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

Hafkamp, W.H.M.

Publication date
2008

7. Referentiemodel

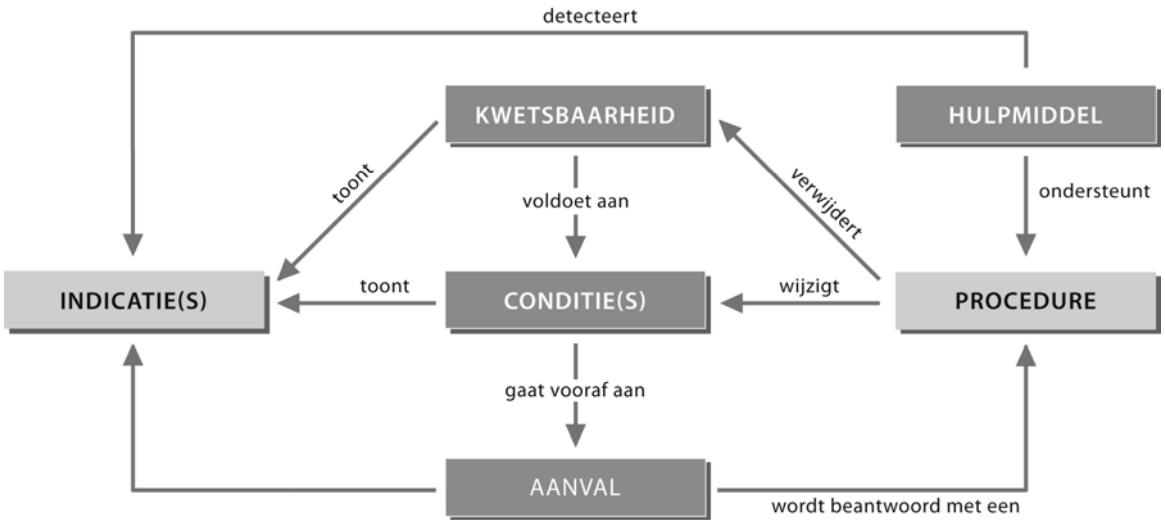
In dit hoofdstuk worden, afgeleid van de bevindingen en conclusies uit het onderzoek, aanbevelingen gedaan voor het optimaliseren van kwetsbaarheden- en incidentenresponseprocessen binnen op ITIL georiënteerde ICT-organisaties [HAFK06].

7.1. Inleiding

Grotere organisaties met een of meer ICT-beheerafdelingen hebben hun incidentenafhandelingsproces meestal sterk gestandaardiseerd, waarbij de uitvoering volgens formele processen verloopt. Soms worden aan ICT-beveiliging gerelateerde incidenten specifiek gelabeld en behandeld. Wanneer een incident niet direct kan worden afgehandeld, of er dreigt een herhaling, dan krijgt het de status van probleem of bij een majeure impact de status van calamiteit. Het opschalen van de classificatie heeft consequenties voor het aantal betrokken functionarissen en impact op diverse ICT-beheerprocessen en de totale doorlooptijd van de afhandeling.

Informatie met betrekking tot een *kwetsbaarheid* wordt meestal anders beantwoord dan informatie met betrekking tot een zich manifesterend incident. De ITIL-beheerprocessen, zoals incident- en probleembeheer, bieden hiertoe onvoldoende handvatten. Met name het binnen de ICT-beheeromgeving gestructureerd analyseren en prioriteren van informatie afkomstig van externe bronnen, wordt in onvoldoende mate op een procesmatige wijze uitgevoerd [NICO04].

Figuur 21 laat zien dat kwetsbaarheden en incidenten aan elkaar gerelateerd zijn middels indicaties, condities en procedure. Zo zal een hacker bij een aanval meestal gebruik maken van een of meerdere kwetsbaarheden om de aanval voor te bereiden en uit te voeren.



Figuur 21: relaties tussen een kwetsbaarheid en een incident

Condities

Dit zijn voorwaarden met betrekking tot een aanval. Pas als deze voorwaarden zijn vervuld kan een aanvalspoging kans van slagen hebben. Voorbeeld: voor het uitnutten van een kwetsbaarheid kan het noodzakelijk zijn dat een aanvaller zich eerst authenticeert op het aan te vallen systeem.

Indicaties
Dit zijn symptomen, bijvoorbeeld bepaalde (status)kenmerken van een computersysteem, die een kwetsbaarheid of geslaagde aanval zichtbaar maken danwel aangeven of de condities hiertoe aanwezig zijn.

Het gebruik van adequate hulpmiddelen bij ICT beveiliging is essentieel. *Hulpmiddelen* ten behoeve van kwetsbaarheden- en incidentenresponse kunnen daarom worden gebruikt voor het:

- detecteren en wegnemen van een kwetsbaarheid(svoorwaarde)
- detecteren van een aanval(spoging)
- ondersteunen van bewijsvergaring
- bevorderen van herstel na een aanval.

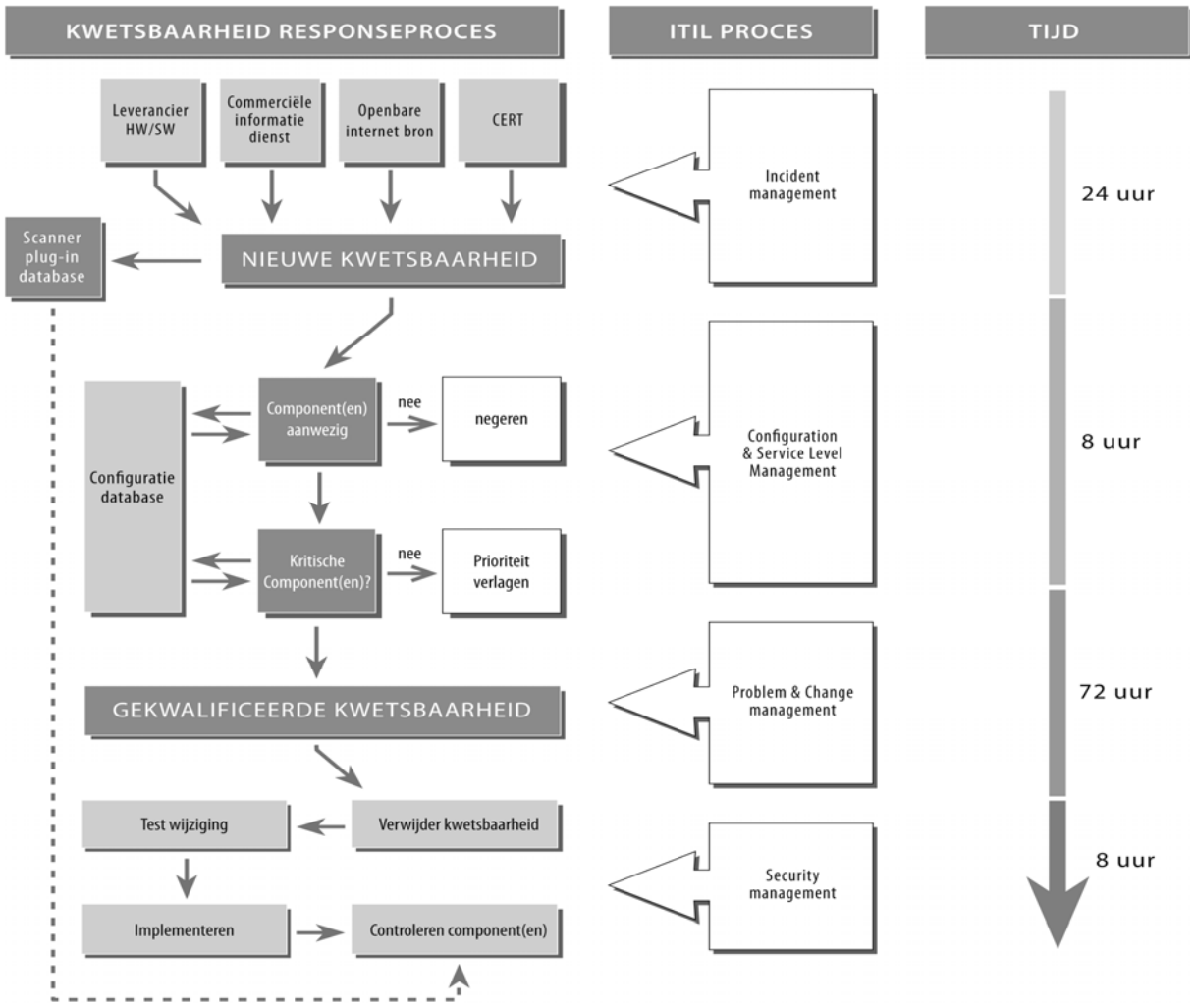
Bij *Procedures* dient in dit kader onderscheid gemaakt te worden tussen preventie-, detectie- en herstelprocedures. Een voorbeeld van een detectieprocedure is het gestructureerd zoeken naar bekende kwetsbaarheden op systemen in het interne netwerk. Het verwijderen van potentiële of geconstateerde kwetsbaarheden is een voorbeeld van een preventieprocedure. Het zoeken naar sporen van een aanval, het veiligstellen van bewijsmateriaal, al dan niet met hulp van speciale programmatuur, en het vervolgens weer operationeel maken van een systeem is een voorbeeld van een gecombineerde detectie- en herstelprocedure.

7.2. Uitgangspunten

Een belangrijk uitgangspunt is dat bestaande beheerprocessen zoveel mogelijk worden ingebed in het nieuwe procesmodel. Uit het onderzoek is gebleken dat ICT-incidenten volgens vaste op ITIL gebaseerde procedures worden afgehandeld. Ook voor het behandelen van externe kwetsbaarhedeninformatie dienen vaste processen en procedures te worden ingericht. Hierbij is het van belang om aansluiting te zoeken bij de ITIL-processen Incident Management, Problem Management, Change Management, Configuration, Service Level Management en Security Management.

De processen zoals beschreven in de paragrafen 7.1 tot en met 7.3, zijn niet of zeer beperkt bruikbaar voor het wegnemen van interne configuratiefouten of fouten in zelf ontwikkelde programmatuur. Het organiseren van interne securityaudits, testen en het beoordelen van programmacodes zijn aanbevolen methoden om dergelijke kwetsbaarheden op te sporen.

7.3. Kwetsbaarhedenresponse



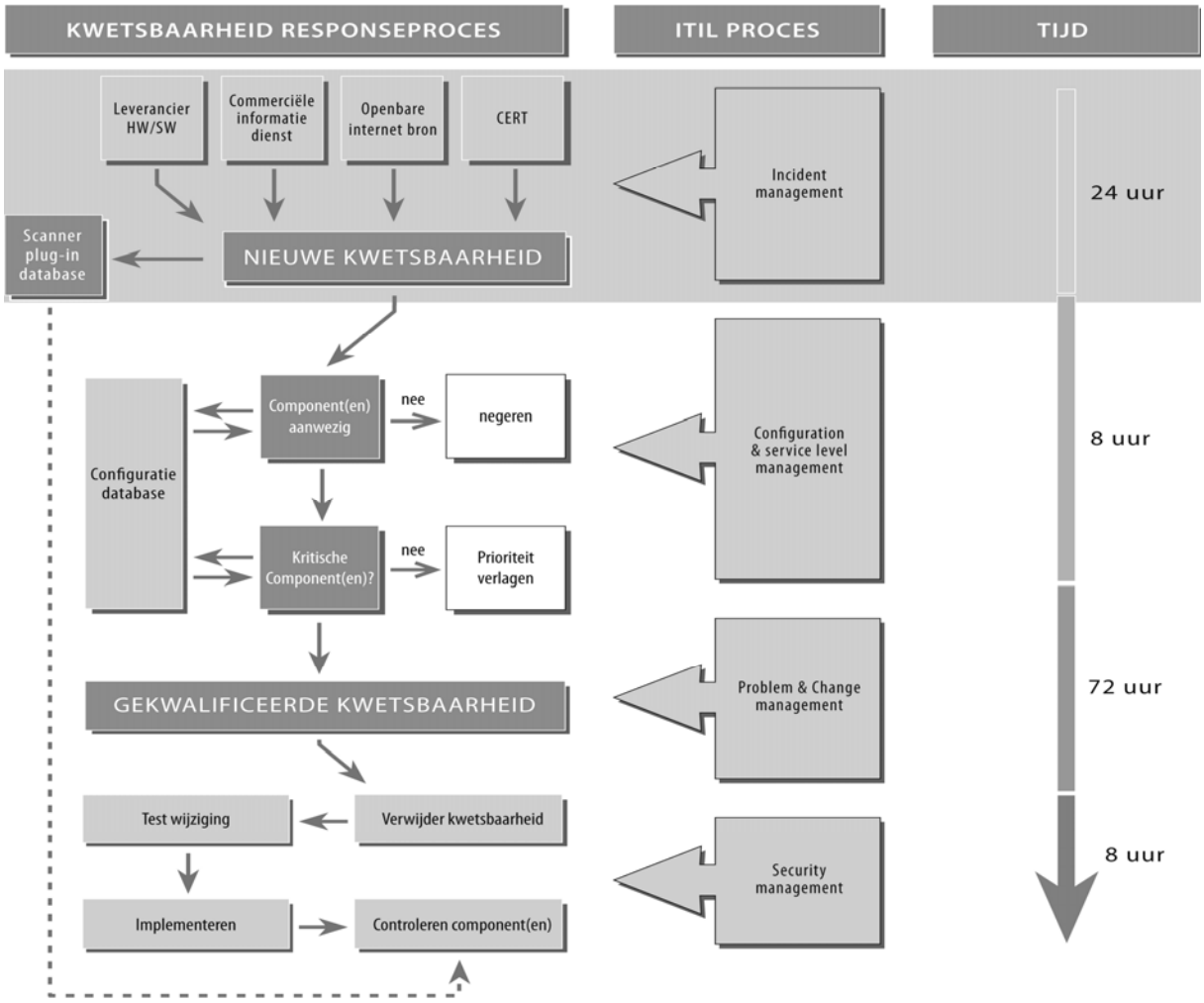
Figuur 22: processchema afhandeling externe kwetsbaarhedeninformatie

Externe kwetsbaarhedeninformatie komt meestal via verschillende informatiekanalen bij de verschillende ICT-medewerkers binnen, zoals ICT-beveiligingfunctionarissen en systeem- en netwerkbeheerders. Ook is vaak sprake van meerdere externe informatiebronnen. De inhoud van de berichten verschilt qua structuur en detailniveau. Door gebruik te maken van een aantal bestaande op ITIL gebaseerde ICT-beheerprocessen is het mogelijk om de berichten gestructureerd te analyseren en te filteren en eventuele vervolgacties te plannen, waarbij het streven is om de levenscyclus van de kwetsbaarheid binnen een organisatie zo kort mogelijk te houden.

Figuur 22 geeft een procesmodel met een totale, maximale, doorlooptijd van honderdentwaalf uur per enkel kwetsbaarheidsbericht. Bij een zevenmaal vierentwintig uur per week aanwezig ICT-beheerproces kan een kwetsbaarheid daarmee binnen vijf dagen na de melding gecontroleerd worden weggenomen. De gehanteerde tijdseenheden

zijn indicatief, gebaseerd op eigen werkervaringen, en zijn getoetst bij drie leden van het International Information Integrity Institute (I-4)[131].

7.3.1. Informatieverzameling



Figuur 23: informatieverzameling (fase 1)

De eerste processtap betreft het selecteren van de informatiebronnen (figuur 23). Een groot deel van de informatie is gratis verkrijgbaar. Zo informeren softwareleveranciers hun klanten (periodiek) over nieuwe kwetsbaarheden en mogelijkheden om deze kwetsbaarheden weg te nemen. Ook zijn er diverse websites op het Internet te vinden waar informatie is te verkrijgen over nieuwe kwetsbaarheden. Verder kan een organisatie zich abonneren op commerciële waarschuwingsdiensten.

Geadviseerd wordt terughoudend om te gaan met het aantal informatiebronnen en deze te beperken tot:

- leveranciers van de in de organisatie aanwezige hard- en software
- maximaal twee externe waarschuwingdiensten.

[131] Meer informatie over I-4 is te vinden op http://www.i4online.com.

Een goede analyse van de berichten vereist dat elk bericht voldoet aan een zeker kwaliteitsniveau. De volgende aspecten zijn van belang:

Tabel 17: kwaliteitskenmerken kwetsbaarheidbericht

Kenmerk	**Omschrijving**
Tijdigheid	De kwetsbaarheid dient voorzien te zijn van een datum. Het bericht bevat verder de (vermoedelijke) ontsluitingsdatum van de kwetsbaarheid.
Betrouwbaarheid	De kwetsbaarheid wordt gemeld door een vertrouwde bron.
Opmaak	In verband met een snelle, mogelijk geautomatiseerde, opvolging binnen de organisatie bevat het bericht een vaste indeling en opmaak.
Impact	Het bericht geeft aan waartoe de kwetsbaarheid kan leiden, zoals het verkrijgen van ongeautoriseerde toegang, onbeschikbaarheid van een systeemcomponent, etc.
Complexiteit	Het bericht geeft een omschrijving van de mogelijkheden en omstandigheden de kwetsbaarheid uit te nutten. - Omgeving: in het bericht staat of fysieke toegang noodzakelijk is om de kwetsbaarheid uit te nutten; - Exploit: het bericht vermeldt of er reeds een 'exploit' is waargenomen.
Oplossing	Het bericht geeft aan of en zo ja welke oplossingen er zijn om de kwetsbaarheid (deels) weg te nemen. Indien er sprake is van herstelsoftware, vermeldt het bericht waar deze te verkrijgen is.
Testen	Het bericht geeft weer of de oplossing is getest en wat het resultaat van deze test was.

CVSS

In 2005 is in FIRST verband gestart met de ontwikkeling van een wereldwijd 'Common Vulnerability Scoring System (CVSS)'. Het nog in ontwikkeling zijnde CVSS vervult een belangrijk deel van de hierboven genoemde kwaliteitsaspecten. Het doel van CVSS is het in samenwerking met de ICT-industrie ontwikkelen van een open standaard voor het classificeren van kwetsbaarheden. CVSS gaat uit van drie zogeheten vulnerability metrics waarbij de impact van een kwetsbaarheid aan de hand van bepaalde karakteristieken wordt gemeten en gewogen. De eerste zogeheten basis-metrics-groep wordt eenmalig vastgesteld door de leverancier van het ICT-product waarin een kwetsbaarheid is ontdekt. De groep bestaat uit zes elementen:

Access vector — Bepalend bij dit element is of de kwetsbaarheid op afstand is uit te nutten of dat lokale toegang noodzakelijk is.

Access complexity — Hier wordt beoordeeld hoe complex de uit te voeren aanval is wanneer eenmaal toegang is verkregen tot een doelsysteem.

Authentication — De te beantwoorden vraag bij dit element is of een aanvaller zich dient te authenticeren op een doelsysteem om de kwetsbaarheid uit te kunnen nutten.

Confidentiality impact — Dit element geeft aan welke impact ontstaat op de vertrouwelijkheid van de informatie na het uitnutten van de kwetsbaarheid op een doelsysteem.

Integrity impact	Dit element geeft aan welke impact ontstaat op de integriteit van de informatie na het uitnutten van de kwetsbaarheid op een doelsysteem.
Availability impact	Dit element geeft aan welke impact ontstaat op de beschikbaarheid van de informatie na het uitnutten van de kwetsbaarheid op een doelsysteem.

Aangezien er zich gedurende de levenscyclus van een kwetsbaarheid gebeurtenissen kunnen voordoen die de dreiging van een kwetsbaarheid veranderen, bestaat er naast de basis-metrics-groep een tijdelijke-metrics-groep. Deze groep bevat de elementen waarschijnlijkheid van uitnutting (exploitability), herstelmogelijkheden (remedation level) en de mate waarin technische aspecten van de kwetsbaarheid openbaar zijn (report confidence). Tenslotte onderkent CVSS een zogeheten omgeving-metrics-groep waarbij de gebruiker zelf vaststelt wat het potentieel aan mogelijke schade is voor de eigen organisatie[132].

Voor elk element dient een vast bepaalde waarde te worden aangegeven. Confidentiality impact kent bijvoorbeeld drie eindwaarden: niet, gedeeltelijk en volledig. De waarde wordt via een berekening vertaald naar een score waarbij nul de laagste en één de hoogste score is. Het bepalen van een eindscore begint met het vaststellen van de totale score voor de basis-metrics-groep. De scores van de tijdelijke- en omgeving-metrics-groep verhogen of verlagen deze score.

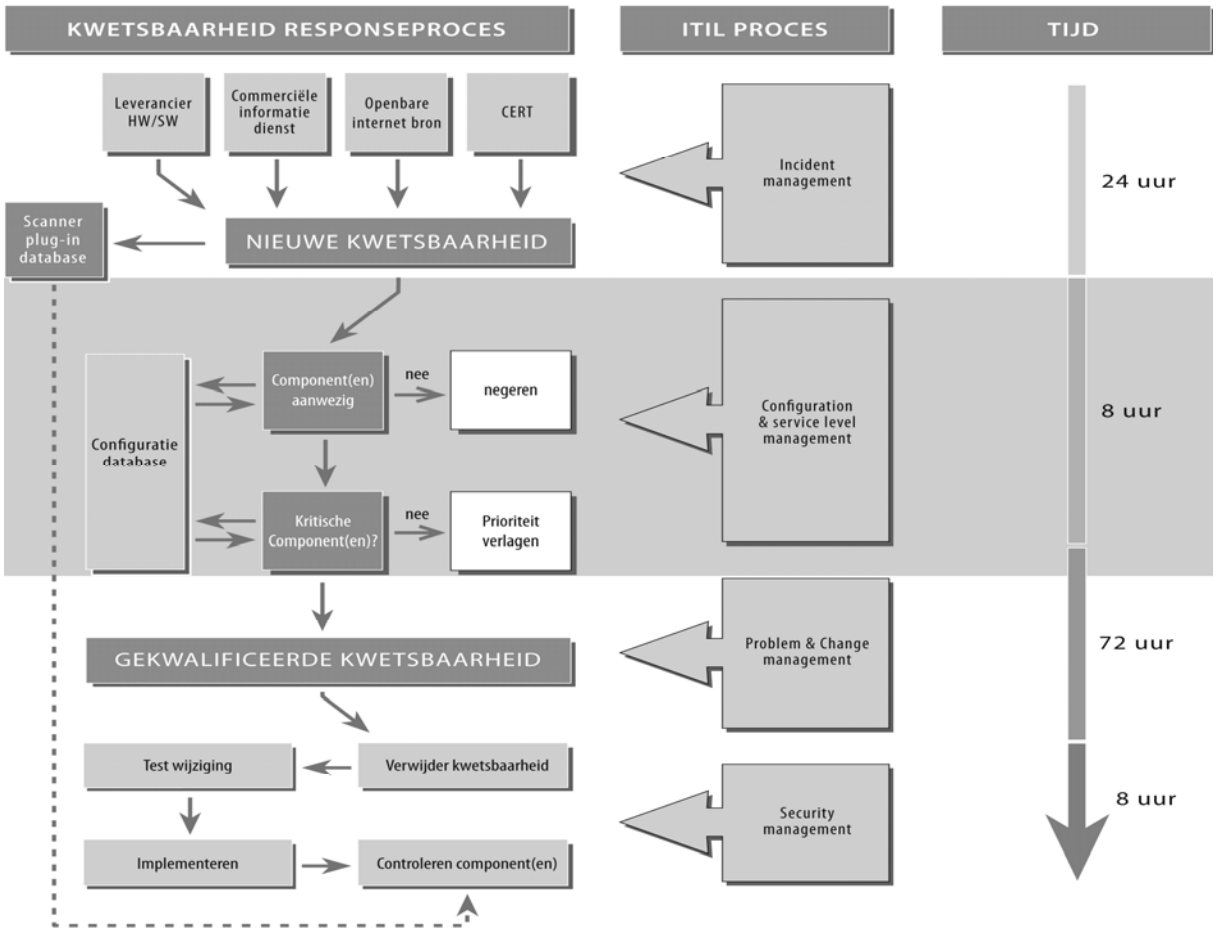
CVSS is een nieuw initiatief voor het classificeren van kwetsbaarheden en kan in zekere zin worden beschouwd als een alternatief voor de bekende en veel gebruikte CVE classificatie van MITRE. CVSS gaat echter verder, omdat het meerdere metrics omvat waarbij een deel van de klassen afhankelijk is van de lokale omstandigheid van een gebruiker en waarbij de waarden in de loop der tijd kunnen veranderen.

Het succes van CVSS wordt enerzijds bepaald door het toepassen van het schema door de ICT industrie en anderzijds door de acceptatie bij (eind)gebruikers.

Registratie
Elk bericht wordt na ontvangst door de ontvanger, meestal de ICT-beveiligingfunctionaris, opgenomen met een uniek nummer en een (CVE- of CVSS-) titel in het ITIL-incidentenregistratiebestand van de organisatie met als label ‘kwetsbaarheid’ en status ‘ongekwalificeerd’. Eventueel nieuwe berichten die betrekking hebben op dezelfde kwetsbaarheid kunnen nu worden geadresseerd, waarbij een nieuw bericht wordt verworpen omdat het geen extra informatie oplevert danwel wordt verwerkt in het incidentenregistratiebestand omdat het gaat om additionele informatie.
Tegelijkertijd dient de ICT-beveiligingfunctionaris ervoor te zorgen dat de vulnerability scanner wordt voorzien van de signatuur van de nieuwe kwetsbaarheid door deze te downloaden van de site van de leverancier van de scansoftware.

[132] Parameters zijn Collateral Damage Potential en Target Distribution.

7.3.2. Informatieanalyse



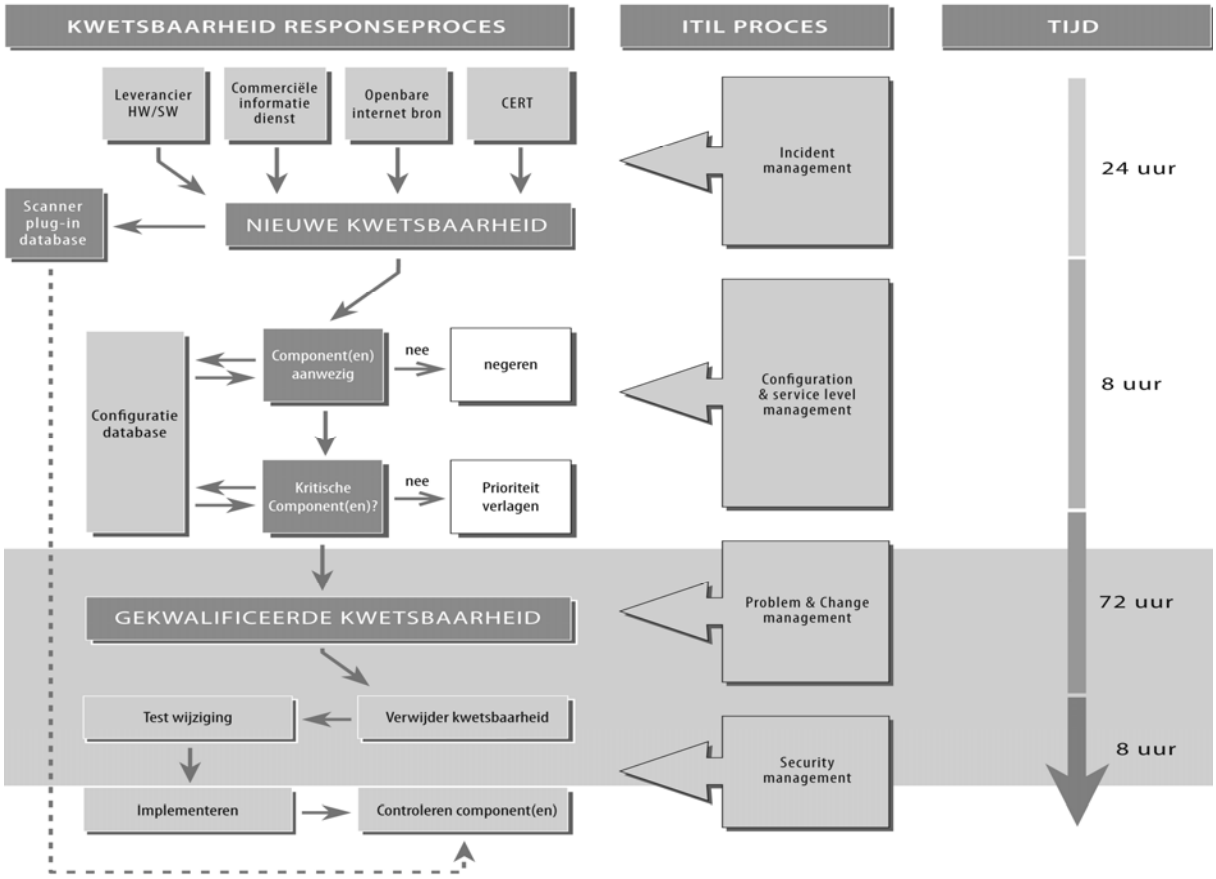
Figuur 24: 'informatieanalyse (fase 2)'

Figuur 24 toont de tweede fase van het procesmodel voor het afhandelen van kwetsbaarhedeninformatie. In deze fase wordt bepaald of de kwetsbaarheidsinformatie in behandeling wordt genomen en, indien dit het geval is, met welke prioriteit. De fase bestaat feitelijk uit twee handelingen. Allereerst wordt bepaald of er ICT-componenten in de infrastructuur aanwezig zijn die gevoelig zijn voor de kwetsbaarheid en vervolgens wordt de mate waarin de ICT-componenten van belang zijn voor de ondersteunde businessprocessen, geverifieerd. Indien uit de eerste handeling blijkt dat de component niet aanwezig is, wordt het responseproces gestaakt. Geadviseerd wordt om het bericht op te nemen in een historiebestand en het incidentnummer te sluiten. Is de component echter wel aanwezig in de infrastructuur dan dient met behulp van informatie uit de configuratiedatabase vastgesteld te worden hoe 'kritisch' de component is voor de organisatie. Voorwaarde is dat elk configuration item in de configuratiedatabase is voorzien van een waardenclassificatie[133]. Is dit niet mogelijk of te complex voor de organisatie dan is het indelen van componenten in de drie categorieën infrastructuur, applicatieserver en overig een alternatieve benadering. Op basis van deze plaatsbepaling wordt het belang van de component(en) voor de organisatie dus gecontroleerd en daarmede de prioriteit van de behandeling van het kwetsbaarheidsbericht bepaald.

[133] Bijvoorbeeld een classificatie waarbij het niveau van beschikbaarheid, integriteit en vertrouwelijkheid middels overeengekomen service level agreements is vastgesteld.

Na de ontvangst en registratie van het bericht en de daaropvolgende analyse wordt het bericht van ongekwalificeerd in het incidentenregistratiebestand door de ICT-beveiligingfunctionaris bijgewerkt tot een gekwalificeerde kwetsbaarheid.

7.3.3. Wijzigingsproces



Figuur 25: 'verwijderen kwetsbaarheid (fase 3)'

Wanneer er sprake is van een of meer kritische componenten en er bovendien sprake is van een risicovolle kwetsbaarheid dan dient via het bestaande change managementproces een spoedwijziging te worden aangevraagd. Tegelijkertijd dient de security patch te worden opgehaald bij de leverancier. Indien er (nog) geen patch beschikbaar is, worden andere in het kwetsbaarheidbericht aangegeven beschermingsmaatregelen voorbereid[134]. Een belangrijk element in deze fase is het testen van de security patch of een andere beschermingsmaatregel, zie figuur 25. Wanneer de betrokken component zich in een sterk gestandaardiseerde infrastructuuromgeving bevindt en er naast de productieomgeving sprake is van een identieke testomgeving, zal het testen een relatief eenvoudig proces zijn. Bij een positief testresultaat kan de patch op grote schaal middels een patchmanagementsysteem geautomatiseerd worden uitgerold. Er zijn verschillende soorten patchmanagementsystemen. Patchmanagementsystemen die werken met

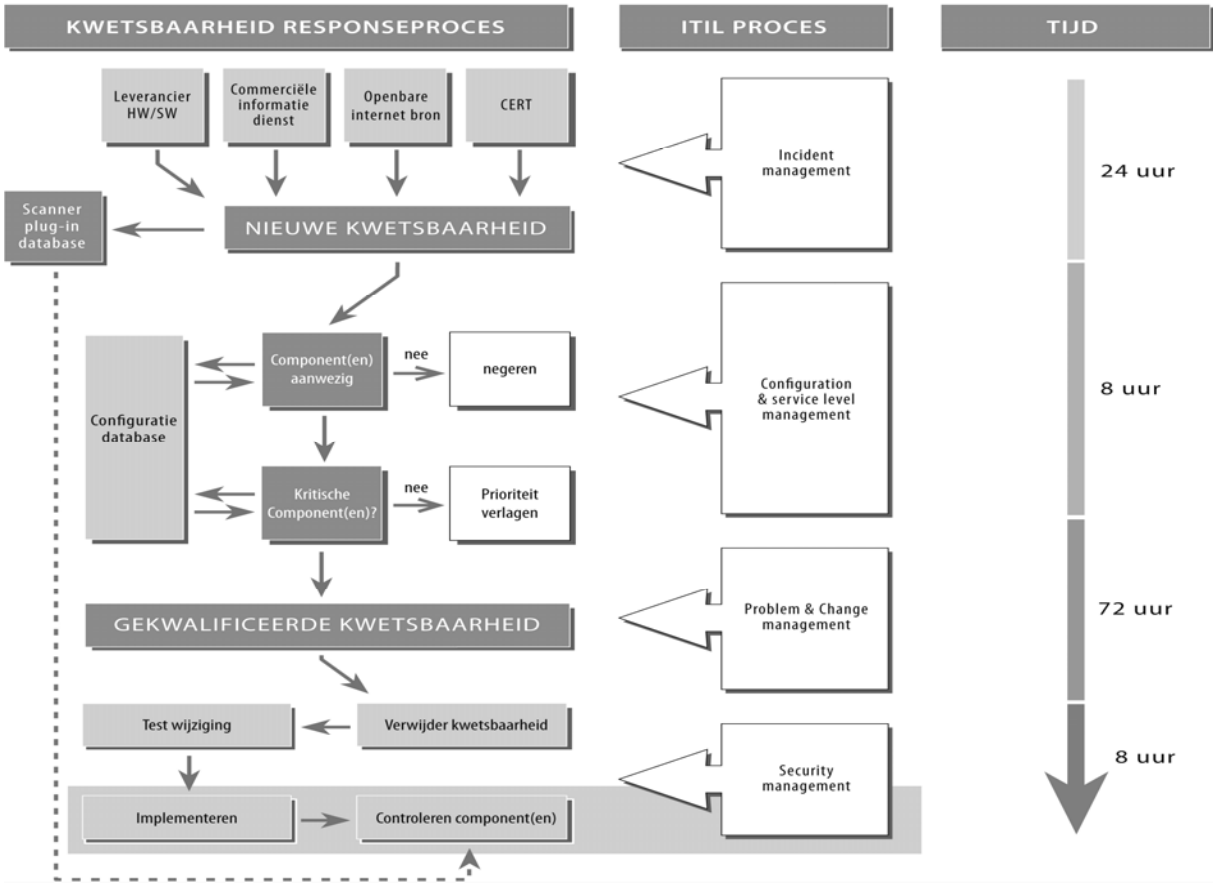
[134] Zoals extra virusprotectie, wijziging van firewallinstellingen, aanpassing van aanwezige intrusion prevention systemen, etc.

zogeheten agents worden aanbevolen wanneer computers (clients) slechts af en toe verbinding hebben met het interne netwerk [KEIJ06].

Is er geen sprake van een standaardconfiguratie of is het niet mogelijk om bepaalde elementen goed te testen[135], dan dient er gefaseerd te worden geïmplementeerd.

De changemanager legt de status van de implementatie (wijziging) vast in een centrale database die de service deliveryprocessen voor ICT ondersteunt. In de database wordt bij de wijzigingsinformatie gerefereerd aan het incidentnummer dat is gekoppeld aan de betreffende kwetsbaarheid.

7.3.4. Controle



Figuur 26: 'controle (fase 4)'

In de laatste fase wordt gecontroleerd of de kwetsbaarheid daadwerkelijk is weggenomen, zie figuur 26. Hiertoe dient een vulnerabilityscan te worden uitgevoerd op alle computersystemen waar de kwetsbaarheid aanwezig wordt verondersteld [MEGR02]. Het resultaat van de scan is een rapport met een overzicht van de systemen waarbij de kwetsbaarheid nog is waargenomen. Het vaststellen van het scanprofiel is een verantwoordelijkheid van de ICT-beveiligingfunctionaris. Het scanprofiel omvat onder meer de te scannen (IP-)adresreeksen, de te scannen kwetsbaarhedensignaturen en een

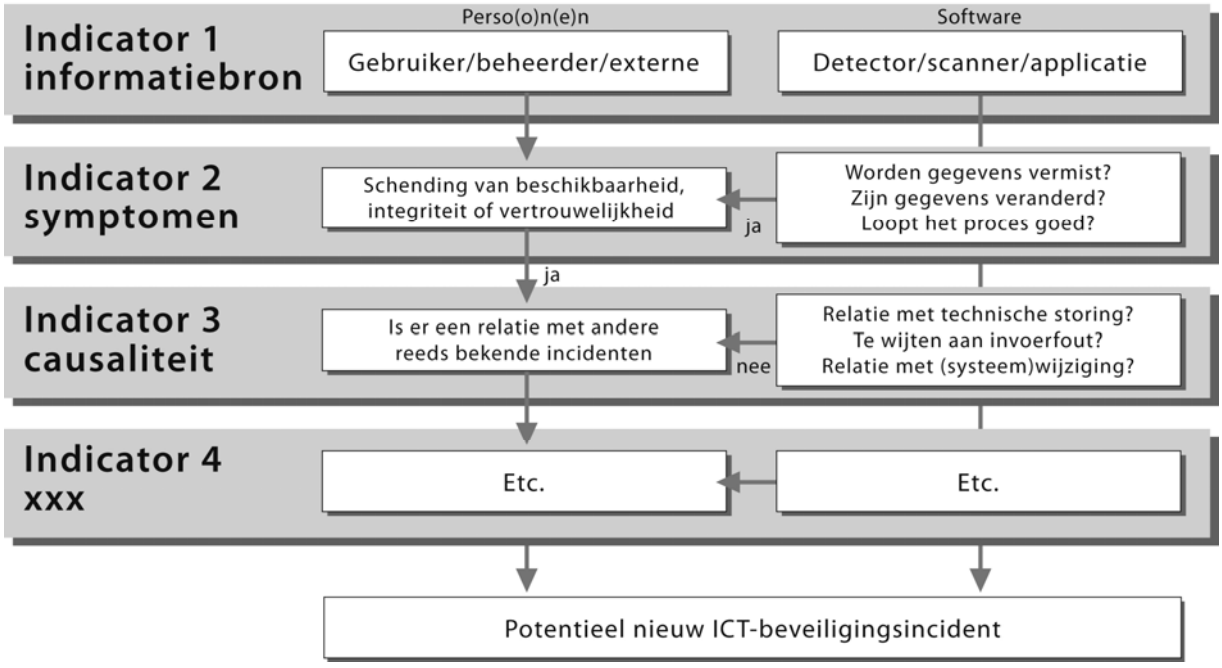
[135] Bijvoorbeeld of de security patch een negatieve invloed heeft op de performance van een computersysteem.

tijdschema. De scanactiviteit zelf kan het beste worden uitgevoerd door de ICT-beheerafdeling onder supervisie van de ICT-beveiligingfunctionaris.
De ICT-beveiligingfunctionaris koppelt de resultaten terug naar de problemmanager en/of het management van de ICT-beheerafdeling. Indien er geen significante kwetsbaarheden worden gevonden tijdens de scan kan het incident worden afgesloten.

7.4. Incidentenresponse

Aan ICT-beveiliging gerelateerde incidenten met strafrechtelijke elementen dienen in een aantal gevallen anders te worden behandeld dan gewone ICT-incidenten. Het detecteren van een indringer op het netwerk door een intrusion detection system vereist nu eenmaal onmiddellijke opvolging om (verdere) schade te voorkomen. Naast het tijdelement is ook het element van bewijs een belangrijk aspect. Het verkeerd behandelen van (potentieel) bewijsmateriaal kan ertoe leiden dat de oorzaak nimmer wordt achterhaald en de dader niet kan worden opgespoord en/of vervolgd.

Herkenning van de hierboven omschreven categorie incidenten is niet altijd eenvoudig. Incidenten worden vaak per telefoon gemeld aan een centrale ICT-helpdesk. De medewerker bepaalt aan de hand van de verstrekte gegevens van de melder en het stellen van vragen wat er met de melding wordt gedaan. Het gebruik van indicatoren kan het herkennen van aan ICT-beveiliging gerelateerde incidenten bevorderen en daarmee zorgen voor een effectieve incidentenafhandeling of doorverwijzing. De indicatoren kunnen worden samengesteld uit ervaringen, opgedaan bij eerdere incidenten of op basis van beschikbare theorie. Door gebruik te maken van een kennismanagementsysteem is het mogelijk om grote aantallen indicatoren op te nemen. Figuur 27 laat een simpel voorbeeld zien met in totaal drie indicatoren.



Figuur 27: ICT-beveiligingsincidentenindicatoren

Informatiebron
De eerste indicator is de bron waar de melding vandaan komt. Is deze bron een ICT-component die afwijkingen detecteert, dan dient dit te leiden tot de indicatie: ICT-beveiligingsincident. De melding kan dan direct worden doorgezet naar een ICT-beveiligingspecialist. Een voorbeeld is een viruschecker op een PC die tijdens een periodieke scan op de werkplek aan de medewerker meldt dat er malicious code is gevonden. De virusspecialist dient dan nader onderzoek te doen naar het scanresultaat om de werkplek virusvrij te maken.

Als een klant of medewerker ongebruikelijkheden meldt, dient de helpdesk eerst indicatief vast te stellen of er sprake is van een aan ICT-beveiliging gerelateerd incident.

Symptomen
Eerst dient te worden vastgesteld of er sprake is van aantasting van een (of meer) kwaliteitsaspect(en) van informatiebeveiliging: beschikbaarheid, integriteit of vertrouwelijkheid van gegevens. Hiertoe kunnen allerlei vragen worden gesteld, bijvoorbeeld of er gegevens zijn gewijzigd of verdwenen, hoe het systeem heeft gereageerd en welke meldingen er zijn of zijn geweest.

Causaliteit
Nadat is vastgesteld dat er daadwerkelijk sprake is van aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens, dient de helpdesk indicatief vast te stellen of er sprake is van opzettelijk handelen of van een (technische) fout. Bij deze analyse van oorzaak-gevolg kan ook worden onderzocht of het incident is te relateren aan eerder gemelde incidenten en/of aan geplande systeemwijzigingen.

Potentieel ICT-beveiligingsincident
In deze laatste fase wordt het incident nader geclassificeerd. In de literatuur worden verschillende indelingen of klassen gedefinieerd. In een door GovCERT en KLPD uitgegeven handleiding over cybercrime [GEES03] is op praktisch wijze een aantal veelvoorkomende incidenten gecategoriseerd. Een tot ICT-beveiligingsincident geclassificeerd incident waarbij sprake is van een (mogelijk) opzettelijk handelen, vereist over het algemeen nader forensisch onderzoek. Afhankelijk van de complexiteit van het incident en de impact voor de organisatie kan het incident worden opgeschaald naar het niveau van een calamiteit. Het behandelen van aan ICT-beveiliging gerelateerde incidenten waarbij sprake is van strafbaar handelen, vergt bijzondere expertise.

7.4.1. Incident response team in een ICT beheerorganisatie

Uit cijfers van FIRST blijkt dat het aantal computer security incident responseteams de afgelopen jaren fors is toegenomen. Welke rol spelen deze teams in ICT-organisaties waar de ICT-beheerprocessen sterk zijn gestandaardiseerd? Als startpunt voor de beantwoording van deze vraag is uitgegaan van de Swin-Lane Chart[ADKR04]. De auteurs maken onderscheid tussen drie kernaspecten bij incidentenresponse: detectie, triage en response.

Detectie
In de detectie fase kan een ICT-beveiliging gerelateerde gebeurtenis zich op twee plaatsen manifesteren: een gebruiker doet een (telefonische) melding bij de ICT-helpdesk, of de ICT-beheerder binnen de organisatie ontdekt iets ongebruikelijks aan de hand van bepaalde (systeem)indicaties. In het eerste geval wordt, na een eerste analyse door de helpdeskmedewerker, het incident vastgelegd in de incidentendatabase. Indien de helpdeskmedewerker het incident niet kan verhelpen, wordt het rapport of de ticket doorgeleid naar de betreffende systeembeheerafdeling voor verder onderzoek. In het tweede geval wordt de gebeurtenis vaak eerst onderzocht door de betreffende systeembeheerder en/of andere specialisten, alvorens het wordt vastgelegd in de incidentendatabase..

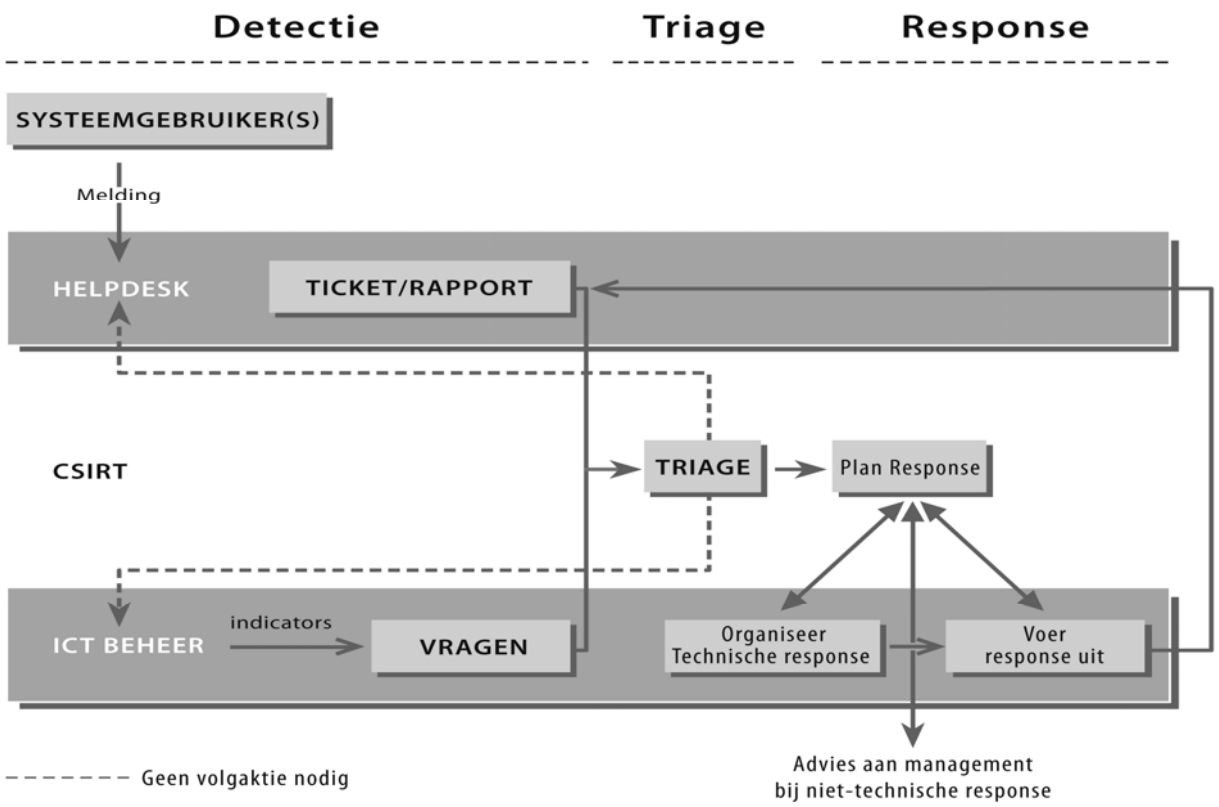
Triage
Gedurende deze fase wordt het incident globaal onderzocht om te kijken hoe ernstig het is en of nader technisch vervolgonderzoek nodig is om het incident op te lossen.

Response
De kern van de responsefase bij een incident bestaat uit het plannen en uitvoeren van een technisch onderzoek en het al dan niet wegnemen van de oorzaak van het incident. Soms is nadere (systeem)informatie nodig om een helder beeld te krijgen van de omvang en ernst van de situatie. Afhankelijk van het incident zijn bij het onderzoek meerdere ICT-specialisten betrokken, zoals systeembeheerders, netwerkspecialisten, beveiligingsmanagers, e.a. Als het gaat om gegevensonderzoek bij mogelijk strafbare activiteiten, is het zorgvuldig vergaren en vastleggen van bewijsmateriaal een voorwaarde. Het resultaat van deze fase is het wegnemen van de oorzaak van het incident en, indien nodig, het inplannen van preventieve maatregelen om incidenten in de toekomst te voorkomen. Aansluitend kan het incident worden afgesloten, de dienstverlening worden hersteld en de melder van het incident worden geïnformeerd.

CSIRT
In figuur 28 is weergegeven dat computer security incident responseteams een bijdrage kunnen leveren tijdens de triagefase en het eerste deel van de responsefase. CSIRT's bestaan vaak uit ervaren ICT-specialisten die op basis van een helpdeskrapport of vragen vanuit systeembeheer de omvang en ernst kunnen inschatten en aansluitend een advies kunnen geven aan de ICT-beheerorganisatie over noodzakelijke vervolgstappen en benodigde middelen voor het uitvoeren van vervolgonderzoek. Het vervolgonderzoek kan zowel technisch als niet-technisch van aard zijn. In dat laatste geval bijvoorbeeld is te denken aan adviezen over het treffen van juridische stappen, het doen van aangifte of het geven van een advies over communicatie aan de gebruikers of naar de pers.

Een mogelijk alternatief voor een incidenten responseteam is het inrichten van een zogeheten WARP (Warning, Advice and Reporting Point) binnen de ICT-helpdeskorganisatie. Een WARP is een door het Britse National Infrastructure Security Coordination Center[136] ontworpen organisatiemodel met als oogmerk het opzetten van een centraal meld- en waarschuwingspunt voor aan ICT-beveiliging gerelateerde incidenten en kwetsbaarheden.

[136] zie http://www.niscc.gov.uk.



Figuur 28: de rol van CSIRT's bij incidentenafhandeling

7.4.2. Vuistregels bij forensisch onderzoek

Bij het beantwoorden van incidenten met strafbare of strafwaardige elementen zijn de drie belangrijkste handelingen:

- stopzetten van de handeling en voorkomen van verdere schade
- verzamelen en veiligstellen van bewijsmateriaal
- bewaken van de chain-of-evidence.

Voor een diepgaand onderzoek naar en analyse van digitale sporen is het verstandig om specifieke specialisten in te schakelen.

Enkele algemene regels
Als vermoed wordt dat een medewerker of computer betrokken is bij een incident en deze nog schade kan veroorzaken, dienen de toegang- en autorisatierechten onmiddellijk te worden beperkt. Verder kan het volgende programma worden doorlopen.

Lokale activiteiten

De (personal) computer dient zoveel mogelijk te worden afgeschermd door nieuwsgierigen te weren, netwerkkabels en andere verbindingsvormen (WiFi, Bluetooth, modem, etc) af te sluiten of af te koppelen. Als er een destructief programma loopt, dient de stroom te worden onderbroken. Als de computer uitstaat, mag deze niet worden aangezet. Verder is

het advies om ter plaatse aantekeningen te maken en foto's te nemen van aanwezige personen, de opstelling van de diverse ICT-componenten en van schermafbeeldingen.

Referentietijd Bij aangifte van een incident is het voor de bewijsvoering van belang dat duidelijk wordt gemaakt hoe de tijdstippen in de betrokken bronnen aan elkaar gerelateerd zijn. Het verdient de voorkeur dat alle tijdstippen die gerefereerd worden in de betrokken bestanden, zoals logbestanden, eenduidig zijn, bijvoorbeeld allemaal op basis van systeemtijden die gesynchroniseerd zijn door middel van het Network Time Protocol (NTP). Ook als systemen niet door middel van NTP gesynchroniseerd zijn, kunnen gegevens waardevol zijn. In zo'n geval is het van belang dat de geconstateerde gebeurtenissen gerelateerd kunnen worden aan gebeurtenissen op machines die wel NTP-gerelateerd zijn.

Informatieverzameling Bij alle incidentenvormen is het van belang informatie uit zoveel mogelijk systemen te verzamelen. Dat betekent dat gegevens niet alleen worden gehaald uit systemen die een bepaalde vorm van cybercrime initiëren of het systeem of de systemen die het doelwit zijn, maar ook uit tussenliggende systemen die een rol vervullen in het delict [MAGE02]. Routers, firewalls of mailrelay servers zijn voorbeelden van dergelijke systemen.

Bronnen Van de gegevens die gebruikt worden voor het vaststellen van cybercrime, dient ook altijd de bron van herkomst te worden vermeld. Hierbij is bijvoorbeeld te denken aan hostnaam, IP-adres, naam van het bestand waar de gegevens vandaan komen, etc.

In de praktijk is het nauwkeurig vastleggen van alle handelingen en de (log)gegevens vaak al voldoende om als bewijsmateriaal te dienen.

Er gelden een drietal voorwaarden:

Tijd Alle gegevens[137] dienen met tijdstempel of referentietijd vastgelegd te worden. Een e-mail bericht bevat tekst die (onder andere) aangeeft wanneer het bericht is aangemaakt en afgeleverd. Een bestand (file) heeft een drietal tijden, die kunnen worden gewijzigd door lezen, kopiëren of benaderen. Geadviseerd wordt om in het onderzoek de instellingen van de klok van de werkplek mee te nemen. Logbestanden geven per regel datum en tijd mee. Dit is in het algemeen de tijd van de computer waarop de log wordt aangemaakt.

[137] Dit kunnen gebruikers of systeembestanden, handelingen, logregels, etc. zijn.

Eigenaarschap	Alle gegevens dienen met het eigenaarschap vastgelegd te worden. Een e-mailbericht bevat tekst over de verzender en ontvanger van het bericht. Een bestand heeft een (oorspronkelijke) eigenaar en een overzicht van gebruikers die ook toegang tot het bestand hebben. Logbestanden geven per regel bron en bestemming of vergelijkbare gegevens aan.
Integriteit	Het is van belang alle gegevens zo vast te leggen dat onderzoek aan die gegevens de integriteit niet aantast. Bij een verdachte PC of server kan dit het beste gebeuren door het maken van een image van alle, dus ook 'onzichtbare' gegevens op de verdachte PC of server op een externe gegevensdrager met behulp van een forensische toolkit [SAJE00]. De toolkit plaatst naast een tijdstempel een hash over de image, zodat eventuele latere wijzigingen kunnen worden aangetoond. Door gebruik van een zogeheten writeblocker bij het analyseren van de data[138] wordt voorkomen dat er onbedoeld wordt teruggeschreven naar de image.
Chain-of-Evidence	De ICT-beveiligingfunctionaris dient ervoor te zorgen dat de image op de gegevensdrager op een veilige, afgesloten plek wordt bewaard. De image kan dan worden gebruikt voor nader onderzoek om de dader(s) op te sporen of is direct bruikbaar als bewijsmateriaal. Elke toegang tot het bewijsmateriaal en elke analyseactiviteit op de image dient te worden vastgelegd in een procesverbaal.

[138] Op een werkplek is het mogelijk bestanden te zoeken, rechten, slackspace en swapspace te onderzoeken, deleted files, registrybestanden te doorzoeken, laatst geopende bestanden, Internet history, cashes, inibestanden, etc te onderzoeken.