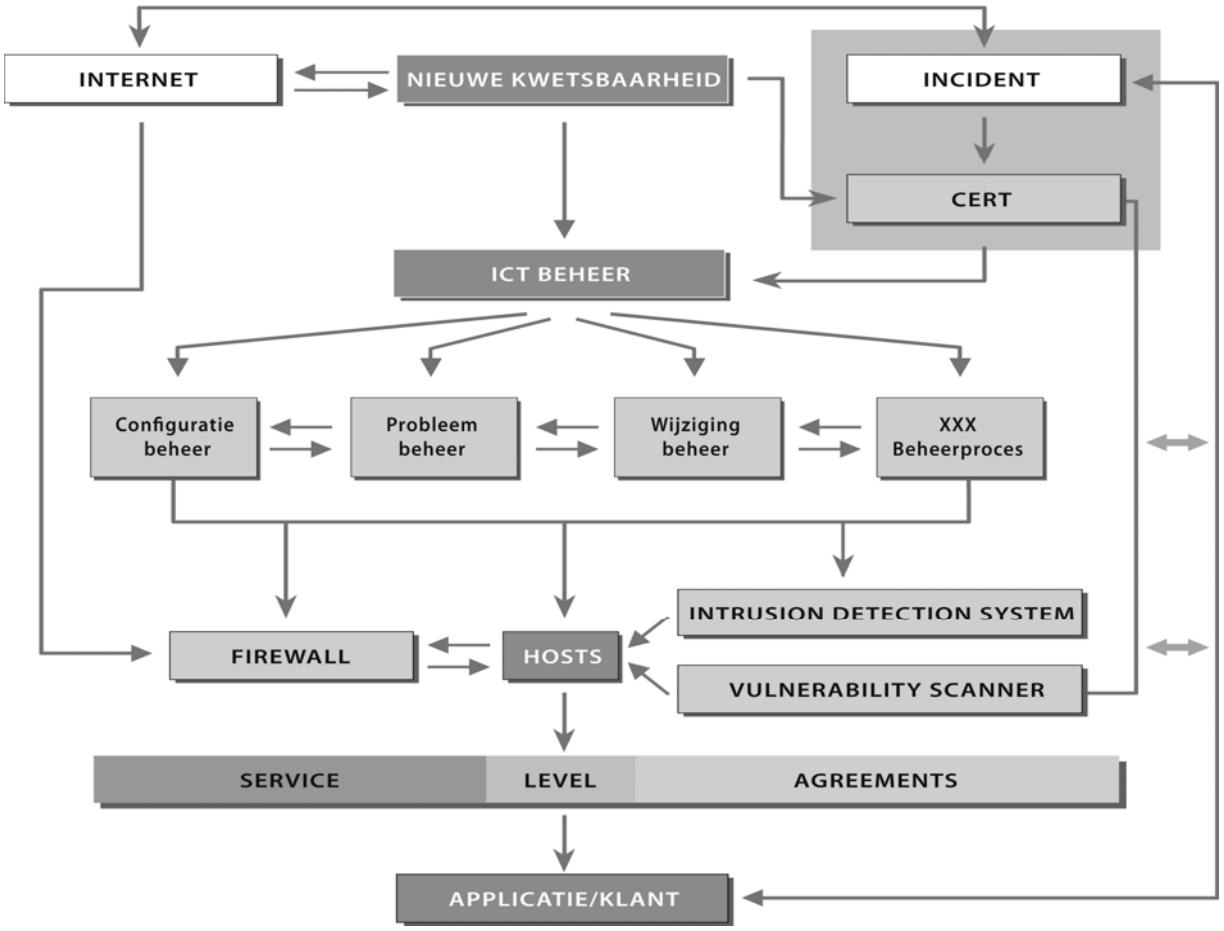
- het karakteriseren van normaalgedrag
- het ontwikkelen van een theorie met betrekking tot indringergedrag welke kan worden gebruikt om detectoren te ontwikkelen die gedragingen kunnen abstraheren en koppelen aan 'aanvalscategorieën'.

Duidelijk is dat wij nog ver verwijderd zijn van een wereld waarin intrusion detection systems optimaal functioneren en een volwaardige bijdrage leveren aan de incident responsecapaciteit van een ICT-organisatie.

[25] Bijvoorbeeld loggegevens, gebruikersprofielen, etc.
[26] Zowel false positives (valse meldingen) als false negatives (niet-gedetecteerde indringersactiviteiten).

## 3.2. Ontwikkelingen rondom incidentenresponse

### 3.2.1. De opkomst van computer security incident response teams




Figuur 8: computer security incident response team in een ICT-beheeromgeving

De afgelopen vijftien jaren is het aantal teams dat zich specialiseert in het coördineren van incidentenresponseactiviteiten sterk toegenomen. Naast het afhandelen van incidenten hebben deze teams een belangrijke rol bij het voorlichten van de ICT-organisatie over nieuw ontdekte kwetsbaarheden, zie ook figuur 8. Het wereldwijde Forum van Incident Response and Security Teams (FIRST)[27] kent ruim honderdveertig deelnemende incidentenresponseteams afkomstig uit overheids-, academische en commerciële organisaties, en het aantal groeit nog jaarlijks. Het samenwerkingsverband is met hulp van het Amerikaanse CERT/CC in 1990 opgericht met als belangrijkste doel het creëren van een overlegplatform tussen beveiligingsexperts van de verschillende via het Internet verbonden netwerken.

Na een aantal grote virusuitbraken en beschikbaarheidsaanvallen op gerenommeerde Amerikaanse websites van eind jaren negentig hebben een aantal overheden een nationaal meldpunt- en coördinatiepunt voor computerbeveiligingsincidenten ingericht. Voorbeelden hiervan zijn de Duitse CERT-Bund, onderdeel van het Bundesamt fuer

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

Sicherheit in der Informationstechnik, en het Belgische waarschuwingscentrum voor virussen. Laatstgenoemde werd destijds ondergebracht bij het Belgische instituut voor postdiensten en telecommunicatie. Het instituut in België was zeer pragmatisch van opzet. Binnengekomen meldingen werden door een kleine dertig virusexperts uit België geanalyseerd en bij voldoende consensus werden waarschuwingen gepubliceerd op de website. In bijzondere gevallen vond een nationale waarschuwing plaats via radio en televisie.

### *3.2.2. Samenwerkingsverbanden*

In 1997 is een initiatief genomen tot oprichting van een gezamenlijk Europees Incident Response Team, EuroCERT geheten [KOEK02]. Het initiatief heeft het niet gehaald. De bedoeling was een informatiecentrum, vergelijkbaar met het Amerikaanse CERT Coordination Center, in te richten. De deelnemende CERT's[28] konden het echter niet eens worden over de soorten diensten die EuroCERT zou moeten leveren. De pilot is in 1999 beëindigd. De huidige Tasc Force CSIRT (TF-CSIRT) vult een aantal uitgangspunten en behoeften van het EuroCERT-initiatief nader in en wordt door een aantal betrokken experts daarom beschouwd als alternatief voor EuroCERT. TF-CSIRT wordt gefaciliteerd door het academische netwerk TERENA[29]. De samenwerking binnen TF-CSIRT kent zijn basis in een 'web of trust' waarbij CSIRT's worden geaccrediteerd volgens een Trusted Introducer-schema. Het schema onderscheidt drie niveaus: 0, 1 en 2. Het belangrijkste onderscheidende criterium is de vastgestelde en gewaarborgde identiteit van de CSIRT.

Door het faciliteren van onderzoek en het uitwisselen van informatie over incidenten tussen in FIRST-verband vertrouwde incidentenresponseteams komt een mondiale aanpak van incidenten een stap dichterbij. Naast de besloten Technical Colloquia organiseert FIRST elk jaar een open Computer Security Incident Handling Conference waar specialisten hun meest recente kennis en kunde inzake incidenten met elkaar kunnen delen. Binnen FIRST wordt onderscheid gemaakt tussen full members en liason members, waarbij een full member een actief en werkzaam incidentenresponseteam dient te zijn, geen individu. FIRST hanteert een strikt eigen protocol met daarin een geheimhoudingsbeleid, de zogeheten non disclosure policy, en een operationeel handboek (operational framework). Lidmaatschap geschiedt op voordracht van een bestaand lid. Computergiganten als Cisco, HP, IBM, SUN en Microsoft zijn lid van FIRST.

Ook de Nederlandse rijksoverheid heeft een aantal initiatieven genomen op het terrein van incidentenresponse. Op 5 juni 2002 is officieel door de toenmalige minister van Boxtel CERT-RO geïnstalleerd. CERT-RO heeft in 2003 haar naam veranderd in GovCERT[30]. Het team van specialisten verleent de aangesloten (overheids)instellingen assistentie bij beveiligingsincidenten en geeft uit oogpunt van preventie zogeheten security advisories uit. GovCERT maakt sinds 1 januari 2006 deel uit van de Gemeenschappelijke Beheer Organisatie van de rijksoverheid.

---

[28] In de praktijk worden computer emergency response teams (CERT's) ook vaak computer security incident response teams (CSIRT's) genoemd.
[29] TERENA = Trans European Research and Education Network Association (zie http://www.terena.nl)
[30] Zie http://www.govcert.nl.

De gezamenlijke ministeries hebben daarnaast van 2001 tot en met 2005 actief geparticipeerd in het programma KWINT van het Electronic Commerce Platform Nederland[31]. Het met overheidsgeld gesubsidieerde programma is voortgekomen uit een onderzoeksrapport over de kwetsbaarheid van Internet [STTN01] en de daaropvolgende behandeling van de kabinetsnota rondom het thema kwetsbaarheid Internet in de zomer van 2001. Het programma KWINT heeft eind 2001 een aantal actielijnen uitgezet waaronder de (tijdelijke) formering van een werkgroep 'Alarmering & Incident Response' [KORS02].

### *3.2.3. Operationeel raamwerk*

Computer security incident response teams kunnen zeer divers zijn in omvang en samenstelling. Een rapport [KILL03] van het Amerikaans Carnegy Mellon Software Engineering Institute onderscheidt vijf varianten:

- Security team
- Internal distributed CSIRT
- Internal centralized CSIRT
- Internal combined Distributed and Centralized CSIRT
- Coordinating CSIRT.

Bij de eerste variant is de formele verantwoordelijkheid voor het behandelen van incidenten ondergebracht bij een (onderdeel van een) organisatie. Beschikbaar personeel zoals netwerk- of beveiligingsspecialisten worden op ad-hocbasis bijeengeroepen, wanneer zich incidenten voordoen. Bij een Internal Distributed CSIRT wordt de bestaande capaciteit benut voor het creëren van een virtueel CSIRT. Er is een manager die de taken coördineert. Specialisten krijgen er een CSIRT-taak bij naast de hoofdtaak van systeembeheer, netwerkbeheer, etc. Een belangrijk doel is het realiseren van een centraal meld- en coördinatiepunt voor incidenten binnen de organisatie en een aanspreekpunt voor de buitenwereld. Het centrale CSIRT-meldpunt, meestal bereikbaar per telefoon en e-mail adres, wordt op roulatiebasis bemand. Bij de derde variant is er sprake van een volledig bemenst incidentenresponseteam. Medewerkers van een dergelijk team zijn volledig belast met het behandelen van incidenten- en kwetsbaarhedenmeldingen en het opstellen van rapportages. Grotere internationaal opererende organisaties beschikken vaak over een dergelijk team. Het team rapporteert soms rechtstreeks aan de hoogste ICT-manager in de organisatie, de Chief Information Officer, en heeft hierdoor een relatief onafhankelijke positie binnen de organisatie. De vierde variant is een combinatie van de Internal Distributed en de Internal Centralized CSIRT. Bij majeure incidenten werken vaak meerdere teams van (vooraf toegewezen) specialisten aan de afhandeling en deze worden hierbij begeleid door een klein, centraal coördinatieteam. Bij de vijfde variant, Coordinating CSIRT, is er sprake van een team dat voor meerdere organisaties, gebruikersgroepen en/of CSIRT's werkt. Een Nederlands voorbeeld is het CSIRT-team van provider Surfnet. Behalve een coördinatietaak biedt dit team ook andere diensten aan, zoals het verzorgen van beveiligingscursussen en het uitvoeren van audits.

Om de dienstverlening, de verantwoordelijkheden en de bevoegdheden helder vast te leggen, hanteren veel CSIRT's een operationeel raamwerk. Het raamwerk omvat meestal

[31] Zie http://www.ecp.nl.

een missieverklaring, een beschrijving van de gemeenschap waarvoor wordt gewerkt[32], de structuur van de CSIRT, de plaats in de organisatie en/of de relatie met andere CSIRT's en operationele procedures.

#### *3.2.3.1. Missieverklaring*

In de missieverklaring wordt de beoogde doelstelling van een CSIRT verwoord. Een missieverklaring legt de basis voor het handelen van een CSIRT. Verder verwijst de verklaring vaak naar de diverse diensten van de CSIRT, geeft aan hoe de kwaliteit van de dienstverlening wordt geborgd en welk beleid en welke procedures van toepassing zijn.

Internal Centralized CSIRT's en Coordinating CSIRT's bieden tegenwoordig een groot scala aan diensten op het terrein van ICT-beveiliging aan. Deze diensten kunnen reactief en proactief van karakter zijn [SCHI05]. Onderstaande tabel geeft een overzicht van veel voorkomende CSIRT-diensten. Het Handbook for Computer Security Incident Response [WESK98] spreekt van optionele diensten met uitzondering van de verplichte dienst incidentenresponse.

Tabel 3: CSIRT-diensten

| **Naam dienst** | **Omschrijving** |
|---|---|
| Incident Response | Het bieden van een centraal loket voor het melden van computerbeveiligingsincidenten en het zorgdragen voor een gecoördineerde beantwoording van de meldingen |
| Announcements | Verspreiden van informatie over te nemen maatregelen tegen bestaande of toekomstige beveiligingsdreigingen |
| Vulnerability Analyses and Response | Het bieden van een centraal loket voor het rapporteren van computerbeveiligingskwetsbaarheden en het zorgdragen voor een gecoördineerde beantwoording van de meldingen |
| Artifact[33] Analysis and Response | Genereren van technische analyserapporten betrekking hebbend op kwaadaardige code |
| Education | Leveren van trainingen om beveiligingsbewustzijn te promoten en kennis te bevorderen |
| Incident Tracing | Ondersteunen van het traceren en volgen van indringersactiviteiten |
| Intrusion Detection | Ondersteunen van actieve detectie van indringersactiviteiten |
| Auditing and Penetration Testing | Ondersteunen van securityonderzoeken en penetratietesten van computersystemen en netwerken |
| Security Consulting | Leveren van deskundigenadvies voor computerbeveiligings- en netwerkzaken |
| Risk Analysis | Uitvoeren van risicoanalysebeoordelingen |
| Technology Watch | Informatie leveren over opkomende technologie die mogelijke beveiligingsdreigingen omvat |
| Security Product Development | Ontwerpen en ontwikkelen van beveiligingshulpmiddelen voor incidentendetectie en -preventie |
| Collaboration | Het vestigen van samenwerkingsverbanden met andere entiteiten zoals justitie, dienstenleveranciers, etc |
| Coordination | Het interacteren met zowel interne als externe partijen teneinde vertrouwensrelaties te ontwikkelen en te onderhouden |

[32] Ook wel aangeduid als de constituency.
[33] Artifacts zijn gevallen van kwaadaardige code.

#### *3.2.3.2. Constituency*

Een operationele CSIRT interacteert vaak met diverse partijen. De belangrijkste interactie gebeurt met de constituency, de specifieke gebruikersgemeenschap waaraan de CSIRT diensten levert. Uniek in dit kader is CERT/CC, die haar diensten onbegrensd aanbiedt aan eenieder die dat wenst. De meeste CSIRT's hebben echter een afgebakende gebruikersgemeenschap. Deze afbakening kan geografisch, politiek, technisch, organisatorisch of contractueel bepaald zijn. Vaak vormt de afbakening een afspiegeling van de inkomstenbron van de CSIRT. In Nederland opereert bijvoorbeeld Surfnet-CERT[34] voor de instellingen aangesloten bij SURFnet. Daarnaast heeft een aantal universiteiten een eigen CSIRT.
Het benoemen van de gebruikersgemeenschap is in meerdere opzichten belangrijk. Het maakt het mogelijk om specifieke dienstverlening af te stemmen op de diverse bloedgroepen binnen de gemeenschap. Daarnaast kan de CSIRT een eigen op maat gemaakt beleid hanteren, bijvoorbeeld ten aanzien van het ontsluiten van informatie. Ook wordt het voor andere instanties, bijvoorbeeld collegiale CSIRT's, duidelijk welke gebruikers reeds worden bediend. Uit oogpunt van nationale preventie is het van belang een overzicht te hebben van de diverse gebruikersgroepen met een eigen CSIRT[35].

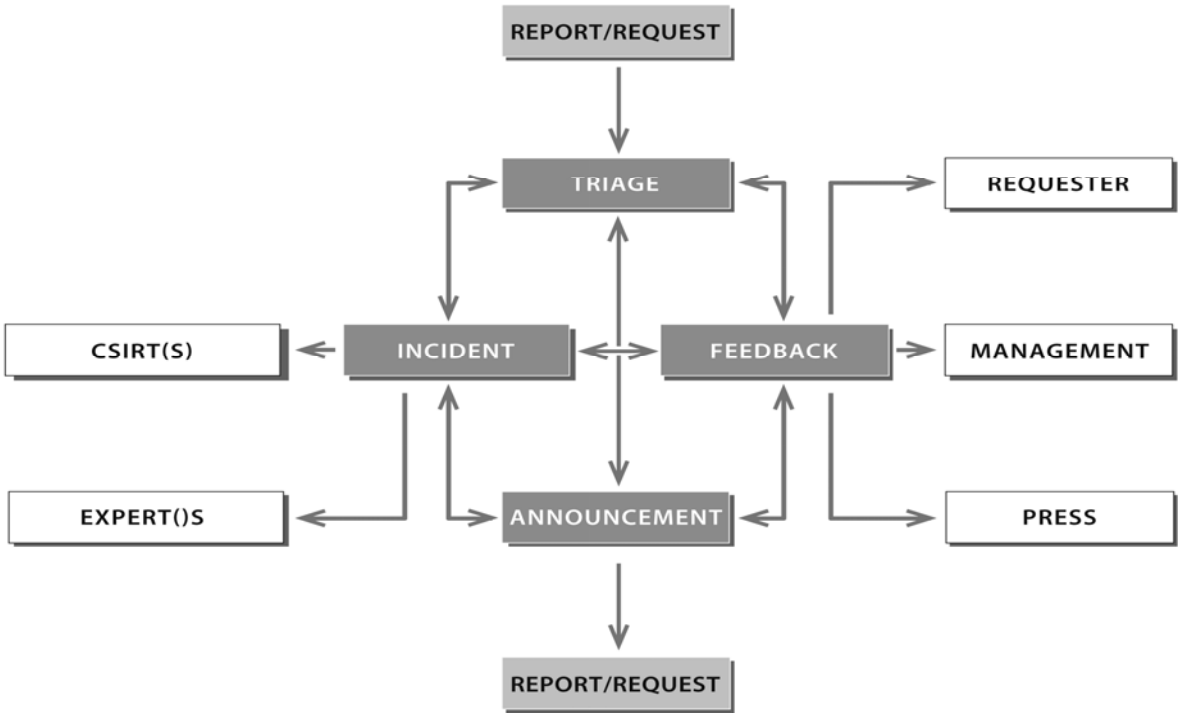
Met de gebruikersgemeenschap worden verschillende afspraken gemaakt over het handelen van de CSIRT. Een belangrijk aspect is de bevoegdheid van de CSIRT. Afhankelijk van de relatie met de gebruikergemeenschap is er sprake van volledige, gedeeltelijke of geen bevoegdheid [WESK03]. Bij volledige bevoegdheid kan de CSIRT bijvoorbeeld eisen dat een gebruiker zich verwijdert van het netwerk, wanneer deze bepaalde acties, zoals het installeren van een security patch, verzuimt. In de praktijk is er echter vaak sprake van een situatie van gedeeltelijke bevoegdheid, waarbij de verantwoordelijke lijnmanager wordt geassisteerd en geadviseerd. In de derde variant is slechts sprake van een bevoegdheid tot informeren.
Om goed te kunnen functioneren dient een CSIRT naast de formele bevoegdheid een vertrouwensbasis te hebben binnen de gebruikersgemeenschap. Goede bereikbaarheid, het spreken van dezelfde taal en het hanteren van heldere gedragscodes zijn daarbij belangrijke randvoorwaarden.

#### *3.2.3.3. Incidentenresponseproces*

Het handboek voor computer security incident response teams uit 2003 [WESK03] onderkent de volgende functies bij het beantwoorden van incidenten:

- triage
- incidentbehandeling (incident handling)
- bekendmaking (announcement)
- terugkoppeling (feedback).

[34] Sedert 1 januari 2004 is de naam CERT-NL formeel gewijzigd in SURFnet-CERT (zie:http://cert.surfnet.nl).
[35] Presentatie 'United States Experiences in Cyberspace Security – a CERT/CC Perspective' door J. Carpenter (CERT/CC) tijdens internationaal symposium CERT-RO, 27 augustus 2002 te Amsterdam.




Figuur 9: relaties tussen incident response service functies [WESK03]

De *triage functie* levert, zoals figuur 9 laat zien, een meld- en aanspreekpunt voor acceptatie, verzameling, sortering en eventuele doorgeleiding van incidentenmeldingen. De meeste CSIRT's hanteren standaardformulieren voor het melden van incidenten. Het kanaliseren van de vaak uit diverse bronnen binnengekomen informatie is een belangrijk doel van deze functie. Grotere organisaties stellen vaak CSIRT-contactpersonen aan. Ook Surfnet- CERT werkt op deze wijze. Elke aangesloten instelling beschikt over één 'site security contact'. Deze verzorgt de eerste opvang van incidentenmeldingen per post, telefoon, fax of e-mail en zorgt voor verdere doorgeleiding naar Surfnet-CERT.

Na ontvangst van een melding dient soms de boodschap te worden ontcijferd en/of wordt de (digitale) handtekening gecontroleerd. Vervolgens wordt gekeken of de informatie kan worden gekoppeld aan een eerder voorgekomen en vastgelegde gebeurtenis. Betreft het een nieuw incident dan wordt deze geregistreerd en wordt een uniek 'tracking'-nummer aan de informatie toegevoegd.

Voor de verdere behandeling van incidenten hanteren CSIRT's vaak een prioriteitsschema. Vanwege het toenemend aantal incidentenmeldingen beschouwt CERT/CC een beperkt aantal incidenten als 'emergencies'. Deze worden door het incidentteam met hoge prioriteit[36] behandeld:

Tabel 4: prioriteitenschema CERT/CC

| **Mogelijke levensbedreigende activiteiten** | **Nieuwe aanvalstypen of kwetsbaarheden** |
|---|---|
| Aanvallen op de Internetinfrastructuur, zoals:<br>* Root name servers<br>* Domain name servers<br>* Major archive sites | Wijdverspreide geautomatiseerde aanvallen tegen Internetsites |

[36] Zie http://www.cert.org.

| | |
|---|---|
| * Network access points (NAPs) | |

*Analyseren* en *kennisgeving* worden beschouwd als belangrijke taken bij de functie *incidentenbehandeling*. Een CSIRT dient daarom te beschikken over actuele lijsten met adresgegevens van contactpersonen uit de gebruikergemeenschap, collegiale CSIRT's, leveranciers en overheidsdiensten.

Een belangrijk doel bij het *analyseren van incidenten* waarbij sprake is van *indringers* is het achterhalen van informatie over:

- welk type aanval werd gebruikt om toegang te verkrijgen
- tot welk systeem en informatie toegang werd verkregen
- wat de indringer deed na het verkrijgen van de toegang
- wat de indringer momenteel doet (indien binnendringing nog mogelijk is).

Het verzamelen van al deze informatie dient te worden afgewogen tegen het feit dat de binnendringer gewaarschuwd wordt door de onderzoeksactiviteiten en besluit om sporen te verwijderen of mogelijk extra schade toe te brengen aan het gecompromitteerde systeem. Het binnen de CSIRT-gemeenschap veelgebruikte boek Responding to Intrusions [KOAC99] adviseert het volgende stappenplan:

1. *Verzamel systeeminformatie en leg tijdelijke gegevens vast.*
   Daarbij gaat het om bestaande netwerkverbindingen, actieve processen en gebruikers, alle geopende bestanden en alle gegevens in werkgeheugen of 'in cache'.

2. *Maak kopieën van de gecompromitteerde systemen.*
   Aangezien het hierbij soms om gerechtelijk bewijsmateriaal gaat, dienen er minimaal twee kopieën (back-ups) te worden gemaakt. Uit forensisch oogpunt is het verstandig om gebruik te maken van speciale forensische programma's die verzegelde kopieën maken van de te onderzoeken data en daarna kunnen worden gebruikt voor het ordenen en nader analyseren van de back-up data [WOLF03]. De handleiding adviseert verder om gebruik te maken van write-once- of hardware-write-protectable media. De tweede back-up dient bovendien in een afgezonderde, beveiligde ruimte te worden opgeslagen.

   Enige aandachtspunten bij het maken van een kopie:

   - de ongebruikelijk hoge schijfactiviteiten bij het maken van een kopie kunnen de binnendringer waarschuwen
   - een indringer kan een trojaans paard hebben geïnstalleerd in het back-up programma dat logbestanden verwijdert tijdens het maken van een kopie.

3. *Isoleer de gecompromitteerde systemen.*
   De meest directe methode is om alle verbindingen naar het systeem te verbreken om vervolgens verdere analyse op het systeem te plegen. Een alternatief is het terugzetten van de uitgevoerde back-ups op een geïsoleerde testomgeving ten behoeve van analyse. Isolatie is hierbij noodzakelijk om verdere ongewilde en vaak ongecontroleerde verspreiding van beveiligingskwetsbaarheden te voorkomen.

4. *Zoek op andere systemen naar tekenen van indringing.*

Indringers creëren vaak meerdere ingangen in een netwerk of systeem nadat zij eenmaal toegang hebben verkregen. Om deze ingangen te vinden dienen vergelijkbare systemen en netwerken te worden onderzocht. Dit kunnen systemen zijn binnen dezelfde reek IP-adressen of hetzelfde netwerksegment, maar ook systemen die dezelfde netwerkdiensten bieden. Hierbij is te denken aan diensten als Domain Name System (DNS), File Transfer Protocol (FTP) en Simple Mail Transfer Protocol (SMTP).

5. *Onderzoek loggegevens gegenereerd door firewalls, netwerkmonitors en routers.*
   Aanvallen laten vaak sporeninformatie, de zogeheten artifacts[37], na die de analist kan leiden tot het systeem of de systemen die zijn gebruikt door de binnendringer. De logs van genoemde componenten leggen tot stand gebrachte verbindingen vast (berichtenbron en -bestemming) en geven allerlei karakteristieke informatie over het berichtenverkeer zelf.

6. *Identificeer de aanvallen die worden gebruikt om toegang te verkrijgen tot de systemen.*
   De systeemlogs van het gecompromitteerde systeem dienen te worden onderzocht om te bepalen wat voor een soort aanval is gedaan en van welke kwetsbaarheid gebruik is gemaakt om toegang te verkrijgen. Hierbij kan worden gelet op veelvuldige foutmeldingen door het raden van wachtwoorden, het blokkeren van bepaalde diensten en de aanwezigheid van zogeheten remnant files[38]. Ook het (trachten te) verwijderen van delen van de systeemlog kan een aanwijzing zijn van een aanval. Soms is het mogelijk om de identiteit van de aanvaller te achterhalen door het gebruik van bepaalde netwerkcommando's of door de inzet van traceprogramma's [DESL02]. Met behulp van speciale online whois-databases[39] kan nadere informatie, zoals de naam van de internetserviceprovider van het te onderzoeken IP-adres van een indringer worden verkregen.

7. *Identificeer wat de indringer heeft gedaan tijdens het indringen.*
   Een laatste analysestap is het achterhalen van de activiteiten van de indringer wanneer deze is binnengedrongen. Bij veel systemen worden (pogingen tot) bestandswijzigingen en schrijfacties vastgelegd in de logs. Uit capaciteitsoogpunt worden leesacties vaak niet vastgelegd. Het is daarom moeilijk of zelfs onmogelijk, om te achterhalen welke informatie van een gecompromitteerd systeem door de indringer is gelezen. Het gebruik van (cryptografische) checksums is een manier om vertrouwde bestanden te vergelijken met bestanden van het gecompromitteerde systeem. Uiteraard dient het systeem te worden nagezocht op de installatie van trojaanse paarden, achterdeuren of nieuwe versies van systeemcommando's. Hierbij dient de onderzoeker alert te zijn op door een indringer aangebrachte wijzigingen in logbestanden en systeemprogramma's waarmee de systeembeheerder processen zichtbaar kan maken.

Bij de analyse kan voorts onderscheid worden gemaakt tussen intra-incidentanalyse en inter-incidentanalyse. Een intra-incidentanalyse, zoals hiervoor beschreven, houdt zich

[37] Scripts, broncode en programma's met potentieel kwaadaardige code worden in het jargon 'artifacts' genoemd.
[38] Ethernet snifferlogbestanden, wachtwoordbestanden, exploitscripts zijn voorbeelden van remnant files
[39] bijvoorbeeld http://www.ripe.net.

bezig met één specifiek incident. Inter-incidentanalyse tracht relaties over en tussen incidenten vast te leggen. Deze analyse heeft tot doel het vinden van overeenkomsten tussen separate incidenten die een indicatie kunnen zijn van gerelateerde bronnen van indringersactivititeiten [ARKI02].

De a*nnouncement function* genereert op maat gesneden informatie voor de gebruikergemeenschap van de CSIRT. Deze informatie varieert van details over voortgaande dreigingen tot trendinformatie over recent gerapporteerde incidenten. De functie behoort formeel niet tot de kernactiviteiten van incidentenresponse, maar wordt beschouwd als een standaardtaak van een CSIRT [WESK03]. Geadviseerd wordt om zorgvuldig om te gaan met het vrijgeven van specifieke aanvalsinformatie. Het detailniveau van de informatie over de aanval dient voldoende te zijn om de dreiging te kunnen begrijpen en de eigen infrastructuur te kunnen controleren op eventuele aanwezigheid van kwetsbaarheden. De verspreide informatie mag hierbij niet zo ver gaan, dat ze kan worden gebruikt om de aanval te imiteren. Ook dient elke mogelijke verwijzing naar een getroffene te worden verwijderd uit de berichtgeving.

De gebruikte typen berichtgevingen zijn sterk CSIRT gebonden. Gebruikelijk is het onderscheid tussen alerts en advisories. Alerts hebben over het algemeen een hogere alarmeringswaarde dan advisories. Nieuw ontdekte kwetsbaarheden en succesvolle aanvallen worden op deze wijze gecommuniceerd naar de gebruikersgemeenschap. Advisories geven (middel)langetermijninformatie over beveiligingsproblemen en oplossingen. Sommige CSIRT's verspreiden daarnaast 'for-your-information'-bulletins via e-mail of de website met korte en minder technische advisories met het oogmerk om een breder publiek te bereiken binnen de gebruikersgemeenschap.

De vierde kernfunctie betreft *feedback & interactions*. Net als bij de anouncement function gaat het hierbij ook voornamelijk over communicatie. CSIRT's koppelen niet altijd terug naar een melder van een incident, maar nemen de informatie geanonimiseerd op in een publieke via het Internet toegankelijke frequently asked questionsdatabase. Bij vragen rondom veelvoorkomende incidenten of kwetsbaarheden wordt dan verwezen naar de database. Bij rechtstreekse terugkoppeling richting de melder van een incident of bij communicatie tussen vertrouwde CSIRT's dienen de vertrouwelijkheid en integriteit van de berichtenuitwisseling te worden gewaarborgd. Om social engineering[40] [MITN02] van kwaadwillenden of nieuwsgierigen of om ongewenst uitlekken naar de media te voorkomen zal tevens de authenticiteit van de communicerende tegenpartij moeten worden vastgesteld. Veel CSIRT's maken gebruik van de mogelijkheden van (open source) PGP om hun op e-mail gebaseerde berichtenuitwisseling te beveiligen. PGP maakt het mogelijk om zowel de authenticiteit als de vertrouwelijkheid en integriteit van berichten over openbare netwerken te beschermen. PGP maakt hierbij gebruik van a-symmetrische en symmetrische encryptiesleutels. Bij een uitgaand e-mailbericht 'tekent' de CSIRT het bericht met zijn geheime PGP-sleutel. De handtekening en daarmee de authenticiteit van de zender kan bijvoorbeeld door de ontvangende partij worden gecontroleerd middels het downloaden van de publieke sleutel van de CSIRT van een openbare PGP-public keydatabase. Bij een geslaagde PGP-'handshake' wordt de symmetrische encryptiesleutel uitgewisseld die is gebruikt om het bericht te vercijferen, waardoor de vertrouwelijkheid van de gegevens in het bericht zelf is gewaarborgd.

[40] Bij social engineering worden sociale vaardigheden gebruikt om vertrouwelijke informatie te verkrijgen.

Het PGP-principe werkt uiteraard alleen bij uitwisseling van gegevens via e-mail en bij niet-anonieme meldingen. Bij communicatie via de fysieke post, telefax of via de telefoon wordt het beveiligen en authenticeren een stuk lastiger. Het handboek voor Computer Security Incident Response Teams meldt dat enkele CSIRT's in de Verenigde Staten van Amerika en Canada gebruik maken van secure telecommunication unit III devices voor het beveiligen van telefoon- en telefaxverkeer tussen vertrouwde partijen. Het Internet (e-mail) is echter verreweg het meest gebruikte kanaal voor uitwisseling van incidenteninformatie tussen CSIRT's onderling en tussen de CSIRT en haar constituency.

Bij het *samenstellen van een CSIRT* spelen zowel kwantitatieve als kwalitatieve aspecten een rol. Het aantal leden van een CSIRT zal mede afhangen van de grootte van de constituency, het verwachte aantal vragen vanuit de constituency en van andere CSIRT's waarmee wordt samengewerkt, en de gewenste dienstverlening/openstelling. Een zeven-maal-vierentwintig-uur-dienstverlening heeft uiteraard een grotere consequentie ten aanzien van het aantal leden van een CSIRT dan een openstelling tijdens kantoortijd op werkdagen.

Het gemiddelde functieprofiel van de CSIRT medewerker gaat uit van materiedeskundigheid evenals van een aantal communicatieve en sociale vaardigheden[41]. Samenwerking, mondelinge en schriftelijke uitdrukkingsvaardigheid, doortastendheid, besluitvaardigheid en stressbestendigheid zijn factoren die een rol kunnen spelen bij interacties en relaties binnen en buiten de CSIRT. Ten aanzien van de techniek wordt verondersteld dat binnen de CSIRT diepgaande kennis en ervaring aanwezig is van systeembeheer en/of systeemprogrammering van de binnen de organisatie aanwezige computerbesturingssystemen, waaronder soms meerdere unix- en/of windows-varianten. Verder dienen CSIRT-medewerkers bekend te zijn met netwerkservices en -protocollen als SMTP, HTTP, FTP, Telnet, IP, TCP en UDP, cryptografische technieken en met bekende aanvalstechnieken zoals Denial-of-Serviceaanvallen en IP-spoofing.

*Standaardformulieren*
Veel processen bij CSIRT's zijn gestandaardiseerd. Al eerder werden genoemd de communicatie tussen de CSIRT en haar constituency en de diverse incidentenresponsefuncties. Voor een aantal activiteiten worden door CSIRT 's ter wille van een vlotte en eenduidige behandeling standaardformulieren beschikbaar gesteld, bijvoorbeeld voor het aanmelden van een nieuw incident.
De meeste incidentenmeldformulieren starten met de vraag om identiteitsgegevens in te vullen. Deze informatie is van belang voor een juiste terugkoppeling van de CSIRT naar de melder. Vervolgens wordt gevraagd om een omschrijving van het incident. Sommige CSIRT's gebruiken hiervoor een lijst met gedefinieerde aanvalsmethodieken. Andere CSIRT's[42] bieden de mogelijkheid om het incident in free-format-text op te nemen. Wel worden vaak richtlijnen meegegeven over de in te vullen gegevens. CERT/CC adviseert om in elk geval melding te maken van misbruik van aanwezige kwetsbaarheden, aangebrachte wijzigingen aan systemen of geïnstalleerde software. Ook wordt gevraagd welke hardware- en softwareversies zijn gecompromitteerd. Tenslotte wordt vaak gevraagd naar de impact van het incident in de zin van aantallen systemen of componenten en/of de veroorzaakte financiële schade.

[41] Interview met Don Stikvoort van de firma Stelvio/M&I (onder meer secretariaat FIRST) d.d. 30 mei 2002.
[42] Zie bijvoorbeeld http://www.auscert.org.

Een ander aandachtspunt is het zogeheten tijdzoneprobleem. CSIRT's die een constituency bedienen met een grote geografische spreiding, krijgen hiermee te maken. Bijvoorbeeld omdat er in de diverse landen verschillende feestdagen gelden en er vanwege het tijdsverschil vaak niet rechtstreeks gecommuniceerd kan worden tussen CSIRT en de incidentenmelder of de vertrouwde CSIRT. Grotere CSIRT's verzoeken daarom de melder ten behoeve van registratie en afhandeling aan te geven in welke tijdzone het incident plaatsvond.

CERT/CC zegt in haar Incident Reporting Guidelines van 15 april 2002:

*'A timezone reference relative to GMT (or UTC) such as GMT-5 is preferred, since less formal timezone designations can be misinterpreted. For example, EST (Eastern Standard Time) may have different meanings for people inside and outside the United States.'*

De verwijzing naar de tijdzone is ook van belang indien er systeemlogs bij de melding worden meegestuurd waarin gegevens zijn opgenomen over data en tijdstippen rondom het incident.

#### *3.2.3.4. Beleid*

De door CSIRT's gehanteerde beleidsregels hebben vooral betrekking op categoriseren van informatie, de ontsluiting van informatie, mediabeleid en gedrag van CSIRT-medewerkers.

*Categoriseren van informatie*
Het categoriseren of classificeren van informatie is van belang om de procedurehandelingen met betrekking tot de informatie eenduidig te onderscheiden en te structureren. Het eenvoudigste model kent twee classificaties: intern gebruik en publiek gebruik. De classificatie bepaalt of de informatie mag worden ontsloten, hoe de informatie dient te worden opgeslagen en wanneer de informatie mag worden verwijderd.

*Mediabeleid*
Vooral bij grotere incidenten bestaat de kans dat leden van CSIRT's worden benaderd door de pers. De CSIRT zal daarom vaak één functionaris aanwijzen die als contactpersoon fungeert naar de media. Andere medewerkers dienen zich te onthouden van communicatie naar buiten. In de meeste gevallen wordt vanwege het specialistische karakter communicatie met de pers overgelaten aan een deskundige binnen de organisatie, bijvoorbeeld een officiële persvoorlichter [MCGI93]. De functionaris zorgt voor een lijst met contactpersonen van de verschillende media, maakt afspraken over de wijze van citeren en de mogelijkheid om het te verspreiden bericht voorafgaand aan verzending te becommentariëren. De inhoud van het bericht wordt mede bepaald door de zogeheten information disclosure policy.

*Gedragscode*
Een gedragscode is een set algemene regels waarin de gewenst houding en het gewenste gedrag van CSIRT-medewerkers worden vastgelegd. De gedragscode dient een weerspiegeling te zijn van de missie en het karakter van de organisatie.

*Ontsluiting van informatie*
Vertrouwen van de gebruikergemeenschap is, zoals eerder gezegd, van cruciaal belang voor een CSIRT. Zonder dit vertrouwen en respect kan de CSIRT niet goed functioneren. De bij FIRST aangesloten CSIRT's hanteren om deze reden een information disclosure policy. In een dergelijke beleidsregel dient te staan wanneer en met wie een CSIRT kan communiceren bij gemelde incidenten.

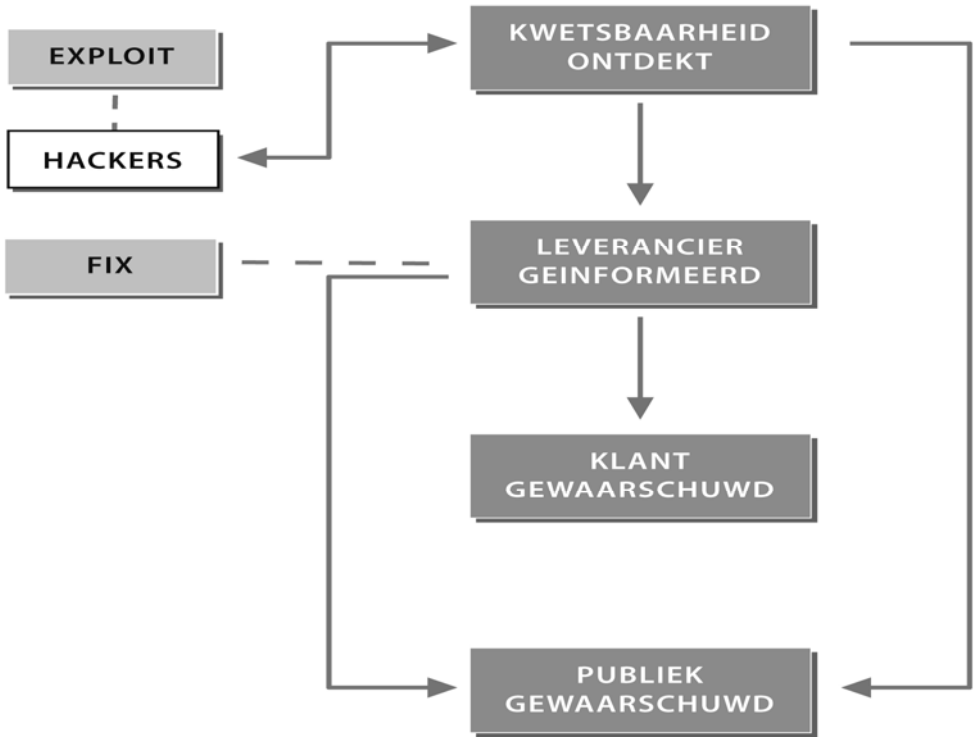
De factoren doel, doelwit en informatiecategorie zijn essentieel bij de bepaling of, tot op welke hoogte en hoe de informatie wordt ontsloten [WESK98].

| | |
|---|---|
| *Doel:* | het ontsluiten van informatie dient een grondslag te hebben. Vaak worden principes als 'need-to-know' of 'need-to-use' gehanteerd om aan te geven waarom bepaalde informatie aan bepaalde personen wordt verstrekt. |
| *Doelwit:* | doelwit van de informatie is diegene(n) die het betreft, zoals CSIRT medewerkers, management van de organisatie, partner-CSIRT, overheidsinstantie, etc. |
| *Informatiecategorie:* | leidend is de classificatie van de informatie. Bijvoorbeeld publieke informatie wordt op de website geplaatst en/of via e-mail verstuurd. Soms wordt hierbij extra informatie meegestuurd om de authenticiteit van de verzender, in casu de CSIRT, te verifiëren. |

Een voortdurende bron van discussie is het tijdstip van ontsluiting bij nieuw ontdekte kwetsbaarheden. Sommige leveranciers van software zijn zeer terughoudend met het geven van informatie over recent ontdekte kwetsbaarheden.

#### *3.2.3.5. Volledige of gedeeltelijke openbaarmaking*

Grotere softwareleveranciers communiceren bevindingen en adviezen over kwetsbaarheden van hun producten of diensten via open mailingslists, speciale websites of, al naar gelang de publicitaire druk, via nationale media. Als we inzoomen op het afhandelingsproces van kwetsbaarheden dan weten we dat het communicatienetwerk wordt gedomineerd door drie partijen: de melder van een kwetsbaarheid, de coördinator (of intermediair) en de ontvanger. Binnen het proces van openbaarmaking van kwetsbaarheden spelen twee componenten een belangrijke rol: het tijdstip en het detailniveau van openbaarmaking (zie figuur 10).




Figuur 10: relatieschema bij ontdekking van een kwetsbaarheid in software

*Tijdstip van openbaarmaking*
Een softwareleverancier zal na de initiële melding van een beveiligingsprobleem met zijn product(en) een aantal stappen ondernemen[43]. Allereerst zal worden onderzocht of het een bekend probleem is. Is dit niet het geval, dan zal een team van specialisten een voorlopige, globale analyse doen om de aard en impact van het incident in kaart te brengen. Vervolgens wordt in detail gekeken wat de kwetsbaarheid veroorzaakt en welke voorwaarden of middelen nodig zijn om de kwetsbaarheid uit te nutten (exploits). Soms wordt hierbij externe expertise ingeschakeld, bijvoorbeeld van een bekend computer security incident response team als CERT/CC. In de volgende fase wordt gewerkt aan een oplossing van het probleem. In veel gevallen betekent dit het ontwikkelen van herstelsoftware (security patch) die de kwetsbaarheid elimineert. Aansluitend zal de leverancier de software testen voor een of meer van zijn producten en deze vervolgens ter beschikking stellen.

De hierboven genoemde fasen kosten uiteraard tijd. Leveranciers zullen uit commerciële overwegingen, vooral uit zorg om het nadeel van negatieve publiciteit rondom hun product of dienstverlening, geneigd zijn niet eerder melding te maken van onvolkomenheden in hun producten dan wanneer er een oplossing voorhanden is[44]. De vraag is of dit communicatiebeleid van de leverancier ethisch verantwoord is. De afnemer van het product loopt in de periode van het bekend worden van de kwetsbaarheid bij de leverancier tot en met het moment van beschikbaar stellen van de patch een risico. Hij

[43] Een door een leverancier zelf ontdekte kwetsbaarheid wordt niet door elke leverancier openbaar gemaakt. Het herstellen van een dergelijke kwetsbaarheid wordt ook wel silent patching genoemd.
[44] Onderzoek heeft aangetoond dat volledige en onmiddelijke bekendmaking van kwetsbaarheden alleen optimaal is, als het direct leidt tot het ontwikkelen van veiliger producten door de leverancier of de gebruiker zich op een andere manier beschermt, bijvoorbeeld door het implementeren van een workaround of additionele perimeter defences [ARTE05].

beschikt immers over een product met een kwetsbaarheid die een bepaald risico kan opleveren voor de beschikbaarheid, integriteit of vertrouwelijkheid van zijn gegevens.

*Detailniveau van openbaarmaking*
Welke informatie over de kwetsbaarheid wil de leverancier vrijgeven? Zeker wanneer er nog geen patch beschikbaar is, zal een leverancier voorzichtig zijn met het geven van teveel details. Kwaadwillenden kunnen op deze manier immers gebruik maken van de informatie om succesvolle aanvallen te ontwikkelen. De leverancier zal alleen die informatie publiceren die noodzakelijk is om de kwetsbaarheid te verminderen of te elimineren. Informatie over de opzet en werking van softwarebeveiligings- of controleprocessen van het product zal daarom slechts in generieke zin worden vermeld. Op zichzelf is dit een begrijpelijke en acceptabele keuze van de leverancier. Toch kleeft er een nadeel aan het aspect van 'partial disclosure'. Door het geven van summiere, niet-gedetailleerde informatie van de werking van het product en de kwetsbaarheid is nader onderzoek door andere teams niet of slechts beperkt mogelijk.

Fins onderzoek [OUUN03] signaleert een duidelijke behoefte aan internationale codificatie van regels waarop effectieve 'disclosure policies' kunnen worden ontwikkeld door partijen die participeren in het communicatienetwerk rondom software kwetsbaarheden.

Een eerste serieus initiatief dateert van februari 2002. Steve Christey (MITRE) en Chris Wysopal (@STAKE) dienden een IETF-Internetdraft in genaamd Responsible Vulnerability Disclosure Process[45]. Het document beschreef de verantwoordelijkheden van de melder, de leverancier van het product en de coördinator van een ontdekte kwetsbaarheid. Zo dient volgens de inhoud van de betreffende Internetdraft de leverancier binnen tien dagen een ontvangstbevestiging te geven en binnen dertig dagen na de initiële melding een oplossing te hebben voor het probleem. Tegelijk kan de leverancier de melder en coördinator om een 'grace period' van dertig dagen verzoeken, waarbij de ontdekking van de kwetsbaarheid niet verder zal worden onthuld. Mocht de leverancier binnen deze termijn geen oplossing voor het probleem hebben, zoals een patch of een workaround, dan dient hij expliciet de reden terug te communiceren aan de melder en eventueel de coördinator.

Microsoft en enige andere softwareleveranciers ondersteunden dit initiatief tot zelfregulering [HILL01]. Het initiatief heeft het niet gehaald. De officiële reden is niet bekendgemaakt, maar een mogelijke reden is dat het IETF-bestuur het initiatief niet ondersteunt omdat er sprake zou zijn van een voorstel voor het oplossen van een organisatorisch probleem en niet een probleem van technische aard. Daardoor zou het strijdig met het doel van de IETF zijn.

De Organization for Internet Safety heeft in 2004 richtlijnen [OIS04] opgesteld voor het openbaren en beantwoorden van beveiligingskwetsbaarheden. Ook hierin worden vaste, gemaximeerde tijdlijnen gehanteerd voor het bevestigen van de melding van de kwetsbaarheid door de leverancier, zeven dagen. Verder dient de leverancier volgens de

[45] Het betreft een in februari 2002 door Steve Christey en Chris Wysopal geplaatste Internet-Draft, textfile 'draft-christey-wysopal-vuln-disclosure-oo.txt' op www.ietf.org binnen de categorie Best Current Practice.

richtlijn elke zeven dagen een update te geven van zijn vervolgacties aan de melder van de kwetsbaarheid. Het rapport spreekt van een conventierichttijd van dertig dagen tussen het melden van de kwetsbaarheid en het leveren van een oplossing door de leverancier. Voorts wordt gesproken van een aansluitende rustperiode van dertig dagen nadat de leverancier een oplossing heeft gevonden. Gedurende deze periode wordt zowel van de melder als de leverancier verwacht, dat details over de kwetsbaarheid uitsluitend worden gemeld aan organisaties en personen die een kritische rol spelen bij het bevorderen van de beveiliging van gebruikers, kritische infrastructuren en het Internet om de leveranciers van producten of diensten tijd te gunnen de oplossing te implementeren binnen hun eigen producten, diensten of infrastructuren. Daarna mogen meer details 'aan het publiek' worden vrijgegeven.

Naast een beschrijving van de communicatieprocesstappen geeft de richtlijn ook aanwijzingen aan de leverancier over de inhoud van het op te stellen kwetsbaarheidonderzoeksrapport.

| | |
|---|---|
| *Kwalificatie onderzoek:* | de leverancier demonstreert dat zijn onderzoek doorgrond en van voldoende technische diepgang was, door het vermelden van een lijst met geteste producten en productversies, de soorten testen en de testresultaten. |
| *Gebrek:* | de leverancier vermeldt in zijn rapport hetzij een bevestiging van het gebrek ('flaw'), een ontkenning van het gebrek, danwel het niet kunnen bevestigen of ontkennen van het gebrek. |
| *Vervolgacties:* | bij bevestiging van het gebrek geeft de leverancier aan wat zijn vervolgacties zijn zoals de wijze van distribueren van de oplossing en de tijdschaal voor het leveren van een oplossing. |

Het formaliseren van richtlijnen over hoe om te gaan met nieuw ontdekte kwetsbaarheden is een nobel streven. Het probleem bij dit soort richtlijnen blijft echter de niet verplichte naleving. Er is geen autoriteit die de naleving van dergelijke richtlijnen kan afdwingen of sanctioneren. De toegevoegde waarde zit evenwel in het feit dat softwareleveranciers en instituten die regelmatig beveiligingskwetsbaarheden ontdekken en melden[46], de richtlijnen formeel adopteren in hun communicatiebeleid en er op deze manier een defacto communicatieprocedure ontstaat.

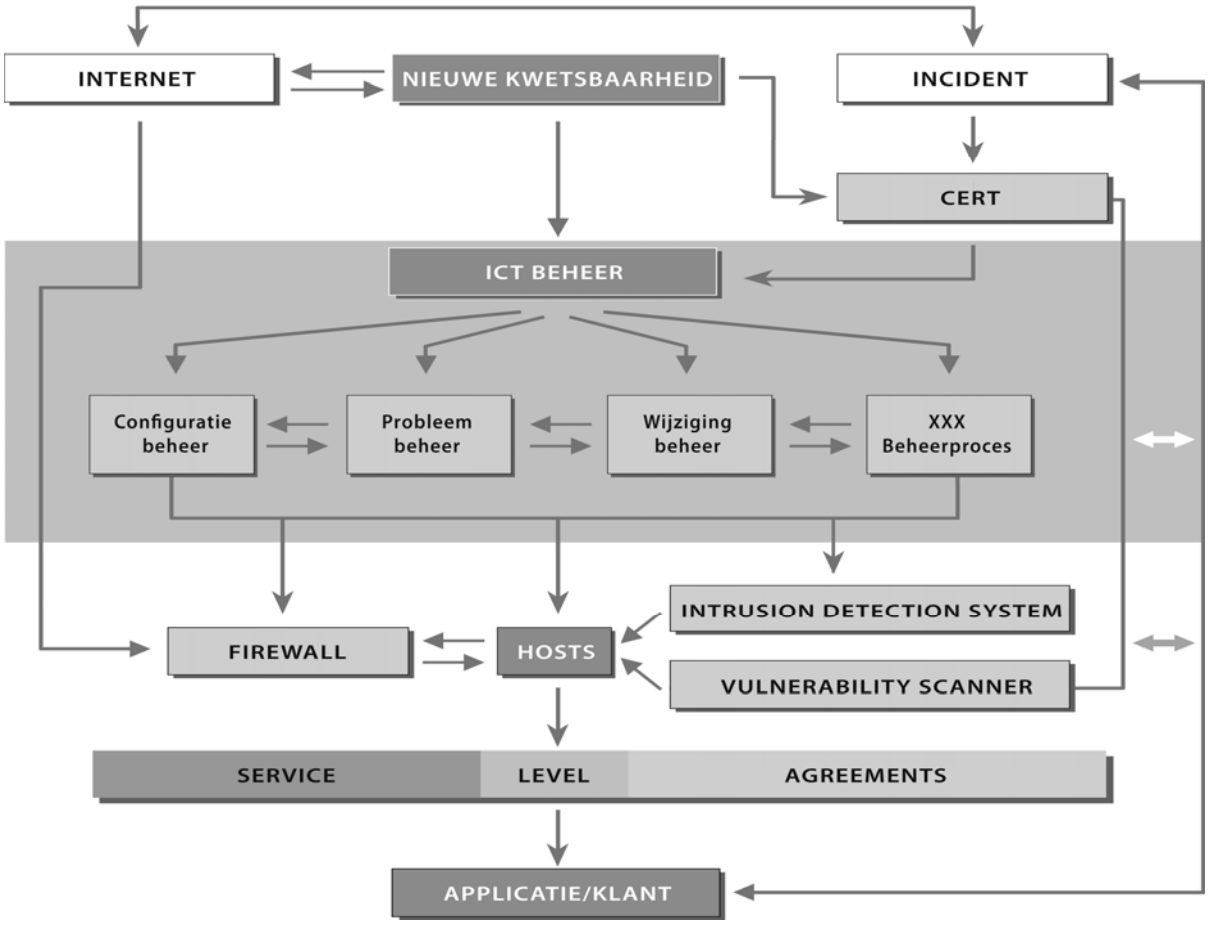
### 3.3. Standaardisatie van ICT-beheerprocessen

IT service management is de verzamelnaam voor een procesgerichte en dienstengerichte benadering van ICT-beheer, waarbij de belangrijkste doelstelling is het leveren van een bijdrage aan de kwaliteit van de IT-dienstverlening [ITSM02]. De in Nederland meest

[46] Het verbeteren van de kwaliteit van de onderzochte software is een belangrijk motief voor het uitvoeren van (wetenschappelijk) onderzoek naar kwetsbaarheden. Het ICT-beveiligingsadviesbureau RTFM heeft de relatie tussen dergelijk onderzoek en de verbetering van de softwarekwaliteit onderzocht en geconcludeerd, dat de huidige beschikbare gegevens deze relatie niet aantonen [RESC05].

bekende benadering voor IT service management, ITIL, beschrijft de samenhang van herkenbare ICT-beheerprocessen (figuur 11)[47].

### 3.3.1. Information Technology Infrastructure Library




Figuur 11: voorbeelden van ITIL service supportprocessen

Aan het eind van de vorige eeuw heeft in Nederland en omringende landen de toepassing van Information Technology Infrastructure Library (ITIL) als standaard voor de inrichting van ICT beheerprocessen een stormachtige vlucht genomen. In 2001 telde het Nederlandse gebruikersplatform, het Information Technology Service Management Forum (ITSMF)[48], ongeveer 500 Nederlandse bedrijven [ITSM02]. Inmiddels zijn er ITSMF organisaties in onder andere België, Duitsland, Oostenrijk, Zwitserland, de Verenigde Staten, Zuid-Afrika en Australië. Oorspronkelijk was ITIL een product van de Central Computer and Telecommunication Agency, onderdeel van de Britse overheid. Per 1 april 2001 is de CCTA opgegaan in de OGC, het Office of Government Commerce[49], dat daarmee de nieuwe eigenaar van ITIL werd. De Nederlandse stichting

[47] In deze paragraaf worden een aantal van de oorspronkelijke, Engelstalige procesnamen van ITIL gehanteerd.
[48] Zie http://www.itsmf.nl.
[49] Zie http://www.ogc.gov.uk.

Exameninstituut voor Informatica (EXIN)[50] en de Engelse Information Systems Examination Board (ISEB) ontwikkelden in overleg met ITSMF en OGC professionele certificeringtrajecten voor ITIL[51]. Er worden drie niveaus onderscheiden:

- Foundation certificate in IT service management
- Practioner certificate in IT service management
- Manager certificate in IT service management.

Het Foundationcertificaat is bestemd voor medewerkers die zich verdiepen in de belangrijkste taken van een ICT-beheerorganisatie. De practionersopleiding richt zich op medewerkers die taken verrichten in een bepaald ITIL-proces zoals change management of service level management. Managers tenslotte worden opgeleid om de processen te beheren en te adviseren over de inrichting en optimalisering van de processen.

ITIL wordt beschouwd als een raamwerk van best practices dat is gebaseerd op de ervaring van professionele gebruikers. Deze best practices zijn door auteurs beschreven in een serie boeken. De auteurs hebben vele jaren ervaring in een bepaald ITIL domein. Oorspronkelijk bestond ITIL uit een vijftigtal boeken die elk een bepaald aandachtsgebied van de ontwikkeling, het onderhoud en de exploitatie van de ICT-infrastructuur beschreven. Tien boeken werden beschouwd als de kern van ITIL. De overige boeken behandelden aanvullende onderwerpen op het gebied van ICT-beheer, uiteenlopend van kabelbeheer tot het managen van klantrelaties. De eerste serie boeken benaderde IT service management vooral vanuit het gezichtspunt van informatietechnologie. Mede hierdoor werd een business perspective set geïntroduceerd om de kloof tussen business en ICT te overbruggen. Onderwerpen binnen de business perspective set zijn business continuity management, partnerships en outsourcing en het overleven van wijzigingen.

Om de samenhang tussen de processen te verstevigen is enkele jaren geleden besloten om de kern van ITIL te herzien en als twee boeken uit te geven: Service Delivery en Service Support.

### *3.3.2. ITIL's Service Delivery*

Het ITIL-boek Service Delivery [BART01] beschrijft de diverse diensten die de business van de klant nodig heeft en wat er nodig is om deze diensten te kunnen leveren. De volgende onderwerpen komen hierbij aan de orde:

- customer relationship management
- service level management
- financial management for IT services
- capacity management
- availability management
- security management
- IT Service Continuity Management.

In de volgende paragrafen worden de processen IT service continuity management en security management nader toegelicht.

[50] Zie http://www.exin.nl.
[51] Zie http://www.itil.co.uk.

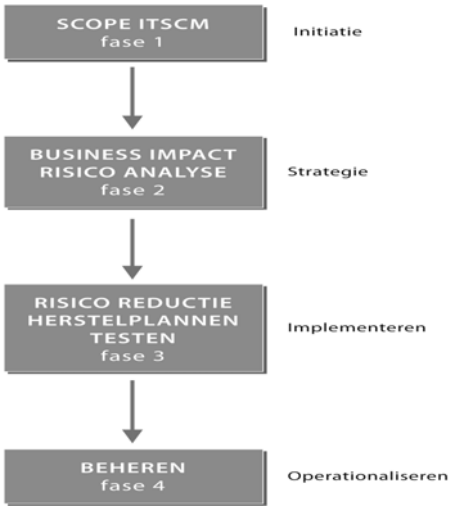
#### *3.3.2.1. IT service continuity management*

Een van de oudste door de CCTA uitgegeven modules had contingency planning als onderwerp. Het proces contingency planning beschreef welke activiteiten moesten worden ondernomen ingeval zich een calamiteit voordeed. In de risicomanagementcyclus wordt deze benadering reactief genoemd. De opvolger van contingency planning, IT service continuity management [OGC01], legt meer de nadruk op preventie, het voorkomen van een calamiteit[52].
Een calamiteit wordt hierin omschreven als *een gebeurtenis die een service of systeem zodanig verstoort dat veelal aanzienlijke maatregelen moeten worden genomen om het originele verwerkingsniveau te herstellen*. Een calamiteit wordt als ernstiger getypeerd dan een incident. Voorbeelden van calamiteiten zijn brand, blikseminslag, inbraak en grootschalige stroomstoringen. Ook beschikbaarheidaanvallen via het Internet die de communicatie van een bedrijf verlammen, worden genoemd in de reeks van voorbeelden van calamiteiten.

De missie van IT service continuity management (ITSCM) is het zeker stellen dat de ICT-infrastructuur en ICT-(ondersteunende-)diensten na een calamiteit zo snel mogelijk worden hersteld. ITSCM ondersteunt het bovenliggende business continuity management (BCM). Business continuity management richt zich op het beheersen van bedrijfsrisico's, teneinde een minimaal noodzakelijke productiecapaciteit en/of dienstverlening te waarborgen.

Figuur 12 laat zien dat ITSCM vier fasen onderscheidt:

1. afbakening
2. strategie en risicobepaling
3. implementatie
4. operationeel beheer.




Figuur 12: IT service continuity management

[52] Een andere in opkomst zijnde best practise op het gebied van bedrijfscontinuiteit is Public Available Specification (PAS)56 ontwikkeld door het British Standards Institute. PAS56 beschrijft een raamwerk voor het implementeren van een BCM-proces in een organisatie. Ook is een internationale standaard voor ICT disaster recovery in ontwikkeling (juni 2006): ISO/IEC CD 24762 Guidelines for Information and Communication Technology Disaster Revocer Scenario.

*Scope*
In deze initiatiefase binnen het ITSCM-proces dient de totale organisatie te worden beschouwd en een beleid en strategie met betrekking tot de continuïteit van de ICT-services nader te worden uitgewerkt. Denk hierbij onder meer aan het maken van keuzes ten aanzien van de managementstructuur en de procesopzet, zoals de toewijzing van resources (mensen en middelen) en de inrichting van de projectorganisatie. Eisen of randvoorwaarden vanuit het overkoepelende bedrijfsbeleid of aanpalende processen, zoals kwaliteitszorg, spelen in deze fase ook een belangrijke rol.

*Strategie en risicobepaling*
Na de afbakening volgt de fase waarin de risico's in kaart dienen te worden gebracht en de continuïteitsstrategie verder wordt uitgewerkt. Allereerst dient er een zogeheten Business Impact Analyse te worden gemaakt. De analyse begint met het vaststellen van de motivaties voor bedrijfscontinuïteit. De motivaties dienen daarbij te vermelden hoeveel en wat een organisatie te verliezen heeft bij ernstige onderbreking van de dienstverlening. Voorbeelden hiervan zijn publicitaire schade en verlies van winstgevendheid. Hierna worden alle bedrijfskritische ICT-diensten geïnventariseerd. Hierbij wordt geadviseerd de beschikbaarheidseis in de service level agreements als uitgangspunt te nemen. Als laatste fase van de business impact analyse dient te worden gekeken naar de afhankelijkheid tussen diensten en productiemiddelen De processen availability management en capacity management kunnen behulpzaam zijn bij het analyseren van de mate waarin productiemiddelen een kritische functie hebben bij een bepaalde ICT-dienst.

Conform het procesmodel dient aansluitend aan de business impact analyse een risicoanalyse te worden uitgevoerd. In de risicoanalyse worden de bedreigingen, afhankelijkheden en kwetsbaarheden van productiemiddelen in kaart gebracht en wordt een inschatting gemaakt van de risico's. De ITIL-methodiek schrijft geen specifieke risicoanalysemethode voor.

Als laatste stap in deze fase wordt de te voeren strategie bepaald. Binnen de strategie wordt onderscheid gemaakt tussen risicobeperking, herstel van zakelijke activiteiten en ICT-herstelopties, bijvoorbeeld uitwijkopties. De afweging van kosten en risico's is doorslaggevend in de keuze van de preventieve en herstelactiviteiten. De meest uitgebreide vorm van preventie heet de fortress approach. Bij deze aanpak zijn praktisch alle kwetsbaarheden weggenomen door bijvoorbeeld een bunker te bouwen met eigen stroomvoorziening. Indien niet alle risico's kunnen worden weggenomen door voorzorgsmaatregelen, dient voor de overblijvende risico's een uitwijkplanning te worden opgesteld, aldus ITSCM. In onderstaande tabel is aangegeven waar zoal rekening mee dient te worden gehouden.

Tabel 5: aandachtspunten bij uitwijkplannen

| **Onderwerp** | **Aandachtspunten** |
|---|---|
| Mensen en accommodatie | Werkschema's, huisvesting, reisafstand |
| (ICT-)Systemen en -netwerken | Uitwijkvorm |
| Facilitaire zaken | Gas, water, licht, telefonie, post, etc |
| Diensten van derden | Internetserviceproviders |
| Archiefmateriaal | Electronische dossiers, papieren systemen |

*Implementatie*
Binnen de implementatiefase worden diverse plannen en procedures uitgewerkt. Op het hoogste niveau wordt een calamiteitenplan opgesteld. Het plan omvat een overzicht van de crisismanagementorganisatie met namen, functies, bevoegdheden en (privé) telefoonnummers en verder per dienst procedures ten behoeve van schadebeoordeling en herstel.

*Operationeel beheer*
Opleiding en training maken onderdeel uit van ITSCM. Het uitgangspunt hierbij is dat iedere medewerker op de hoogte is van de aanwezigheid van calamiteitenresponse- en herstelplannen binnen de organisatie en weet welke rol er van hem wordt verwacht gedurende de uitvoer van deze plannen.

Daarnaast dienen alle producten van het ITSCM-proces met regelmaat te worden gecontroleerd op actualiteit. Voor de ICT-infrastructuur geldt dat bij belangrijke wijzigingen, zoals nieuwe systemen, netwerken of serviceproviders de plannen dienen te worden gecontroleerd. Hier wordt een duidelijke relatie gelegd met het change managementproces: bij elke wijziging dient te worden gekeken in hoeverre dit invloed heeft op de herstelplannen. Ook bij veranderingen van strategie wordt geadviseerd om een audit uit te voeren.

Een derde belangrijk aspect van operationeel beheer is testen. Met het testen wordt gekeken of de beschreven calamiteitenplannen, uitwijkplannen en/of herstelplannen in de praktijk voldoen. Tekortkomingen worden op deze wijze zichtbaar gemaakt.

#### *3.3.2.2. Availability management*

Het hoofddoel van het ITIL-proces availability management is te zorgen voor een kosteneffectief en vastgesteld niveau van beschikbaarheid van de ICT-dienstverlening, teneinde ‘de business’ in staat te stellen om haar doelstellingen te bereiken. De volgende afhankelijkheden worden hierbij onderkend:

- complexiteit van de architectuur van de ICT-infrastructuur
- betrouwbaarheid van de componenten
- vermogen om snel en adequaat op storingen te reageren
- kwaliteit van de onderhoud- en supportorganisatie en toeleveranciers
- kwaliteit en reikwijdte van operationele beheerprocessen.

Om aan de vraagstelling ten aanzien van beschikbaarheid te kunnen voldoen, zal de ICT-organisatie bepaalde foutdetectie- en correctiemechanismen dienen te hanteren. Ook zal het veelal noodzakelijk zijn om bepaalde essentiële componenten dubbel uit te voeren.

Availability management kent een aantal fasen:

*Bepalen van beschikbaarheidbehoeften:* in deze fase speelt het bedrijfsproces een hoofdrol. Zo wordt onder meer vastgesteld welke bedrijfsfuncties belangrijk zijn, beschikbaarheidseisen gekwantificeerd en afspraken gemaakt over onderhoudsperioden.

ITIL adviseert het resultaat van de analyse vast te leggen in een service level agreement.

*Het ontwerpen van beschikbaarheid:* kwetsbaarheden die van invloed (kunnen) zijn worden vervolgens door de ICT-organisatie geïnventariseerd. Meestal wordt hiervoor een risicoanalysemethodiek gebruikt. Het resultaat van de inventarisatie geeft bijvoorbeeld inzicht in de aanwezigheid van zogeheten single point of failures[53]. Na de inventarisatie wordt een beschikbaarheidsplan opgesteld waarbij op basis van de beschikbaarheideisen een voorstel wordt gedaan voor de inzet van bepaalde technologie of extra servicemanagement hulpmiddelen.

*Managen van onderhoudsactiviteiten:* deze fase maakt geplande en daarmee afgestemde momenten van niet-beschikbaarheid zichtbaar. Tijdens onderhoud worden preventieve werkzaamheden uitgevoerd zoals software- en hardware-upgrades, en is de invoering van wijzigingen mogelijk. Onderhoudsactiviteiten in het kader van availability management dienen te worden afgestemd met change management-procesactiviteiten.

*Het ontwerpen van herstelbaarheid:* honderd procent beschikbaarheid is praktisch onmogelijk. Elk beschikbaarheidsontwerp dient rekening te houden met onverwachte verstoringen van ICT services. Bij het ontwerpen van herstelbaarheidsactiviteiten zijn incident management, communicatie en back-up en recovery van belang. Hier ligt ook een duidelijk relatie met het ITSCM-proces. Bij availability management worden vaak de volgende storingswaarden gehanteerd:

- mean time to repair (MTTR), de gemiddelde tijd tussen het optreden van een storing en herstel van de service
- mean time between failures (MTBF), de gemiddelde tijd tussen het herstel van het ene incident en het optreden van een volgend incident

[53] Kritische component waar veel (ICT) processen van afhankelijk zijn. Uitval of verminderde werking van deze component heeft direct effect op diverse achterliggende processen.

- mean time between system incidents (MTBSI), de som van MTTR en MTBF.

#### *3.3.2.3. Security management*

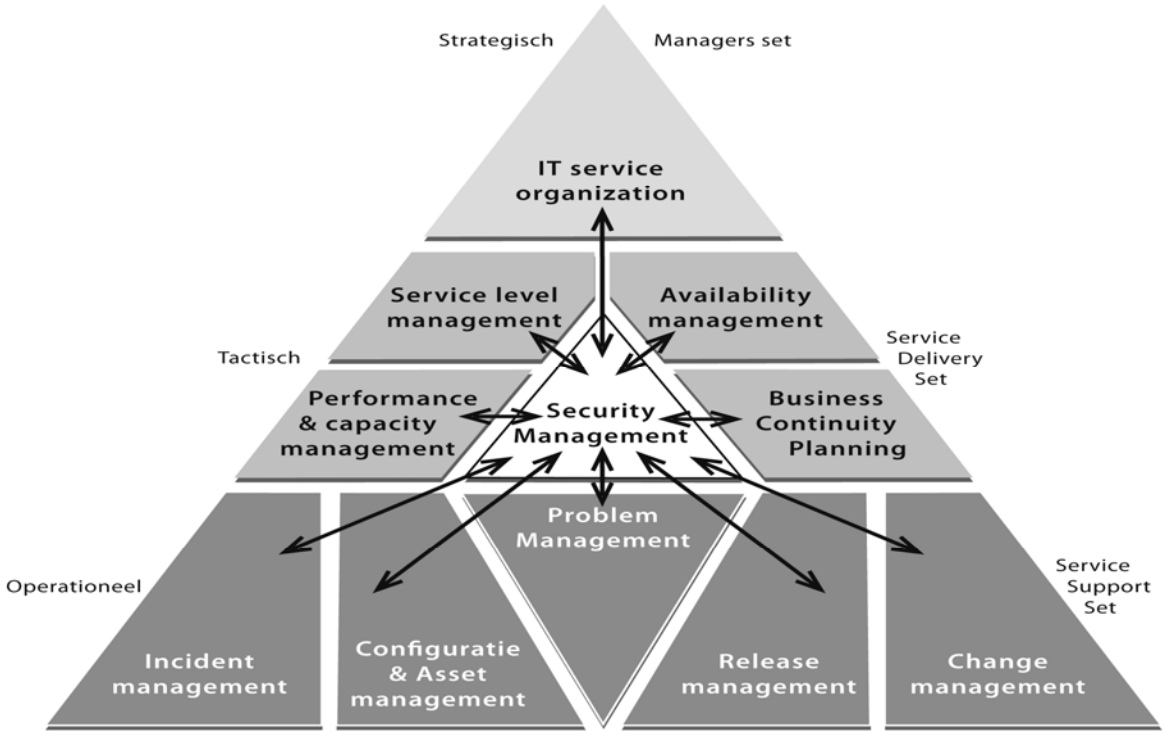
In 1999 is de reeks ITIL-boeken uitgebreid met ITIL security management [CAOP99]. De doelstelling van deze module wordt als volgt omschreven:

- voldoen aan (externe) eisen voortvloeiend uit SLA's, wetgeving, beleid, etc.
- realiseren van een zeker basisniveau van beveiliging.

Centraal in deze module staat het beveiligen van de waarde van informatie. Deze waarden worden uitgedrukt in de drie elementen: vertrouwelijkheid, integriteit en beschikbaarheid. Beveiligingsmaatregelen dienen ervoor te zorgen dat onderkende risico's met betrekking tot informatie en ICT worden gereduceerd. De maatregelen kunnen een (gecombineerd) preventief, detectief of repressief karakter hebben.

Activiteiten in het kader van informatiebeveiliging zijn aan veranderingen onderhevig door veranderingen in de ICT-omgeving, nieuwe behoeften aan veiligheid en veranderende risico's. ITIL security management introduceert daarom een ICT-beveiligingsbeheerproces volgens het plan-implement-evaluate-maintain-principe.

ITIL security management heeft nauwe relaties met andere ITIL-processen, zie figuur 13. Een aantal van deze relaties zoals beschreven in ITIL security management, worden hieronder kort aangehaald.




Figuur 13: Positionering van ITIL Security management [ITSM02]

*Configuration management* is voor security management vooral van belang omdat het de mogelijkheid biedt om configuration items (CI's) te classificeren voor de aspecten beschikbaarheid, vertrouwelijkheid en integriteit. Indien drie niveaus, hoog, midden en laag, worden gehanteerd, ontstaat een schema met in totaal negen mogelijke classificaties. De classificatie kan hiermee een CI koppelen aan bepaalde technische, procedurele of organisatorische beveiligingsmaatregelen. Een hoge classificatie leidt logischerwijs tot zwaardere beveiligingsinspanningen.

*Incident management* geldt als centraal proces voor alle ICT incidenten, inclusief beveiligingsincidenten. Voor de afhandeling van beveiligingsincidenten worden soms separate procedures gehanteerd. Uit oogpunt van geheimhouding bijvoorbeeld wordt het incident niet rechtstreeks of niet geheel geregistreerd in het centrale incidentenregistratiesysteem. Het is daarom belangrijk dat aan ICT-beveiliging gerelateerde incidenten door incident management als zodanig worden herkend. Aanbevolen wordt om in de SLA een lijst op te nemen met kenmerkende beveiligingsincidenten. Voorbeelden hiervan zijn ongeautoriseerde toegang tot informatiesystemen, diefstal van laptops en virusbesmettingen.

Activiteiten in het kader van *change management* kunnen een directe relatie hebben met security management. Immers een wijziging op een bestaande omgeving kan direct leiden tot een lager niveau van beveiliging. Change management moet daarom, aldus de ITIL-module security management, middels een aantal vaste stappen het beveiligingsniveau waarborgen. Aan de eerder beschreven RFC worden de parameters urgentie en impact toegevoegd. In de ITIL-module security management wordt gepleit voor het extra opnemen van een parameter invloed op informatiebeveiliging. Wanneer er bijvoorbeeld sprake is van een majeure impact op informatiebeveiliging, verplicht dit tot meer stringente acceptatietesten en –procedures. Ook wordt geconstateerd dat het testen van beveiliging anders is dan bij normale, functionele testen. Bij het testen van beveiliging wordt naast de beveiligingsfunctionaliteit ook gekeken naar de aanwezigheid van overbodige en/of ongewenste functionaliteit. Laatstgenoemde introduceert soms een of meer gaten in het systeem en creëert aldus een beveiligingsrisico.
De ITIL-module security management beveelt voorts aan om de securitymanager als vertegenwoordiger van de klant, plaats te laten nemen in de zogeheten change advisory board.

### *3.3.3. ITIL's Service Support*

Het ITIL-boek over Service Support [BERK00] beschrijft, de naam zegt het ten dele, hoe de klant toegang krijgt tot de diverse ICT-dienstverleners om zijn 'business' te ondersteunen. Het boek beschrijft de volgende onderwerpen:

- service desk
- incident management
- problem management
- configuration management
- change management
- release management.

Een aantal van deze processen raakt rechtstreeks aan het proces van kwetsbaarheden- en incidentenresponse. Deze processen worden nader toegelicht.

#### *3.3.3.1. Incident & problem management*

ITIL maakt bij de processen incident management en problem management onderscheid tussen de begrippen incident, problem en known error.

Een incident wordt omschreven als *elke gebeurtenis die niet tot een standaardoperatie van een service behoort en die een interruptie of een vermindering van de kwaliteit van die service kan veroorzaken*. Een problem is een *ongewenste situatie die wordt afgeleid uit infrastructuurgegevens, bijvoorbeeld uit een serie incidenten met gelijke kenmerken, of uit een enkel doch zeer belangrijk incident.* Problemen hebben een nog onbekende oorzaak. Dit in tegenstelling tot known errors. Dit zijn *problemen waarvoor een succesvolle diagnose is gesteld en waarvoor een workaround bekend is*.

##### *3.3.3.1.1 Incident management*

ITIL verstaat onder incidenten hardware- en softwarestoringen alsmede de zogenaamde service requests, dat wil zeggen verzoeken van een gebruiker om ondersteuning, levering, informatie, advies of documentatie [ITSM02]. Incidenten kunnen hun oorzaak vinden in verschillende delen van de infrastructuur. Behalve door gebruikers kunnen incidenten ook worden ontdekt door beheerafdelingen. Ook de zogeheten events uit detectiesystemen kunnen leiden tot incidentvastleggingen. De servicedesk is meestal het centrale punt voor melding, registratie en classificatie van incidenten. Zij bepaalt, al dan niet in overleg met de melder of een andere vertegenwoordiger van de gebruikersorganisatie, impact en urgentie van een incident. Wanneer een incident niet binnen de afgesproken tijdlijnen kan worden verholpen, wordt de tweedelijnssupport, de beheerafdeling, ingeschakeld.

De ITIL-module incident management geeft aan dat bij de (eerste) melding van een incident een uniek incidentnummer dient te worden toegekend. Meestal gebeurt dit automatisch door het registratiesysteem. Vervolgens dient de organisatie een aantal basisgegevens vast te leggen, zoals tijdstip, gebruiker, verstoorde service of het betrokken apparaat (CI-nummer) en de symptomen.
Na de vastlegging volgt de classificatie. Allereerst wordt het incident ingedeeld in een categorie, bijvoorbeeld netwerk of systeemsoftware. Hierna kan een prioriteit worden toegekend en indien de servicedesk het incident niet direct zelf kan afhandelen, een oplosgroep. Bij het opzetten van categorieën dient rekening te worden gehouden met deze oplosgroepen. Na de classificatie wordt geadviseerd om te onderzoeken of een soortgelijk incident eerder is voorgekomen en of er een oplossing, bijvoorbeeld een workaround, beschikbaar is. In deze fase kan een incident gekoppeld worden aan een problem of known error.
Als een incident door de behandelaar(s) succesvol is opgelost, dient het incidentrecord in het registratiesysteem te worden bijgewerkt en afgesloten. Voor sommige incidenten kan dit overigens enige tijd duren, bijvoorbeeld omdat er eerst een wijziging dient te worden uitgevoerd.

Het doel van incident management is het zo snel mogelijk herstellen van de dienstverlening naar het normale, in de SLA vastgestelde niveau. Tevens levert het incident managementproces belangrijke meetgegevens voor andere ITIL-processen.

##### *3.3.3.1.2 Problem management*

Het doel van problem management is het voorkomen van incidenten. Problem management zoekt naar structurele oorzaken van voorgekomen incidenten en probeert als

zodanig via verbeteringsvoorstellen of correctieve maatregelen nieuwe incidenten te voorkomen. Problem management onderkent drie belangrijke activiteiten.

| | |
|---|---|
| *Probleemcontrole:* | het definiëren en onderzoeken van problemen. |
| *Foutcontrole:* | bewaken van known errors en het doen van wijzigingsvoorstellen (requests for changes). |
| *Managementinformatie:* | rapportages over problemen en resultaten. |

De activiteit ‘identificeren van problemen’, onderdeel van het Problem controlproces, wordt vaak toegekend aan speciale probleemcoördinatoren. Uit de analyse van beschikbare incidentengegevens kunnen organisaties herhalingsincidenten of incidenten met een grote impact destilleren en als problem of known error onderkennen. Ook een tijdens een beveiligingsscan ontdekte zwakke plek in de ICT-infrastructuur kan worden gekenmerkt als een ‘problem’.

Net als bij incidenten kunnen ook problemen worden ingedeeld in categorieën. Bij de indeling wordt geadviseerd ook de impact, urgentie en status van het probleem vast te leggen. Het error controlproces is belast met de bewaking en correctie van de known errors. De hoofdactiviteiten hiervan zijn het initiëren en laten uitvoeren van wijzigingen en vervolgens het evalueren van de wijzigingen. Soms is hierbij sprake van noodoplossingen.

De ITIL-module problem management spreekt verder van een pro-active problem management dat zich concentreert op de kwaliteit van de infrastructuur. Het belangrijkste doel van dit proces is het identificeren van potentiële incidenten. Er wordt onder meer gekeken naar zwakke of overbelaste componenten in de ICT-infrastructuur.

Uit bovenstaande definities valt af te leiden dat de begrippen incident, problem en known error binnen de context van ITIL in een bepaalde verhouding tot elkaar staan. Immers uit de incidentendatabase kan op basis van frequentie en/of impact van incidenten een probleem worden afgeleid. Onderzoek en verdere diagnose leiden tenslotte tot een situatie waarbij oorzaak of oorzaken bekend zijn, inclusief de betrokken configuratie-items.

#### *3.3.3.2. Change- & configuration management*

##### *3.3.3.2.1 Change management*

Change management volgens ITIL beoogt het gebruik van een effectieve en efficiënte methodiek voor de uitvoering en afhandeling van wijzigingen, opdat de negatieve impact op de kwaliteit van de dienstverlening zo gering mogelijk is [ITSM04]. Mede ter voorkoming van storingen, veroorzaakt door de uitvoering van wijzigingen, worden de activiteiten binnen het wijzigingsproces zoveel als mogelijk gestandaardiseerd en worden diverse waarborgen binnen dit proces ingebouwd.

ITIL Change management onderkent een tweetal autoriteiten die betrokken zijn bij de invoering van changes:

| | |
|---|---|
| *Change Manager:* | verantwoordelijk voor de acceptatie en classificatie van alle wijzigingsvoorstellen (requests-for-changes). |
| *Change Advisory Board (CAB):* | gremium dat op geregelde tijdstippen bij elkaar komt om ingediende wijzigingen te bespreken en te autoriseren en uitgevoerde wijzigingen te evalueren. |

Incident management, problem management, service level management, capacity management zijn voorbeelden van ITIL-processen die input kunnen leveren voor het changeproces. Meestal gaat het hierbij om noodzakelijke verbeteringen in de ICT-infrastructuur, bijvoorbeeld het oplossen van de eerder genoemde known errors. Change management heeft een nauwe relatie met configuratiebeheer. Het configuration managementproces dient immers een correcte set configuratie-items aan te leveren waarop het wijzigingsvoorstel van toepassing is. Ook zal de configuration management database (CMDB) moeten worden bijgewerkt na voltooiing van de wijziging.

Een ITIL change managementproces start met het indienen van een request-for-change (RFC). Een RFC bestaat meestal uit een elektronisch formulier met een vaste indeling. Het dient op een door de changemanager voorgeschreven wijze te worden aangeleverd, bijvoorbeeld door het sturen van een e-mail naar een functionele mailbox die wordt beheerd door de changemanager. De RFC bevat hierbij minimaal de volgende punten:

- datum/tijd van de aanvraag
- uniek Identificatienummer
- beschrijving van de betrokken CI's
- voorgestelde wijziging inclusief motivatie
- gewenste termijn van invoering
- naam en adresgegevens van aanvrager.

Na de registratie en indiening beoordeelt de changemanager de aanvraag. Hij controleert hierbij of alle verplichte velden zijn ingevuld en toetst globaal op elementen als noodzaak, werkbaarheid, etc. Eventueel koppelt de changemanager terug met de aanvrager. Afhankelijk van de afspraken die zijn gemaakt, kan de verdere behandeling worden uitgesteld tot het eerstvolgende CAB-overleg. Als de RFC wordt geaccepteerd, wordt het change record door de changemanager bijgewerkt voor wat betreft prioriteit en impact.

Voor elke wijziging wordt urgentie vastgesteld. Hierbij wordt meestal onderscheid gemaakt tussen normale wijzigingen en spoedwijzigingen. De laatste categorie heeft uiteraard voorrang boven de normale, niet-spoedeisende wijzigingen. Het verhelpen van een grote storing of het voorkomen van verdere escalaties van een probleem kan een reden zijn voor hogere prioriteit. Soms betekent dit een extra spoedvergadering van de change advisory board.
De changemanager dient naast prioriteit ook de impact van de change vast te stellen. Hij kijkt hierbij naar de noodzakelijk inspanningen van de ICT-beheerorganisatie en de mogelijke gevolgen voor de dienstverlening. De changemanager let onder meer op doorlooptijd van een wijziging, de hersteltijd van de ICT-dienst na uitvoering van een change, de aanwezigheid van een uitwijkplan, de gevolgen voor capaciteit en performance van de dienstverlening en de benodigde middelen en kosten. Bij wijzigingen

met een hoge impact is meestal zowel de toestemming van de CAB als die van de gebruiker(s) van de betrokken dienst vereist.

Goedgekeurde wijzigingen worden door de changemanager in een (elektronische) changekalender opgenomen. Eventueel conflicterende wijzigingen worden hiermee inzichtelijk gemaakt. Ook kan een te zware belasting van ICT-personeel, betrokken bij de uitvoering van wijzigingen worden voorkomen door middel van het in de tijd spreiden van niet-spoedeisende wijzigingen.

Tenslotte speelt de changemanager een belangrijke rol bij het evalueren van uitgevoerde, of foutgelopen wijzigingen. Hij onderzoekt dan of de juiste, vooraf geplande inspanning is geleverd en of het gewenste resultaat is bereikt. Eventuele, onverwachte problemen worden door de changemanager veelal vastgelegd in een zogeheten post implementation reviewdocument.

#### *3.3.3.2.2 Configuration management*

Configuration management legt gegevens, de zogeheten configuratie-items (CI's), vast om betrouwbare informatie te kunnen leveren over de totale ICT-infrastructuur. Naast de vastlegging van aanwezige systeem- en netwerkcomponenten worden soms ook procedures en onderdelen van de dienstverlening als CI geregistreerd. Alle CI's worden geregistreerd in een configuration management database (CMDB). Een goed ingericht configuration management is meer dan een inventarisatie van aanwezige componenten. Het geeft ook informatie over autorisatie met betrekking tot CI's en hun onderlinge relatie. Naast het eerder genoemde change management speelt de CMDB bij nog enkele ITIL beheerprocessen een belangrijke rol. Problem management maakt bijvoorbeeld gebruik van de database om problems en known errors te koppelen aan CI's. Availability management maakt gebruik van de CMDB om te analyseren welke CI's een bijdrage leveren aan een bepaalde dienst. IT service continuity management gebruikt standaardconfiguraties uit de CMDB om de uitwijkcondities te specificeren en bewaakt vervolgens of deze configuratie ook op de uitwijklocatie aanwezig is.

Een lastig en tegelijk belangrijk aandachtspunt bij configuration management is het bepalen van de mate van detaillering van de vastlegging. Teveel detailinformatie brengt immers een onnodige hoeveelheid werk met zich mee. Dit resulteert onder meer in beslaglegging van menscapaciteit ten behoeve van de actualisatie en het onderhoud van de database. Te weinig informatie daarentegen betekent dat een aantal ITIL-processen niet de beschikking heeft over de vereiste informatie om het proces adequaat en zorgvuldig te laten verlopen.

Iedere configuratie-item is opgebouwd uit zogeheten attributen. Tabel 6 geeft een overzicht van veel voorkomende attributen.

Tabel 6: Configuration Item attributen

| **Attribuut** | **Omschrijving** |
|---|---|
| CI-nummer | Uniek nummer van het configuratie-item |
| Serienummer | Serie-/licentienummer toegekend door leverancier |
| Modelnummer | Uniek model-/catalogusnummer van de leverancier |
| Merk | Fabrikantnaam |
| Categorie | Classificatie: hardware, software, procedure, etc |
| Type | Verdere omschrijving van het CI-type |

| | |
|---|---|
| Locatie | Fysieke locatie van het CI |
| Eigenaar | Functionele eigenaar |
| Bron | Herkomst, bijvoorbeeld naam en adres van de leverancier van het CI |
| Aanschafdatum | Datum van aanschaf of levering aan de organisatie |
| Huidige status | Status van het CI: test, in productie, afbouw, etcetera |
| Aanschafprijs | Koopprijs van het CI |
| RFC/Change | RFC of changenummer dat voor dit CI openstaat |
| Incident/Problem | Incident- of probleemnummer dat voor dit CI openstaat |
| Fysieke relatie | Legt eventuele fysieke relatie met andere CI's vast |
| Logische relatie | Legt eventuele logische relatie met andere CI's vast (bijvoorbeeld relatie tussen uitwijkcomponent en een SLA) |

#### *3.3.3.3. Release Management*

De ITIL-module release management is de opvolger van wat voorheen het software control & distributionproces werd genoemd. Release management beoogt de kwaliteit van de ICT-productieomgeving te waarborgen door gebruik te maken van formele procedures en controles bij de implementatie van nieuwe softwareversies. Binnen release management wordt de zogeheten definitive software library (DSL) bijgehouden. In de DSL dienen alle moederkopieën veilig te zijn opgeslagen. Release management, change management en configuration management werken nauw samen onder meer om zeker te stellen dat na releases de CMDB actueel is. Veel voorkomende categorieën binnen release management zijn:

*Major release:* roll-out van nieuwe hard- of software waarbij vaak sprake is van (aanzienlijke) uitbreiding van de functionaliteit. Een dergelijke release vervangt vaak eerder aangebrachte workarounds.

*Emergency fix:* (tijdelijke) noodoplossing om een problem of known error weg te nemen.

Release management omvat zes basisstappen, zie figuur 14.


Figuur 14*:* fasen in een software release managementproces

ITIL adviseert een releasemanager te benoemen. Een belangrijke taak van deze functionaris is het opstellen van een beleid waarin wordt vastgelegd hoe en wanneer releases worden samengesteld. Vaak wordt er naast een strategisch beleidsdocument een jaar– en/of kwartaalplanning opgesteld waar majeure releases ingepland worden. In het kader van nieuwe releases wordt geïnventariseerd wat de impact van de release op de dienstverlening is en op de benodigde hoeveelheid resources ten behoeve van samenstellen, testen en uitrollen. Na het beleidsmatige voorwerk dient de release gebouwd danwel samengesteld te worden en voor zover mogelijk te worden uitgetest. Ook dienen in deze fase de zogeheten back-outscenario's te worden beschreven, bijvoorbeeld terugkeer naar de oude situatie of uitwijk naar een reserveomgeving. Vervolgens is er de fase van testen en volgt, na het eventueel aanbrengen van wijzigingen in (onderdelen van) de releasecomponenten, installatiescripts of documentatie, de acceptatiefase. In het tweede deel van het proces dient de planning voor de definitieve uitrol te worden gemaakt, tevens de voorbereiding voor de distributie en de communicatie hieromtrent met medewerkers en klanten te worden afgestemd, waarna de uiteindelijke installatie kan worden ingepland en uitgevoerd.

### 3.3.4. De toekomst van ITIL

Of ITIL in haar huidige vorm als best practice blijft voortbestaan is onzeker. De komst [BS1502] van de Britse standaard BS 15000-1:2002[54] en recent de ISO/IEC 20000 (Information technology – service management) en de mogelijkheid om hiervoor een kwaliteitscertificaat te verkrijgen, lijken de aanzet tot een verdere formalisering van de standaardisering van ITIL-gerelateerde beheerprocessen binnen ondernemingen. Ook factoren als uitbesteding van ICT-ontwikkel- en beheeractiviteiten spelen een rol. Vooral in een formele klantleverancierrelatie zal de ICT-dienstverlener geneigd zijn zich meer en meer te concentreren op de service delivery processen.

Beide standaards staan nadrukkelijk stil bij het element incident management. De BS 15000-2 stelt onder meer dat majeure incidenten en de achterliggende organisatie goed gedefinieerd dienen te zijn. Ook gaat de norm in paragraaf 8.2.3 uitgebreid in op het fenomeen spoedwijziging.

### 3.3.5. ASL

Application Services Library (ASL) is de naam voor een publiekdomeinstandaard voor applicatiebeheer. ASL is, net als ITIL, een raamwerk, ontstaan uit een aantal best practices op het terrein van applicatiebeheer. Drijvende kracht achter ASL was de Nederlandse ICT-dienstverlener PinkRoccade. Het raamwerk en de daarbij behorende 'best practices' zijn in 2001 overgedragen aan de ASL-Foundation[55][BAPO04].

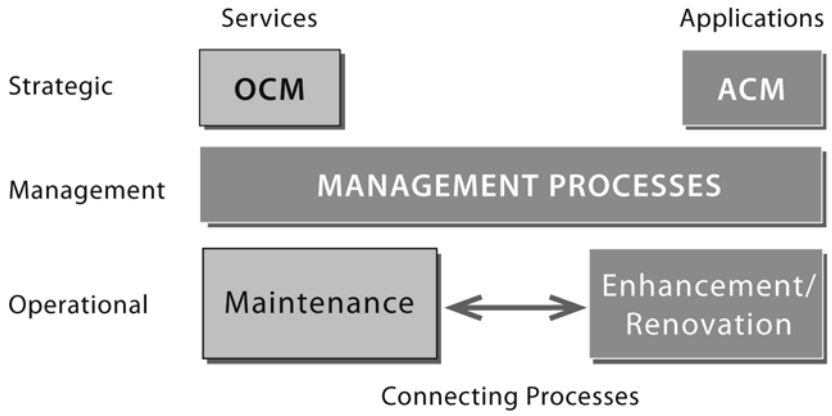
Binnen de ASL-filosofie wordt applicatiebeheer verantwoordelijk gehouden voor instandhouding van de applicatieprogrammatuur en de gegevensbanken (beheer en onderhoud). Het technisch beheer is verantwoordelijk voor de instandhouding van de operationalisering van het informatiesysteem, dat bestaat uit apparatuur, programmatuur

[54] De standaard bestaat uit twee delen: deel 1: specification for service management; deel 2: code of practice for service management.
[55] Zie http://www.aslfoundation.org.

en gegevensverzamelingen [POLS01]. Binnen ASL wordt ITIL beschouwd als de bekendste internationale standaard voor technisch beheer.

De binnen ASL omschreven (beheer)processen lijken deels op ITIL-processen. ASL beschouwt ze echter als gescheiden applicatiebeheerprocessen, vanwege onder meer verschillende eisen en prestatiekarakteristieken. Daar waar ITIL zich meer richt op de infrastructuur, vult ASL het publiek domein voor beheer en onderhoud van applicaties in. Er is volgens de ASL-filosofie sprake van een n-op-m-relatie: technisch beheer kan verschillende applicaties draaien, waarvoor verschillende applicatiebeheerorganisaties verantwoordelijk zijn. Ook de invulling van de processen verschilt. Applicatiebeheer vertaalt de bedrijfswensen en -eisen ten aanzien van een informatiesysteem naar een technische oplossing, die door technisch beheer geëxploiteerd kan worden. Kenmerkend hierbij is de vertaalslag van functionaliteit naar techniek.

Naast het beschrijven van ITIL-achtige processen voor applicatiebeheer, zoals configuratiebeheer, wijzigingenbeheer en capaciteitsbeheer geeft ASL ook een aanzet tot lifecycleprocesmanagement (applications cycle management (ACM)), zie figuur 15. Het ASL-proces organization cycle management (OCM) houdt zich bezig met het vormgeven van de toekomst van de dienstverlening (services) en de inrichting van de applicatiebeheerorganisatie.




Figuur 15: het application services library model

### *3.3.6. Overige standaardisatieontwikkelingen*

Het vakgebied informatiebeveiliging heeft zich de afgelopen 10 jaar verder ontwikkeld. Een aantal universiteiten en hogescholen in Nederland biedt inmiddels het vak als aparte leerstof[56] aan. Ook heeft een aantal standaardisatieorganisaties, in het bijzonder de Internet Engineering Tasc Force (IETF) en de in 1947 opgerichte International Organization for Standardization (ISO), standaarden of richtlijnen op dit terrein laten ontwikkelen. Zo was er reeds in 1991 een IETF RFC 1244[57], getiteld Site Security Handbook. De RFC behandelt diverse aspecten van informatiebeveiliging, gerelateerd aan het Internet. Denk hierbij aan beveiligingsbeleid, identificatie- en autorisatieprocedures, incidentenresponsemechanismen, etc. Ook binnen de Organization

[56] Bijvoorbeeld de tweejarige masteropleiding Information Security bij TIAS-Business School, een samenwerkingsverband tussen de Universiteit van Tilburg en de Technische Universiteit Eindhoven.
[57] RFC 1244 van juli 1991, opgesteld door elf medewerkers, afkomstig van verschillende Amerikaanse universiteiten en enkele soft- en hardwareleveranciers.

for Economic Cooperation and Development (OECD)[58] en ISO heeft informatiebeveiliging de afgelopen jaren een plek verworven.

#### 3.3.6.1. ISO/IEC JTC1 SC27

Joint Technical Committee 1 (JTC1) is een gezamenlijk comité van ISO en de International Electrotechnical Commission (IEC) dat zich bezighoudt met het realiseren van standaarden op het gebied van informatietechnologie. Subcommittee SC27[59] houdt zich specifiek bezig met de standaardisatie van generieke methoden en technieken voor ICT-beveiliging.

Het werkgebied omvat:
- identificatie van generieke eisen voor ICT system security services
- ontwikkeling van securitytechnieken en -mechanismen (incl. registratieprocedures)
- ontwikkeling van securityrichtlijnen (bijvoorbeeld risicoanalyses)
- ontwikkeling van management support documentatie en standaarden (bijvoorbeeld terminologie en security evaluatie criteria).

Eind jaren negentig van de vorige eeuw groeide de belangstelling voor computer security incident response binnen de standaardisatieorganisaties. Zo heeft ISO/IEC JTC1 SC27 in 2004 een 'technisch rapport' uitgegeven onder de titel Information Security Incident Management [ISO04]. In hoofdstuk vijf van dit rapport worden sleutelkenmerken voor een adequaat incidentenbeheer beschreven. Het betreft de kenmerken managementondersteuning, bewustzijn, wet- en regelgeving, operationele efficiëntie, anonimiteit, vertrouwelijkheid en typologie. De standaard gaat onder meer uitgebreid in op de gevolgen én noodzaak van wet-en regelgeving in relatie tot incidentenbeheer.

#### 3.3.6.2. Internet Engineering Task Force

*Inleiding IETF*
De Internet Engineering Task Force (IETF) wordt beschouwd als de protocol engineering and development arm of the Internet[60]. Binnen de IETF worden jaarlijks vele, vooral technische standaarden ontwikkeld en bekrachtigd. De IETF is formeel opgericht door de Internet Architecture Board (IAB) in 1986. Ze omvat een grote internationale gemeenschap van netwerkontwerpers, operators, leveranciers en onderzoekers, betrokken bij de verdere ontwikkeling van de architectuur en het operationeel beheer van het Internet. De IETF is een open organisatie: ieder individu kan zich aansluiten[61]. Communicatie binnen de IETF vindt hoofdzakelijk plaats via mailinglijsten (e-mail). De IETF houdt driemaal per jaar een bijeenkomst. Het daadwerkelijke werk in IETF-verband wordt gedaan in werkgroepen met een bepaald aandachtsgebied zoals routing, transport en security. Iedere werkgroep wordt geleid door een zogeheten area director. Deze directors zijn lid van de Internet Engineering Steering Group (IESG). IETF, IAB en IESG maken onderdeel uit van de wereldwijde Internet society (ISOC). De ISOC is een

[58] Zie bijvoorbeeld de 'OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security', geadopteerd als aanbeveling van de OECD-Council tijdens zijn 1037ste sessie op 25 juli 2002.
[59] Zie http://www.din.de/ni/sc27 (website secretariaat ISO/IEC JTC1/SC27).
[60] zie http://www.ietf.org/glossary.html.
[61] Aldus IETF RFC 3160, TAO of IETF, versie augustus 2001 door S. Harris.

professionele organisatie met meer dan honderdvijftig organisaties en elfduizend individuele leden in ruim hondertachtig[62] landen. Haar belangrijkste taken zijn het adresseren van onderwerpen die de toekomst van het Internet raken en het faciliteren van de eerdergenoemde drie task forces. De ISOC is gehuisvest in Reston U.S.A.

*IETF RFC 2350*
Een poging beleid, taken en inrichting van incidentenresponseteams verder te standaardiseren is de introductie van IETF RFC[63] 2350, getiteld Expectations for Computer Security Incident Response uit 1998. De RFC spreekt niet meer van een computer emergency response team (CERT), een tot die tijd gangbare benaming, maar van een computer security incident response team (CSIRT). Dit heeft vermoedelijk te maken met het feit dat de term Computer Emergency Response Team auteursrechtelijk is beschermd.
Volgens de IETF RFC dient iedere CSIRT een duidelijk beleid kenbaar te maken inzake het type incidenten dat in behandeling wordt genomen en het niveau van ondersteuning hierbij. Om de vertrouwelijkheid van de melder te garanderen, dient de CSIRT naast het voeren van een geheimhoudingsbeleid een betrouwbaar en veilig communicatiekanaal ter beschikking te stellen. In de IETF RFC wordt aanbevolen gebruik te maken van gangbare mechanismen, zoals het beveiligen van e-mail berichten met S/MIME of PGP.

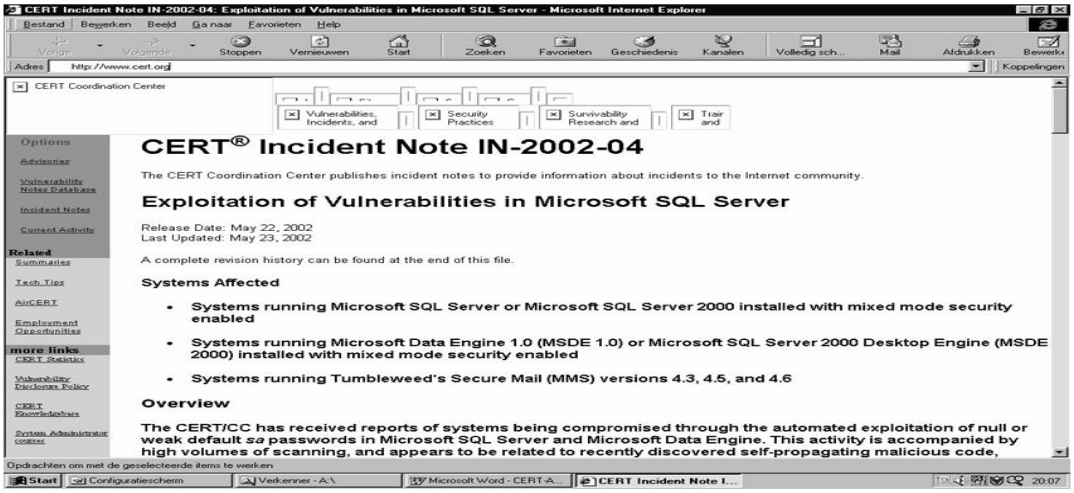
De diensten van een CSIRT worden in de IETF RFC gesplitst in twee hoofdgroepen:

- real-time activiteiten, direct gerelateerd aan de hoofdtaak incidentenresponse
- non real-time proactieve activiteiten, ondersteunend aan de hiervoor genoemde taak.

Incidentenresponse wordt binnen de RFC uitgewerkt in incident triage, incident coordination en incident resolution. Een belangrijk aspect bij incident triage is het vaststellen of een incident werkelijk heeft plaatsgevonden en, na een bevestiging, het bepalen van de omvang. Incident coordination omvat het categoriseren van het aan het incident gerelateerde informatie met betrekking tot het geheimhoudingsbeleid. Hierbij is te denken aan logfiles, contactinformatie, etc. In dit stadium worden ook andere betrokken partijen geïnformeerd. Dit alles uiteraard onder de uitgangspunten en voorwaarden van het eerder genoemde beleid. De IETF RFC geeft bij incident resolution drie gangbare diensten: technische assistentie, inclusief analyse van het gecompromitteerde systeem, eradication[64]en herstel. Onder eradication wordt verstaan het elimineren van de oorzaak van het incident en zijn effect. Veelal gebeurt dit door het installeren van een fix of het wijzigen van instellingen om de kwetsbaarheid weg te nemen.

De andere CSIRT-hoofdtaak wordt samengevat onder de noemer pro-actieve activiteiten. Er worden vijf voorbeelden genoemd: informatievoorziening over bekende kwetsbaarheden en tegenmaatregelen (zie een voorbeeld in figuur 16), waaronder het bijhouden van een historiedatabase, hulpmiddelen voor audits, scholing en training, productevaluatie en advies.

[62] Stand van zaken per december 2002.
[63] Request for Comments van de Internet Engineering Task Force.
[64] Letterlijk vertaald: ontworteling.




Figuur 16: Incident Note van het CERT Coordination Center

### *3.3.6.3. TERENA: TF-CSIRT*

De Trans-European Research and Education Networking Association (TERENA) werd opgericht in oktober 1994 door een samenvoeging van de organisaties RARE (Réseaux Associés pour la Recherche Européenne) en EARN (European Academic and Research Network). Een van de belangrijkste doelstellingen[65] van TERENA is het promoten van en participeren in activiteiten ter promotie en ontwikkeling van een hoog gekwalificeerde internationale informatie- en telecommunicatie-infrastructuur ten behoeve van onderzoek en onderwijs.

Onder de vlag van het technische programma van TERENA is de taskforce TF-CSIRT opgericht teneinde de samenwerking tussen computer security incident response teams in Europa en naburige landen te bevorderen.

De doelstellingen van TF-CSIRT zijn:

- het leveren van een forum voor het uitwisselen van kennis en ervaring
- het oprichten van pilotdiensten ten behoeve van de Europese CSIRT-gemeenschap
- het promoten van gemeenschappelijke standaarden en procedures voor het beantwoorden van incidenten
- het ondersteunen van de oprichting van nieuwe CSIRT's en het trainen van CSIRT-medewerkers.

Het project *IODEF*[66] betreft een van de grootste TF-CSIRT-activiteiten. Het project had tot doel het ontwikkelen van formaten voor het vastleggen en uitwisselen van berichten met betrekking tot incidentgegevens. Verder *Trusted Introducer for CSIRTs*, een accreditatiedienst om nieuwe CSIRT's toegang te geven tot het Web of Trust van de

[65] zie http://www.terena.nl.

[66] incident object description and exchange format requirements, zie ook IETF RFC 3067 en [ARVI02]. TERENA's IODEF-activiteiten zijn in 2002 overgenomen door de IETF-werkgroep INCH (Extended Incident Handling).

gemeenschap van CSIRT's in Europa en *TRANSITS,* een driejarig Europees project om het probleem van het tekort aan gespecialiseerde CSIRT-medewerkers te adresseren.

#### *3.3.6.4. Initiatieven Europese Commissie*

De afgelopen jaren zijn er vanuit de Europese Commissie verschillende initiatieven gelanceerd die direct of indirect samenhangen met informatiebeveiliging, De activiteiten vallen uiteen in een drietal categorieën [COLF04]:

| | |
|---|---|
| *Juridisch raamwerk:* | de Europese Commissie heeft een stelsel van richtlijnen geformuleerd die moeten zorgen voor een balans tussen enerzijds het beschermen van burgers en anderzijds het beschermen van de infrastructuur en informatiesystemen[67]. |
| *Promotie van informatiebeveiliging:* | het lanceren van een aantal beleidsinitiatieven met als doel het promoten van de verbetering van netwerk- en informatiebeveiliging. Voorbeelden zijn te vinden in de twee 'e-Europe Action Plans' en de oprichting van een nieuw agentschap, het European Network and Information Security Agency (ENISA)[68]. |
| *Onderzoek:* | in het kader van het Information Society Technology raamwerkprogramma wordt onderzoek en ontwikkeling van netwerk- en informatiebeveiliging ondersteund, inclusief hieraan gerelateerde standaardisatie-activiteiten[69]. |

De verwachtingen met betrekking tot ENISA bleken hooggespannen op het E-Security EU2004-congres van 27 en 28 oktober 2004 te Amsterdam. Op 13 december 2003 besloten de regeringsleiders tijdens de Eurotop in Brussel het agentschap te vestigen in Griekenland. De tweede helft van 2004 en een belangrijk deel van 2005 werd vooral gebruikt voor het opstellen van een werkprogramma en het operationaliseren van het agentschap. Eind 2005 werden drie ad-hocwerkgroepen ingericht die een belangrijke aanzet moesten vormen voor het uitvoeren van ENISA's doelstellingen. De vier doelstellingen van ENISA zijn:

---

[67] Zo heeft in 2002 de Commissie een kaderbesluit ingediend bij de Europese Raad inzake ongeoorloofde aanvallen op informatiesystemen, dat als belangrijkste doelstelling had het harmoniseren van het strafrecht van de lidstaten op het gebied van aanvallen op informatiesystemen (waaronder hacking) en te zorgen voor een optimale politiële en justitiële samenwerking op het gebied van de bestrijding van strafbare feiten die verband houden met aanvallen op informatiesystemen. Daarnaast is de 'directive on electronic signatures' een andere belangrijke pijler van het juridische raamwerk.

[68] Verordening (EG) Nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004, zie ook http://www.enisa.eu.int.

[69] In het zesde Framework Programme van de Europese Unie is ongeveer honderdvijftig miljoen euro gealloceerd voor onderzoek naar: 'security, dependability, privacy & digital asset management'.

1. adviseren en assisteren van de Commissie en de lidstaten op het terrein van informatiebeveiliging en in hun dialoog met de industrie om beveiligingsgerelateerde problemen in hardware- en softwareproducten te adresseren

2. verzamelen en analyseren van beveiligingsincidenten en opkomende risico's in Europa

3. promoten van risicoanalyses en risicoanalysemethoden

4. verhogen van het bewustzijn van en de samenwerking tussen actoren in het informatiebeveiligingsspeelveld, onder meer door het ontwikkelen van publiek-private samenwerking op dit terrein.

### *3.4. Managed Security Services*

Het aantal bedrijven dat operationele ICT-beveiligingsactiviteiten uitbesteedt aan zogeheten managed security services providers (MSSP) is groeiende. Een Gartner-analist voorspelde op Gartner's ICT-security summit van september 2004 dat in 2005 zestig procent van het bedrijfsleven tenminste 'één perimeter securitytechnologiecomponent' zou uitbesteden. Het succesverhaal van de MSSP's is begonnen in de Verenigde Staten waar vooral grote multinationals met complexe, wereldwijde ICT-infrastructuren delen van hun ICT-beveiligingsbeheer uitbesteden [BERG04]. Richtte de MSSP dienstverlening zich aanvankelijk op het verzorgen van ICT-netwerksecuritybeheer, zoals virusdetectie, firewallbeheer en intrusion detection, tegenwoordig kan vrijwel elke ICT-beveiligingsactiviteit worden uitbesteed, waaronder ook autorisatiebeheer en de ICT-gerelateerde aspecten van Business Continuity Management zoals ICT-uitwijkvoorzieningen.

Verhoging van de dienstverlening, waaronder een zeven-maal-vierentwintig-uur-bemensing, gebrek aan specialistische kennis en menscapaciteit in de eigen organisatie kunnen argumenten zijn om ICT-beveiliging uit te besteden. Andere, meer generieke uitbestedingsargumenten zijn [BEUL04]: vergroting van de flexibiliteit, toegang tot nieuwe technologieën, verlaging van de kosten en betere voorspelbaarheid van kosten. Nadelen bij uitbesteding zijn er ook, zoals het probleem van het waarborgen van de vertrouwelijkheid van gegevens en de afhankelijkheid van de leveranciers.

Traditionele objecten voor ICT-uitbesteding zijn werkplekbeheer, netwerkbeheer, rekencentra en ontwikkelactiviteiten [HAPE01]. Hoewel het besluit tot uitbesteding meestal een bedrijfseconomische afweging is, wordt als uitgangspunt vaak gehanteerd dat de uitbesteding het bestaande beveiligingsniveau niet mag verminderen [BAHA01]. Bij het uitbesteden van ICT-diensten speelt vooral service level management een cruciale rol. Dit beheerproces dient te zorgen voor duidelijke en reële afspraken tussen leverancier en afnemer in de vorm van een service level agreement (SLA). In de SLA worden onder meer de afspraken vastgelegd over aard, omvang en kosten van de te leveren ICT-diensten. Daarnaast is het van belang dat in de SLA de eisen ten aanzien van informatiebeveiliging worden beschreven, zoals, responsetijden van de server, beschikbaarheid van het netwerk, uitwijkvoorzieningen en afscherming van vertrouwelijke gegevens [FRLV05].

Bij de selectie van een managed security service provider spelen meestal de volgende vijf criteria [ISS00]:

- beveiligingskennis en reputatie
- compatibiliteit met bestaande apparatuur
- dienstverlening en ondersteuning
- financiële stabiliteit
- breed scala aan virtual private networks[70] en beveiligingsdiensten.

### *3.4.1. Security Operations Center (SOC)*

Een aantal MSSP's heeft zijn internationale activiteiten ondergebracht in een of meer zogeheten security operations center(s). Vanuit een centrale operations room worden ICT-componenten van klanten permanent gemonitord op de aanwezigheid of dreiging van kwetsbaarheden, indringers of kwaadaardige code [SCHE01]. Hiertoe worden alarmberichten van detectoren of sensoren gefilterd en nader geanalyseerd. Het SOC waarschuwt bij acute dreiging de betreffende klant en neemt, afhankelijk van de overeengekomen dienstverlening, maatregelen om het incident te stoppen of te verminderen.

[70] Een virtual private network (VPN) is een dynamisch gebouwde, beveiligde netwerkverbinding tussen twee computersystemen waarbij gebruik wordt gemaakt van ingekapselde versleutelingsmethoden.