UM-CERT
Operationeel model voor een CSIRT

UM-CERT **Herziening beschrijving/organisatie CSIRT UM**			
Datum 1ste versie	Registratie nummer	Auteur	Wijzigingsbeheer
31 oktober 2005	ICTS/IS-2006-00128	Bart van den Heuvel	CISO (Bart van den Heuvel)
Status: DEFINITIEF			
Verspreiding document	Concept: ICTS, DO-ICT, LO-L, Besluitvorming: CvB Definitief: http://www.maastrichtuniversity.nl/informatiebeveiliging en http://www.maastrichtuniversity.nl/UM-CERT		

Versie	Datum	Omschrijving wijziging
1.0	november 1994	Oprichtingsdocument CERT-RL . Electronisch beschikbaar als gescanned document: IS-2005-00217. Dit document komt geheel te vervallen
2.0	4 juli 2006	Nieuwe opzet n.a.v. naamgeving UM, actualisering MAASnetreglement, verandering informatiebeveiligingsorganisatie, CSIRT-standaarden etc.
2.1	1 januari 2013	Actualisatie adressen, telefoonnummers, lay-out etc.

UM-CERT
Operationeel model voor een CSIRT

Inhoudsopgave

1. Inleiding
2. Aanleiding
   - CERT en CSIRT
   - Van CERT-RL naar UM-CERT: de CSIRT van de Universiteit Maastricht
3. Doelstelling en Doelgroep
4. Taken, Bevoegdheden en Verantwoordelijkheden
5. Positie en borging in de UM-organisatie
6. Externe Coördinatie en Contacten
7. Teamsamenstelling
8. Bereikbaarheid
9. Communicatie en Classificatie
10. Interne operationele procedures

UM-CERT
Operationeel model voor een CSIRT

1. Inleiding

Dit document beschrijft het operationele model van UM-CERT: het Computer Security Incident Response Team van de Universiteit Maastricht. UM-CERT is niet zomaar een nieuwe naam voor het sinds 1994 bestaande CERT-RL team, maar staat voor een nieuwe organisatie, toegespitst op de actuele ontwikkelingen op het gebied van informatiebeveiligingsincidenten en de ICT- en informatiebeveiligings-organisatie van de UM.
In dit document worden de doelstelling, de taken, de bevoegdheden, de verantwoordelijkheden en de plaats in de organisatie van UM-CERT beschreven. Verder staan de primaire operationele activiteiten en de bereikbaarheid nader uitgewerkt. Hierbij is in belangrijke mate uitgegaan van de reeds bestaande operationele procedures en de organisatie binnen de UM en van modellen van (Inter)nationaal vergelijkbare instellingen.
UM-CERT concentreert zich uiteindelijk vooral op het coördineren van activiteiten naar aanleiding van informatiebeveiligingsincidenten: corrigerende maatregelen en zonodig bewijsgaring, maatregelen om verdere schade te beperken en communicatie en voorlichting daarover.

2. Aanleiding

CERT en CSIRT
Met de snelle internationale ontwikkelingen rondom researchnetwerken en internet is vanaf midden jaren '90 van de vorige eeuw sprake van een groeiend aantal informatiebeveiligingsincidenten en dreigingen daartoe. Organisaties met aansluitingen op internet hadden daarom behoefte aan een goede interne organisatie om beveiligingsincidenten te kunnen pareren.
De oorspronkelijke benaming voor zo'n interne organisatie was "Computer Emergency Response Team": "CERT" . "CERT" is echter een geregistreerd handelsmerk van MIT in Boston, zodat deze afkorting zelfstandig niet meer gebruikt kan worden buiten MIT. De internationaal gangbare benaming is nu "Computer Security Incident Response Team": CSIRT. Om historische redenen hebben veel CSIRT's de afkorting CERT nog wel verwerkt in hun naamgeving, vandaar "UM-CERT".
Om de internationale verwachtingen rondom CSIRTs te stroomlijnen is hiervoor in 1998 de internationale standaard RFC2350 vastgesteld. Ook voor UM-CERT is een RFC-2350 beschrijving beschikbaar via HTTP://www.maastrichtuniversity.nl/um-cert
.
Van CERT-RL naar UM-CERT; de CSIRT van de Universiteit Maastricht
In 1994 heeft SURFnet de taak op zich genomen om voor Nederland een CSIRT (toen nog CERT) op te richten: CERT-NL. In navolging daarvan heeft de toenmalige Rijksuniversiteit Limburg in november 1994 een eigen CERT opgericht: CERT-RL[1].

[1] CERT-RL is opgericht door de toenmalige "stuurgroep beveiliging", qua samenstelling vergelijkbaar met het huidige CBB. Het oorspronkelijke document "CERT-RL ; operationeel model computer emergency response team Rijksuniversiteit Limburg" van november 1994 is beschikbaar in het digitaal archief van ICTS onder nummer IS-2005-00217.

UM-CERT
Operationeel model voor een CSIRT

Met name in de eerste jaren van het bestaan van CERT-RL was er sprake van een beperkt aantal incidenten met een relatief lage impact op de bedrijfsvoering van de universiteit, maar telkens weer min of meer nieuw. Hierdoor was per incident veel overleg binnen de CERT-RL noodzakelijk.

Naarmate het internetgebruik toenam, nam vanaf ca. 2000 het aantal incidenten sterk toe, maar de aard van de incidenten werd meer en meer standaard en de impact was nog steeds relatief laag. In de praktijk is tussen 2000 en 2003 het overgrote deel van de incidenten afgehandeld binnen de afdeling operations van ICTS: de teams systemen en netwerken, met een verschuiving naar standaard handelingen door de Servicedesk.

In 2002 is evenwel enerzijds sprake geweest van een aantal ernstige incidenten en anderzijds heeft het management van de UM onderkend dat Informatie Beveiliging niet langer alleen incident gedreven benaderd kan worden, maar verankerd moet zijn in het instellingsbeleid en in de organisatie van de informatievoorziening van de UM. In 2002 is daartoe een aanzet gemaakt, resulterend in het najaar van 2002 met de vaststelling van een formeel Informatiebeveiligingsbeleid [2], de formele aanstelling van een beleidsmedewerker informatiebeveiliging [3] en de start van een informatie-beveiligingsprogramma voor de hele UM. Tevens is toen onderkend dat CERT-RL geactualiseerd moest worden. Vanwege het feit dat de incidentafhandeling operationeel gezien relatief probleemloos verliep is besloten om daar op dat moment geen prioriteit aan te geven. In 2002 is alleen de naam omgezet naar UM-CERT en een verwijzing van de bestaande CERT opgenomen in ondermeer het MAASnetreglement (Versie 1, vastgesteld op 6 mei 2002).

De belangrijkste redenen om nu tot een hernieuwde vaststelling van UM-CERT als CSIRT voor de UM te komen zijn:

- Inbedding in informatiebeveiligingsorganisatie
- Taakverdeling aan de hand van type incident:
    - Standaard incidenten (Servicedesk)
    - Complexere Incidenten met grotere impact (ad-hoc team)
    - Specifieke incidenten m.b.t. vertrouwelijkheid, justitie etc. (CISO)
- Samenstelling team aanpassen aan aangepaste taakstelling en profiel, verstrengeling van systemen en netwerken, enzovoort:
    - Aandacht voor bewijsgaring (forensisch onderzoek)
    - profiel op basis van expertise, niet meer op doelgroep (geografisch)
    - Multidisciplinaire ad-hoc teams per (niet standaard) incident
- Conformering aan de (Inter)nationale standaarden.

[2] Documenten m.b.t. het informatiebeveiligingsbeleid, het organisatiemodel en de inmiddels vastgestelde aanvullende huisregels en policies zijn te vinden op de website http://www.maastrichtuniversity.nl/informatiebeveiliging.

[3] De beleidsmedewerker informatiebeveiliging heet “Central Information Security Officer”: CISO

3. Doelstelling en Doelgroep

De belangrijkste doelstelling van UM-CERT is het bieden van een platform teneinde de UM in staat te stellen adequaat te reageren op informatiebeveiligingsincidenten: Zowel actief, tijdens of onmiddellijk na constatering van een incident, als preventief. De activiteiten zijn niet alleen corrigerend, maar in sommige gevallen ook gericht op bewijsgaring. De doelgroep van UM-CERT is de Universiteit Maastricht alsmede alle overige op het instellingsnetwerk Maasnet aangesloten instanties.
Hoewel de primaire focus van UM-CERT gericht is op de centrale infrastructuur van de UM en daarmee de continuïteit van de bedrijfsvoering, strekken de activiteiten zich uit tot alle werkstations, gebruikers en informatie(systemen) die op enigerlei wijze gebruikmaken van voorzieningen van de UM.

4. Taken, Bevoegdheden en Verantwoordelijkheden

De primaire taak van UM-CERT is het operationeel houden van een centraal coördinatiepunt en bijbehorende achterliggende organisatie voor het afhandelen en voorkomen van computer- en netwerk-beveiligingsincidenten (kortweg: security-incidenten), betrekking hebbend op haar doelgroep. Ter verdere coördinatie buiten haar directie doelgroep, werkt UM-CERT zeer nauw samen met SURFnet-CERT, de overkoepelende landelijke organisatie binnen SURFnet. De taken van UM-CERT zijn:

- Het afhandelen van binnenkomende beveiligingsincidenten conform de incidentafhandeling binnen ICTS.
- Het analyseren en zonodig actief verspreiden of centraal beschikbaar stellen van binnenkomende algemene beveiligingsadviezen (zoals de security-advisories van SURFnet-CERT of de Waarschuwingsdienst van de overheid.
- Het zo nodig coördineren van te ondernemen acties bij security-incidenten;
- Het daadwerkelijk (helpen) oplossen van beveiligingsproblemen door:
    - Analyse en documentatie van het probleem
    - Opschonen van gecompromitteerde systemen
    - Afschermen of isoleren van gecompromitteerde (deel)systemen
    - Bewijsgaring
- Educatie in algemene zin van systeem en netwerkbeheerders en computergebruikers middels het aanreiken van relevante informatie.
- Het (adviseren over) het ontwikkelen en verspreiden van hulpmiddelen

De UM-CERT leden zullen hun taken doorgaans kunnen uitvoeren binnen de reguliere dagelijkse UM bedrijfsvoering en doorgaans ook binnen hun eigen taakstelling daarin, met in achtneming van de gangbare procedures, overlegstructuren, lijnverantwoordelijkheden en mandaten. Dit houdt mede in dat de noodzakelijke bevoegdheden individueel zijn gemandateerd danwel vooraf specifiek zijn geautoriseerd en dat bijbehorende verantwoordelijkheden vast liggen.

UM-CERT kan adviezen geven omtrent gewenste of noodzakelijke aanpassingen in implementaties, configuraties etc. De feitelijke uitvoering daarvan valt onder de reguliere taakstelling van (de)centrale beheerders en het lijnmanagement. Deze

aanpassingen dienen dan ook ingebracht te worden in de voor betreffende eenheid vastgestelde procedures rondom incident- change- en problem-management.

UM-CERT heeft daarnaast – indien daar uit optiek van beveiliging gegronde redenen voor zijn – in voorkomende gevallen, ten principale de bevoegdheid om, zonder overleg met eindgebruikers, beheerders of lijnverantwoordelijken:

- systemen en gebruikers van het netwerk te weren
- (deel)systemen of netwerkdelen af te koppelen of te isoleren
- verkeersgegevens en feitelijke data vast te leggen en te waarmerken
- systemen in eigendom van de UM zeker te stellen en te waarmerken

UM-CERT moet dergelijke gevallen registreren en communiceren aan betrokken beheerders of gebruikers, met inachtneming van het gestelde hierover in artikel 5 van het MAASnetreglement (zie http://www.maastrichtuniversity.nl/informatiebeveiliging); e.e.a. ter verantwoording achteraf inzake de gevolgde handelwijze.

Alle vaste leden van UM-CERT dienen schriftelijk vast te leggen zich te conformeren aan de Integriteits- en Gedragscode ICT-functionarissen UM. Registratie hiervan valt onder verantwoording van Directeur ICTS, conform zijn mandaten, namens het CvB. Indien leden van UM-CERT assistentie inroepen van derden, dienen zij deze derden op de hoogte te stellen van de Integriteits- en Gedragscode ICT-functionarissen UM als dwingende werkinstructie voor alle werkzaamheden onder verantwoording van UM-CERT.

5. Positie en borging in de UM-organisatie

UM-CERT maakt deel uit van de informatiebeveiligingsorganisatie van de UM[4]. UM-CERT is verantwoording schuldig aan de portefeuillehouder bedrijfsvoering binnen het CvB, waarmee het strategisch beleidskader van UM-CERT onderdeel is van de agenda van het Coördinerend Beraad Bedrijfsvoering (CBB) .

Tactische en operationele zaken rondom UM-CERT komen op de agenda van het Discipline Overleg Information Security (DO-IS)[5]

In geval van calamiteit heeft UM-CERT rechtstreeks toegang tot de verantwoordelijke portefeuillehouder en daarmee het hoogste bestuurlijke niveau binnen de universiteit.

Binnen de informatiebeveiligingsorganisatie is verder bewust gekozen het voorzitterschap van UM-CERT op te nemen in de taakomschrijving van de CISO (zie voetnoot 3) om een borging te hebben tussen het UM-beleid op het gebied van informatiebeveiliging en de operationele werk rondom incidentafhandeling.

In de dagelijkse praktijk vallen de werkzaamheden van UM-CERT binnen de mandatenregeling van de UM onder de verantwoordelijkheid van directeur ICTS. De leden van UM-CERT zijn (en blijven) normaal werkzaam bij hun UM-onderdelen; zij vervullen hun UM-CERT werkzaamheden als een erkende nevenactiviteit welke

[4] Vastgesteld in 2002 : zie http://www.maastrichtuniversity.nl/informatiebeveiliging.
[5] Ten tijde van de vaststelling van dit document worden de taken van het DO-IS waargenomen door het Discipline Overleg ICT (DO-ICT) .

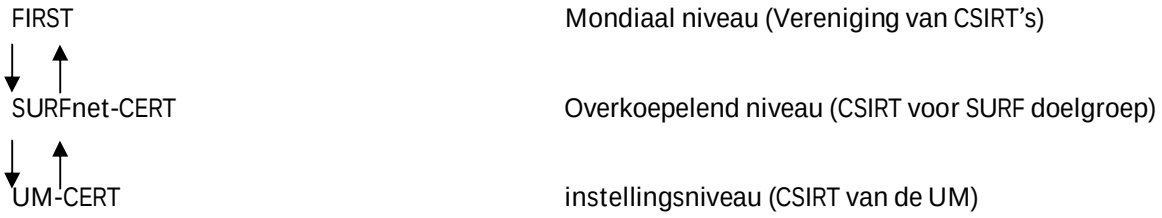
met de hoogst denkbare prioriteit moet kunnen worden vervuld (vergelijk 1e hulp, brandweer e.d.). Dit houdt in dat zij – indien de omstandigheden dit vereisen – terstond de benodigde tijd zullen vrijmaken voor alle noodzakelijk een voorkomende werkzaamheden in het kader van UM-CERT. Handelend vanuit een UM-CERT-rol staan de leden van UM-CERT dus hiërarchies rechtstreeks onder (de betreffende portefeuillehouder van) het CvB met alleen directeur ICTS als gemandateerd verantwoordelijke.

Periodiek rapporteert UM-CERT middels een jaarverslag aan de portefeuillehouder CvB. Daarnaast kan UM-CERT op reguliere basis rapporteren over haar werkzaamheden en bevindingen aan het DO-IS.

6. Externe Coördinatie en Contacten

Op mondiaal niveau zijn er honderden CSIRT's actief, enkele tientallen grote c.q. overkoepelende CSIRT's zijn verenigd in het FIRST (Forum on Incident and Response Security Teams). Het doel van FIRST is een platform te bieden aan de aangesloten CSIRT's om de onderlinge communicatie snel, gemakkelijk en betrouwbaar te maken.
SURFnet-CERT opereert op landelijk niveau als CSIRT voor de SURF doelgroep. SURFnet-CERT is dus bedoeld als platform voor informatie-uitwisseling inzake beveiligingsincidenten voor alle op SURFnet aaneengesloten instellingen. SURFnet-CERT is aangesloten bij FIRST en werkt landelijk met name samen met de CSIRT van de Nederlandse overheid: GOVCERT.NL

UM-CERT positioneert zich als lokale CSIRT binnen SURFnet.
Schematisch samengevat:



UM-CERT heeft bij SURFnet een Security Entry Point (SEP) geregistreerd[6].
SURFnet-CERT onderscheidt binnen de SEP-registratie 3 communicatielijnen:

- De Site Security Contact (SSC), voor meer organisatorische zaken
- Het Security Entry Point (SEP), voor alle incident gerelateerde zaken
- Een e-mail adres t.b.v. de Security Advisories

[6] SURFnet-CERT hanteert een zogenaamde Security Entry Point (SEP) registratie, waarin ook gegevens staan die niet algemeen beschikbaar mogen zijn (zoals nood- en privé- telefoonnummers). De SEP registratiegegevens zijn alleen op het intranet van UM-CERT beschikbaar.

7. Teamsamenstelling

UM-CERT bestaat naast de voorzitter uit 5 kernleden, geselecteerd vanuit de primaire focus op de centrale infrastructuur, en maximaal 5 leden die toegevoegd zijn op basis van hun specifieke expertises. Door het CvB zijn voor de kernleden en de expertiseleden de volgende combinaties van noodzakelijke expertises vastgesteld:

KERNLEDEN:

- Voorzitter, tevens SURFnet-SSC: CISO
- Incident-manager, tevens verantwoordelijk voor het SURFnet-SEP: teamleider Servicedesk
- Deskundige op terrein van Concern Informatiesystemen
- Systeem-manager Centrale Serversystemen
- Netwerkmanager
- Deskundige op het gebied van standaardisatie van werkstation-operatingsystemen (standaard desktop)

EXPERTISE LEDEN:

- Technisch (operating-)systeemspecialist centrale serversystemen
- Technisch netwerkspecialist
- Technisch (operating-)systeemspecialist standaard desktop
- Technisch (operating-)systeemspecialist decentrale serversystemen
- Technisch (operating-)systeemspecialist decentrale werkstations

Een UM-CERT lid wordt door Directeur ICTS, conform mandatenregeling UM, aangesteld op basis van specifieke deskundigheid (heden) op bovengenoemde aandachtsvelden.
Het lidmaatschap wordt aangegaan op vrijwillige basis, voor zover niet impliciet gekoppeld aan de feitelijke functie. Gezien het gemeenschappelijke belang is er geen vergoedingsregeling richting beheerseenheid uitgewerkt (vergelijk bedrijfsbrandweer). Naar de individuele UM-CERT-leden toe zijn de normale regelingen inzake overwerkvergoedingen en verlofcompensatie van toepassing.

Een UM-CERT lid kan op ieder moment door de directeur ICTS uit deze functie ontheven worden. UM-CERT leden verplichten zich tot het bijhouden van een logboek waarin notitie wordt gehouden van de voor UM-CERT verrichte werkzaamheden.

UM-CERT kan indien gewenst een ad-hoc commissie samenstellen die zich concentreert op een actueel specifiek security-probleem. In zo'n ad-hoc commissie kunnen externe specialisten zitting hebben. Commissieleden dienen zich te conformeren aan de "Integriteits- en Gedragscode ICT-functionarissen UM" en overige richtlijnen en werkprocedures van UM-CERT. Een conclusie van een ad-hoc commissie zal worden gezien als een aanbeveling richting UM-CERT kernleden.

8. Bereikbaarheid

Goede bereikbaarheid is een primaire voorwaarde voor het naar behoren kunnen functioneren van UM-CERT.
UM-CERT is op de navolgende wijze bereikbaar:

- e-mail intern: UM-CERT-L@maastrichtuniversity.nl
- Alternatieve e-mail extern: UM-CERT@maastrichtuniversity.nl
- Telefoon Servicedesk ICTS +31 (043)-3885555 binnen openingstijden. zie: http://www.maastrichtuniversity.nl/ICTS
- Fax +31 (0)43-3885566
- Post p/a ICT Servicecentrum, Postbus 616, 6200 MD Maastricht

Voor het aanmelden van security incidenten (en contact met UM-CERT in het algemeen) zijn er een drietal prioriteitniveaus gedefinieerd, elk gekoppeld aan een bepaalde technische communicatie voorziening of procedure.

Normale prioriteit

Communicatie met betrekking tot security-incidenten van normale prioriteit vindt bij voorkeur via e-mail plaats. UM-CERT zal in het algemeen binnen 24 uur na ontvangst reageren op berichten die op deze wijze zijn binnengekomen.

Hoge prioriteit

Gedurende de openingstijden van de servicedesk van ICTS kan telefonisch contact gelegd worden met UM-CERT voor security-incidenten van hoge prioriteit. De Servicedesk beschikt over instructies over hoe met deze meldingen om te gaan. Direct doorverbinden met een UM-CERT lid is onderdeel van die instructie.
Voor UM-CERT-leden, portefeuillehouder CvB, directeur ICTS en SURFnet-CERT is een noodtelefoonnummer bij de Servicedesk van ICTS ingericht. Verder zijn intern UM voor deze betrokkenen elkaars privé en mobiele telefoonnummers beschikbaar.

Extreem hoge prioriteit

Buiten de reguliere openingstijden van de servicedesk van ICTS, alsmede tijdens collectieve verlofdagen en erkende feestdagen is UM-CERT vooralsnog niet rechtstreeks bereikbaar. In geval van ernstige security-incidenten buiten kantooruren kunnen de UM-CERT-leden alleen worden ingeschakeld via tussenkomst van het lijnmanagement.

9. Communicatie en Classificatie

Alle UM-CERT informatie en communicatie wordt gearchiveerd en beschikbaar gesteld, rekening houdende met de oorsprong en vertrouwelijkheid van de betreffende informatie. UM-CERT hanteert daartoe drie classificatieniveau's:

INTERNE VERTROUWELIJKE INFORMATIE (Internal Classified):

UM-CERT zal interne informatie alleen voor de UM-CERT-leden, Portefeuillehouder CvB en Directeur ICTS ontsluiten middels een afgeschermde Elektronische Community: "UM_CERT" . Te denken valt dan aan privé en mobiele

telefoonnummers, de feitelijke actuele ledenlijst van de CERT, vertrouwelijke en nog niet voor het publiek vrijgegeven documenten etc.
Verder zal onderlinge communicatie geschieden via e-mail. Zodra de techniek het toestaat om gebruikersvriendelijk en plaats/computer onafhankelijk gebruik te maken van encryptie-technologie zal dit voor de vertrouwelijke e-mails worden toegepast.
Op basis van ‘ Need to know’ kan interne informatie ook beschikbaar gesteld worden aan personen buiten UM-CERT. Verslagen/notulen van de UM-CERT vergaderingen maken deel uit van deze informatie.
In die gevallen waar interne vertrouwelijke informatie buiten de UM-CERT en het topmanagement wordt gecommuniceerd, zal deze informatie voorzien worden van een disclaimer waarin de vertrouwelijkheid en “need to know” status wordt toegelicht.

EXTERNE VERTROUWELIJKE INFORMATIE (External Classified):

Het betreft informatie die uitgewisseld wordt met de afzonderlijke externe CSIRT’s, de SURFnet Site Security Contacts en de interne (Informatie)beveiligings-functionarissen van de UM (DO-IS, DO-ICT en FD/AVM). Met al deze groeperingen bestaan (impliciete) afspraken dat onderlinge informatie vertrouwelijk wordt behandeld en alleen op “need to know” basis verder beschikbaar gesteld mag worden. Communicatie geschiedt doorgaans via e-mail.
Ook in deze gevallen, zal de informatie voorzien worden van een disclaimer waarin de vertrouwelijkheid en “need to know” status wordt toegelicht.
Relevante bijbehorende files worden opgeslagen op de Elektronische Community als intern vertrouwelijk, omdat deze files doorgaans geen disclaimer in de file zelf hebben opgenomen.

PUBLIEKE INFORMATIE (Not Classified, Public):

UM-CERT zal publieke informatie, specifiek met betrekking tot UM-CERT publiceren op de web-site www.maastrichtuniversity.nl/um-cert
Afgeleide informatie zoals security advisories worden conform de operationele procedures van ICTS gepubliceerd op de bestaande specifieke ondersteunings-pagina’s zoals de LO-Portal c.q. worden per e-mail verzonden naar de bestaande specifieke mailinglijsten, zoals UM-LO-L

10. Interne operationele procedures

De feitelijke activiteiten van UM-CERT zijn meestal incident-gestuurd. Afhankelijk van de aard en de impact van het incident, worden de activiteiten deels uitgevoerd buiten de reguliere bedrijfsuren van de UM en dus buiten de reguliere beschikbaarheid van het lijnmanagement. De activiteiten kunnen derhalve niet conform strikte procedures worden uitgevoerd. Als werkwijze is daarom gekozen voor een pragmatische benadering. UM-CERT-leden handelen conform onderstaande werkinstructie, waarbij sommige instructiestappen in voorkomende gevallen zo spoedig mogelijk achteraf worden uitgevoerd:

1. Zodra een incident binnenkomt bij een UM-CERT lid, op basis van dat UM-CERT lidmaatschap, wordt naar de indiener teruggekoppeld dat:
    a. het incident vanaf dat moment onder de noemer van UM-CERT wordt behandeld. Werkwijze vervolgen bij 2.

   b. Het incident conform de reguliere incident-procedures (doorgaans bij ICTS) dient te worden gemeld. Melding wordt geregistreerd als “niet terecht” en het incident is afgesloten.
2. Er worden (naar eigen inschatting al of niet onmiddellijk) relevante acties ondernomen conform doelstelling, taken en bevoegdheden UM-CERT.
3. Van de ondernomen acties wordt een beknopte registratie bijgehouden, met daarin:
   a. Datum en tijdstip
   b. Betrokken UM-CERT-leden, lijnmanagement en eventuele derden
   c. Aard van actie (informatie-vergaring, informatie-uitwisseling, aanpassen configuratie etc.)
4. Het incident wordt (indien nog niet gebeurd) aangemeld bij servicedesk ICTS
5. Het incident wordt (indien nog niet gebeurd) gecommuniceerd via UM-CERT-L
6. Er worden werk- en communicatieafspraken gemaakt met minimaal 1 ander lid van UM-CERT en/of met het lijnmanagement conform onderstaande prioriteit:
   a. Lid UM-CERT,
   b. Directeur ICTS,
   c. Portefeuillehouder CvB
   d. Eigen lijnmanager
   e. Lijnmanagement eventueel betrokken beheerseenheid
7. Afhankelijk van aard en impact van het incident wordt in overleg met de op dat moment betrokken UM-CERT-leden en lijnmanagement het overige lijnmanagement conform bovenstaande lijst ingelicht, danwel betrokken in het proces.
8. De voor het incident noodzakelijke vervolgactiviteiten worden uitgevoerd en geregistreerd
9. Het incident wordt geregistreerd conform onderstaande richtlijnen:
   a. Standaard, niet vertrouwelijk: Binnen incident-registratie ICTS
   b. Vertrouwelijk intern UM:
      - minimaal geanonimiseerd en indien noodzakelijk ontdaan van overige aard en impactgegevens binnen incident-registratie ICTS.
      - Overige informatie binnen UM-CERT community, met ICTS-ticket-nummer als referentie.
      - Indien nodig afschriften van informatie en loggings geparafeerd door de behandelaars in vertrouwelijk archief ICTS en ingescanned in het document registratiesysteem van ICTS, opgeslagen met hoogste vertrouwelijkheidsniveau.

De UM-CERT leden komen minimaal vier keer per jaar bijeen. De notulen van die vergaderingen worden gepresenteerd aan directeur ICTS en portefeuillehouder CvB. Verder kunnen (delen van) deze notulen op basis van “need to know” worden gecommuniceerd conform richtlijnen in hoofdstuk 9.

BIJLAGE 1: Voorstel teamsamenstelling

VERTROUWELIJK

(wordt bijgehouden op het afgeschermde deel van de UM-CERT community)

BIJLAGE 2: Interne bereikbaarheid en SEP-registratie bij SURFnet(-CERT)

VERTROUWELIJK !!!

======= SEP-aanmelding Universiteit Maastricht ==========
De SEP wordt gevormd door onze ICT servicedesk.
Het genoemde alarmnummer is ons INTERN NOODNUMMER en moet dus alleen bij echte calamiteiten gebruikt worden en mag NIET GECOMMUNICEERD WORDEN naar andere relaties. Voor andere relaties en voor meer reguliere operationele vragen gelden (naast e-mail) de nummers:
Servicedesk: +31 (0)43-3885555
Secretariaat: +31 (0)43-3885511

(1) Instellingsnaam : Universiteit Maastricht
(2) afkorting van het SEP : UM-CERT
(3) email-adres : Servicedesk-ICTS@MAASTRICHTUNIVERSITY.NL
(4) advisory-email-adres : Servicedesk-ICTS@MAASTRICHTUNIVERSITY.NL
(5) telefoonnummer (kantooruren) : +31 (0)43-3885555
(6) alarmnummer (noodgevallen):
"servicedesk"-uren : **VERTROUWELIJK**
24/7 (nog in beraad): voorlopig **VERTROUWELIJK** (mobiel CISO)
(7) faxnummer : +31 (0)43-3885566
(8) postadres: Universiteit Maastricht
t.a.v. UM-CERT, Bart van den Heuvel, ICTS
P.O.Box 616
6200 MD MAASTRICHT

SSC: 1) Bart van den Heuvel: Bart.vandenHeuvel@Maastrichtuniversity.nl
Telefoon: +31 (0)43-3885526 / 3885511
Fax: +31 (0)43-3885566
2) Jo Weijers: J.Weijers@Maastrichtuniversity.nl
Telefoon: +31 (0)43-3885504 / 3885511
Fax: +31 (0)43-3885566

Voor de volledigheid:
Voor Abuse-meldingen is ook beschikbaar:
abuse@maastrichtuniversity.nl (de servicedesk)
UM-CERT is bereikbaar onder:
UM-CERT@maastrichtuniversity.nl (een mailinglijst)
======= Einde SEP-aanmelding Universiteit Maastricht ==========

Interne nummers nog in te vullen op het afgeschermde deel van de UM-CERT-community.

BIJLAGE 3: Disclaimer

UM-CERT maakt indien nodig, conform de richtlijnen in hoofdstuk 9, gebruik van disclaimers om de vertrouwelijkheid van informatie te waarborgen. Een disclaimer zal in sommige gevallen aangepast moeten worden aan de specifieke situatie (bv. het noemen van specifieke geadresseerden) en (ook) in het Engels moeten worden aangeboden.
Een aantal standaard disclaimers zal op het afgeschermde deel van de UM-CERT community geplaatst worden.

Het algemene template voor de disclaimers is:

<geadresseerde>,

U ontvangt deze informatie vanwege uw betrokkenheid bij een incident wat behandeld wordt door UM-CERT (www.maastrichtuniversity.nl/um-cert). U dient deze informatie strikt vertrouwelijk te behandelen. Kopieën van deze informatie onder uw beheer (elektronisch danwel op papier) dienen opgeslagen te worden op een niet voor ongeautoriseerde derden toegankelijke wijze. Indien het voor de voortgang van het onderhavige incident noodzakelijk is dat deze informatie verder verspreid wordt, dient dit te geschieden op individuele basis, met gebruikmaking van deze disclaimer en met een afschrift naar UM-CERT.

BIJLAGE 4: Lijnmanagement UM-CERT-leden

VERTROUWELIJK !!!

(wordt bijgehouden op het afgeschermde deel van de UM-CERT community)