EEN STAPSGEWIJZE AANPAK VOOR HET SAMENSTELLEN VAN EEN CSIRT

Resultaat WP2006/5.1(CERT-D1/D2)

Index

1 Managementsamenvatting

In onderhavig document wordt het proces beschreven voor de samenstelling van een CSIRT (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) vanuit alle relevante invalshoeken, zoals bedrijfsvoering, procesbeheer en technische aspecten. Dit document is het resultaat van de praktische uitwerking van twee van de doelstellingen die zijn beschreven in hoofdstuk 5.1 van het ENISA-werkprogramma 2006:

- Dit document: *Schriftelijk rapport over stapsgewijze aanpak voor het samenstellen van een CERT of soortgelijke faciliteiten, met voorbeelden* (**CERT-D1**)
- Hoofdstuk 12 en externe bestanden: *Uittreksel van het stappenplan in itemvorm voor een eenvoudige toepassing van het stappenplan in de praktijk* (**CERT-D2**)

2 Juridische kennisgeving

Er zij op gewezen dat deze publicatie een weerspiegeling is van de opvattingen en interpretaties van de auteurs en redacteurs, tenzij anders vermeld. Deze publicatie mag niet worden beschouwd als een actie van ENISA of de ENISA-organen, tenzij goedgekeurd op grond van de ENISA-Verordening (EG) nr. 460/2004. Deze publicatie is niet noodzakelijkerwijs een weergave van de laatste stand van zaken en kan van tijd tot tijd worden bijgewerkt.

Externe bronnen worden waar nodig geciteerd. ENISA is niet verantwoordelijk voor de inhoud van de externe bronnen zoals externe websites waarnaar in deze publicatie wordt verwezen.

Deze publicatie is uitsluitend bedoeld voor instructie- en informatiedoeleinden. ENISA noch enige andere persoon die namens ENISA optreedt, is verantwoordelijk voor het gebruik dat van de informatie in deze publicatie kan worden gemaakt.

3 Dankbetuiging

ENISA bedankt alle instellingen en personen die hebben bijgedragen aan dit document. Een speciaal woord van dank gaat uit naar:

- Henk Bronk, die als consultant de eerste versie van dit document heeft verzorgd;
- CERT/CC en in het bijzonder het CSIRT-ontwikkelingsteam, dat uiterst nuttig materiaal en het voorbeeldcursusmateriaal heeft aangeleverd in de bijlage;

- GovCERT.NL voor de levering van *CERT-in-a-box*;
- het TRANSITS-team, dat heeft bijgedragen aan het voorbeeldcursusmateriaal in de bijlage;
- de collega's van de sectie Beveiligingsvoorschriften in de technische afdeling, die hoofdstuk 6.6 hebben verzorgd;
- de talloze mensen die dit document hebben doorgenomen en gereviseerd.

4 Inleiding

Communicatienetwerken en informatiesystemen zijn essentieel geworden voor de economische en maatschappelijke ontwikkeling. Computers en netwerken groeien uit tot alomtegenwoordige nutsvoorzieningen, vergelijkbaar met elektriciteits- en water-voorziening.

De beveiliging van communicatienetwerken en informatiesystemen, en met name de beschikbaarheid ervan, is daarom van steeds groter belang voor de maatschappij gezien het risico op problemen in essentiële informatiesystemen ten gevolge van de complexiteit van de systemen, ongevallen, vergissingen en aanvallen op de fysieke infrastructuren die diensten leveren die voor het welzijn van de EU-burgers van cruciaal belang zijn.

Op 10 maart 2004 is het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) opgericht[1]. Het Agentschap heeft tot doel te zorgen voor een hoog en effectief niveau van netwerk- en informatiebeveiliging in de gemeenschap en de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging ten behoeve van de burgers, consumenten, bedrijven en organisaties uit de publieke sector in de Europese Unie te bevorderen, en aldus bij te dragen tot de goede werking van de interne markt.

Al verscheidene jaren werken diverse beveiligingsgemeenschappen in Europa, zoals CERT's/CSIRT's, Abuse-teams en WARP's, samen aan een veiliger internet. ENISA probeert deze gemeenschappen bij hun inspanningen te ondersteunen door informatie te verschaffen over maatregelen die een gepast niveau van servicekwaliteit waarborgen. ENISA beoogt verder zijn capaciteiten uit te breiden om de EU-lidstaten en de EU-organen te kunnen adviseren over vragen met betrekking tot goede beveiligingsdiensten voor specifieke groepen IT-gebruikers. Voortbouwend op de bevindingen van de ad-hocwerkgroep CERT Cooperation and Support, opgericht in 2005, zal de nieuwe werkgroep zich dan ook bezighouden met vragen die verband houden met de verlening van adequate beveiligingsdiensten ("CERT-diensten") aan specifieke (categorieën of groepen) gebruikers.

ENISA ondersteunt de vorming van nieuwe CSIRT's door de uitgave van dit ENISA-rapport "*Een stapsgewijze aanpak voor het samenstellen van een CSIRT, met een aanvullende controlelijst",* waarmee u zelf een CSIRT kunt opzetten.

[1] Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor Netwerk- en Informatiebeveiliging. Een "agentschap van de Europese Gemeenschap" is een orgaan dat door de EU is ingesteld voor de uitvoering van een zeer specifieke technische of wetenschappelijke taak of een beheerstaak binnen het "communautaire domein" ("eerste pijler") van de EU.

4.1 Doelgroepen

De primaire doelgroepen van dit rapport zijn overheidsinstellingen en andere instellingen die een CSIRT willen samenstellen ter beveiliging van hun eigen IT-infrastructuur of die van de betrokken belanghebbenden.

4.2 Hoe dit document gebruiken?

Dit document bevat informatie over wat een CSIRT is, welke diensten een CSIRT te bieden heeft en welke stappen noodzakelijk zijn om aan de slag te gaan. Hiermee zou de lezer een goed en pragmatisch overzicht moeten hebben van de aanpak, structuur en inhoud voor de samenstelling van een CSIRT.

Hoofdstuk 4 *"Inleiding"*
Inleiding tot dit rapport

Hoofdstuk 5 *"Algemene strategie voor het plannen en samenstellen van een CSIRT"*
De eerste sectie bevat een beschrijving van wat een CSIRT is. Er staat ook informatie in over de verschillende omgevingen waarin CSIRT's kunnen werken en welke diensten ze te bieden hebben.

Hoofdstuk 6 *"Het bedrijfsplan ontwikkelen"*
In dit hoofdstuk wordt de aanpak op het niveau van de bedrijfsvoering beschreven voor het opzetten van een CSIRT.

Hoofdstuk 7 *"Het bedrijfsplan promoten"*
In dit hoofdstuk komen de zakelijke en financiële aspecten aan bod.

Hoofdstuk 8 *"Voorbeelden van operationele en technische procedures"*
In dit hoofdstuk wordt de procedure beschreven voor het verzamelen van informatie en het weergeven ervan in een beveiligingsbulletin. Dit hoofdstuk bevat tevens een beschrijving van een werkstroom voor de afhandeling van incidenten.

Hoofdstuk 9 *"CSIRT-training"*
Dit hoofdstuk bevat een overzicht van beschikbare CSIRT-trainingen. Voorbeeldcursusmateriaal is in de bijlage opgenomen.

Hoofdstuk 10 *"Oefening: een aanbeveling opstellen"*
Dit hoofdstuk bevat een oefening voor het uitvoeren van een van de basisdiensten (of kerntaken) van een CSIRT: het opstellen van een beveiligingsbulletin (of aanbeveling).

Hoofdstuk 12 "Beschrijving van het projectplan"
In dit hoofdstuk wordt verwezen naar het aanvullende projectplan (de controlelijst) bij deze leidraad. Dit plan is bedoeld als eenvoudig hulpmiddel voor de implementatie van deze leidraad.

4.3 In dit document gebruikte conventies

Als richtsnoer voor de lezer begint elk hoofdstuk met een samenvatting van de stappen die tot dusver in het proces voor de samenstelling van een CSIRT zijn uitgevoerd. Deze samenvattingen worden als volgt in kaders weergegeven:

We hebben de eerste stap uitgevoerd

Elk hoofdstuk eindigt met een praktisch voorbeeld van de besproken stappen. In dit document is “Fictief CSIRT” een kleine, onafhankelijke CSIRT voor een middelgrote onderneming of instelling. Een samenvatting is opgenomen in de bijlage.

Fictief CSIRT

5 Algemene strategie voor het plannen en samenstellen van een CSIRT

Voor een geslaagde start bij het opzetten van een CSIRT is het van belang een heldere visie te hebben op de mogelijke diensten die het team kan verlenen aan de afnemers ervan, in de 'CSIRT-wereld' ook wel 'constituenten' genoemd. Het is dan ook noodzakelijk om de behoeften van de constituenten te begrijpen zodat u tijdig de juiste diensten kunt verlenen met de juiste kwaliteit.

5.1 Wat is een CSIRT?

CSIRT staat voor Computer Security Incident Response Team. De term CSIRT wordt voornamelijk in Europa gebruikt in plaats van de beschermde term CERT, die in de Verenigde Staten is geregistreerd door het CERT Coordination Center (CERT/CC).
Er zijn diverse acroniemen in gebruik voor dezelfde soorten teams:

- CERT of CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

De eerste grote uitbraak van een worm in de wereldwijde IT-infrastructuur was aan het einde van de jaren '80. Die worm heette Morris[2] en verspreidde zich snel. Daarbij werden talloze IT-systemen over de hele wereld geïnfecteerd.

Dit incident schudde iedereen wakker: men werd zich plotseling bewust van de dringende behoefte aan samenwerking en coördinatie tussen systeembeheerders en IT-managers om dit soort problemen het hoofd te bieden. Aangezien tijd een cruciale rol speelde, was er behoefte aan een meer georganiseerde en structurele aanpak voor de afhandeling van IT-beveiligingsincidenten. Enkele dagen na het 'Morris-incident' kwam het DARPA-instituut (Defence Advanced Research Projects Agency) van het Amerikaanse ministerie van Defensie met het eerste CSIRT: het CERT Coordination Center (CERT/CC[3]), ondergebracht bij de Carnegie Mellon-universiteit in Pittsburgh (Pennsylvania).

Dit model werd al snel overgenomen in Europa, en in 1992 lanceerde de Nederlandse aanbieder van computernetwerken voor hoger onderwijs SURFnet het eerste CSIRT in Europa, SURFnet-CERT genaamd.[4] Vele teams volgden en tegenwoordig worden in het ENISA-overzicht van CERT-activiteiten in Europa[5] meer dan 100 bekende teams in Europa vermeld.

[2] Meer informatie over de Morris-worm vindt u op http://nl.wikipedia.org/wiki/Morris-worm

[3] CERT-CC: http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

[5] ENISA-overzicht: http://www.enisa.europa.eu/cert_inventory/

In de loop der jaren hebben CERT's hun capaciteiten uitgebreid van slechts een responsteam naar een volwaardige aanbieder van beveiligingsdiensten, inclusief preventiediensten zoals waarschuwingen, beveiligingsadviezen, training en diensten op het gebied van beveiligingsbeheer. De term 'CERT' dekte al snel niet meer de lading. Aan het eind van de jaren '90 werd dan ook de nieuwe term 'CSIRT' geïntroduceerd. Tegenwoordig worden beide termen (CERT en CSIRT) als synoniemen gebruikt, maar CSIRT is de meest nauwkeurige term.

5.1.1 De term *constituency*

Hierna wordt de (in CSIRT-kringen) ingeburgerde naam 'constituency' gebruikt om te verwijzen naar het verzorgingsgebied van een CSIRT. Een klant wordt een 'constituent' genoemd.

5.1.2 Definitie van een CSIRT

Een CSIRT is een team van IT-beveiligingsexperts dat zich vooral bezighoudt met het afhandelen van computerbeveiligingsincidenten. Het team levert de benodigde diensten voor de afhandeling van de incidenten en biedt ondersteuning aan de constituenten om inbreuken te herstellen.

De meeste CSIRT's verzorgen tevens diensten op het gebied van preventie en training voor hun constituency om de risico's en het aantal nodige tussenkomsten zo veel mogelijk te beperken. Zij brengen adviezen uit over kwetsbaarheden en beveiligingslekken in de gebruikte software en hardware, en informeren de gebruikers over misbruikpraktijken en virussen die zich op basis daarvan kunnen voordoen. De constituenten zijn daardoor in staat hun systemen snel te repareren en bij te werken. Zie hoofdstuk 5.2 voor een volledig overzicht van mogelijke diensten.

5.1.3 De voordelen van een CSIRT

Een speciaal IT-beveiligingsteam kan een organisatie helpen het aantal en de ernst van de beveiligingsincidenten tot een minimum te beperken en zo waardevolle bedrijfsmiddelen beschermen.

Andere mogelijke voordelen zijn:

- een centrale coördinatie voor IT-beveiligingskwesties binnen de organisatie (Point of Contact, PoC of aanspreekpunt);
- gecentraliseerde en gespecialiseerde afhandeling van en reactie op IT-incidenten;
- deskundigheid binnen handbereik om gebruikers te ondersteunen bij een spoedig herstel van beveiligingsincidenten;
- afhandeling van juridische kwesties en bewijsvoering bij een eventuele rechtszaak;
- bijhouden van de ontwikkelingen op beveiligingsgebied;
- stimuleren van samenwerking binnen de constituency betreffende IT-beveiliging (bewustmaking).

Fictief CSIRT (stap 0)
Begrijpen wat een CSIRT is:

Het voorbeeld-CSIRT verzorgt diensten voor een middelgrote instelling met maximaal 200 medewerkers. De instelling heeft een eigen IT-afdeling en twee andere filialen in hetzelfde land. IT speelt een sleutelrol in het bedrijf en wordt toegepast voor de interne communicatie, het gegevensnetwerk en een continue e-business (24x7). Het instituut heeft een eigen netwerk en beschikt over een redundante verbinding met internet via twee verschillende ISP's.

5.1.4 Beschrijving van de verschillende soorten CSIRT-omgevingen

We hebben de eerste stap uitgevoerd

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.

>> De volgende stap is het beantwoorden van de vraag: "Aan welke sector worden CSIRT-diensten geleverd?"

Bij het starten van een CSIRT (net als bij andere zakelijke activiteiten) is het van groot belang snel een heldere visie te hebben op wie de constituenten zijn en op welk type omgeving de CSIRT-diensten zich gaan richten. Op dit moment onderscheiden we de volgende 'sectoren':

- CSIRT voor academische sector
- Commercieel CSIRT
- CSIRT voor CIP/CIIP-sector
- CSIRT voor overheidssector
- Intern CSIRT
- CSIRT voor militaire sector
- Nationaal CSIRT
- CSIRT voor midden- en kleinbedrijf (MKB)
- CSIRT voor leveranciers

CSIRT voor academische sector
Focus
Een CSIRT voor de academische sector levert CSIRT-diensten aan academische instellingen en onderwijsinstellingen, zoals universiteiten of onderzoeksfaciliteiten, en de bijbehorende internetomgevingen op de campus.

Constituenten
Constituenten van dit type CSIRT zijn veelal medewerkers en studenten van universiteiten.

Commercieel CSIRT
Focus
Een commercieel CSIRT levert commerciële CSIRT-diensten aan de constituenten. In het geval van een ISP levert het CSIRT doorgaans diensten aan eindgebruikers (inbellen, ADSL) op het gebied van misbruik en CSIRT-diensten aan professionele klanten.

Constituenten
Commerciële CSIRT's leveren hun diensten doorgaans aan constituenten die ervoor betalen.

CSIRT voor CIP/CIIP-sector
Focus
CSIRT's in deze sector zijn voornamelijk gericht op de beveiliging van cruciale informatie en/of infrastructuren. Meestal werkt een dergelijk gespecialiseerd CSIRT nauw samen met een CIIP-afdeling van de overheid. De beveiliging strekt zich uit tot alle essentiële IT-sectoren en de burgers van het desbetreffende land.

Constituenten
Overheid; cruciale IT-activiteiten; burgers

CSIRT voor overheidssector
Focus
Een CSIRT voor de overheidssector levert diensten aan overheidsinstellingen en in sommige landen aan de burgers.

Constituenten
Overheid en aan de overheid gerelateerde instellingen. In sommige landen worden tevens waarschuwingsdiensten verzorgd voor de burgers (bijvoorbeeld in België, Hongarije, Nederland, het Verenigd Koninkrijk of Duitsland).

Intern CSIRT
Focus
Een intern CSIRT levert uitsluitend diensten aan zijn hostorganisatie. De klemtoon ligt hier meer op de manier van functioneren dan op een bepaalde sector. Vele organisaties op het gebied van telecommunicatie en banken hebben bijvoorbeeld hun eigen CSIRT's. Gewoonlijk houden ze geen website bij voor het publiek.

Constituenten
Interne medewerkers en de IT-afdeling van de hostorganisatie.

CSIRT voor militaire sector
Focus
Een CSIRT in deze sector levert diensten aan militaire organisaties met verantwoordelijkheden voor de IT-infrastructuur voor defensiedoeleinden.

Constituenten
Personeel van militaire organisaties of nauw verwante entiteiten, zoals het ministerie van Defensie.

Nationaal CSIRT
Focus
Een CSIRT met nationale focus, fungerend als centraal aanspreekpunt voor de beveiliging in een land. Soms fungeert het CSIRT voor de overheid ook als nationaal PoC (zoals UNIRAS in het Verenigd Koninkrijk).

Constituenten
Dit type CSIRT heeft doorgaans geen directe constituenten, aangezien het nationale CSIRT alleen een intermediaire rol speelt voor het hele land.

CSIRT voor midden- en kleinbedrijf (MKB)
Focus
Een op eigen initiatief georganiseerd CSIRT dat diensten verleent aan de eigen bedrijfssector of een groep gelijksoortige gebruikers.

Constituenten
Constituenten van deze CSIRT's kunnen kleine en middelgrote ondernemingen zijn en de medewerkers daarvan, of speciale belangengroepen zoals de Vereniging van Nederlandse Gemeenten.

CSIRT voor leveranciers
Focus
CSIRT's van leveranciers richten zich op ondersteuning voor de specifieke producten van de leveranciers. Het doel is gewoonlijk het ontwikkelen en aanbieden van oplossingen voor beveiligingslekken en kwetsbaarheden en het minimaliseren van mogelijke negatieve effecten van fouten.

Constituenten
Producteigenaren

Zoals al is opgemerkt in de paragraaf over nationale CSIRT's, kan een team meerdere sectoren bedienen. Dit is van invloed op bijvoorbeeld de analyse van de constituency en de behoeften daarvan.

Fictief CSIRT (stap 1)
Startfase In de startfase wordt het nieuwe CSIRT gepland als een intern CSIRT, waarbij de diensten worden verleend aan het hostbedrijf, de lokale IT-afdeling en het personeel. Tevens vindt ondersteuning en coördinatie plaats bij de afhandeling van IT-beveiligingsincidenten voor de verschillende filialen.

5.2 Mogelijke diensten die een CSIRT kan verlenen

We hebben de eerste twee stappen uitgevoerd

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?

>> De volgende stap is het beantwoorden van de vraag *welke diensten aan de constituenten worden verleend*.

Er zijn vele diensten die een CSIRT kan verlenen, maar tot dusver verleent geen enkel bestaand CSIRT al die diensten. De selectie van de juiste reeks diensten is dus een cruciale beslissing. Hieronder vindt u een beknopt overzicht van alle bekende CSIRT-diensten, volgens het handboek voor CSIRT's dat door het CERT/CC is uitgegeven.[6]

Reactieve diensten	**Proactieve diensten**	**Afhandeling van artefacten**
• **Alarmeringen en waarschuwingen** • **Afhandeling van incidenten** • **Analyse van incidenten** • **Ondersteuning bij reacties op incidenten** • **Coördinatie van reacties op incidenten** • Reacties op incidenten op locatie • Afhandeling van beveiligingslekken • Analyse van beveiligingslekken • Reactie op beveiligingslekken • Coördinatie van reacties op beveiligingslekken	• **Mededelingen** • Technologiebewaking • Beveiligingscontroles of -beoordelingen • Configuratie en bijhouden van beveiliging • Ontwikkeling van beveiligingstools • Diensten voor detectie van aanvallen • Verspreiding van beveiligingsgerelateerde informatie	• *Analyse van artefacten* • *Reactie op artefacten* • *Coördinatie van reacties op artefacten*
		Kwaliteitsbeheer en beveiliging
		• *Analyse van risico's* • *Bedrijfscontinuïteit en noodherstel* • *Beveiligingsadvies* • *Bewustmaking* • *Opleiding/training* • *Productevaluatie of -certificatie*

Fig. 1 Lijst met CSIRT-diensten van CERT/CC[7]

De kerndiensten (gemarkeerd in vetgedrukte letters): er is onderscheid gemaakt tussen reactieve en proactieve diensten. Proactieve diensten zijn gericht op de preventie van incidenten door bewustmaking en training. Reactieve diensten zijn gericht op het afhandelen van incidenten en het minimaliseren van de eruit voortkomende schade.

Afhandeling van artefacten omvat de analyse van in een systeem aangetroffen bestanden of objecten die mogelijk betrokken zijn bij kwaadaardige acties, zoals de restanten van virussen, wormen, scripts, Trojaanse paarden en dergelijke. Het omvat tevens de afhandeling en distributie van de resulterende informatie aan leveranciers en andere belanghebbenden om verdere verspreiding van malware te voorkomen en de risico's tot een minimum te beperken.

Diensten voor beveiligings- en kwaliteitsbeheer zijn diensten met doelstellingen voor de langere termijn en omvatten maatregelen op het gebied van advisering en onderwijs.

Zie de bijlage voor een nadere uiteenzetting van CSIRT-diensten.

[6] Handboek voor CSIRT's van het CERT/CC: http://www.cert.org/archive/pdf/csirt-handbook.pdf

[7] Lijst met CSIRT-diensten van CERT/CC: http://www.cert.org/csirts/services.html

Het kiezen van de juiste diensten voor uw constituenten is een belangrijke stap en komt verder ter sprake in hoofdstuk *6.1 Het financiële model definiëren*.

De meeste CSIRT's beginnen met de verspreiding van 'alarmeringen en waarschuwingen', doen 'mededelingen' en verzorgen de 'afhandeling van incidenten' voor hun constituenten. Deze kerndiensten zorgen doorgaans voor een goed profiel en een hoge attentiewaarde bij de constituency, en worden veelal als toegevoegde waarde beschouwd.

Een goede werkwijze is om met een kleine groep 'proefconstituenten' te beginnen, de kerndiensten gedurende een bepaalde proefperiode aan te bieden en nadien om feedback te vragen.
Belangstellende proefgebruikers geven meestal nuttige feedback en kunnen u helpen bij het ontwikkelen van diensten op maat.

Fictief CSIRT (stap 2)
De juiste diensten kiezen
In de beginfase wordt besloten dat het nieuwe CSIRT zich voornamelijk zal richten op het bieden van enkele kerndiensten aan de medewerkers.

Er is besloten dat na een testfase uitbreiding van het dienstenpakket valt te overwegen, plus de toevoeging van enkele diensten op het gebied van beveiligingsbeheer. Deze beslissing wordt genomen op basis van de feedback van de proefconstituenten en in nauwe samenwerking met de afdeling Kwaliteitsbeheer.

5.3 Analyse van de constituency en mission statement

We hebben de eerste drie stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?

>> De volgende stap is het beantwoorden van de vraag *welke aanpak wordt gekozen bij het opstarten van een CSIRT*.

De volgende stap is een nadere analyse van de constituency met als voornaamste doel het kiezen van de juiste communicatiekanalen:

- De wijze van communicatie met de constituenten definiëren
- De mission statement definiëren
- Een realistisch implementatie-/projectplan opstellen
- De CSIRT-diensten definiëren
- De organisatiestructuur definiëren

- Het beleid voor informatiebeveiliging definiëren
- Het juiste personeel inhuren
- Uw CSIRT-kantoor gebruiken
- Samenwerking zoeken met andere CSIRT's en mogelijke landelijke initiatieven

Deze stappen worden in de volgende alinea's nader besproken. U kunt ze gebruiken als bouwstenen voor uw bedrijfs- en projectplan.

5.3.1 Wijze van communicatie met de constituency

Zoals al eerder is opgemerkt, is het van groot belang de behoeften van de constituency te kennen, alsook uw eigen communicatiestrategie. Daarbij horen de communicatie-kanalen die het meest geschikt zijn om de constituenten van informatie te voorzien.

Uit de managementtheorie zijn diverse manieren bekend om het analyseren van een doelgroep aan te pakken. In dit document worden er twee beschreven: de SWOT- en de PEST-analyse.

SWOT-analyse
Een SWOT-analyse (acroniem voor **S**trengths, **W**eaknesses, **O**pportunities en **T**hreats) is een hulpmiddel voor strategische planning, waarbij de sterke en zwakke punten plus de kansen en bedreigingen worden geëvalueerd van een project, een zakelijke activiteit of een andere situatie waarvoor een beslissing nodig is. Deze techniek is ontwikkeld door Albert Humphrey, die in de jaren '60 en '70 van de vorige eeuw leiding gaf aan een onderzoeksproject van de Stanford University en daarbij gegevens gebruikte van Fortune 500-bedrijven.[8]

Sterkte	**Zwakte**
Kansen	**Bedreigingen**

Fig. 2 SWOT-analyse

[8] SWOT-analyse op Wikipedia: http://nl.wikipedia.org/wiki/SWOT-analyse

PEST-analyse

De PEST-analyse is eveneens een belangrijk en veelgebruikt hulpmiddel om de constituency te analyseren. Het doel daarbij is inzicht in de **P**olitieke, **E**conomische, **S**ociaal-culturele en **T**echnologische omstandigheden van de omgeving waarin een CSIRT actief is. U kunt daardoor beter nagaan of de planning nog steeds is afgestemd op de omgeving en voorkomen dat u acties onderneemt op basis van onjuiste veronderstellingen.

Politiek	**Economisch**
• Ecologie/milieukwesties • Huidige binnenlandse wetgeving • Toekomstige wetgeving • Europese/internationale wetgeving • Regelgevende instanties en processen • Overheidsbeleid • Regeerperioden en veranderingen • Handelsbeleid • Financiering, subsidies en initiatieven • Binnenlandse lobby's/pressiegroepen • Internationale pressiegroepen	• Situatie van binnenlandse economie • Trends in binnenlandse economie • Overzeese economieën en trends • Algemene belastingkwesties • Specifieke belastingen voor producten/diensten • Seizoens-/weersgebonden kwesties • Markt- en handelscycli • Specifieke industriefactoren • Marktroutes en distributietrends • Drijfveren van klanten/eindgebruikers • Rentetarieven en wisselkoersen
Sociaal	**Technologisch**
• Trends in levensstijl • Demografische gegevens • Opvattingen en houding van consumenten • Kijk van de media • Wetswijzigingen die invloed hebben op sociale factoren • Imago van merk, bedrijf, technologie • Kooppatronen van consumenten • Mode en rolmodellen • Belangrijke gebeurtenissen en invloeden • Koopmogelijkheden en trends • Etnische/religieuze factoren • Reclame en publiciteit	• Concurrerende technologische ontwikkelingen • Financiering van onderzoek • Samenhangende/afhankelijke technologieën • Vervangende technologieën/oplossingen • Stabiliteit van technologie • Stabiliteit en capaciteit van productie • Informatie en communicatie • Koopmechanismen/-technologie van consumenten • Technologiewetgeving • Innovatiemogelijkheden • Toegang tot technologie, licenties, patenten • Kwesties betreffende intellectuele eigendom

Fig. 3 PEST-analysemodel

Een nadere beschrijving van de PEST-analyse vindt u op Wikipedia[9].

Beide hulpmiddelen zorgen voor een uitgebreid en gestructureerd overzicht van de behoeften van de constituenten. De resultaten vullen het zakelijke voorstel aan en helpen bij het verkrijgen van financiële middelen voor het opzetten van het CSIRT.

Communicatiekanalen

Een belangrijk item bij de analyse is de mogelijke methode voor communicatie en verspreiding van informatie ("Hoe vindt communicatie met de constituency plaats?").

[9] PEST-analyse op Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Als dat mogelijk is, zijn regelmatige persoonlijke bezoeken aan de constituenten zeker de moeite waard. Het staat vast dat persoonlijke ontmoetingen de samenwerking bevorderen. Als beide partijen tot samenwerking bereid zijn, werken deze bezoeken een opener relatie in de hand.

CSIRT's werken meestal met een reeks communicatiekanalen. De volgende kanalen hebben in de praktijk hun nut bewezen:

- Openbare website
- Besloten gedeelte voor leden op de website
- Webformulieren voor het melden van incidenten
- Mailinglists
- Persoonlijke e-mail
- Telefoon/fax
- Sms
- 'Traditionele' brieven
- Maand- of jaarrapporten

Het gebruik van e-mail, webformulieren, telefoon of fax bevordert een goede afhandeling van incidenten (het ontvangen van incidentmeldingen van de constituency, afstemmen met andere teams of geven van feedback en ondersteuning aan de getroffen partijen). Daarnaast publiceren de meeste CSIRT's hun eigen beveiligingsadviezen op een openbaar toegankelijke website en via mailinglists.

! Informatie moet indien mogelijk op een veilige manier worden verspreid. E-mail kan bijvoorbeeld digitaal worden ondertekend met PGP, en gevoelige gegevens over incidenten moet altijd gecodeerd worden verzonden.

Zie hoofdstuk *8.5 Beschikbare CSIRT-hulpprogramma's* voor meer informatie. Zie ook hoofdstuk *2.3* van *RFC2350*[10].

Fictief CSIRT (stap 3a)

Een analyse maken van de constituency en de juiste communicatiekanalen

Een brainstormsessie met enkele sleutelfiguren uit het management en de constituency heeft genoeg materiaal opgeleverd voor een SWOT-analyse. De conclusie is getrokken dat er behoefte is aan de kerndiensten:

- Alarmeringen en waarschuwingen
- Afhandeling van incidenten (analyse, ondersteuning bij reacties en coördinatie van reacties)
- Mededelingen

[10] http://www.ietf.org/rfc/rfc2350.txt

De informatie moet op een goed georganiseerde manier worden verspreid om het grootst mogelijke deel van de constituency te bereiken. Er is dan ook besloten om de alarmeringen, waarschuwingen en mededelingen in de vorm van beveiligingsadviezen te publiceren op een speciale website en via een mailinglist te verspreiden. Het CSIRT moet incidentmeldingen kunnen ontvangen via e-mail, telefoon en fax. Een uniform webformulier staat gepland als volgende stap.

Hieronder volgt een voorbeeld van een SWOT-analyse.

Sterkte • Er is enige kennis binnen het bedrijf • Men juicht het plan toe en is gewillig om samen te werken • Ondersteuning en financiële middelen door directie	**Zwakte** • Niet veel communicatie tussen de verschillende afdelingen en filialen • Geen coördinatie bij IT-incidenten • Veel ‘eigen afdelinkjes”
Kansen • Enorme stroom niet-gestructureerde informatie over beveiligingslekken • Grote behoefte aan coördinatie • Verliezen vanwege incidenten reduceren • Veel open einden wat betreft de IT-beveiliging • Personeel bewust maken van IT-beveiliging	**Bedreigingen** • Niet veel geld beschikbaar • Niet veel personeel beschikbaar • Hoge verwachtingen • Cultuur

Fig. 4 Voorbeeld van SWOT-analyse

5.3.2 Mission statement

Na het analyseren van de wensen en behoeften van de constituency wat betreft CSIRT-diensten, is de volgende stap het opstellen van een mission statement.

Een mission statement beschrijft de basisfunctie van de organisatie in de samenleving in termen van de producten en diensten die ze aan de constituenten levert. Het bestaan en de functie van het nieuwe CSIRT worden er helder mee omschreven.

Een goede mission statement is wel compact maar ook weer niet té en moet enkele jaren meegaan.

Hierna volgen enkele voorbeelden van mission statements van actieve CSIRT's:

"<Naam van CSIRT> biedt informatie en ondersteuning aan <constituenten (definieer uw constituenten)> door de implementatie van proactieve maatregelen om de kans op computerbeveiligingsincidenten te verkleinen en te reageren op dergelijke incidenten wanneer ze zich voordoen."

"Het bieden van ondersteuning aan <constituenten> bij de preventie van en reactie op IT-gerelateerde beveiligingsincidenten"[11]
De mission statement is een wezenlijke en noodzakelijke stap om mee te beginnen. Zie hoofdstuk *2.1* van *RFC2350*[12] voor een uitgebreide beschrijving van welke informatie een CSIRT zou moeten publiceren.

Fictief CSIRT (stap 3b)
Het management van het fictieve CSIRT heeft de volgende mission statement opgesteld: *"Fictief CSIRT biedt informatie en ondersteuning aan de medewerkers van de hostorganisatie om de kans op computerbeveiligingsincidenten te verkleinen en te reageren op dergelijke incidenten wanneer ze zich voordoen."* Hiermee maakt het fictieve CSIRT duidelijk dat het een intern CSIRT betreft en dat de kernactiviteit is gericht op kwesties rondom IT-beveiliging.

[11] Mission statement van Govcert.nl: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Het bedrijfsplan ontwikkelen

We hebben de volgende stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?
4. Analyse van de omgeving en constituenten.
5. De mission statement definiëren.

>> De volgende stap is het definiëren van het bedrijfsplan.

De resultaten van de analyse geven u een goed overzicht van de behoeften en de (veronderstelde) zwakten van de constituency en worden als basis gebruikt voor de volgende stap.

6.1 Het financiële model definiëren

Na de analyse zijn enkele kerndiensten gekozen om mee te beginnen. De volgende stap is nadenken over het financiële model: welke parameters van de dienstverlening zijn zowel geschikt als betaalbaar.

In een volmaakte wereld is er altijd genoeg geld om in de behoeften van de constituency te voorzien, maar in de werkelijkheid bepaalt het beschikbare budget welke diensten mogelijk zijn. Beginnen met de financiële kant is dus wel net zo realistisch.

6.1.1 Kostenmodel

De twee voornaamste factoren die de kosten beïnvloeden zijn het vaststellen van het aantal service-uren en het aantal medewerkers (plus de kwaliteit ervan) die worden ingezet. Is er behoefte aan continue reactie op incidenten en technische ondersteuning (24x7) of worden deze diensten alleen tijdens kantooruren verleend?

Afhankelijk van de gewenste beschikbaarheid en de kantoorfaciliteiten (kan er bijvoorbeeld van thuis worden gewerkt?) kan het voordelen hebben om te werken volgens een oproepbaarheidsrooster of een rooster met geplande beschikbaarheid.

Een denkbaar scenario is het leveren van zowel proactieve als reactieve diensten tijdens kantooruren. Buiten kantooruren worden alleen beperkte diensten geboden, bijvoorbeeld alleen in dringende noodsituaties of grote incidenten, door een medewerker die op oproep beschikbaar is.

Een andere optie is te kijken naar internationale samenwerking met andere CSIRT's. Er zijn al voorbeelden van samenwerking met opeenvolgende diensten in verschillende tijdzones. Zo is samenwerking tussen Europese en Amerikaanse teams nuttig gebleken en een goede manier om van elkaars capaciteit te profiteren. Het CSIRT van Sun Microsystems kent meerdere afdelingen in verschillende tijdzones in de hele wereld

(maar iedereen maakt deel uit van hetzelfde CSIRT) en levert continue dienstverlening (24x7) via de opeenvolgende diensten van de teams over de wereld. Hierdoor blijven de kosten beperkt, omdat de teams altijd op normale kantooruren werken en tevens hun diensten verlenen aan het “slapende deel” van de wereld.

Het is verstandig om met name de behoefte aan continue diensten (24x7) in de constituency grondig te analyseren. Alarmeringen en waarschuwingen tijdens de nacht zijn niet echt zinvol als de ontvanger deze pas de volgende ochtend leest. Het verschil tussen “servicebehoefte” en “servicewens” is niet altijd even duidelijk, maar vooral de werkuren maken een groot verschil in het aantal medewerkers en de faciliteiten die nodig zijn. Het kostenmodel wordt hierdoor in belangrijke mate beïnvloed.

6.1.2 Financieringsmodel

Wanneer de kosten bekend zijn, is een volgende goede stap het nadenken over mogelijke financieringsmodellen: hoe kunnen de geplande diensten worden bekostigd. Hier zijn enkele mogelijke scenario’s om te evalueren:

Gebruik van bestaande middelen
Het is altijd gunstig om de al aanwezige middelen in andere delen van de organisatie onder de loep te nemen. Zijn er al medewerkers in dienst (bijvoorbeeld op de bestaande IT-afdeling) met de vereiste achtergrond en deskundigheid? In de beginfase kunnen deze medewerkers wellicht worden aangewezen om deel te nemen aan het CSIRT, of incidenteel ondersteuning te bieden aan het CSIRT waar en wanneer dat nodig is.

Abonnementskosten
Een andere mogelijkheid is het verkopen van uw diensten aan de constituency door middel van een bijdrage per jaar of kwartaal. Aanvullende diensten kunnen per afgenomen dienst in rekening worden gebracht, zoals adviezen of controles op beveiligingsgebied.

Nog een mogelijk scenario: aan de (interne) constituency verleende diensten zijn gratis, maar diensten aan externe klanten zijn niet gratis. Een ander idee is om aanbevelingen en informatiebulletins te publiceren op de openbare website, met een gedeelte “alleen voor leden” met meer gedetailleerde en relevante informatie.

Uit de praktijk blijkt een abonnement op basis van verleende CSIRT-diensten niet echt voldoende financiële middelen te genereren, vooral in de beginfase. Er zijn bijvoorbeeld vaste kosten voor het team en de voorzieningen die vooraf moeten worden betaald. Deze kosten zijn vaak niet door het verkopen van CSIRT-diensten terug te verdienen. Er is dan ook een zeer gedetailleerde financiële analyse nodig om het omslagpunt te berekenen.

Subsidie
Het valt ook te overwegen een aanvraag te doen voor projectsubsidie van de overheid of een overheidsinstantie, aangezien de meeste landen tegenwoordig geld beschikbaar hebben voor IT-beveiligingsprojecten. Neem bijvoorbeeld eens contact op met het desbetreffende ministerie.

Uiteraard kunt u gebruikmaken van meerdere modellen tegelijk.

6.2 De organisatiestructuur definiëren

De geschikte organisatiestructuur van een CSIRT is grotendeels afhankelijk van de bestaande structuur van de hostorganisatie en de constituency. Ook speelt een rol of ervaren experts permanent of incidenteel werkzaam zullen zijn.

Een doorsnee-CSIRT definieert de volgende rollen binnen het team:

Algemeen
- Algemeen manager

Personeel
- Algemeen manager
- Accountant
- Communicatieadviseur
- Juridisch adviseur

Operationeel technisch team
- Hoofd van technisch team
- CSIRT-technici die de CSIRT-diensten verlenen
- Onderzoekers

Externe adviseurs
- Ingehuurd wanneer dat nodig is

Het is zeker in de beginfase van het CSIRT uitermate handig om een juridisch specialist erbij te betrekken. De extra kosten verdienen zich uiteindelijk terug doordat tijd wordt bespaard en onnodige juridische problemen worden vermeden.

Afhankelijk van de diversiteit van de deskundigheid binnen de constituency, en tevens wanneer het CSIRT veel aandacht van de media trekt, is een communicatiedeskundige in het team ook nuttig gebleken. Deze specialisten kunnen zich bezighouden met het vertalen van moeilijke technische kwesties in begrijpelijke boodschappen voor de constituenten of mediapartners. De communicatiedeskundige geeft ook feedback van de constituency door aan de technische experts, zodat hij of zij als “vertaler” en “facilitator” optreedt tussen deze twee groepen.

Hierna volgen enkele voorbeelden van organisatiemodellen die door actieve CSIRT’s worden toegepast.

6.2.1 Het onafhankelijke bedrijfsmodel

Het CSIRT is opgezet en werkt als een zelfstandige organisatie, met eigen management en medewerkers.

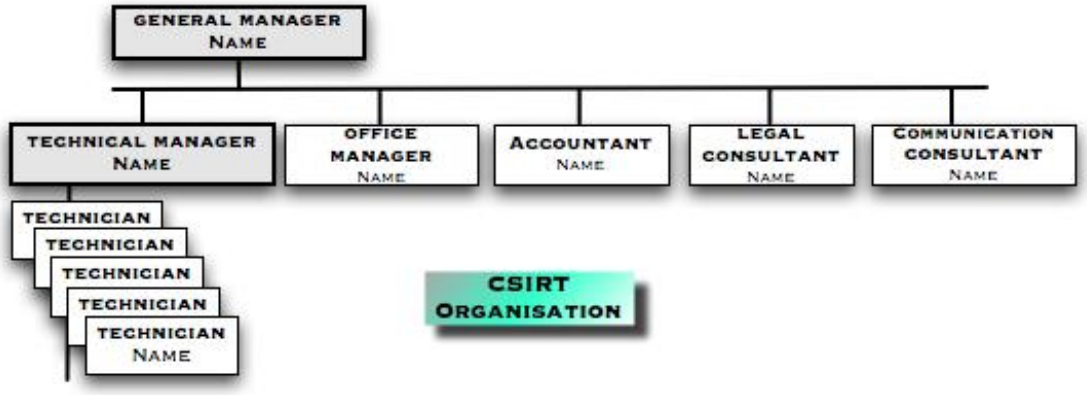


Fig. 5 Onafhankelijk bedrijfsmodel

6.2.2 Het ingesloten model

Dit model is bruikbaar als binnen een bestaande organisatie een CSIRT wordt opgezet waarvoor bijvoorbeeld een bestaande IT-afdeling wordt gebruikt. Het CSIRT wordt geleid door een teamleider, die verantwoordelijk is voor de CSIRT-activiteiten. De teamleider verzamelt de benodigde technici bij het oplossen van incidenten of het werken aan CSIRT-activiteiten. Hij of zij kan binnen de bestaande organisatie assistentie vragen voor specialistische ondersteuning.

Dit model kan worden aangepast in het geval van bijzondere situaties. In dat geval krijgt het team een vast aantal FTE's (Full Time Equivalents) toegewezen. De helpdesk voor misbruik bij een ISP is bijvoorbeeld een fulltimetaak voor één of (meestal) meer dan één FTE.

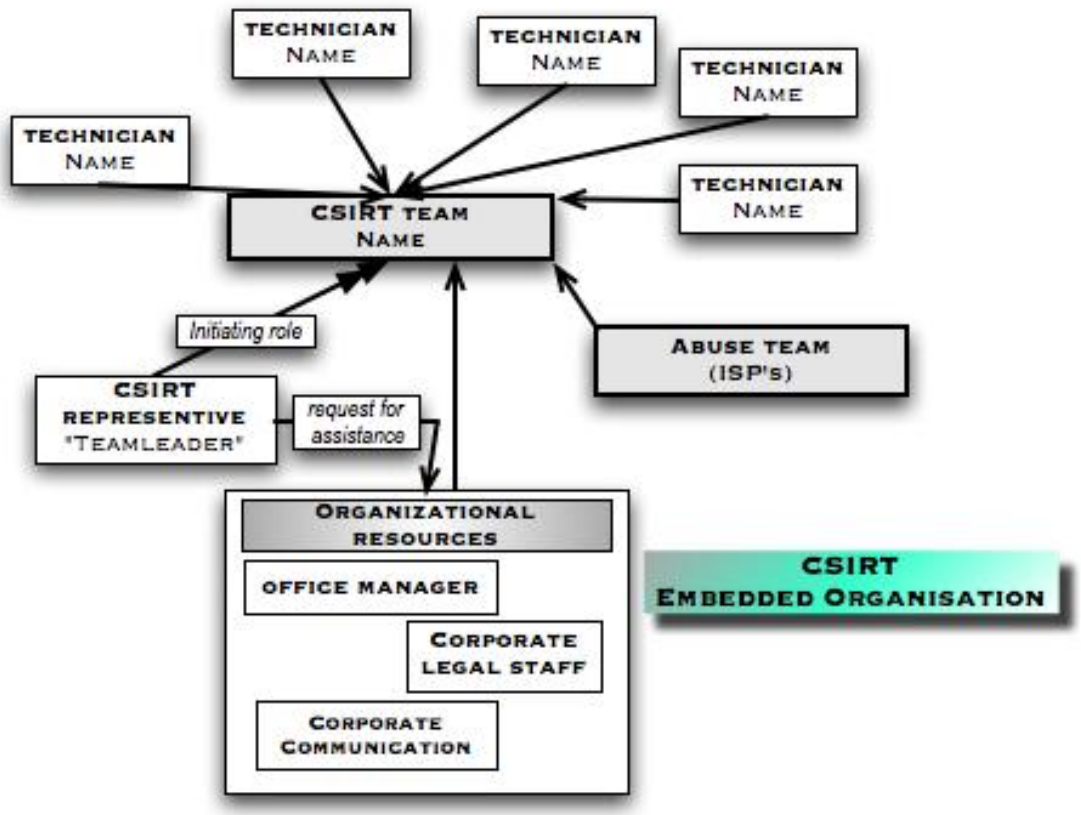


Fig. 6 Ingesloten organisatiemodel

6.2.3 Het campusmodel

Het campusmodel (de naam zegt het al) wordt meestal toegepast door CSIRT's voor academische of onderzoeksinstellingen. De meeste academische of onderzoeks-organisaties bestaan uit meerdere universiteiten en campussen op verschillende locaties in een regio of zelfs een heel land, zoals de zogenaamde NREN's (National Research Networks). Deze organisaties zijn doorgaans onafhankelijk van elkaar en hebben elk hun eigen CSIRT. Deze CSIRT's vallen gewoonlijk wel onder de paraplu van een overkoepelend CSIRT. Het overkoepelende CSIRT coördineert en is het aanspreekpunt voor de buitenwereld. In de meeste gevallen verzorgt het overkoepelende CSIRT tevens de CSIRT-kerndiensten, alsook de verspreiding van incidentinformatie aan de desbetreffende campus-CSIRT.

Sommige CSIRT's laten de CSIRT-kerndiensten circuleren onder de andere campus-CSIRT's, wat resulteert in minder overhead voor het overkoepelende CSIRT.

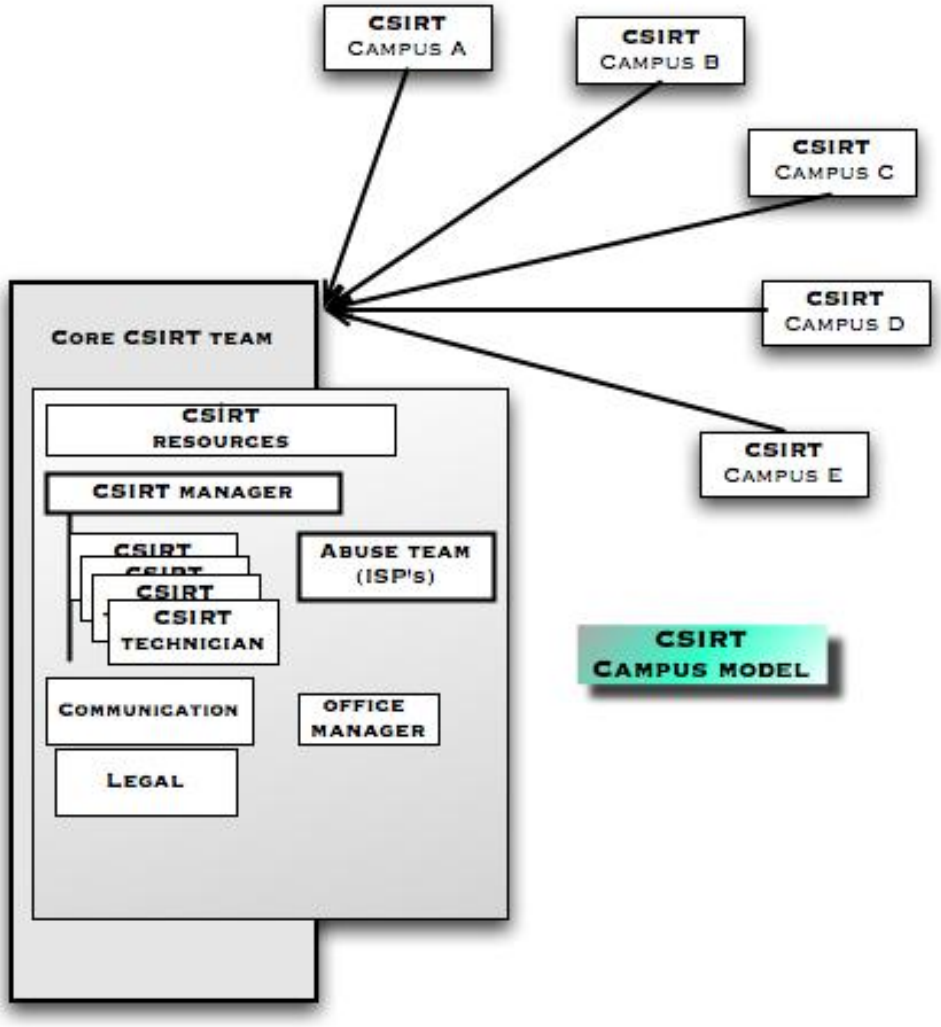


Fig. 7 Campusmodel

6.2.4 Het vrijwillige model

Dit organisatiemodel beschrijft een groep mensen (specialisten) die onderling zorgen voor advies en ondersteuning aan elkaar (en anderen) op vrijwillige basis. Er is geen strakke organisatie en alles staat of valt met de motivatie van de deelnemers.

Dit model wordt bijvoorbeeld gebruikt door de WARP-gemeenschap[13].

6.3 Het juiste personeel inhuren

Na het vaststellen van de te verlenen diensten en het niveau van ondersteuning, en na het kiezen van een organisatiemodel, is de volgende stap het vinden van de juiste hoeveelheid ervaren mensen om het werk te doen.

Harde cijfers over het benodigde aantal technisch geschoolde medewerkers is in dit opzicht niet te geven. De volgende aantallen geven vanuit de praktijk echter vaak een goede indicatie:

- voor de levering van de twee kerndiensten voor verspreiding van adviesbulletins en afhandeling van incidenten: minimaal **4** FTE's;
- voor een CSIRT dat tijdens de kantooruren alle diensten verleent en instaat voor het onderhoud van systemen: minimaal **6 tot 8** FTE's;
- voor een volledig bemande continudienst (24x7, 2 diensten buiten kantooruren): minimaal circa **12** FTE's.

In deze getallen zijn overtolligheden verwerkt voor ziekte, vakantie en dergelijke. Ook moet u de lokale CAO's erop naslaan. Als mensen buiten kantooruren werken, zijn vaak toeslagen (en dus extra kosten) van toepassing.

Hierna volgt een beknopt overzicht van de belangrijkste competenties voor de technische experts van een CSIRT.

Algemene items in de taakomschrijving van technisch personeel:

Persoonlijke competenties

- Flexibel, creatief en goede teamgeest
- Goede analytische vaardigheden
- Vaardigheid om moeilijke technische zaken in eenvoudige woorden uit te leggen
- Een goed gevoel voor vertrouwelijkheid en het werken in een procedurele zaak
- Goede organisatorische vaardigheden
- Stressbestendig
- Goede communicatieve en schriftelijke vaardigheden
- Ruimdenkend en leergierig

Technische competenties

- Brede kennis van internettechnologie en -protocollen

[13] Het WARP-initiatief: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

- Kennis van Linux- en Unix-systemen (afhankelijk van de gebruikte apparatuur in de constituency)
- Kennis van Windows-systemen (afhankelijk van de gebruikte apparatuur in de constituency)
- Kennis van apparatuur voor de netwerkinfrastructuur (router, switches, DNS, Proxy, Mail, etc.)
- Kennis van internetapplicaties (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Kennis van bedreigingen voor de beveiliging (DDoS, phishing, defacing, sniffing, etc.)
- Kennis van risicoanalyses en praktische implementaties

Aanvullende competenties

- Bereidheid om in diensten op basis van 24x7 of oproepbaarheid te werken (afhankelijk van het servicemodel)
- Maximale reisafstand (in het geval van aanwezigheid bij noodsituaties op kantoor; maximale reistijd)
- Opleidingsniveau
- Werkervaring op het gebied van IT-beveiliging

Fictief CSIRT (stap 4)

Het bedrijfsplan definiëren

Financieel model

Het bedrijf heeft een e-business van 24x7 en tevens een IT-afdeling die 24x7 inzetbaar is. Er is dan ook besloten om volledige service te verlenen tijdens kantooruren en een oproepbaarheidsdienst buiten kantooruren. De aan de constituency verleende diensten zullen gratis zijn. De mogelijkheid om diensten aan externe klanten te bieden wordt nader bekeken in de test- en evaluatiefase.

Financieringsmodel

In de start- en testfase wordt het CSIRT gefinancierd door het hostbedrijf. In de test- en evaluatiefase worden extra financieringsbronnen besproken, waaronder de mogelijkheid om diensten aan externe klanten te verkopen.

Organisatiemodel

De hostorganisatie is een kleine onderneming, dus wordt het ingesloten model gekozen. Tijdens kantooruren verzorgen drie medewerkers de kerndiensten (verspreiding van beveiligingsadviezen en afhandeling/coördinatie van incidenten).

Op de IT-afdeling van het bedrijf werken al mensen met de benodigde ervaring. Met die afdeling is de afspraak gemaakt dat het nieuwe CSIRT op incidentele basis ondersteuning kan vragen wanneer dat nodig is. Ook de tweede lijn van hun oproepbare technici kan worden gebruikt.
Er komt een CSIRT-basisteam met vier fulltime-medewerkers en vijf extra CSIRT-teamleden. Een van die medewerkers is beschikbaar in circulerende diensten.

Personeel

De teamleider van het CSIRT heeft een achtergrond in beveiliging en ondersteuning op het eerste en tweede niveau en werkervaring op het gebied van veerkracht/crisisbeheer. De drie andere teamleden zijn beveiligingsspecialisten. De parttime-CSIRT-teamleden van de IT-afdeling zijn specialisten op hun gebied van de infrastructuur van het bedrijf.

6.4 Gebruik en inrichting van het kantoor

De inrichting en het gebruik van de kantoorruimte en de fysieke beveiliging zijn nogal ruime onderwerpen. In dit document kan dan ook geen uitputtende beschrijving worden gegeven. Dit hoofdstuk is bedoeld als een kort overzicht van dit onderwerp.

Meer informatie over fysieke beveiliging is te vinden op:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"Het gebouw versterken"
CSIRT's werken doorgaans met zeer gevoelige informatie. Het team kan dan ook best de fysieke beveiliging van het kantoor regelen. Dit hangt in grote mate af van de bestaande faciliteiten en infrastructuur en het gehanteerde informatiebeveiligingsbeleid van de hostorganisatie.

Overheden werken bijvoorbeeld met classificatieschema's en gaan zeer strikt om met vertrouwelijke informatie. Vraag bij uw eigen bedrijf of instelling na welke plaatselijke regels en voorschriften gelden.

Een nieuw CSIRT moet door de hostorganisatie op de hoogte worden gebracht van lokale regels, voorschriften en andere juridische zaken.

Een uitgebreide beschrijving van alle benodigde faciliteiten en beveiligingsmaatregelen kan in dit document niet worden gegeven. Hieronder staat echter wel een kort overzicht van de basisfaciliteiten voor uw CSIRT:

Algemene regels voor het gebouw
- Zorg voor toegangscontroles
- Maak het CSIRT-kantoor, op zijn minst, alleen toegankelijk voor CSIRT-personeel
- Bewaak de kantoren en ingangen met camera's
- Archiveer vertrouwelijke informatie in afgesloten plekken of in een kluis
- Gebruik beveiligde IT-systemen

Algemene regels voor IT-faciliteiten
- Gebruik apparatuur waarvoor het personeel ondersteuning kan geven
- Versterk alle systemen
- Zorg voor patches en updates van alle systemen voordat u verbinding maakt met internet
- Gebruik beveiligingssoftware (firewalls, meerdere antivirusscanners, antispyware, etc.)

Communicatiekanalen onderhouden
- Openbare website
- Besloten gedeelte voor leden op de website
- Webformulieren voor het melden van incidenten
- E-mail (ondersteuning van PGP/GPG/S/MIME)
- Software voor mailinglists
- Zorg voor een speciaal telefoonnummer die voor de constituency beschikbaar is:
    - Telefoon
    - Fax
    - Sms

Volgsystemen
- Contactdatabase met gegevens van teamleden, andere teams, etc.
- CRM-programma's
- Ticketsysteem voor afhandeling van incidenten

Gebruik vanaf het begin de "huisstijl van de organisatie" voor:
- De indeling van gewone e-mailberichten en adviesbulletins
- 'Traditionele' brieven
- Maand- of jaarrapporten
- Incidentmeldingsformulieren

Overige zaken
- Zorg voor alternatieve communicatiemiddelen in het geval van aanvallen
- Zorg voor redundantie van internetverbindingen

Zie hoofdstuk *8.5 Beschikbare CSIRT-hulpprogramma's* voor meer informatie over specifieke CSIRT-hulpprogramma's.

6.5 Een beleid voor informatiebeveiliging ontwikkelen

Afhankelijk van het type CSIRT hebt u een eigen beleid voor informatiebeveiliging. Dit beleid geeft een beschrijving van de gewenste status van operationele en administratieve processen en procedures. Daarnaast moet het beleid in lijn zijn met geldende wetgeving en normen, vooral met betrekking tot de aansprakelijkheid van het CSIRT. Het CSIRT is gewoonlijk gebonden aan nationale wetten en voorschriften. Deze worden veelal geïmplementeerd in de context van Europese wetgeving (richtlijnen) en andere internationale afspraken. Normen zijn niet altijd direct bindend, maar kunnen door wetten en voorschriften verplicht worden gesteld of worden aanbevolen.

Hieronder volgt een lijst met mogelijke wetten en beleidsregels:

Nationaal
- Diverse wetten inzake informatietechnologie, telecommunicatie, media
- Wetten inzake de bescherming van gegevens en de privacy
- Wetten en voorschriften inzake het bewaren van gegevens
- Wetgeving inzake financiën, boekhouding en bedrijfsvoering

- Gedragscodes voor het besturen van bedrijven en IT-beheer

Europees
- Richtlijn betreffende elektronische handtekeningen (1993/93/EG)
- Richtlijnen betreffende de bescherming van gegevens (1995/46/EG) en de privacy in elektronische communicaties (2002/58/EG)
- Richtlijnen betreffende elektronischecommunicatienetwerken en -diensten (2002/19/EG – 2002/22/EG)
- Richtlijnen betreffende bedrijfsrecht (bijvoorbeeld de Achtste Richtlijn)

Internationaal
- Basel II-akkoord (vooral met betrekking tot het beheersen van operationele risico's)
- Verdrag van de Raad van Europa inzake cybercriminaliteit
- Verdrag van de Raad van Europa tot bescherming van de rechten van de mens (artikel 8 over privacy)
- International Accounting Standards (IAS; stellen in zekere mate IT-controles verplicht)

Normen
- Britse norm BS 7799 (informatiebeveiliging)
- Internationale normen ISO2700x (systemen voor informatiebeveiligingsbeheer)
- IT-Grundschutzbuch (Duits), EBIOS (Frans) en andere nationale varianten

Raadpleeg uw juridisch adviseur om uit te maken of uw CSIRT handelt in overeenstemming met de nationale en internationale wetgeving.

De meest elementaire vragen die u moet beantwoorden in uw beleidsregels voor de behandeling van informatie zijn:

- Hoe wordt binnenkomende informatie "gelabeld" of "geclassificeerd"?
- Hoe wordt informatie behandeld, vooral met betrekking tot exclusiviteit?
- Welke overwegingen spelen mee voor het onthullen van informatie, vooral bij het doorgeven van incidentgerelateerde informatie aan andere teams of locaties?
- Zijn er juridische aspecten waarbij rekening moet worden gehouden bij de behandeling van informatie?
- Hanteert u een beleid voor het gebruik van cryptografie ter bescherming van de exclusiviteit en integriteit in archieven en/of de communicatie van gegevens, vooral in e-mail?
- Omvat dit beleid mogelijke juridische begrenzingen, zoals key-escrow of gedwongen decodering bij rechtszaken?

Fictief CSIRT (stap 5)

Kantoorfaciliteiten en -locatie

Het hostbedrijf is al voorzien van een efficiënte fysieke beveiliging en het CSIRT is in dat opzicht dan ook prima gehuisvest. Er is een “crisisruimte” beschikbaar voor coördinatiedoeleinden in noodsituaties. Er is een kluis aangeschaft voor het versleutelingsmateriaal en vertrouwelijke documenten. Er is een aparte telefoonlijn met een schakelkast als hotline tijdens kantooruren en een mobiele telefoon voor oproepen buiten kantooruren met hetzelfde telefoonnummer.

Bestaande apparatuur alsook de website van het bedrijf zijn beschikbaar voor het melden van CSIRT-gerelateerde informatie. Er wordt een mailinglist geïnstalleerd en bijgehouden, met een besloten gedeelte voor de communicatie tussen teamleden en met andere teams. Alle contactgegevens van de medewerkers zijn opgeslagen in een database, met een afgedrukt exemplaar veilig opgeborgen in de kluis.

Voorschriften
Het CSIRT maakt deel uit van een bedrijf met bestaande beleidsregels voor de informatiebeveiliging, zodat het beleid voor het CSIRT is vastgesteld met de hulp van de juridisch adviseur van het bedrijf.

6.6 Samenwerking zoeken met andere CSIRT's en mogelijke landelijke initiatieven

Het bestaan van andere CSIRT-initiatieven en de dringende behoefte aan samenwerking is al enkele keren genoemd in dit document. Het is verstandig om zo vroeg mogelijk contact te leggen met andere CSIRT's, om zo contact te krijgen met de CSIRT-gemeenschappen. Andere CSIRT's staan doorgaans zeer open om nieuwe teams op gang te helpen.

Het ENISA-overzicht van CERT-activiteiten in Europa[14] kan u helpen bij het zoeken naar andere CSIRT's in het land of naar landelijke activiteiten waarbij CSIRT's samenwerken.

Neem contact op met de CSIRT-experts van ENISA voor hulp bij het zoeken naar geschikte bronnen met CSIRT-informatie:

CERT-Relations@enisa.europa.eu

Hierna volgt een overzicht van activiteiten van CSIRT-gemeenschappen. Raadpleeg het overzicht van ENISA voor een uitgebreidere beschrijving en meer informatie.

Europees CSIRT-initiatief

TF-CSIRT[15]
De TF-CSIRT-taakgroep stimuleert de samenwerking tussen CSIRT's in Europa. De hoofddoelen van deze taakgroep zijn het bieden van een forum voor de uitwisseling van kennis en ervaring, het instellen van pilotservices voor de Europese CSIRT-gemeenschap en het bieden van ondersteuning bij het opzetten van nieuwe CSIRT's.

De taakgroep houdt zich met name bezig met het volgende:
- Het bieden van een forum voor de uitwisseling van kennis en ervaring
- Het instellen van pilotservices voor de Europese CSIRT-gemeenschap
- Het stimuleren van gemeenschappelijke normen en procedures voor de afhandeling van beveiligingsincidenten

[14] ENISA-overzicht: http://www.enisa.europa.eu/cert_inventory/

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

- Het bieden van ondersteuning bij het opzetten van nieuwe CSIRT's en het trainen van CSIRT-personeel.
- De activiteiten van TF-CSIRT zijn gericht op Europa en naburige landen, overeenkomstig de referentievoorwaarden die zijn goedgekeurd door het TTC (TERENA Technical Committee) op 15 september 2004.

Wereldwijd CSIRT-initiatief

FIRST[16]
FIRST is de eerste organisatie en erkend wereldleider op het gebied van incidentafhandeling. Lidmaatschap in FIRST stelt beveiligingsteams in staat om effectiever te reageren op beveiligingsincidenten – niet alleen reactief maar ook proactief.

FIRST brengt diverse CSIRT's uit de sectoren overheid, bedrijfsleven en onderwijs samen. FIRST streeft ernaar de samenwerking en coördinatie op het gebied van preventie van incidenten en een snelle reactie op incidenten te bevorderen, alsook het uitwisselen van informatie tussen leden en de gemeenschap in het algemeen te stimuleren.

Naast het vertrouwde netwerk dat FIRST vormt in de wereldwijde CSIRT-gemeenschap, levert FIRST ook diensten met toegevoegde waarde.

Fictief CSIRT (stap 6)
Samenwerking zoeken Met behulp van het ENISA-overzicht zijn enkele CSIRT's in hetzelfde land gevonden en benaderd. Voor de nieuwe teamleider werd een bezoek aan een van die CSIRT's geregeld. Hij leerde over landelijke CSIRT-activiteiten en woonde een bijeenkomst bij. Deze bijeenkomst was uiterst nuttig voor het verzamelen van voorbeelden van werkmethoden en het verkrijgen van ondersteuning van enkele andere teams.

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

7 Het bedrijfsplan promoten

We hebben tot nu toe de volgende stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?
4. Analyse van de omgeving en constituenten.
5. De mission statement definiëren.
6. Het bedrijfsplan ontwikkelen.
    a. Het financiële model definiëren
    b. De organisatiestructuur definiëren
    c. Personeel inhuren
    d. Gebruik en inrichting van het kantoor
    e. Een beleid voor informatiebeveiliging ontwikkelen
    f. Samenwerkingspartners zoeken

>> De volgende stap is het bovenstaande in een projectplan op te nemen en aan de slag te gaan!

Een praktische, zakelijke onderbouwing of 'business case' is een goed begin voor het definiëren van uw project. Deze zakelijke onderbouwing wordt gebruikt als basis voor het projectplan en tevens voor het vragen van de ondersteuning en financiële of andere middelen aan het management.

Het werpt zijn vruchten af om het management voortdurend op de hoogte houden en zo de problemen van de IT-beveiliging hoog op de agenda te houden. Dat is ook nodig voor permanente ondersteuning van het eigen CSIRT.

Een zakelijke onderbouwing begint met een analyse van de problemen en kansen met behulp van een analysemodel (zie hoofdstuk *5.3 Analyse van de constituency*) en het zoeken van nauw contact met de potentiële constituency.

Zoals al eerder is beschreven, zijn er veel aandachtspunten bij het starten van een CSIRT. Het eerder genoemde materiaal kan het best gaandeweg worden aangepast aan de groeiende behoeften van het CSIRT.

Bij het rapporteren aan het management kunt u de eigen zakelijke onderbouwing best zo actueel mogelijk maken. Dit kan door recente artikelen uit dagbladen of internet te gebruiken en uit te leggen waarom de CSIRT-diensten en interne coördinatie van incidenten cruciaal zijn voor de veiligheid van bedrijfsmiddelen. Ook moet u duidelijk maken dat alleen continue ondersteuning op het gebied van IT-beveiliging een bedrijf of instelling stabiel maakt, zeker als men afhankelijk is van IT.

(Een prominente uitspraak van Bruce Schneier is raak wat dat betreft: *"Beveiliging is geen product maar een proces[17]!"*)

Een bekend hulpmiddel ter illustratie van de beveiligingsproblemen is de volgende grafiek van het CERT/CC:

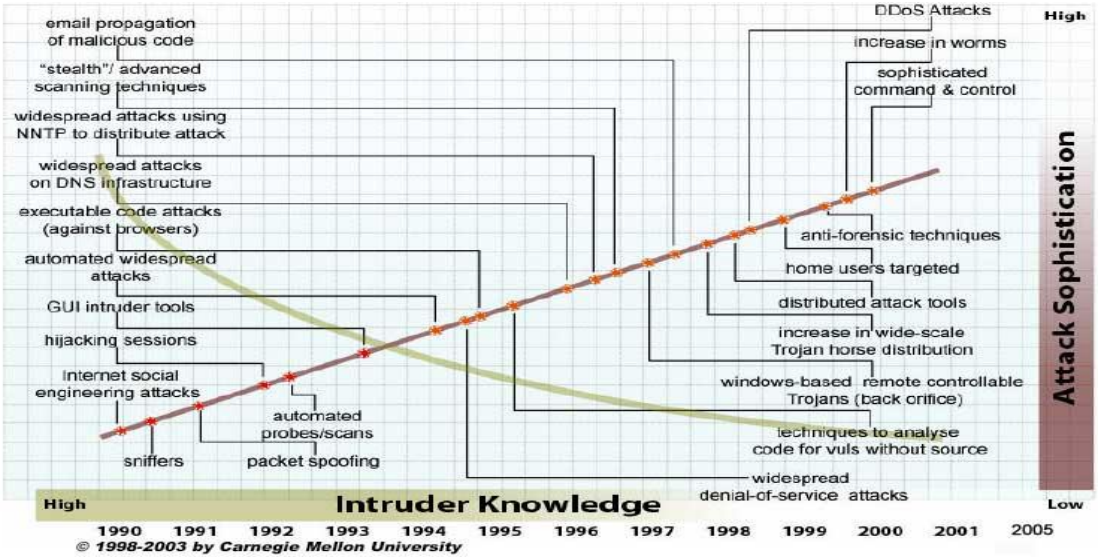


Fig. 8 Kennis van indringers versus complexiteit van aanvallen (bron CERT-CC[18])

De grafiek visualiseert de trends in IT-beveiliging, met name de afnemende kennis die nodig is om steeds complexere aanvallen uit te voeren.

Nog een punt om te vermelden is de steeds kortere tijd tussen de beschikbaarheid van software-updates voor beveiligingslekken en kwetsbaarheden en het begin van nieuwe aanvallen ertegen:

Patch -> Misbruik		**Verspreidingssnelheid**	
Nimda:	11 maanden	Code Red:	Dagen
Slammer:	6 maanden	Nimda:	Uren
Nachi:	5 maanden	Slammer:	Minuten
Blaster:	3 weken		
Witty:	1 dag (!)		

Verzamelde incidentgegevens, mogelijke verbeteringen en opgedane ervaringen zetten een presentatie eveneens kracht bij.

[17] Bruce Schneier: http://www.schneier.com/

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1 Beschrijving van bedrijfsplannen en overtuiging van het management

Een presentatie aan het management met de promotie van alleen het CSIRT biedt onvoldoende zakelijke onderbouwing. Doet u dit echter op de juiste manier, dan zal het management in de meeste gevallen bereid zijn het CSIRT te ondersteunen. Aan de andere kant heeft de zakelijke onderbouwing niet alleen als doel het management te overtuigen, maar moet u deze ook communiceren naar het team en de constituency. Zakelijke onderbouwing klinkt als term wellicht nogal commercieel en ver weg van de dagelijkse CSIRT-praktijk, maar geeft wel focus en richting bij het opzetten van een CSIRT.

De antwoorden op de volgende vragen kunnen bij een goede zakelijke onderbouwing een rol spelen (de voorbeelden zijn hypothetisch en dienen alleen ter illustratie. De “werkelijke” antwoorden zijn afhankelijk van de “werkelijke” omstandigheden).

- Wat is het probleem?
- Wat wilt u bereiken met de constituenten?
- Wat gebeurt er als u niets doet?
- Wat gebeurt er als u actie onderneemt?
- Wat gaat het kosten?
- Wat levert het op?
- Wanneer begint u en wanneer is het klaar?

Wat is het probleem?
Vaak ontstaat het idee om een CSIRT op te zetten wanneer IT-beveiliging een essentieel onderdeel is geworden van de kernactiviteiten van een bedrijf of instelling. IT-beveiligingsincidenten vormen dan een bedrijfsrisico en het bevorderen van de veiligheid is een normale bedrijfsactiviteit geworden.

De meeste bedrijven of instellingen hebben een reguliere helpdesk of afdeling voor ondersteuning, maar beveiligingsincidenten worden minder goed en minder gestructureerd afgehandeld dan zou moeten. Voor beveiligingsincidenten zijn doorgaans speciale vaardigheden en aandacht vereist. Een meer gestructureerde aanpak werpt bovendien vruchten af en beperkt de bedrijfsrisico’s en schade voor de organisatie.

Het probleem is meestal een gebrek aan coördinatie en het feit dat de aanwezige kennis niet wordt benut om incidenten aan te pakken. Nochtans kunnen zo in de toekomst dezelfde incidenten en de mogelijke financiële verliezen en/of beschadigde reputatie van de organisatie worden voorkomen.

Wat zijn de doelen om te bereiken met de constituenten?
Al eerder is uitgelegd dat uw CSIRT diensten verleent aan zijn constituenten en ze ondersteunt bij het oplossen van IT-beveiligingsincidenten en -problemen. Het kennisniveau op het gebied van IT-beveiliging verhogen en een veiligheidsbewuste cultuur kweken zijn aanvullende doelen.

Vanuit deze cultuur worden vanaf het begin proactieve en preventieve maatregelen genomen, waardoor de operationele kosten worden gedrukt.

Het vestigen van een dergelijke cultuur van samenwerking en ondersteuning in een bedrijf of instelling kan vaak stimulerend werken op de efficiëntie in het algemeen.

Wat gebeurt er als er niets wordt gedaan?
Een ongestructureerde afhandeling van IT-beveiligingsincidenten kan tot verdere schade leiden, inclusief de reputatie van de organisatie. Financiële verliezen en juridische gevolgen zijn eveneens goed mogelijk.

Wat gebeurt er als er actie wordt ondernomen?
Men wordt zich bewuster van het optreden van beveiligingsproblemen. Zo zijn een efficiëntere oplossing van deze problemen en voorkoming van toekomstige verliezen beter mogelijk.

Wat gaat het kosten?
Afhankelijk van het organisatiemodel zijn er kosten voor de salarissen van de CSIRT-teamleden en de organisatie, inrichting, hulpmiddelen en softwarelicenties.

Wat levert het op?
Afhankelijk van de activiteiten en de verliezen in het verleden is sprake van meer transparantie in procedures en beveiligingspraktijken. Dit resulteert in de bescherming van essentiële bedrijfsmiddelen.

Wat is het tijdsbestek?
Zie hoofdstuk *12. Beschrijving van het projectplan* voor de beschrijving van een voorbeeldprojectplan.

Voorbeelden van bestaande praktijksituaties met zakelijke onderbouwingen en werkwijzen
Hierna volgen enkele voorbeelden van de zakelijke praktijk van CSIRT's die de moeite waard zijn om nader te bekijken:

- http://www.cert.org/csirts/AFI_case-study.html
  Een CSIRT opzetten voor een financiële instelling in de praktijk.

  Het doel van dit document is het delen van de ervaringen doe een financiële instelling (in dit document AFI genoemd) heeft opgedaan bij de ontwikkeling en implementatie van een plan voor de aanpak van beveiligingsproblemen en een CSIRT.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Samenvatting van de zakelijke praktijk van CERT POLSKA (diapresentatie in pdf-formaat).

- http://www.auscert.org.au/render.html?it=2252
  Het samenstellen van een Incident Response Team (IRT) in de jaren '90 kan een lastige zaak zijn. Veel mensen vormen een IRT zonder daarin ervaring te hebben. In

dit document wordt de rol bestudeerd die een IRT kan spelen in de gemeenschap, plus de problemen die moeten worden aangepakt bij het opzetten van het IRT en na het starten ervan. Bestaande IRT's kunnen er baat bij hebben door probleemgebieden te zien waar eerder geen aandacht voor was.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Informatiebeveiliging en beveiliging van de onderneming in de praktijk (door Roger Benton).

  Deze praktijkstudie gaat over de migratie van een verzekeringsfirma naar een beveiligingssysteem voor de hele onderneming. Het doel van deze praktijkstudie is het bieden van een pad dat men kan volgen bij het vestigen van of migreren naar een beveiligingssysteem. Aanvankelijk was een primitief onlinebeveiligingssysteem het enige controlemechanisme voor toegang tot de bedrijfsgegevens. Het blootstellingsgevaar was ernstig – er waren geen integriteitscontroles buiten de onlineomgeving. Iedereen met een beetje programmeerervaring kon productiegegevens toevoegen, wijzigen en/of verwijderen.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  De strategie van Marriot voor elektronische beveiliging door samenwerking tussen bedrijf en IT.

  In de ervaring van Chris Zoladz van Marriott International, Inc. is de beveiliging van e-business een proces en geen project. Dat was de boodschap die Zoladz bracht op de recente E-Security Conference & Expo in Boston, gesponsord door de Intermedia Group. Als vice-president voor de bescherming van informatie bij Marriott rapporteert Zoladz via de juridische afdeling, hoewel hij geen jurist is. Zijn functie is het identificeren waar de meest waardevolle bedrijfsinformatie van Marriott is opgeslagen en hoe deze zich binnen en buiten de onderneming verplaatst. Marriott heeft een afzonderlijke verantwoordelijkheid gedefinieerd voor de ondersteunende beveiliging van de technische infrastructuur, die is toegewezen aan de IT-beveiligingsarchitect.

Fictief CSIRT (stap 7)

Het bedrijfsplan promoten

Er is besloten om feiten en cijfers te verzamelen uit de geschiedenis van het bedrijf. Dit is uiterst nuttig als statistisch overzicht van de IT-veiligheidssituatie. Als het CSIRT eenmaal actief is, blijft het verzamelen van deze statistische gegevens nuttig om alles actueel te houden.

Andere nationale CSIRT's werden benaderd en ondervraagd over hun business case. Zij boden ondersteuning door enkele dia's samen te stellen over recente ontwikkelingen in IT-beveiligingsincidenten en de kosten van incidenten.

In dit voorbeeld van Fictief CSIRT was geen sprake van een dringende noodzaak om het management te overtuigen van het belang van IT-beveiliging. Er was dan ook snel toestemming om de eerste stap te zetten. Er werden een zakelijke onderbouwing en een projectplan opgesteld, inclusief een schatting van de aanloopkosten en de operationele kosten.

8 Voorbeelden van operationele en technische procedures (werkstromen)

We hebben tot nu toe de volgende stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?
4. Analyse van de omgeving en constituenten.
5. De mission statement definiëren.
6. Het bedrijfsplan ontwikkelen.
   a. Het financiële model definiëren
   b. De organisatiestructuur definiëren
   c. Personeel inhuren
   d. Gebruik en inrichting van het kantoor
   e. Een beleid voor informatiebeveiliging ontwikkelen
   f. Samenwerkingspartners zoeken
7. Het bedrijfsplan promoten.
   a. De zakelijke onderbouwing laten goedkeuren
   b. Alles in een projectplan opnemen

>> De volgende stap is: het CSIRT operationeel maken

Werkstromen zorgen voor een betere kwaliteit en snellere afhandeling van incidenten of beveiligingslekken.

Fictief CSIRT beperkt zich in de voorbeelden tot het leveren van de volgende CSIRT-kerndiensten:

- Alarmeringen en waarschuwingen
- Afhandeling van incidenten
- Mededelingen

Dit hoofdstuk bevat voorbeelden van werkstromen die de kerndiensten van een CSIRT beschrijven. Dit hoofdstuk bevat ook informatie over het verzamelen van gegevens uit verschillende bronnen, het beoordelen van de relevantie en authenticiteit ervan plus de verspreiding van de informatie in de constituency. Tot slot bevat dit hoofdstuk voorbeelden van basisprocedures en specifieke CSIRT-hulpprogramma's.

8.1 De installaties in de constituency in kaart brengen

De eerste stap is het verzamelen van een overzicht van de geïnstalleerde IT-systemen in de constituency. Zo kan het CSIRT de relevantie van binnenkomende informatie evalueren en deze vóór verdere verspreiding filteren. De constituenten worden dan niet overspoeld met informatie waar ze eigenlijk niets aan hebben.

Het is verstandig om eenvoudig te beginnen. U kunt bijvoorbeeld als volgt een Excel-werkblad gebruiken:

Categorie	Applicatie	Software-product	Versie	Besturings-systeem	Versie van besturings-systeem	Constituent
Desktop	Office	Excel	x-x-x	Microsoft	XP Pro	A
Desktop	Browser	IE	x-x-	Microsoft	XP Pro	A
Netwerk	Router	CISCO	x-x-x	CISCO	x-x-x	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Services	Webserver	Apache		Unix	x-x-x	B

Met de filterfunctie in Excel kunt u eenvoudig de gewenste software selecteren en zien welke constituent welke software gebruikt.

8.2 Alarmeringen, waarschuwingen en mededelingen genereren

Het genereren van alarmeringen, waarschuwingen en mededelingen gebeurt allemaal volgens dezelfde werkstromen:

- Informatie verzamelen
- De informatie evalueren naar relevantie en bron
- Risicoanalyses uitvoeren op basis van de verzamelde informatie
- De informatie verspreiden

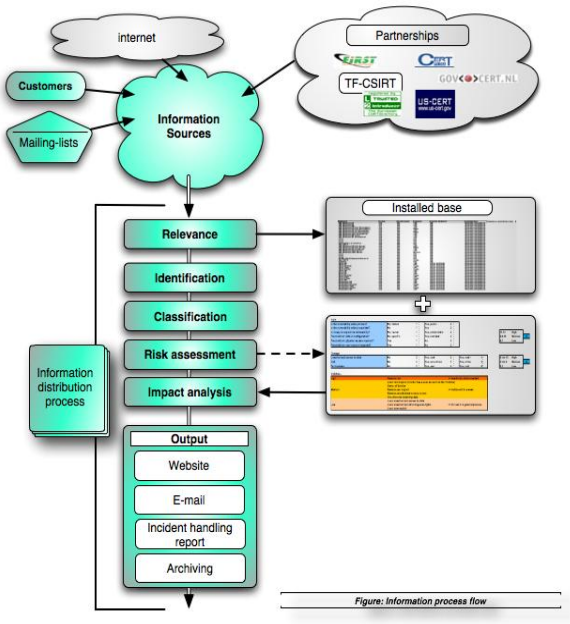
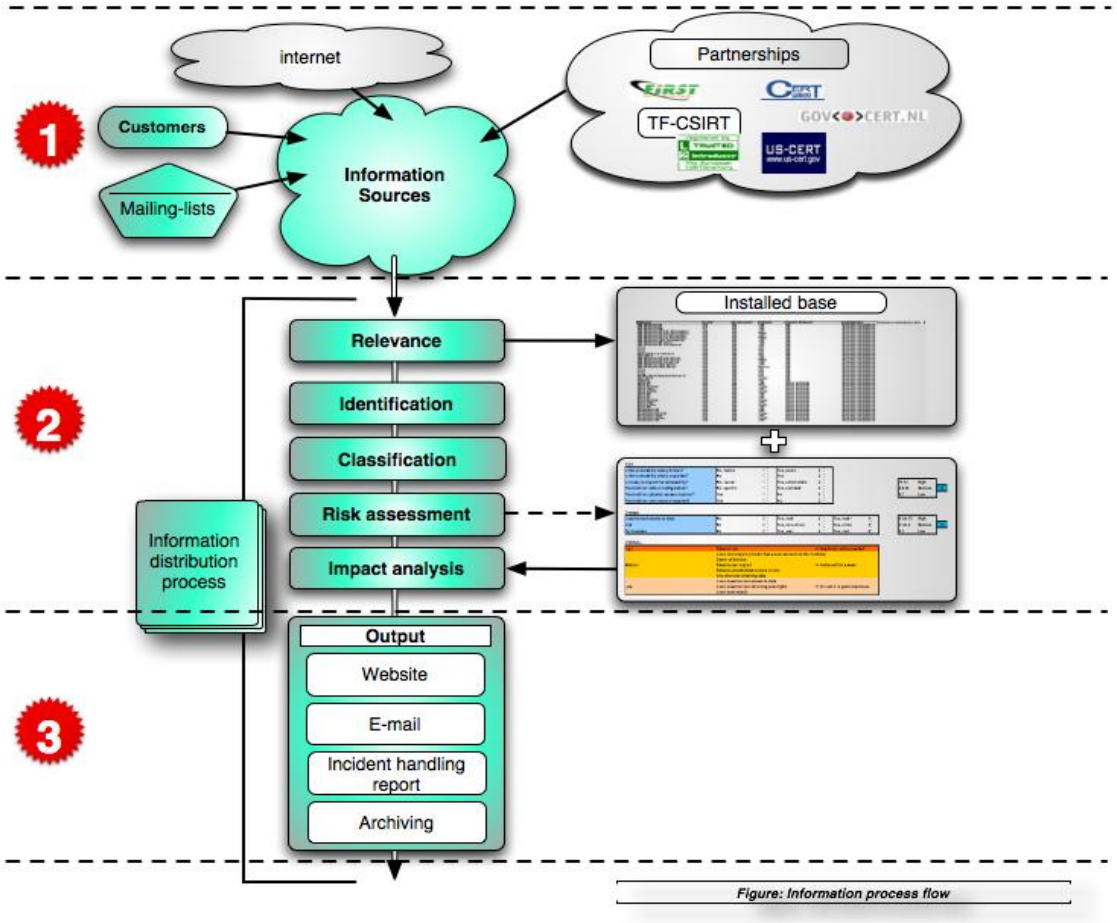


Fig. 9 : Processtroom voor informatie

In de volgende alinea's wordt deze werkstroom nader beschreven.



1 Stap 1: Informatie over beveiligingslekken verzamelen

Meestal komen de gegevens die als basis dienen voor de dienstverlening uit twee typen informatiebronnen:

- Informatie over beveiligingslekken in (uw) IT-systemen
- Incidentmeldingen

Afhankelijk van het type bedrijf en de IT-infrastructuur zijn er vele openbare en besloten bronnen voor informatie over beveiligingslekken en kwetsbaarheden:

- Openbare en besloten mailinglists
- Productinformatie over beveiligingslekken van leveranciers
- Websites
- Informatie op internet (Google, etc.)
- Publieke en private samenwerkingsverbanden die zorgen voor informatie over beveiligingslekken en kwetsbaarheden (FIRST, TF-CSIRT, CERT-CC, US-CERT…)

Al deze informatie draagt bij aan de hoeveelheid kennis over specifieke kwetsbaarheden en beveiligingslekken in IT-systemen.

Er zijn vele goede en toegankelijke bronnen met beveiligingsinformatie op internet te vinden. De ad-hocwerkgroep van ENISA voor CERT-diensten (WG-CS) komt met een uitgebreid overzicht in 2006[19].

Stap 2: De informatie evalueren en risicoanalyses uitvoeren

Deze stap resulteert in een analyse van de impact of gevolgen van een specifiek beveiligingslek voor de IT-infrastructuur van de constituency.

Identificatie
De bron en de betrouwbaarheid van binnenkomende informatie over beveiligingslekken moeten altijd worden vastgesteld voordat de informatie naar de constituency gaat. Anders kunnen mensen onnodig gealarmeerd worden en bedrijfsprocessen verstoord raken, wat uiteindelijk de reputatie van het CSIRT zal schaden.

[19] Ad-hocwerkgroep voor CERT-diensten (WG-CS):
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

De volgende procedure toont een voorbeeld van de identificatie van de authenticiteit van een bericht:

Procedure voor de identificatie van de authenticiteit van een bericht en de bron ervan

Algemene controlelijst
1. Is de bron bekend en als zodanig geregistreerd?
2. Komt de informatie via een regulier kanaal?
3. Is er “vreemde” informatie die niet goed “aanvoelt”?
4. Volg uw gevoel. Indien er bestaat twijfel over de informatie, controleer deze dan opnieuw voordat u verdere actie onderneemt!

E-mailbronnen
1. Is het adres van de bron bekend bij de organisatie en komt het voor in de lijst met bronnen?
2. Is de PGP-handtekening correct?
3. Controleer bij twijfel de complete headers van een bericht.
4. Gebruik bij twijfel “nslookup” of ”dig” om het domein van de afzender te controleren[20].

WWW-bronnen
1. Controleer browsercertificaten bij verbindingen met een beveiligde website (https://).
2. Controleer de bron op inhoud en validiteit (technisch).
3. Klik bij twijfel niet op koppelingen en download geen software.
4. Gebruik bij twijfel “lookup” en ”dig” om het domein te controleren en voer “traceroute” uit.

Telefoon
1. Luister goed naar de naam.
2. Herkent u de stem?
3. Vraag bij twijfel naar een telefoonnummer en vraag of u de beller terug kunt bellen.

Fig. 10 Voorbeeld van een procedure voor de identificatie van informatie

Relevantie
Op basis van het eerder gemaakte overzicht van de geïnstalleerde hardware en software kunt u de binnenkomende informatie over beveiligingslekken met behulp van de volgende vragen filteren op relevatie: “Gebruikt de constituency dit stukje software?”; “Is de informatie relevant voor hen?”

Classificatie
Sommige binnenkomende informatie kan als vertrouwelijk worden geclassificeerd of gelabeld (zoals binnenkomende incidentmeldingen van andere teams). Alle informatie moet worden behandeld op basis van het verzoek van de afzender en het eigen beleid

[20] Hulpprogramma’s in CHIHT om identiteiten te controleren:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

voor informatiebeveiliging. Een goede vuistregel is: "*Verspreid geen informatie als niet duidelijk is of dat de bedoeling is; vraag bij twijfel de afzender om toestemming.*"

Analyse van risico en impact
Er zijn diverse methoden om het risico en de impact van een (mogelijk) beveiligingslek te bepalen.

Risico wordt gedefinieerd als de potentiële kans dat het beveiligingslek kan worden misbruikt. Onder andere de volgende belangrijke factoren spelen een rol:

- Is het beveiligingslek algemeen bekend?
- Komt het beveiligingslek veel voor?
- Is het beveiligingslek gemakkelijk te misbruiken?
- Is het beveiligingslek extern te misbruiken?

Al deze vragen geven een goed beeld van de ernst van het beveiligingslek.
Het risico is met de volgende formule bijvoorbeeld eenvoudig te berekenen:

Impact = risico x potentiële schade

Potentiële schade kan zijn:

- Ongeautoriseerde toegang tot gegevens
- Denial of Service (DoS)
- Machtigingen verkrijgen of uitbreiden

(Aan het einde van dit hoofdstuk staan enkele uitgebreidere classificatieschema's.)

Met de antwoorden op deze vragen kan een algemene aanduiding van de mogelijke risico's en schade aan de aanbeveling worden toegevoegd. Vaak worden daarvoor eenvoudige termen als LAAG, GEMIDDELD en HOOG gebruikt.

Andere en uitgebreidere schema's voor risicoanalyse zijn onder meer:

Matrix van GOVCERT.NL[21]

Het CSIRT GOVCERT.NL van de Nederlandse overheid heeft een matrix ontwikkeld voor de risicoanalyse die in de beginfase van Govcert.nl is ontwikkeld en nog steeds wordt bijgewerkt met de nieuwste trends.

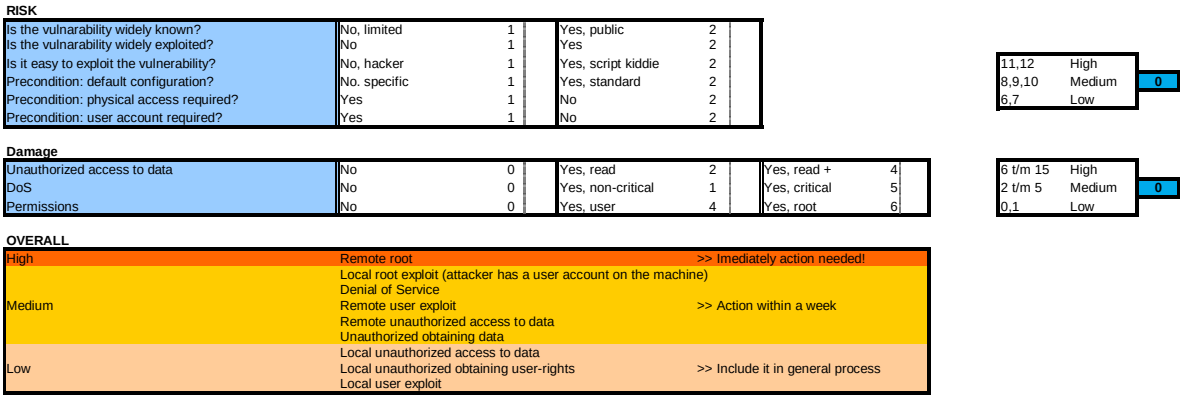


Fig. 11 De matrix van GOVCERT.NL

Beschrijving van gemeenschappelijke indeling van aanbevelingen door EISPP[22]

Het EISPP (European Information Security Promotion Programme) is een project dat mede wordt gefinancierd door de Europese Gemeenschap en valt onder het vijfde kaderprogramma. Het EISPP-project streeft naar de ontwikkeling van een Europees kader voor niet alleen het delen van kennis op het gebied van beveiliging, maar ook om de inhoud en de manieren van verspreiding van beveiligingsinformatie voor het MKB te definiëren. Door het MKB in Europa te voorzien van de benodigde IT-beveiligingsdiensten worden bedrijven gestimuleerd om vertrouwen te ontwikkelen in en gebruik te maken van e-commerce, wat leidt tot meer en betere kansen voor nieuwe zakelijke activiteiten. Het EISPP is een voorloper in de visie van de Europese Comissie voor het vormen van een Europees expertisenetwerk binnen de Europese Unie.

DAF (Deutsches Advisory Format)[23]

DAF is een initiatief van het Duitse CERT-Verbund en vormt een basisonderdeel van een infrastructuur voor het genereren en uitwisselen van beveiligingsadviezen door verschillende teams. DAF is met name toegespitst op de behoeften van de Duitse CERT's. De standaardnorm wordt ontwikkeld en onderhouden door CERT-Bund, DFN-CERT, PRESECURE en Siemens-CERT.

[21] Kwetsbaarheidsmatrix: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

Stap 3: De informatie verspreiden

Een CSIRT kan kiezen uit diverse verspreidingsmethoden, afhankelijk van de wensen van de constituenten en uw communicatiestrategie.

- Website
- E-mail
- Rapporten
- Archivering en onderzoek

Beveiligingsadviezen van een CSIRT moeten altijd dezelfde structuur hebben. Dit vergroot de leesbaarheid en de lezer kan zo snel alle relevante informatie vinden.

Een beveiligingsadvies of aanbeveling moet minimaal de volgende informatie bevatten:

Titel van de aanbeveling ……
Referentienummer …… **Systemen waarin het probleem optreedt** **-** …… **-** …… **Gerelateerd besturingssysteem + versie** …… **Risico** (hoog, gemiddeld, laag) …… **Impact/potentiële schade** (hoog, gemiddeld, laag) …… **Externe id's:** (CVE, id's voor bulletins met informatie over beveiligingslekken) ……
Overzicht van het beveiligingslek …… **Impact** …… **Oplossing** …… **Beschrijving (details)** …… **Bijlage** ……

Fig. 12 Voorbeeldaanbeveling

Zie hoofdstuk *10. Oefening* voor een compleet voorbeeld van een beveiligingsadvies.

8.3 Incidenten afhandelen

De behandeling van informatie bij het afhandelen van incidenten komt sterk overeen met de procedure voor het opstellen van alarmeringen, waarschuwingen en mededelingen. De wijze van informatie verzamelen is doorgaans echter anders. Incidentgerelateerde gegevens worden gewoonlijk verkregen door middel van incidentmeldingen van de constituency of andere teams, of via de feedback van betrokken partijen tijdens het proces van incidentafhandeling. Informatiestromen vinden meestal plaats via (gecodeerde) e-mail. Soms is het gebruik van telefoon of fax noodzakelijk.

Bij het ontvangen van informatie via de telefoon doet u er goed aan elk detail direct te noteren met behulp van een speciaal formulier of programma voor de afhandeling/rapportage van incidenten of door een memo te maken. Voordat het gesprek is beëindigd, moet u een incidentnummer genereren (als er voor het incident nog geen bestaat). Dit nummer moet u ter referentie bij latere communicatie aan de beller geven (of in een samenvattend e-mailbericht dat u na afloop verstuurt).

De rest van dit hoofdstuk bevat een beschrijving van het basisproces voor de afhandeling van incidenten. Een grondige analyse van het volledige proces van incidentenbeheer en alle betrokken werkstromen en subwerkstromen is te vinden in de documentatie van het CERT/CC over het definiëren van processen voor incidentenbeheer voor CSIRT's[24].

[24] Definiëren van processen voor incidentenbeheer: http://www.cert.org/archive/pdf/04tr015.pdf

In principe wordt bij de afhandeling van incidenten de volgende werkstroom gebruikt:

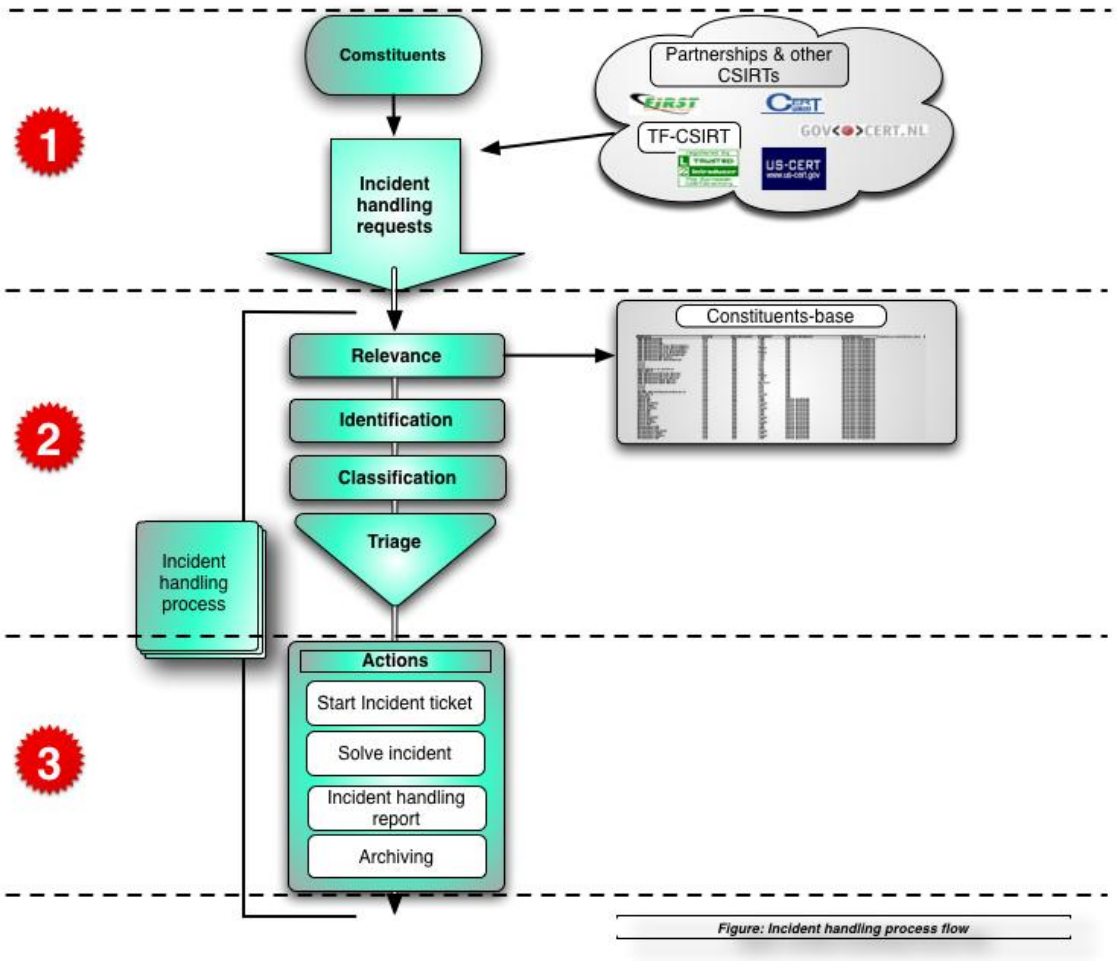


Fig. 13 Processtroom voor incidenten

Stap 1: Incidentmeldingen ontvangen

Incidentmeldingen bereiken een CSIRT via diverse kanalen, vooral per e-mail maar ook via telefoon of fax.

Bij het ontvangen van een incidentmelding is het verstandig alle details volgens een vaste indeling te noteren. Zo gaat geen essentiële informatie verloren. Hieronder staat een voorbeeldformulier:

RAPPORTAGEFORMULIER INCIDENT

Dit formulier invullen en faxen of e-mailen naar: ……..
*Regels met een * zijn verplicht.*

Naam en organisatie
1. Naam*:
2. Naam van organisatie*:
3. Type sector:
4. Land*:
5. Plaats:
6. E-mailadres*:
7. Telefoonnummer*:
8. Overige:

Host(s) waar het probleem optreedt
9. Aantal hosts:
10. Hostnaam en IP*:
11. Functie van de host*:
12. Tijdzone:
13. Hardware:
14. Besturingssysteem:
15. Software waarin het probleem optreedt:
16. Bestanden waarin het probleem optreedt:
17. Beveiliging:
18. Hostnaam en IP:
19. Protocol/poort:

Incident
20. Referentienummer:
21. Type incident:
22. Begin van incident:
23. Dit is een voortdurend incident: JA NEE
24. Tijdstip en methode van detectie:
25. Bekende beveiligingslekken:
26. Verdachte bestanden:
27. Tegenmaatregelen:
28. Gedetailleerde beschrijving*:

Fig. 14 Inhoud van een incidentenrapport

Stap 2: Incidenten evalueren

Tijdens deze stap worden de authenticiteit en de relevantie van een gemeld incident gecontroleerd en wordt de classificatie ervan bepaald.

Identificatie

Ter voorkoming van onnodige actie is het een goed gebruik om na te gaan of de meldende partij betrouwbaar is en een van uw eigen constituenten of die van een ander CSIRT is. Dezelfde regels gelden als in hoofdstuk *8.2 Alarmeringen genereren*.

Relevantie

In deze stap controleert u of het verzoek om afhandeling van het incident uit de constituency van het CSIRT afkomstig is, dan wel of het gemelde incident IT-systemen van de constituency aangaat. Als geen van beide opties aan de orde is, wordt de melding doorgaans doorgestuurd naar het juiste CSIRT[25].

Classificatie

Met deze stap wordt de triage voorbereid door de ernst van het incident te classificeren. Een gedetailleerde bespreking van de classificatie van incidenten valt buiten het bestek van dit document. Het classificatieschema voor CSIRT-incidenten kan u bijvoorbeeld verder op weg helpen:

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Fig. 15 Classificatieschema voor incidenten (bron: FIRST)[26]

[25] Hulpprogramma's in CHIHT om identiteiten te controleren:

http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Classificatie van CSIRT-incidenten http://www.first.org/resources/guides/csirt_case_classification.html

Triage
Triage is een systeem dat door medisch personeel en hulpverleners wordt gebruikt om slachtoffers in te schalen in verschillende categorieën wanneer het aantal gewonden de beschikbare zorgvoorzieningen overstijgt, zodat toch zoveel mogelijk mensen kunnen worden geholpen[27].

Het CERT/CC geeft de volgende beschrijving:

Triage is een essentieel element bij alle vormen van incidentbeheer, met name voor gevestigde CSIRT's. Triage is cruciaal om te begrijpen wat in de organisatie wordt gerapporteerd. Het is een middel om alle informatie naar één PoC of aanspreekpunt te laten stromen voor een compleet beeld van de actuele activiteiten en een correlatie van alle gerapporteerde gegevens. Triage maakt een eerste beoordeling mogelijk van een binnenkomende melding, waarna de melding in de wachtrij wordt geplaatst voor verdere afhandeling. Het vormt tevens een beginpunt voor initiële documentatie en invoer van gegevens voor een rapport of verzoek voor zover dat nog niet in het detectieproces is gebeurd.

De triagefunctie biedt een snelle momentopname van de huidige status van alle gemelde activiteiten: welke meldingen open of gesloten zijn, welke acties nog moeten plaatsvinden en hoeveel van elk type melding is binnengekomen. Dit proces kan helpen bij het vaststellen van potentiële beveiligingsproblemen en het stellen van prioriteiten bij de uitvoering van werkzaamheden. De met de triage verzamelde informatie kan als basis dienen om trends en statistieken te genereren voor het management wat betreft beveiligingslekken en incidenten[28].

Triage dient alleen door de meest ervaren teamleden te worden uitgevoerd. Er komt namelijk een diepgaand inzicht bij kijken in de mogelijke gevolgen van incidenten voor specifieke onderdelen van de constituency, plus de competentie om te beslissen welk teamlid het meest geschikt is om het incident af te handelen.

Stap 3: Acties

Na triage komen incidenten vaak in een wachtrij terecht in een hulpprogramma voor incidentafhandeling. Degenen die het incident afhandelen, voeren in principe de volgende stappen uit.

Incidentticket starten
Het ticketnummer van het incident is mogelijk al in een eerdere stap gegenereerd (bijvoorbeeld bij de melding van het incident via de telefoon). Is dat niet het geval, dan is de eerste stap het aanmaken van dit nummer dat bij alle verdere communicatie over dit incident zal worden gebruikt.

[27] Triage in Wikipedia: http://nl.wikipedia.org/wiki/Triage

[28] Definiëren van processen voor incidentenbeheer: http://www.cert.org/archive/pdf/04tr015.pdf

Levenscyclus van een incident
De afhandeling van een incident verloopt niet zozeer volgens een serie opeenvolgende stappen die uiteindelijk tot een oplossing leiden, maar veeleer volgens een serie herhalende stappen totdat het incident is opgelost en alle betrokken partijen over alle benodigde informatie beschikken. Deze cyclus, ofwel de "levenscyclus van een incident", omvat de volgende processen:

Analyse:	Alle details van het gerapporteerde incident worden geanalyseerd.
Contactgegevens verkrijgen:	Om informatie over het incident te kunnen meedelen aan alle betrokken partijen (zoals andere CSIRT's, getroffen partijen en wellicht de eigenaars van systemen die mogelijk zijn misbruikt voor een aanval).
Technische ondersteuning:	Help slachtoffers snel te herstellen van de gevolgen van het incident en verzamel meer informatie over de aanval.
Coördinatie:	Informeer andere betrokken partijen, zoals het CSIRT dat verantwoordelijk is voor het aangevallen IT-systeem, of andere slachtoffers.

Deze structuur wordt een "levenscyclus" genoemd, omdat de ene stap tot de andere leidt en de laatste stap (coördinatie) tot een nieuwe analyse kan leiden en de cyclus zo opnieuw begint. Het proces stopt wanneer alle betrokken partijen alle benodigde informatie hebben ontvangen en gerapporteerd.

Zie het CSIRT-handboek van het CERT/CC voor een uitgebreide beschrijving van de levenscyclus van incidenten[29].

Rapport van incidentafhandeling
Wees voorbereid op vragen van het management over incidenten door een rapport samen te stellen. Het is een goed gebruik om een document over de "opgedane ervaringen" op te stellen (alleen voor intern gebruik) om het personeel kennis bij te brengen en fouten in de processen voor afhandeling van incidenten in de toekomst te vermijden.

Archivering
Kijk in de archiveringsregels die zijn beschreven in hoofdstuk *6.6 Een beleid voor informatiebeveiliging ontwikkelen*.

Zie het gedeelte *A.1 Meer literatuur* in de bijlage voor uitgebreide handleidingen over incidentbeheer en de levenscyclus van incidenten.

[29] CSIRT-handboek: http://www.cert.org/archive/pdf/csirt-handbook.pdf

8.4 Voorbeeld van een reactietijdschema

De definitie van reactietijden wordt vaak vergeten maar moet een onderdeel zijn van elke goed opgestelde SLA (Service Level Agreement) tussen een CSIRT en de constituency ervan. Het geven van tijdige feedback aan constituenten tijdens de afhandeling van incidenten is cruciaal, zowel voor de eigen aansprakelijkheid van de constituenten als voor de reputatie van het team.
De reactietijden moeten duidelijk aan de constituency worden gecommuniceerd om geen verkeerde verwachtingen te scheppen. Het volgende simpele tijdschema kan dienen als vertrekpunt voor een meer gedetailleerde SLA met de constituency van een CSIRT.

Hieronder staat een voorbeeld van een praktisch reactietijdschema vanaf een binnenkomend verzoek om assistentie:

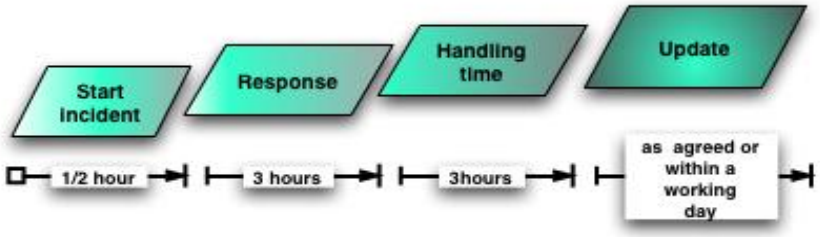


Fig. 16 Voorbeeld van reactietijdschema

Het is ook goed constituenten te wijzen op hun eigen reactietijden, vooral wat betreft het melden van een noodsituatie bij het CSIRT. In de meeste gevallen is zo vroeg mogelijk contact opnemen met het CSIRT het beste, ook bij twijfel, dus moedig de constituency daartoe aan.

8.5 Beschikbare CSIRT-hulpprogramma's

Dit hoofdstuk bevat enkele verwijzingen naar veelgebruikte hulpprogramma's voor CSIRT's. Er worden alleen voorbeelden gegeven; meer verwijzingen staan in CHIHT (*Clearinghouse of Incident Handling Tools*)[30].

Coderingssoftware voor e-mail en berichten

- GNUPG http://www.gnupg.org/
  GnuPG van het GNU-project is de complete en gratis implementatie van de OpenPGP-standaard volgens RFC2440. Met behulp van GnuPG kunt u uw gegevens en communicatie coderen en ondertekenen.

- PGP http://www.pgp.com/
  Commerciële variant

Hulpprogramma voor incidentafhandeling

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Hiermee kunt u incidenten beheren en opvolgen en al dan niet ondernomen acties bijhouden.

- RTIR http://www.bestpractical.com/rtir/
  RTIR is een gratis open-sourcesysteem voor incidentafhandeling gericht op de behoeften van CERT-teams en andere beveiligingsteams.

CRM-programma's
Wanneer u veel verschillende constituenten hebt en alle afspraken en gegevens bij moet houden, komt een CRM-database goed van pas. Er zijn veel verschillende variaties, waarvan er hierna enkele worden genoemd:

- SugarCRM http://www.sugarcrm.com/crm/

- SugarForge (gratis open-sourceversie) http://www.sugarforge.org/

Informatiecontrole
- Website-Watcher http://www.aignes.com/index.htm
  Dit programma controleert websites op updates en wijzigingen.

- WatchThatPage http://www.watchthatpage.com/
  Met deze service ontvangt u informatie over wijzigingen in websites via e-mail (gratis en commercieel).

Contactgegevens vinden
Het vinden van de juiste contactgegevens om incidenten te melden is vaak niet zo eenvoudig. Er zijn enkele informatiebronnen die u daarbij kunnen helpen:

- RIPE[31]
- IRT-object[32]
- TI[33]

Ook CHIHT bevat een lijst met enkele hulpprogramma's voor het vinden van contactgegevens[34].

[31] RIPE-database: http://www.ripe.net/whois

[32] IRT-object in de RIPE database: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Hulpprogramma's in CHIHT om identiteiten te controleren:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Fictief CSIRT (stap 8)

Processtromen en operationele en technische procedures instellen

Fictief CSIRT richt zich op het verlenen van CSIRT-kerndiensten:

- Alarmeringen en waarschuwingen
- Mededelingen
- Afhandeling van incidenten

Het team heeft procedures ontwikkeld die goed werken en voor elk teamlid gemakkelijk te begrijpen zijn. Fictief CSIRT heeft ook een juridisch adviseur ingezet voor kwesties rondom de aansprakelijkheid en het beleid voor informatiebeveiliging. Het team heeft enkele nuttige hulpprogramma's in gebruik genomen en bruikbare informatie ingewonnen door operationele kwesties met andere CSIRT's te bespreken.

Er is een vaste sjabloon gegenereerd voor beveiligingsadviezen en incidentrapporten. Het team gebruikt RTIR voor de afhandeling van incidenten.

9 CSIRT-training

We hebben tot nu toe de volgende stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?
4. Analyse van de omgeving en constituenten.
5. De mission statement definiëren.
6. Het bedrijfsplan ontwikkelen.
   a. Het financiële model definiëren
   b. De organisatiestructuur definiëren
   c. Personeel inhuren
   d. Gebruik en inrichting van het kantoor
   e. Een beleid voor informatiebeveiliging ontwikkelen
   f. Samenwerkingspartners zoeken
7. Het bedrijfsplan promoten.
   a. De zakelijke onderbouwing laten goedkeuren
   b. Alles in een projectplan opnemen
8. Het CSIRT operationeel maken.
   a. Werkstromen ontwikkelen
   b. CSIRT-hulpprogramma's implementeren

>> De volgende stap is: het personeel opleiden.

Dit hoofdstuk geeft een overzicht van de twee belangrijkste bronnen speciaal gericht op CSIRT-training: de cursussen van TRANSITS en het CERT/CC.

9.1 TRANSITS

TRANSITS is een Europees project geweest ter bevordering van het vestigen van nieuwe CSIRT's en het verbeteren van bestaande CSIRT's door het tekort aan deskundig CSIRT-personeel aan te pakken. Dit doel werd gerealiseerd door het bieden van specialistische training en cursussen voor personeel van (nieuwe) CSIRT's over organisatorische, operationele, technische, marktgerelateerde en juridische aspecten bij het verzorgen van CSIRT-diensten.

In het bijzonder heeft TRANSITS

- modulair cursusmateriaal ontwikkeld, bijgewerkt en regelmatig herzien;
- workshops georganiseerd waarbij de cursusmaterialen werden gebruikt;
- de deelname van personeel van (nieuwe) CSIRT's in deze workshops mogelijk gemaakt, met de nadruk op deelname uit de toetredende EU-staten;
- de cursusmaterialen verspreid en het gebruik van de resultaten gewaarborgd[35].

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

ENISA faciliteert en ondersteunt de TRANSITS-cursussen. Als u informatie wilt over aanmelding, de vereisten en de kosten voor de cursussen, neemt u contact op met de CSIRT-experts van ENISA:

CERT-Relations@enisa.europa.eu

Voorbeeldcursusmateriaal treft u aan in de bijlage van dit document!

9.2 CERT/CC

De complexiteit van computer- en netwerkinfrastructuren en de moeilijkheid om die te beheren werken een goed beheer van de netwerkbeveiliging niet in de hand. Netwerk- en systeembeheerders beschikken over onvoldoende mensen en beveiligingspraktijken om aanvallen af te slaan en de schade zo beperkt mogelijk te houden. Er zijn dan ook steeds meer beveiligingsincidenten met computers.
Wanneer deze beveiligingsincidenten optreden, moeten organisaties snel en effectief reageren. Hoe sneller een organisatie een incident herkent, analyseert en erop reageert, hoe beter men de schade en herstelkosten in de hand kan houden. Het opzetten van een CSIRT is een goede manier om snel te kunnen reageren op incidenten en toekomstige incidenten tegen te gaan.

CERT-CC biedt cursussen voor managers en technisch personeel op gebieden als het samenstellen en beheren van CSIRT's, het reageren op en analyseren van beveiligingsincidenten, en het verbeteren van de netwerkbeveiliging. Tenzij anders aangegeven, worden alle cursussen gegeven in Pittsburgh (Pennsylvania). Ook worden cursussen gegeven op het gebied van veiligheid en beveiliging aan de Carnegie Mellon University.

Beschikbare CERT/CC-cursussen[36] gericht op CSIRT's

Een CSIRT samenstellen
CSIRT's beheren
Basisbeginselen van incidentafhandeling
Geavanceerde incidentafhandeling voor technisch personeel

Voorbeeldcursusmateriaal treft u aan in de bijlage van dit document!

Fictief CSIRT (stap 9)
Het personeel opleiden Fictief CSIRT besluit het voltallige technische personeel naar de eerstvolgende TRANSITS-cursussen te sturen. De teamleider volgt daarnaast de cursus voor het beheren van CSIRT's van het CERT/CC.

[36] CERT/CC-cursussen: http://www.sei.cmu.edu/products/courses

10 Oefening: een aanbeveling opstellen

We hebben tot nu toe de volgende stappen uitgevoerd:

1. Begrijpen wat een CSIRT is en wat de voordelen ervan kunnen zijn.
2. Aan welke sector zal het nieuwe team zijn diensten verlenen?
3. Welke diensten kan een CSIRT leveren aan de constituency?
4. Analyse van de omgeving en constituenten.
5. De mission statement definiëren.
6. Het bedrijfsplan ontwikkelen.
   a. Het financiële model definiëren
   b. De organisatiestructuur definiëren
   c. Personeel inhuren
   d. Gebruik en inrichting van het kantoor
   e. Een beleid voor informatiebeveiliging ontwikkelen
   f. Samenwerkingspartners zoeken
7. Het bedrijfsplan promoten.
   a. De zakelijke onderbouwing laten goedkeuren
   b. Alles in een projectplan opnemen
8. Het CSIRT operationeel maken.
   a. Werkstromen ontwikkelen
   b. CSIRT-hulpprogramma's implementeren
9. Het personeel opleiden

>> De volgende stap is oefenen om klaar te zijn voor het echte werk!

Ter illustratie wordt in dit hoofdstuk een voorbeeldoefening gegeven voor een alledaagse CSIRT-taak: het opstellen van een beveiligingsadvies.

De aanleiding was het volgende originele beveiligingsadvies van Microsoft:

Bulletin-id	**Microsoft-beveiligingsbulletin MS06-042**
Bulletintitel	**Cumulatieve beveiligingsupdate voor Internet Explorer (918899)**
Management-samenvatting	Met deze update worden diverse beveiligingslekken in Internet Explorer waardoor externe code kan worden uitgevoerd, opgelost.
Maximaal prioriteitsniveau	Kritiek
Gevolgen van beveiligingslek	Uitvoering van externe code mogelijk
Software waarin het probleem optreedt	**Windows, Internet Explorer.** Zie het gedeelte Geteste software en downloadlocaties voor meer informatie.

Dit leveranciersbulletin biedt een oplossing voor een recent aangetroffen beveiligingslek in Internet Explorer. De leverancier stelt meerdere fixes beschikbaar voor deze software voor meerdere versies van Microsoft Windows.

Na het ontvangen van deze informatie over het beveiligingslek via een mailinglist, begint Fictief CSIRT met de werkstroom die is beschreven in hoofdstuk *8.2 Alarmeringen, waarschuwingen en mededelingen genereren*.

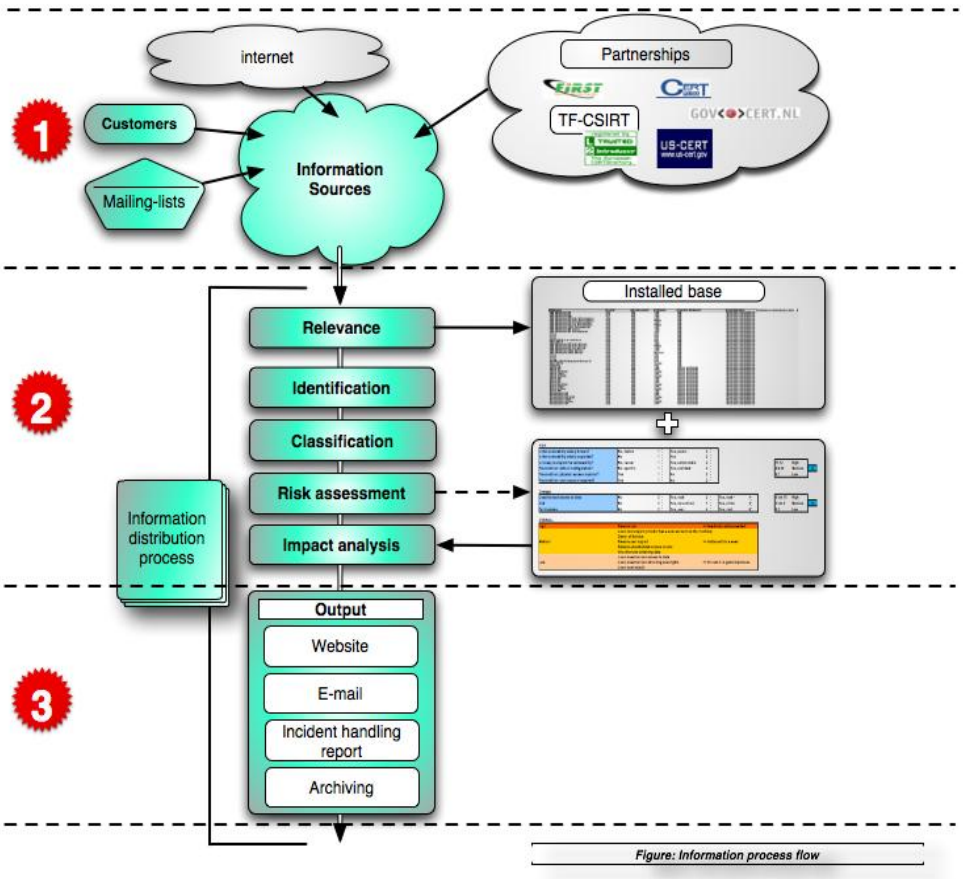


Figure: Information process flow

1 Stap 1: Informatie over beveiligingslekken verzamelen

De eerste stap is de website van de leverancier bezoeken. Daar controleert Fictief CSIRT de authenticiteit van de informatie en wordt nadere informatie verzameld over het beveiligingslek en de IT-systemen waarin het probleem optreedt.

Stap 2: De informatie evalueren en risicoanalyses uitvoeren

Identificatie
De informatie in de e-mail is al geverifieerd door een bezoek aan de website van de leverancier.

Relevantie
Fictief CSIRT loopt aan de hand van de lijst op de website met systemen waarin het probleem optreedt de lijst met gebruikte systemen in de constituency na. Internet Explorer wordt door minstens een van de constituenten gebruikt, zodat de informatie over het beveiligingslek inderdaad relevant is.

Categorie	Applicatie	Software-product	Versie	Besturings-systeem	Versie van besturings-systeem	Constituent
Desktop	Browser	IE	x-x-	Microsoft	XP Pro	A

Classificatie
De informatie is openbaar en kan dus gebruikt en verder verspreid worden.

Analyse van risico en impact
De antwoorden op de vragen tonen aan dat het risico en de impact *hoog* zijn (*kritiek* genoemd door Microsoft).

RISICO

Is het beveiligingslek algemeen bekend?	J
Komt het beveiligingslek veel voor?	J
Is het beveiligingslek gemakkelijk te misbruiken?	J
Kan het beveiligingslek extern worden misbruikt?	J

SCHADE
Mogelijke gevolgen zijn externe toegang en uitvoering van externe code. Dit beveiligingslek omvat meerdere kwesties, dus is het risico op schade *hoog*.

Stap 3: Verspreiding

Fictief CSIRT is een intern CSIRT. Als communicatiekanalen zijn e-mail, telefoon en de interne website beschikbaar. Het CSIRT produceert deze aanbeveling, op basis van de sjabloon in hoofdstuk *8.2 Alarmeringen, waarschuwingen en mededelingen genereren*.

Titel van de aanbeveling
Meerdere beveiligingslekken ontdekt in Internet Explorer

Referentienummer
082006-1

Systemen waarin het probleem optreedt
- Alle desktopsystemen met Microsoft

Gerelateerd besturingssysteem + versie
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 en Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 en Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 voor Itanium-based Systems en Microsoft Windows Server 2003 met SP1 voor Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Risico (hoog, gemiddeld, laag)
HOOG

Impact/potentiële schade (hoog, gemiddeld, laag)
HOOG

Externe id's: (CVE, id's voor bulletins met informatie over beveiligingslekken)
MS-06-42

Overzicht van het beveiligingslek
Microsoft heeft diverse beveiligingslekken in Internet Explorer aangetroffen waardoor externe code kan worden uitgevoerd.

Impact
Een aanvaller kan volledige controle krijgen over het systeem, programma's installeren, gebruikers toevoegen en gegevens bekijken, wijzigen of verwijderen. Verzachtende factor is dat het bovenstaande alleen kan optreden als de gebruiker is aangemeld met beheerdersrechten. Gebruikers die zijn aangemeld met minder rechten, lopen minder risico.

Oplossing
Pas de patch onmiddellijk toe op uw IE.

Beschrijving (details)
Zie ms06-042.mspx voor meer informatie.

Bijlage
Zie ms06-042.mspx voor meer informatie.

Deze informatie is nu gereed voor verdere verspreiding. Omdat dit een kritiek bulletin betreft, is het raadzaam de constituenten zo mogelijk ook te bellen.

Fictief CSIRT (stap 10)
Oefening In de eerste actieve weken van het fictief CSIRT werden op basis van voorbeelden van andere CSIRT's diverse fictieve gevallen geoefend. Verder heeft het CSIRT enkele beveiligingsadviezen uitgebracht op basis van actuele informatie over beveiligingslekken afkomstig van hardware- en softwareleveranciers, die verder zijn aangepast en afgestemd op de behoeften van de constituency.

11 Conclusie

Deze gids eindigt hier. Het voorliggende document is bedoeld als een beknopt overzicht van de diverse processen die nodig zijn voor het opzetten van een CSIRT. Volledigheid wordt niet gepretendeerd en er wordt niet te diep op specifieke details ingegaan. Zie het gedeelte *A.1 Meer literatuur* in de bijlage voor verdere nuttige literatuur over verschillende onderwerpen.

De volgende belangrijke stappen voor Fictief CSIRT zijn vervolgens nog:

- Feedback ontvangen van de constituency om de geleverde diensten verder te verfijnen
- Routine opdoen in het dagelijkse werk
- Noodsituaties oefenen
- Nauw contact houden met de verschillende CSIRT-gemeenschappen met als doel in de toekomst ook bij te dragen aan dit vrijwillige werk

12 Beschrijving van het projectplan

OPMERKING: Het projectplan is een eerste schatting van de benodigde tijd. Afhankelijk van de beschikbare mensen en middelen kan de feitelijke duur van het project anders uitpakken.

Het projectplan is beschikbaar in verschillende formaten op cd en op de website van ENISA. Het bevat alle processen die in dit document zijn beschreven.

Op de eerste plaats is Microsoft Project gebruikt voor dit materiaal, zodat het direct in dit projectbeheerprogramma kan worden gebruikt.

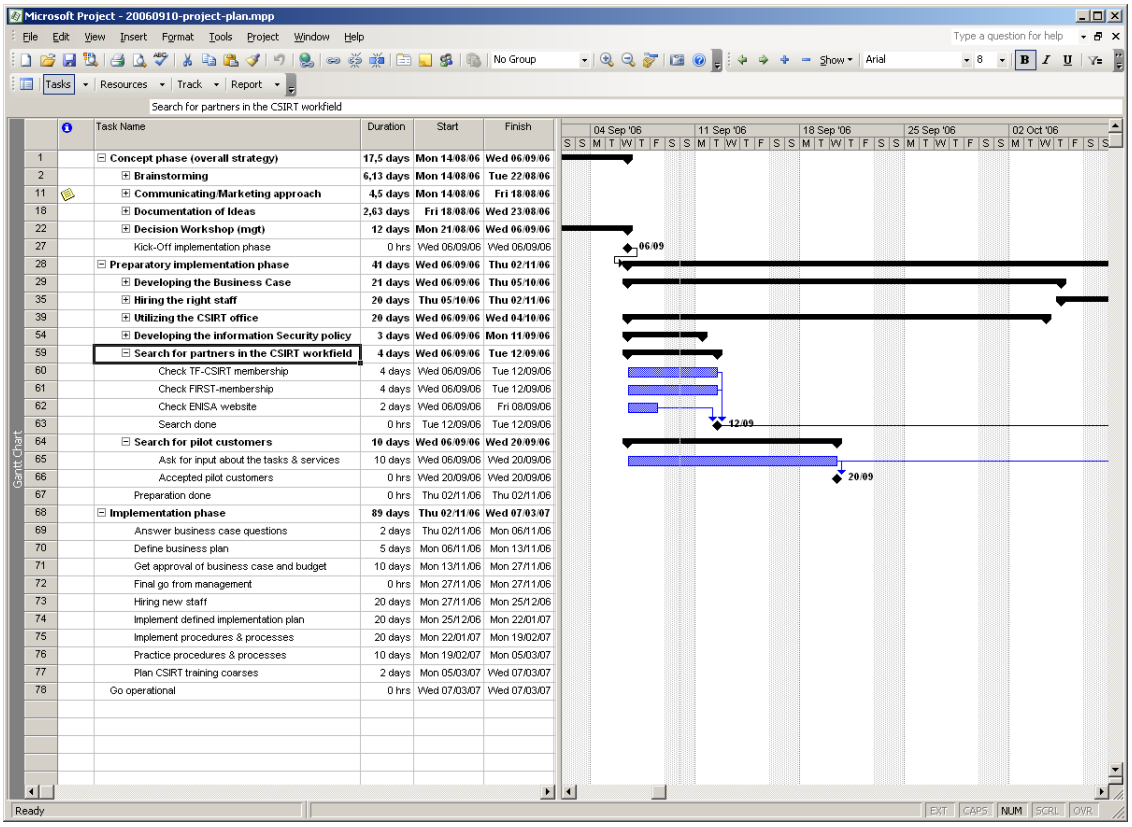
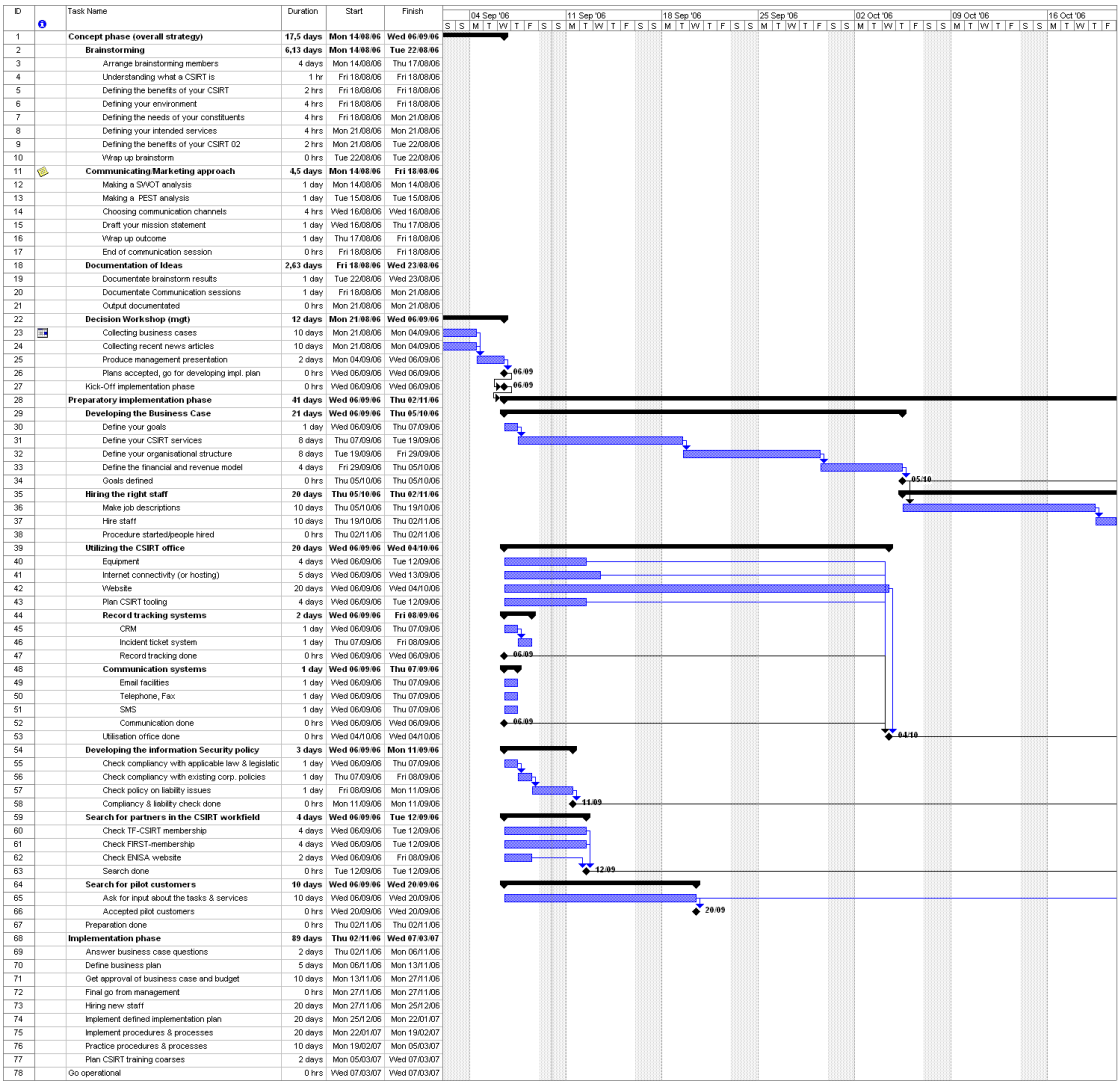


Fig. 17 Projectplan



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Fig. 18 Het projectplan met alle taken en een deel van het Gantt-schema

Het projectplan is ook beschikbaar in CSV- en XML-formaat. Verder gebruik kan worden aangevraagd bij de CSIRT-experts van ENISA: CERT-Relations@enisa.europa.eu

BIJLAGE

A.1 Meer literatuur

Handbook for CSIRTs (CERT/CC)
Een zeer uitgebreid handboek met alle relevante onderwerpen voor het werk van een CSIRT.
Bron: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
Een diepteanalyse van incidentbeheer.
Bron: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
Een uitgebreide analyse van de huidige situatie van het wereldwijde CSIRT-landschap, inclusief geschiedenis, statistische gegevens en nog veel meer.
Bron: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Een uitgebreide beschrijving van de opgedane ervaringen met het opzetten van GOVCERT.NL en 'De Waarschuwingsdienst' (de Nederlandse nationale waarschuwingsdienst).
Bron: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
Bron: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide
Bron: http://www.securityunit.com/publications/sp800-61.pdf

ENISA-overzicht van CERT-activiteiten in Europa
Een overzicht van CSIRT's in Europa en de verschillende activiteiten ervan.
Bron: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies

A.2 CSIRT-diensten

Speciale dank gaat uit naar CERT/CC, dat deze lijst heeft samengesteld.

Reactieve diensten	***Proactieve diensten***	***Afhandeling van artefacten***
• Alarmeringen en waarschuwingen • Afhandeling van incidenten • Analyse van incidenten • Reacties op incidenten op locatie • Ondersteuning bij reacties op incidenten • Coördinatie van reacties op incidenten • Afhandeling van beveiligingslekken • Analyse van beveiligingslekken • Reactie op beveiligingslekken • Coördinatie van reacties op beveiligingslekken	• Mededelingen • Technologiebewaking • Beveiligingscontroles of -beoordelingen • Configuratie en bijhouden van beveiliging • Ontwikkeling van beveiligingstools • Diensten voor detectie van aanvallen • Verspreiding van beveiligingsgerelateerde informatie	• Analyse van artefacten • Reactie op artefacten • Coördinatie van reacties op artefacten ***Kwaliteitsbeheer en beveiliging*** • Analyse van risico's • Bedrijfscontinuïteit en noodherstel • Beveiligingsadvies • Bewustmaking • Opleiding/training • Productevaluatie of -certificatie

Fig. 19 Lijst met CSIRT-diensten van CERT/CC

Beschrijving van de diensten

Reactieve diensten

Reactieve diensten zijn gericht op het reageren op verzoeken om assistentie, meldingen van incidenten uit de CSIRT-constituency en alle soorten bedreigingen of aanvallen tegen CSIRT-systemen. Sommige diensten kunnen worden geïnitieerd door de melding van derden of door bewakings- of IDS-logboeken en -alarmeringen te bekijken.

Alarmeringen en waarschuwingen

Deze dienst omvat het verspreiden van informatie met een beschrijving van een aanval van indringers, beveiligingslekken, alarmering bij aanvallen, computervirus of nepmelding. Ook wordt een eventuele aanbevolen werkwijze op korte termijn gegeven om met het resulterende probleem om te gaan. De alarmering, waarschuwing of aanbeveling wordt als reactie op het bestaande probleem verzonden. Dit om constituenten van de activiteit op de hoogte te stellen en richtlijnen te bieden voor de bescherming van hun systemen of het herstellen van getroffen systemen. De informatie kan van het CSIRT zelf afkomstig zijn of verspreid worden op basis van een bericht van

leveranciers, andere CSIRT's of beveiligingsexperts, of andere delen van de constituency.

Afhandeling van incidenten

Incidentafhandeling omvat het ontvangen van en uitvoeren van triage en reageren op verzoeken en meldingen, plus het analyseren van incidenten en gebeurtenissen. Mogelijke activiteiten zijn:

- actie ondernemen om systemen en netwerken te beschermen die door activiteiten van indringers zijn of kunnen worden misbruikt,
- oplossingen en risicobeperkende maatregelen bieden op basis van relevante aanbevelingen of waarschuwingen,
- andere delen van het netwerk controleren op mogelijk misbruik,
- netwerkverkeer filteren,
- systemen opnieuw opbouwen,
- systemen herstellen of er patches op toepassen,
- andere reactieve maatregelen of tijdelijke oplossingen ontwikkelen.

De afhandeling van incidenten gebeurt op diverse manieren door verschillende soorten CSIRT's. Deze dienst is dan ook als volgt verder onderverdeeld op basis van het type uitgevoerde activiteiten en het soort ondersteuning dat wordt geboden:

Analyse van incidenten

Er zijn vele niveaus van incidentanalyse en vele subdiensten. Incidentanalyse is in wezen het onderzoeken van alle beschikbare informatie en ondersteunend bewijsmateriaal of artefacten in verband met een incident of gebeurtenis. Het doel van de analyse is het identificeren van de omvang van het incident, de omvang van de schade door het incident, de aard van het incident en mogelijke reactieve maatregelen of tijdelijke oplossingen. Het CSIRT kan aan de hand van de resultaten van de analyse van beveiligingslekken of artefacten (zie beschrijving hieronder) over een zo compleet en actueel mogelijke analyse beschikken van wat er in een bepaald systeem is gebeurd. Het CSIRT correleert activiteiten voor verschillende incidenten om eventuele verbanden, trends, patronen of handtekeningen van indringers vast te stellen. Twee subdiensten die als onderdeel van de incidentanalyse kunnen worden uitgevoerd, zijn (afhankelijk van de missie, doelstellingen en processen van het CSIRT):

Verzamelen van forensisch bewijs

Het verzamelen, bewaren, documenteren en analyseren van bewijsmateriaal uit een getroffen computersysteem. Het doel daarvan is veranderingen aan het systeem vast te stellen en te assisteren bij de reconstructie van gebeurtenissen die tot de inbreuk hebben geleid. De informatie en het bewijsmateriaal moeten zo worden verzameld dat een keten van gebeurtenissen kan worden aangetoond die in een rechtszaak steekhoudend en rechtsgeldig is. Het verzamelen van forensisch bewijsmateriaal omvat onder andere de volgende taken: een bit-imagekopie maken van de vaste schijf van het getroffen systeem, controleren op veranderingen aan het systeem zoals nieuwe programma's, bestanden, services en gebruikers, onderzoeken van actieve processen en open poorten, en het zoeken naar Trojaanse paarden en toolkits. CSIRT-personeel met deze functie moet mogelijk ook bereid zijn om als deskundig getuige in juridische procedures op te treden.

Tracking of tracering

De tracering van de oorsprong van een indringer of identificatie van systemen waartoe de indringer toegang had. Deze activiteit omvat mogelijk de tracking of tracering van hoe de indringer de getroffen systemen en gerelateerde netwerken is binnengekomen, met welke systemen die toegang is verkregen, van waaruit de aanval is uitgevoerd en welke andere systemen en netwerken als onderdeel van de aanval zijn gebruikt. Ook kan worden geprobeerd de identiteit van de indringer te achterhalen. Dit werk kan alleen worden uitgevoerd, hoewel meestal wordt samengewerkt met autoriteiten, ISP's of andere betrokken organisaties.

Reacties op incidenten op locatie

Het CSIRT biedt directe assistentie op locatie om constituenten te helpen bij het herstellen van een incident. Het CSIRT zorgt zelf voor fysieke analyses van de getroffen systemen. Ook voert het team de herstelwerkzaamheden uit voor de systemen in plaats van alleen ondersteuning te bieden per telefoon of e-mail om te reageren op het incident (zie hieronder). Deze dienst omvat alle benodigde acties op lokaal niveau als een incident zich voordoet of wordt vermoed. Als het CSIRT zich niet op de desbetreffende locatie bevindt, gaan er teamleden naartoe om de acties uit te voeren. In andere gevallen is een lokaal team mogelijk al aanwezig, dat als onderdeel van de normale werkzaamheden op incidenten reageert. Dit geldt vooral als het afhandelen van incidenten onder de normale taakomschrijving valt van systeem-, netwerk- of beveiligingsbeheerders in plaats van een gevestigd CSIRT.

Ondersteuning bij reacties op incidenten

Het CSIRT assisteert en ondersteunt de slachtoffers van de aanval bij het herstellen van een incident via de telefoon, e-mail, fax of documentatie. Dit kan variëren van technische assistentie bij de interpretatie van de verzamelde gegevens tot het bieden van contactinformatie en hulp bij het ontwikkelen van maatregelen voor risicobeperking en herstel. Hierbij is geen sprake van directe acties op locatie zoals hierboven is beschreven. Het CSIRT biedt in plaats daarvan begeleiding op afstand zodat het personeel ter plekke zelf het herstel kan uitvoeren.

Coördinatie van reacties op incidenten

Het CSIRT coördineert alle reacties en inspanningen van de bij het incident betrokken partijen. Daar vallen doorgaans het slachtoffer van de aanval en andere betrokken locaties onder, plus eventuele locaties die assistentie nodig hebben bij het analyseren van de aanval. Ook de partijen die IT-ondersteuning bieden aan het slachtoffer kunnen erbij betrokken zijn, zoals ISP's, andere CSIRT's en systeem- en netwerkbeheerders op de locatie. Onder de coördinatiewerkzaamheden vallen onder meer het verzamelen van contactinformatie, het inlichten van locaties over mogelijk betrokkenheid (als slachtoffer of bron van een aanval), het verzamelen van statistische gegevens over het aantal betrokken locaties en het faciliteren van de uitwisseling en analyse van informatie. Bij een coördinerende taak horen mogelijk ook het informeren van en samenwerken met de juridische afdeling, de afdeling personeelszaken of de PR-afdeling van een organisatie. Ook coördinatie met de autoriteiten kan hierbij komen kijken. Bij deze dienst is geen sprake van directe acties op locatie.

Afhandeling van beveiligingslekken

Bij de afhandeling van beveiligingslekken komen de volgende zaken aan de orde: informatie en meldingen ontvangen over beveiligingslekken of kwetsbaarheden in hardware en software, de aard, technische details en effecten van de beveiligingslekken analyseren, en reactieve maatregelen ontwikkelen voor het detecteren en repareren van de beveiligingslekken. De afhandeling van beveiligingslekken gebeurt op diverse manieren door verschillende soorten CSIRT's. Deze dienst is dan ook als volgt verder onderverdeeld op basis van het type uitgevoerde activiteiten en het soort ondersteuning dat wordt geboden:

Analyse van beveiligingslekken

Het CSIRT voert technische analyses en onderzoeken uit van en naar beveiligingslekken in hardware of software. Dit omvat de verificatie van verdachte beveiligingslekken en het technische onderzoek van de beveiligingslekken in hardware of software om vast te stellen waar de problemen zich bevinden en hoe daarvan misbruik kan worden gemaakt. De analyse kan er onder meer in bestaan dat de broncode nader wordt bekeken, met behulp van een foutopsporingsprogramma de plaats van het beveiligingslek wordt vastgesteld of geprobeerd wordt om het probleem op een testsysteem te reproduceren.

Reactie op beveiligingslekken

Onder deze dienst valt het vaststellen van de juiste reactie om het risico en de impact van het beveiligingslek te beperken of het lek te repareren. Daarbij kan het ontwikkelen of onderzoeken van patches, fixes en tijdelijke oplossingen een rol spelen. Anderen op de hoogte stellen van de risicobeperkende maatregelen hoort daar ook bij, mogelijk door het opstellen en verspreiden van aanbevelingen of waarschuwingen. Daarnaast vormt het installeren van patches, fixes of tijdelijke oplossingen eventueel een onderdeel van deze dienst.

Coördinatie van reacties op beveiligingslekken

Het CSIRT informeert de verschillende partijen van de organisatie of constituency over het beveiligingslek en geeft aan hoe men de risico's of gevolgen kan beperken of het probleem kan oplossen. Het CSIRT verifieert dat de reactieve maatregelen met succes zijn geïmplementeerd. Deze dienst omvat bijvoorbeeld ook de communicatie met leveranciers, andere CSIRT's, technische experts, constituenten en de personen of groepen die het beveiligingslek aanvankelijk hebben ontdekt of gemeld. Mogelijke activiteiten zijn het faciliteren van de analyse van een beveiligingslek of melding daarvan, het coördineren van de geplande release van relevante documenten, patches of tijdelijke oplossingen, en het samenbrengen van technische analyses die door verschillende partijen zijn uitgevoerd. Bij deze dienst hoort mogelijk ook het bijhouden van een openbaar of besloten archief of kennisdatabase met informatie over beveiligingslekken en bijbehorende reactieve maatregelen.

Afhandeling van artefacten

Een artefact is een in een systeem aangetroffen bestand of object dat betrokken kan zijn bij het indringen in of aanvallen van systemen en netwerken, of dat wordt gebruikt om beveiligingsmaatregelen te omzeilen of uit te schakelen. Artefacten zijn bijvoorbeeld computervirussen, Trojaanse paarden, wormen, kwaadaardige scripts en toolkits.
Bij de afhandeling van artefacten hoort het ontvangen van informatie en kopieën van de artefacten die bij aanvallen van indringers, afluisterpraktijken en andere ongeoorloofde of ontwrichtende activiteiten worden gebruikt. Na ontvangst wordt het artefact onderzocht. Dit omvat het analyseren van de aard, technische details, versie en het gebruik van de artefacten en het ontwikkelen (of voorstellen) van reactieve maatregelen voor het detecteren, verwijderen en afweren ervan. De afhandeling van artefacten gebeurt op diverse manieren door verschillende soorten CSIRT's. Deze dienst is dan ook als volgt verder onderverdeeld op basis van het type uitgevoerde activiteiten en het soort ondersteuning dat wordt geboden:

Analyse van artefacten

Het CSIRT voert technische analyses en onderzoeken uit van de aangetroffen artefacten in een systeem. Bij deze analyse kunnen bijvoorbeeld het bestandstype en de structuur van het artefact worden geïdentificeerd. Ook kan een nieuw artefact met bestaande artefacten worden vergeleken om overeenkomsten en verschillen te zien, of reverse engineering of decompilatie van code plaatsvinden om het doel en de functie van het artefact te achterhalen.

Reactie op artefacten

Met deze dienst worden de juiste acties vastgesteld voor de detectie en verwijdering van artefacten in een systeem, plus acties om de installatie van artefacten te voorkomen. Daarbij is de aanmaak van handtekeningen mogelijk die aan antivirussoftware of IDS kunnen worden toegevoegd.

Coördinatie van reacties op artefacten

Deze dienst omvat het uitwisselen en samenbrengen van analyseresultaten en reactieve maatregelen aangaande een artefact met andere onderzoekers, CSIRT's, leveranciers en andere beveiligingsexperts. Daarbij horen het inlichten van anderen en samenbrengen van technische analyses uit verschillende bronnen. Mogelijke activiteiten zijn ook het bijhouden van een openbaar of besloten archief (voor de constituent) van bekende artefacten met de impact ervan plus bijbehorende reactieve maatregelen.

Proactieve diensten

Proactieve diensten zijn gericht op het verbeteren van de infrastructuur en beveiligingsprocessen van de constituency voordat een incident of gebeurtenis optreedt of wordt gedetecteerd. De hoofddoelen zijn het voorkomen van incidenten en het beperken van de impact en omvang ervan als ze wel optreden.

Mededelingen

Voorbeelden hiervan zijn alarmeringen bij aanvallen, waarschuwingen voor beveiligingslekken en beveiligingsadviezen. Dergelijke mededelingen informeren constituenten over nieuwe ontwikkelingen met gevolgen voor de middellange of lange termijn. Denk bijvoorbeeld aan recent ontdekte beveiligingslekken of tools voor indringers. Op basis van de mededelingen kunnen constituenten hun systemen en netwerken beschermen tegen nieuwe problemen voordat misbruik kan plaatsvinden.

Technologiebewaking

Het CSIRT bewaakt en volgt nieuwe technische ontwikkelingen, activiteiten van indringers en daaraan gerelateerde trends om toekomstige bedreigingen beter te zien aankomen. De onderwerpen kunnen worden uitgebreid met jurisprudentie en nieuwe wetten en voorschriften, sociale of politieke bedreigingen en technologieën die in opkomst zijn. Deze dienst omvat het volgen van mailinglists en websites op het gebied van beveiliging, evenals het actuele nieuws en publicaties waarbij wetenschap, technologie, politiek en overheid een rol spelen. Dit alles met het oog op relevante informatie voor de beveiliging van de systemen en netwerken van de constituenten. Dit kan ook communicatie inhouden met andere deskundige partijen op een of meer van deze gebieden om er zeker van te zijn dat men over de beste en meest accurate informatie beschikt. Het resultaat van deze dienst kan de vorm aannemen van mededelingen, richtlijnen of aanbevelingen gericht op beveiligingskwesties op de middellange tot lange termijn.

Beveiligingscontroles of -beoordelingen

Deze dienst biedt een gedetailleerde controle en analyse van de beveiligingsinfrastructuur van een organisatie op basis van de gedefinieerde vereisten van de organisatie zelf of van andere industrienormen die van toepassing zijn. Ook kan worden gekeken naar de beveiligingspraktijken van de organisatie. Er zijn vele verschillende soorten controles of beoordelingen mogelijk, waaronder:

Beoordeling van de infrastructuur

Handmatige controle van de hardware- en softwareconfiguraties, routers, firewalls, servers en desktopapparaten om te beoordelen of ze voldoen aan het beveiligingsbeleid en beste praktijken van de organisatie of de industrienormen en standaardconfiguraties.

Beoordeling van de praktijk

Het interviewen van medewerkers en systeem- en netwerkbeheerders om na te gaan of de beveiliging in de praktijk overeenkomt met het gedefinieerde beleid van de organisatie of sommige specifieke industrienormen.

Scannen

Virusscanners en soortgelijke software toepassen om vast te stellen welke systemen en netwerken kwetsbaar zijn.

Indringingstests

Het testen van de beveiliging van een locatie door de systemen en netwerken ervan opzettelijk aan te vallen.
Voor het uitvoeren van dergelijke controles of beoordelingen is toestemming vooraf van het hogere management vereist. Sommige methoden zijn mogelijk niet toegestaan volgens het beleid van de organisatie. Deze dienst kan bestaan uit het ontwikkelen van een algemene set werkwijzen voor de uitvoering van tests of beoordelingen, eventueel gekoppeld aan de ontwikkeling van een vereiste set vaardigheden of certificatievereisten voor het personeel dat de tests, beoordelingen, controles of onderzoeken uitvoert. Deze dienst kan ook aan een externe partij worden uitbesteed met de nodige ervaring in het uitvoeren van controles en beoordelingen op beveiligingsgebied.

Configureren en bijhouden van beveiligingstools, -applicaties, -infrastructuren en -diensten

Deze dienst zorgt voor de gepaste begeleiding bij het veilig configureren en bijhouden van tools, programma's en de algemene computerinfrastructuur van de CSIRT-constituency of het CSIRT zelf. Naast het bieden van begeleiding kan het CSIRT ook configuratie-updates en onderhoud uitvoeren voor beveiligingstools en -diensten, zoals IDS, netwerkscans of -bewakingssystemen, filters, wrappers, firewalls, VPN's (virtual private networks) of verificatiemechanismen. Het CSIRT kan deze diensten zelfs als onderdeel van de hoofdfunctie ervan leveren. Het CSIRT kan op basis van beveiligingsrichtlijnen ook servers, desktops, laptops, PDA's (personal digital assistants) en andere draadloze apparaten configureren en bijhouden. Deze dienst omvat tevens het melden aan het management van configuratiekwesties of problemen met programma's en applicaties die volgens het CSIRT een systeem kwetsbaar maken voor aanvallen.

Ontwikkeling van beveiligingstools

Deze dienst omvat het ontwikkelen van nieuwe, specifieke tools voor constituenten op basis van de vereisten of wensen van de constituency of het CSIRT zelf. Dit kunnen bijvoorbeeld beveiligingspatches zijn voor aangepaste software in de constituency of beveiligde softwaredistributies waarmee getroffen hosts opnieuw kunnen worden gebouwd. Ook kan er sprake zijn van de ontwikkeling van tools of scripts die de functionaliteit van bestaande beveiligingstools uitbreiden. Denk bijvoorbeeld aan een nieuwe invoegtoepassing voor netwerkscanners, scripts die het gebruik van versleutelingstechnologieën faciliteren, of mechanismen voor geautomatiseerde patchdistributie.

Diensten voor detectie van aanvallen

CSIRT's die deze diensten verzorgen, bekijken bestaande IDS-logboeken en analyseren en initiëren een reactie voor elke gebeurtenis die aan de gedefinieerde drempelwaarden voldoet. Ook kan men een alarmering of waarschuwing verzenden volgens een vooraf gedefinieerde SLA of escalatiestrategie. De detectie van aanvallen en de analyse van de bijbehorende beveiligingslogboeken kunnen een lastige zaak zijn, niet alleen bij het bepalen waar de sensoren in de omgeving moeten worden geplaatst, maar ook bij het verzamelen en analyseren van de grote hoeveelheden vastgelegde gegevens. In veel gevallen komen er speciale tools of deskundigheid aan te pas om de informatie samen te brengen en te interpreteren, dit met het doel om valse alarmen, aanvallen of

netwerkgebeurtenissen te identificeren en maatregelen te implementeren die dergelijke gebeurtenissen uitschakelen of minimaliseren. Sommige organisaties besteden deze activiteit liever uit aan anderen met meer ervaring op dit gebied, zoals leveranciers van beheerde beveiligingsdiensten.

Verspreiding van beveiligingsgerelateerde informatie

Deze dienst biedt constituenten een uitgebreide en overzichtelijke verzameling nuttige informatie voor het verbeteren van de beveiliging. Deze informatie kan onder andere het volgende bevatten:

- richtlijnen voor meldingen en contactinformatie voor het CSIRT,
- archieven met alarmeringen, waarschuwingen en andere mededelingen,
- documentatie over actuele beste praktijken,
- algemene richtlijnen voor computerbeveiliging,
- beleidsregels, procedures en controlelijsten,
- informatie over ontwikkeling en distributie van patches,
- koppelingen naar leverancier,
- actuele statistieken en trends in incidentmeldingen,
- andere informatie die de algemene beveiligingspraktijken kan verbeteren.

Deze informatie kan door het CSIRT worden ontwikkeld en gepubliceerd, of door een ander onderdeel van de organisatie (IT, personeelszaken of mediarelaties). De informatie kan (deels) afkomstig zijn uit externe bronnen, zoals andere CSIRT's, leveranciers en beveiligingsexperts.

Kwaliteitsbeheer en beveiligingsdiensten

Diensten in deze categorie zijn niet alleen beperkt tot incidentafhandeling of CSIRT's in het bijzonder. Het gaat hier om bekende, gevestigde diensten om de algehele beveiliging van een organisatie te verbeteren. Vanuit hun opgedane ervaringen met de hierboven beschreven reactieve en proactieve diensten kunnen CSIRT's unieke invalshoeken toevoegen aan deze diensten voor kwaliteitsbeheer. Deze diensten richten zich op het toepassen van feedback en opgedane kennis bij de afhandeling van incidenten, beveiligingslekken en aanvallen. Als deze feedback en kennis worden opgenomen in de gevestigde traditionele diensten (zie hieronder) als onderdeel van een proces voor kwaliteitsbeheer en beveiliging, komt dit de beveiliging in een organisatie op lange termijn ten goede. Afhankelijk van de organisatiestructuren en verantwoordelijkheden kan een CSIRT deze diensten verlenen of er in groter verband aan bijdragen voor de organisatie.
Hierna wordt beschreven hoe de expertise van CSIRT's een aanvullende rol kan vervullen bij elk van deze diensten voor kwaliteitsbeheer.

Analyse van risico's

CSIRT's kunnen bij de analyse en beoordeling van risico's zorgen voor een zekere meerwaarde. Hierdoor is de organisatie beter in staat werkelijke bedreigingen te beoordelen en tot realistische kwalitatieve en kwantitatieve beoordelingen van de risico's voor de informatie en voorzieningen op dit gebied te komen. Ook is een betere evaluatie van de beschermende en reactieve maatregelen mogelijk. CSIRT's dragen dan bij door het (mede) uitvoeren van analyses van de beveiligingsrisico's voor nieuwe systemen en bedrijfsprocessen, of ze evalueren bedreigingen van en aanvallen op de voorzieningen en systemen van constituenten.

Planning van bedrijfscontinuïteit en noodherstel

Op basis van eerdere voorvallen en voorspellingen van trends wat betreft incidenten of beveiligingskwesties, hebben incidenten potentieel steeds grotere gevolgen voor de continuïteit van de bedrijfsactiviteiten. Bij de bedrijfsplanning spelen de ervaringen en aanbevelingen van CSIRT's dan ook een onmisbare rol bij het bepalen van de beste aanpak voor dergelijke incidenten teneinde de continuïteit van de bedrijfsactiviteiten te waarborgen. CSIRT's die deze dienst leveren, zijn betrokken bij de planning van de bedrijfscontinuïteit en het noodherstel in geval van bedreigingen van en aanvallen op de computerbeveiliging.

Beveiligingsadvies

CSIRT's kunnen begeleiding en advies geven aangaande de beste beveiligingspraktijken in verband met de bedrijfsactiviteiten van constituenten. Deze CSIRT's zorgen dan voor aanbevelingen of een omschrijving van de vereisten voor de aankoop, installatie of beveiliging van nieuwe systemen, netwerkapparatuur, softwareapplicaties of bedrijfsprocessen. Deze dienst omvat tevens het bieden van richtsnoeren en assistentie bij de ontwikkeling van het beveiligingsbeleid voor de organisatie of constituency. Ook kan sprake zijn van het optreden als getuige of geven van advies aan wetgevende instanties of andere overheidsorganen.

Bewustmaking

CSIRT's kunnen mogelijk vaststellen waar constituenten meer informatie en begeleiding nodig hebben om beter te voldoen aan gangbare beveiligingspraktijken en het beveiligingsbeleid van de organisatie. Als de constituenten zich in algemene zin meer bewust zijn van het belang van beveiliging, vergroot dit niet alleen hun inzicht in beveiligingskwesties, maar zal dit ook helpen de dagelijkse werkzaamheden op een veiliger manier uit te voeren. Hierdoor zullen minder aanvallen hun doel bereiken en constituenten beter in staat zijn de aanvallen te herkennen en te melden. Zo gaat minder tijd verloren aan herstel en blijven ook verdere verliezen beperkt.
CSIRT's die zich richten op bewustmaking, doen dat bijvoorbeeld door het ontwikkelen van artikelen, posters, nieuwsbrieven, websites of andere informatieve bronnen en hulpmiddelen met uitleg over de beste aanpak van de beveiliging en advies over preventieve maatregelen. Ook kunnen bijeenkomsten en seminars worden georganiseerd om constituenten op de hoogte te houden van beveiligingsprocedures en mogelijke bedreigingen voor systemen in de organisatie.

Opleiding/training

Deze dienst omvat het verstrekken van informatie over computerbeveiligingsthema's aan constituenten via seminars, workshops, cursussen en handleidingen. Tot de mogelijke onderwerpen horen richtsnoeren voor het melden van incidenten, gepaste reactiemethoden en tools en methoden voor de afhandeling en preventie van incidenten. Kortom, alle nuttige informatie voor de bescherming tegen, detectie en melding van en reactie op computerbeveiligingsincidenten.

Productevaluatie of -certificatie

Het CSIRT kan productevaluaties uitvoeren van hulpprogramma's, applicaties of andere diensten om de veiligheid van de producten te waarborgen en na te gaan of ze voldoen aan de normen en beveiligingspraktijken die het CSIRT of de organisatie nastreeft. De

beoordeelde hulpprogramma's en applicaties kunnen open-source- of commerciële producten zijn. Deze dienst kan als evaluatie of via een certificatieprogramma worden verleend, afhankelijk van de normen die bij de organisatie of het CSIRT worden gehanteerd.

A.3 De voorbeelden

Fictief CSIRT

Stap 0 - Begrijpen wat een CSIRT is:

Het voorbeeld-CSIRT verzorgt diensten voor een middelgrote instelling met maximaal 200 medewerkers. De instelling heeft een eigen IT-afdeling en twee andere filialen in hetzelfde land. IT speelt een sleutelrol in het bedrijf en wordt toegepast voor de interne communicatie, het gegevensnetwerk en een continue e-business (24x7). Het instituut heeft een eigen netwerk en beschikt over een redundante verbinding met internet via twee verschillende ISP's.

- -

Stap 1: Startfase

In de startfase wordt het nieuwe CSIRT gepland als een intern CSIRT, waarbij de diensten worden verleend aan het hostbedrijf, de lokale IT-afdeling en het personeel. Tevens vindt ondersteuning en coördinatie plaats bij de afhandeling van IT-beveiligingsincidenten voor de verschillende filialen.

- -

Stap 2: De juiste diensten kiezen

In de beginfase wordt besloten dat het nieuwe CSIRT zich voornamelijk zal richten op het bieden van enkele kerndiensten aan de medewerkers.

Er is besloten dat na een testfase uitbreiding van het dienstenpakket valt te overwegen, plus de toevoeging van enkele diensten op het gebied van beveiligingsbeheer. Deze beslissing wordt genomen op basis van de feedback van de proefconstituenten en in nauwe samenwerking met de afdeling Kwaliteitsbeheer.

- -

Stap 3: Een analyse maken van de constituency en de juiste communicatiekanalen

Een brainstormsessie met enkele sleutelfiguren uit het management en de constituency heeft genoeg materiaal opgeleverd voor een SWOT-analyse. De conclusie is getrokken dat er behoefte is aan de kerndiensten:

- Alarmeringen en waarschuwingen
- Afhandeling van incidenten (analyse, ondersteuning bij reacties en coördinatie van reacties)
- Mededelingen

De informatie moet op een goed georganiseerde manier worden verspreid om het grootst mogelijke deel van de constituency te bereiken. Er is dan ook besloten om de alarmeringen, waarschuwingen en mededelingen in de vorm van beveiligingsadviezen te publiceren op een speciale website en via een mailinglist te verspreiden. Het CSIRT faciliteert e-mail, telefoon en fax voor het ontvangen van incidentmeldingen. Een uniform webformulier staat gepland als volgende stap.

- -

Stap 4: Mission statement

Het management van het fictieve CSIRT heeft de volgende mission statement opgesteld:
"Fictief CSIRT biedt informatie en ondersteuning aan de medewerkers van de hostorganisatie om de kans op computerbeveiligingsincidenten te verkleinen en te reageren op dergelijke incidenten wanneer ze zich voordoen."

Hiermee maakt het fictieve CSIRT duidelijk dat het een intern CSIRT betreft en dat de kernactiviteit is gericht op kwesties rondom IT-beveiliging.

- -

Stap 5: Het bedrijfsplan definiëren

Financieel model

Het bedrijf heeft een e-business van 24x7 en tevens een IT-afdeling die 24x7 inzetbaar is. Er is dan ook besloten om volledige service te verlenen tijdens kantooruren en een oproepbaarheidsdienst buiten kantooruren. De aan de constituency verleende diensten zijn gratis, maar de mogelijkheid om diensten aan externe klanten te bieden wordt nader bekeken in de test- en evaluatiefase.

Financieringsmodel

In de start- en testfase wordt het CSIRT gefinancierd door het hostbedrijf. In de test- en evaluatiefase worden extra financieringsbronnen besproken, waaronder de mogelijkheid om diensten aan externe klanten te verkopen.

Organisatiemodel

De hostorganisatie is een kleine onderneming, dus wordt het ingesloten model gekozen.
Tijdens kantooruren verzorgen drie medewerkers de kerndiensten (verspreiding van beveiligingsadviezen en afhandeling/coördinatie van incidenten).

Op de IT-afdeling van het bedrijf werken al mensen met de benodigde ervaring. Met die afdeling is de afspraak gemaakt dat het nieuwe CSIRT op incidentele basis ondersteuning kan vragen wanneer dat nodig is. Ook de tweede lijn van hun oproepbare technici kan worden gebruikt.
Er komt een CSIRT-basisteam met vier fulltime-medewerkers en vijf extra CSIRT-teamleden. Een van die medewerkers is beschikbaar in circulerende diensten.

Personeel

De teamleider van het CSIRT heeft een achtergrond in beveiliging en ondersteuning op het eerste en tweede niveau en werkervaring op het gebied van veerkracht/crisisbeheer. De drie andere teamleden zijn beveiligingsspecialisten. De parttime-CSIRT-teamleden van de IT-afdeling zijn specialisten op hun gebied van de infrastructuur van het bedrijf.

- -

Stap 5: Gebruik van het kantoor en informatiebeveiligingsbeleid
Kantoorfaciliteiten en -locatie
Het hostbedrijf is al voorzien van een efficiënte fysieke beveiliging en het CSIRT is in dat opzicht dan ook prima gehuisvest. Er is een “crisisruimte” beschikbaar voor coördinatiedoeleinden in noodsituaties. Er is een kluis aangeschaft voor het versleutelingsmateriaal en vertrouwelijke documenten. Er is een aparte telefoonlijn met een schakelkast als hotline tijdens kantooruren en een mobiele telefoon voor oproepen buiten kantooruren met hetzelfde telefoonnummer.

Bestaande apparatuur alsook de website van het bedrijf zijn beschikbaar voor het melden van CSIRT-gerelateerde informatie. Er wordt een mailinglistprogramma geïnstalleerd en bijgehouden, met een besloten gedeelte voor de communicatie tussen teamleden en met andere teams. Alle contactgegevens van de medewerkers zijn opgeslagen in een database, met een afgedrukt exemplaar veilig opgeborgen in de kluis.

Voorschriften
Het CSIRT maakt deel uit van een bedrijf met bestaande beleidsregels voor de informatiebeveiliging, zodat het beleid voor het CSIRT is vastgesteld met de hulp van de juridisch adviseur van het bedrijf.
- -

Stap 7: Samenwerking zoeken
Met behulp van het ENISA-overzicht zijn enkele CSIRT’s in hetzelfde land gevonden en benaderd. Voor de nieuwe teamleider werd een bezoek aan een van die CSIRT’s geregeld. Hij leerde over landelijke CSIRT-activiteiten en woonde een bijeenkomst bij. Deze bijeenkomst was uiterst nuttig voor het verzamelen van voorbeelden van werkmethoden en het ontvangen van ondersteuning van enkele andere teams.
- -

Stap 8: Het bedrijfsplan promoten

Er is besloten feiten en cijfers te verzamelen uit de geschiedenis van het bedrijf. Dit is uiterst nuttig als statistisch overzicht van de IT-veiligheidssituatie. Als het CSIRT eenmaal actief is, blijft het verzamelen van deze statistische gegevens nuttig om alles actueel te houden.

Andere nationale CSIRT’s werden benaderd en ondervraagd over hun business case. Zij boden ondersteuning door enkele dia’s samen te stellen over recente ontwikkelingen in IT-beveiligingsincidenten en de kosten van incidenten.

In dit voorbeeld van Fictief CSIRT was geen sprake van een dringende noodzaak om het management te overtuigen van het belang van IT-beveiliging. Er was dan ook snel toestemming om de eerste stap te zetten. Er werden een zakelijke onderbouwing en een projectplan opgesteld, inclusief een schatting van de aanloopkosten en de operationele kosten.
- -

Stap 9: Processtromen en operationele en technische procedures instellen
Fictief CSIRT richt zich op het verlenen van CSIRT-kerndiensten:

- Alarmeringen en waarschuwingen
- Mededelingen
- Afhandeling van incidenten

Het team heeft procedures ontwikkeld die goed werken en voor elk teamlid gemakkelijk te begrijpen zijn. Fictief CSIRT heeft ook een juridisch adviseur ingezet voor kwesties rondom de aansprakelijkheid en het beleid voor informatiebeveiliging. Het team heeft enkele nuttige hulpprogramma's in gebruik genomen en bruikbare informatie ingewonnen door operationele kwesties met andere CSIRT's te bespreken.

Er is een vaste sjabloon gegenereerd voor beveiligingsadviezen en incidentrapporten. Het team gebruikt RTIR voor de afhandeling van incidenten.

- -

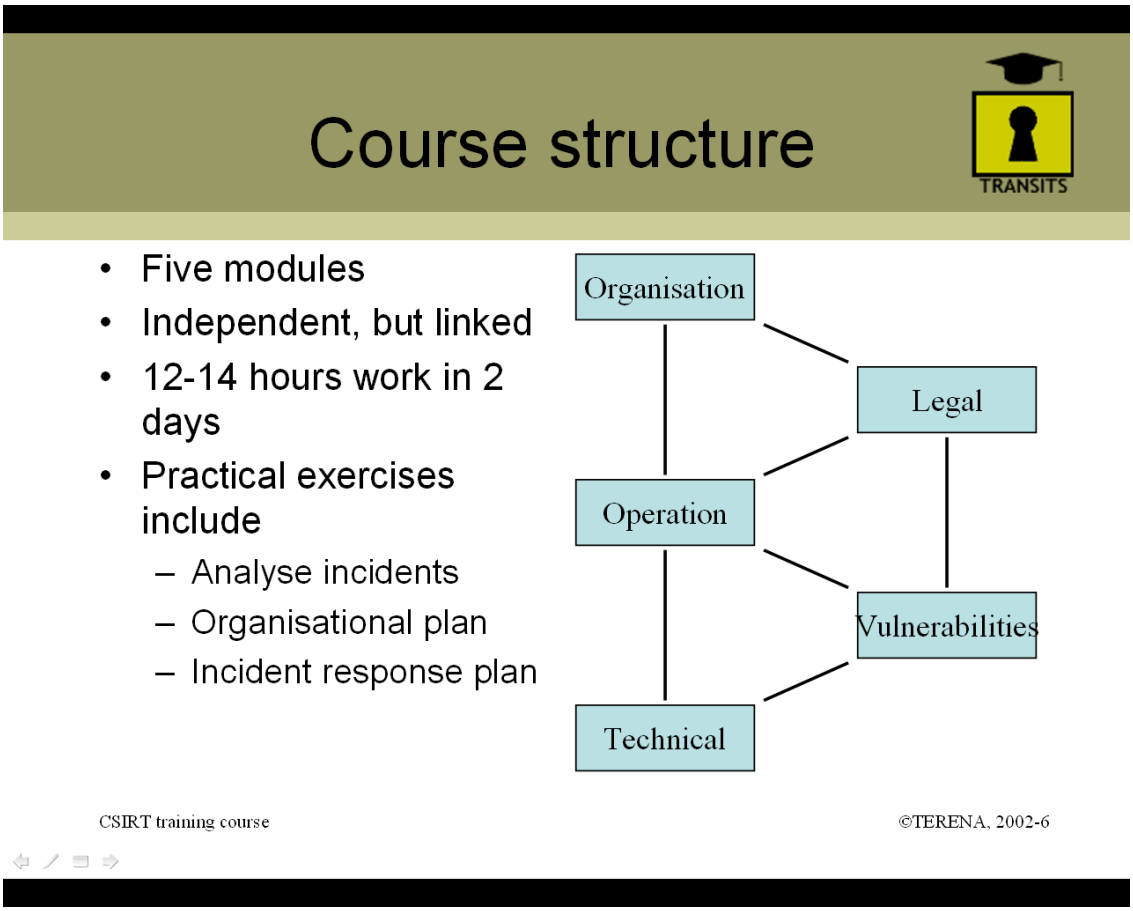
Stap 10: Het personeel opleiden
Fictief CSIRT besluit het voltallige technische personeel naar de eerstvolgende TRANSITS-cursussen te sturen. De teamleider volgt daarnaast de cursus voor het beheren van CSIRT's van het CERT/CC.

- -

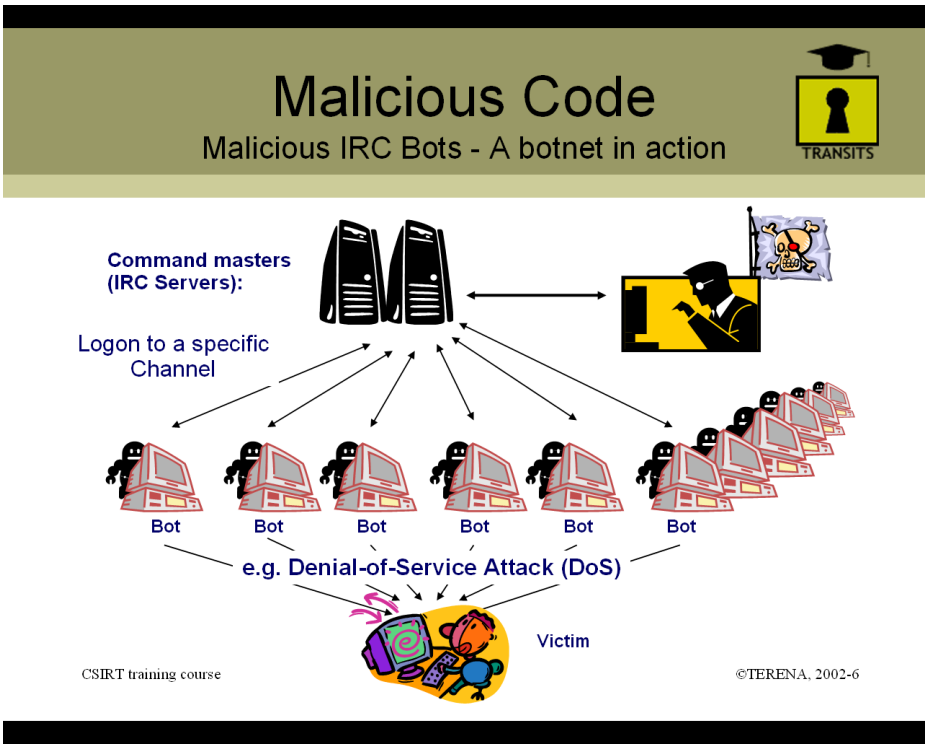
Stap 11: Oefening
In de eerste actieve weken van het fictief CSIRT werden op basis van voorbeelden van andere CSIRT's diverse fictieve gevallen geoefend. Verder heeft het CSIRT enkele beveiligingsadviezen uitgebracht op basis van actuele informatie over beveiligingslekken afkomstig van hardware- en softwareleveranciers, die verder zijn aangepast en afgestemd op de behoeften van de constituency.

A.4 Voorbeeldmateriaal van CSIRT-cursussen

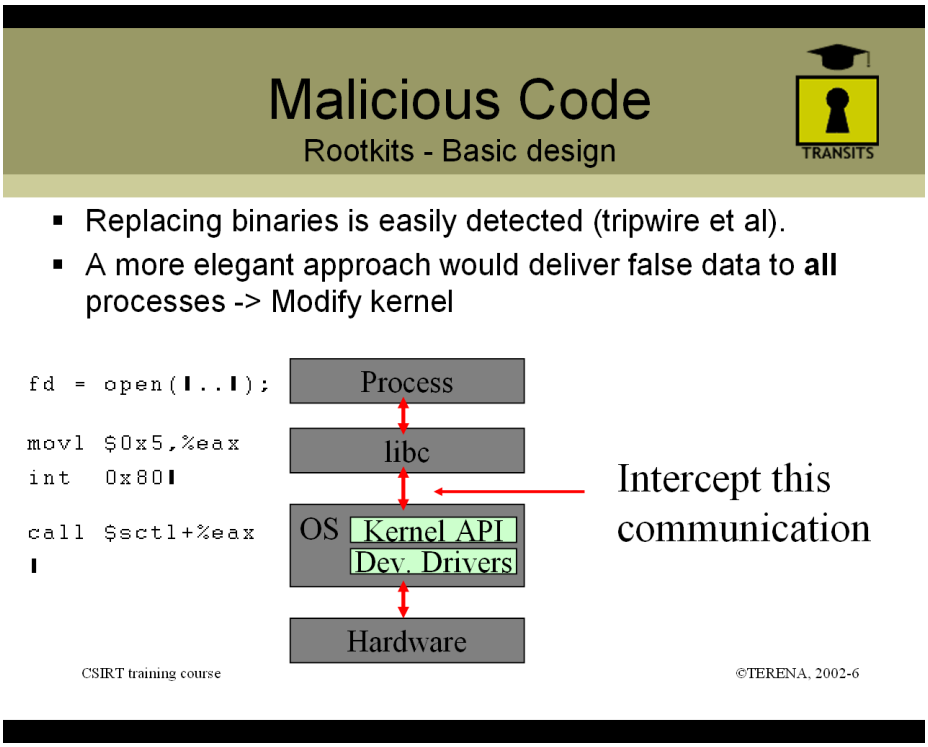
TRANSITS (met welwillende toestemming van Terena, http://www.terena.nl)



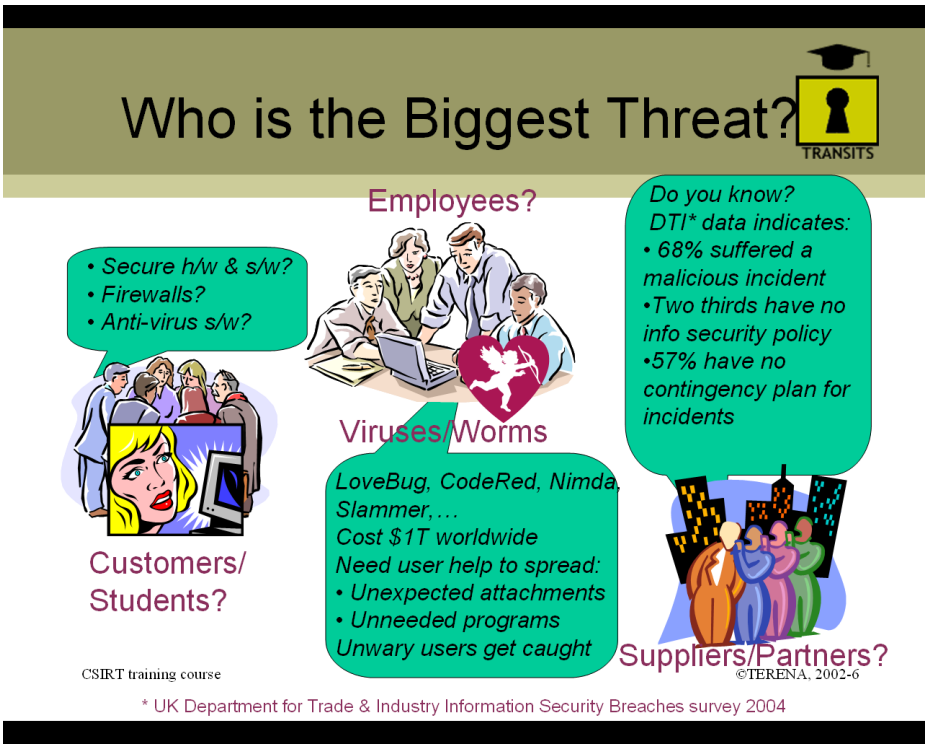
Overzicht: de cursusstructuur



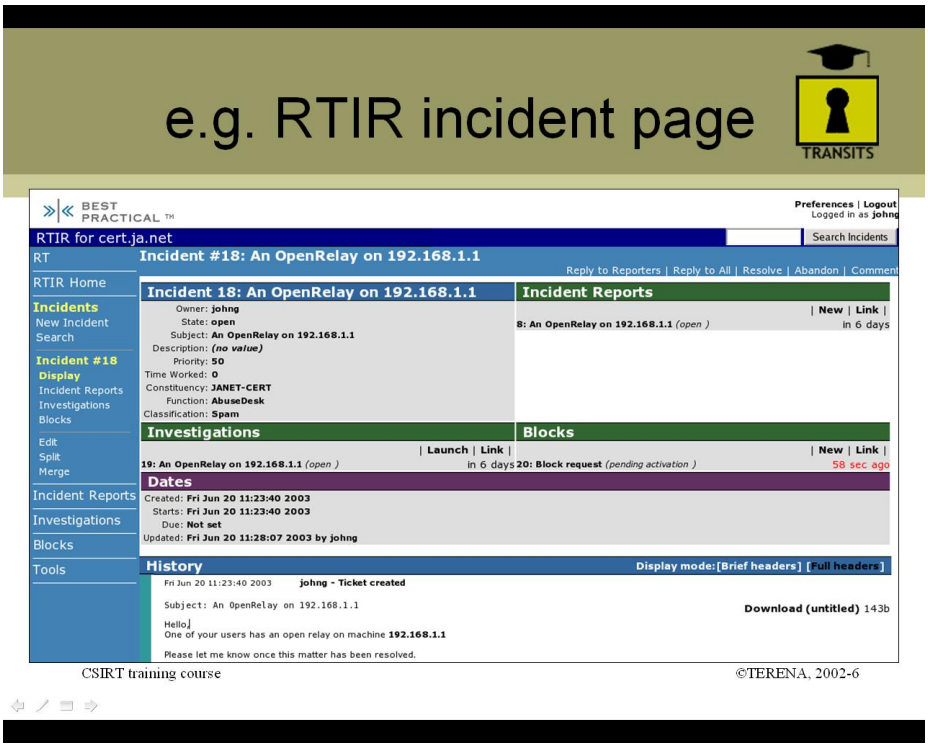
Uit de technische module: beschrijving van een botnet



Uit de technische module: basisontwerp van een rootkit



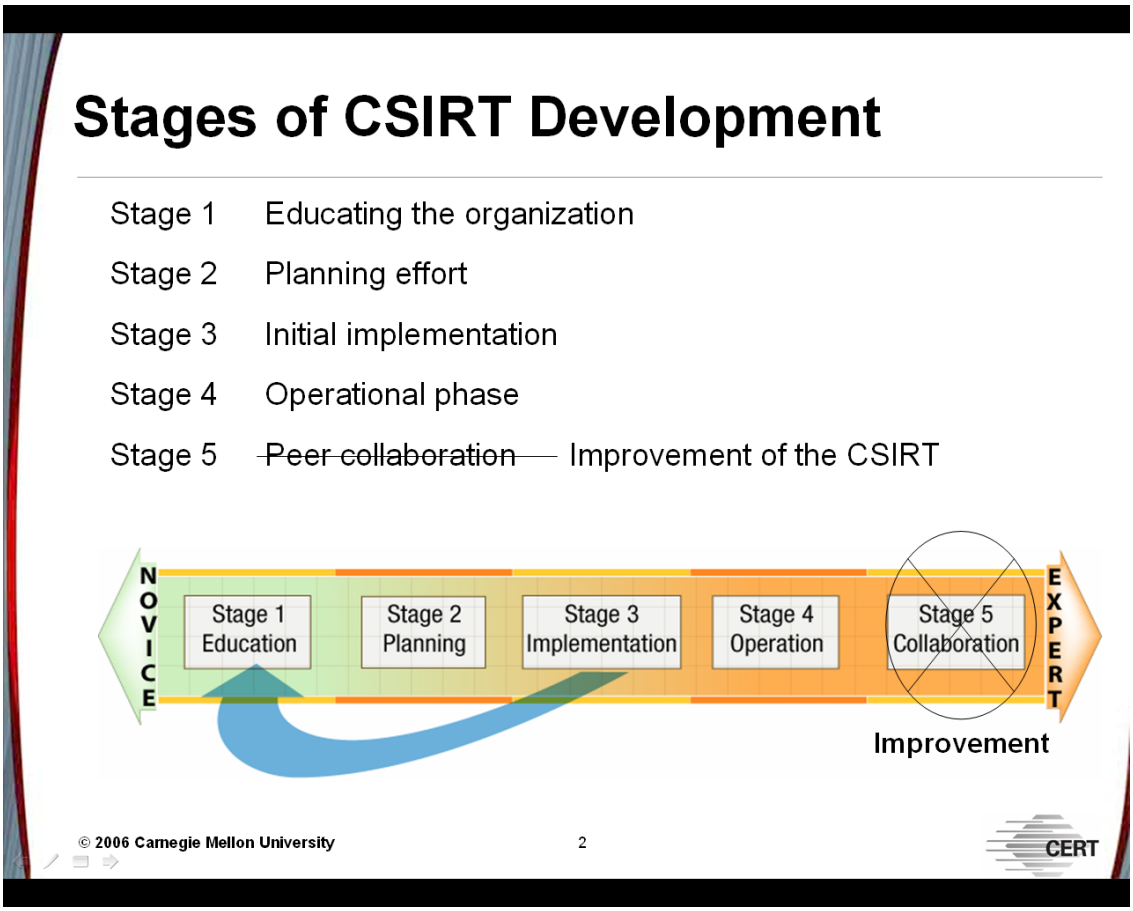
Uit de organisatiemodule: insider of outsider – waar ligt de grootste bedreiging?



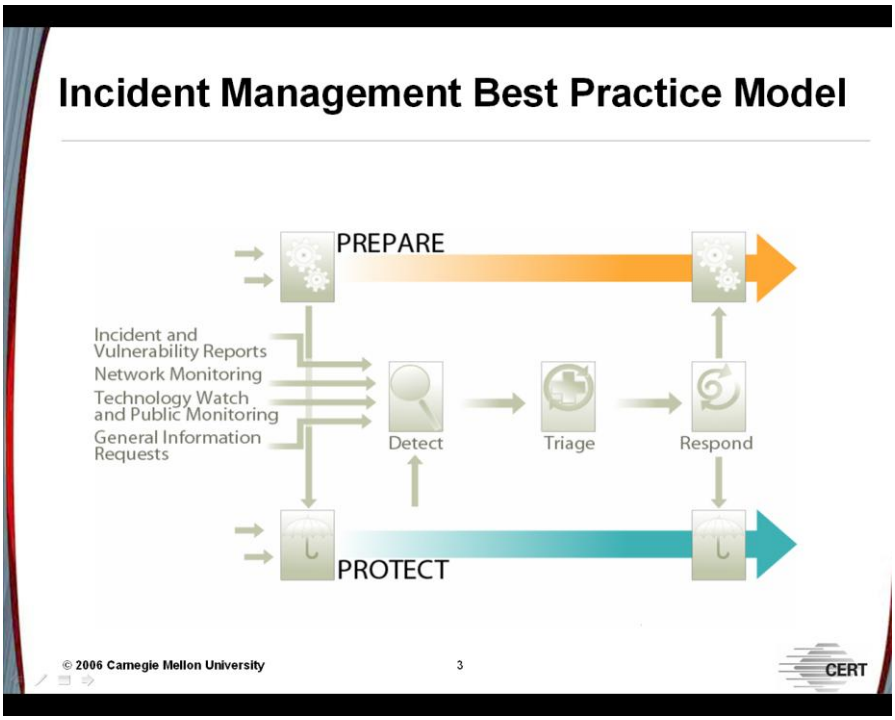
Uit de module voor operationele controle: Request Tracker for Incident Response (RTIR)

CSIRTS opzetten (met welwillende toestemming van CERT/CC, http://www.cert.org)

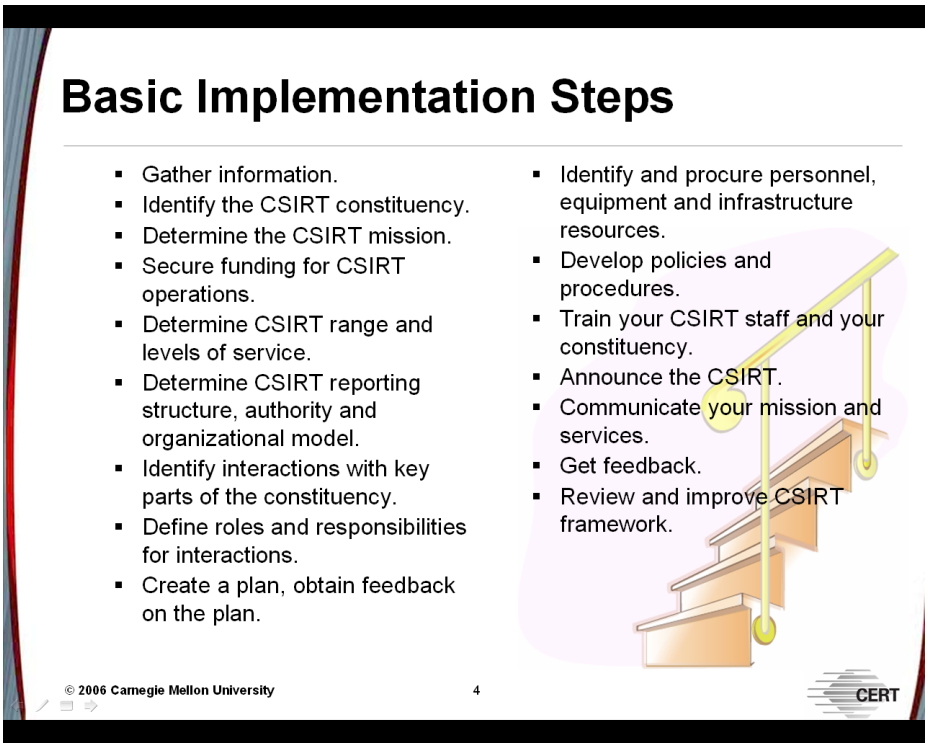
ENISA is het CSIRT-ontwikkelingsteam van het CERT-programma zeer erkentelijk voor de toestemming om inhoud van hun cursusmateriaal te mogen gebruiken!



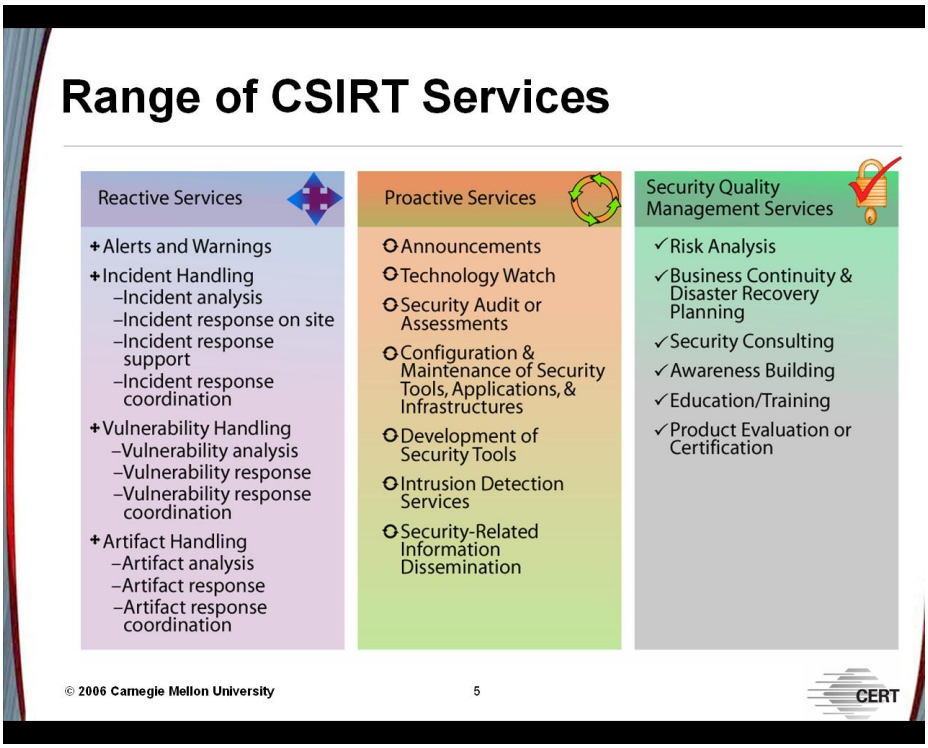
Uit de CERT/CC-trainingscursus: fasen van CSIRT-ontwikkeling



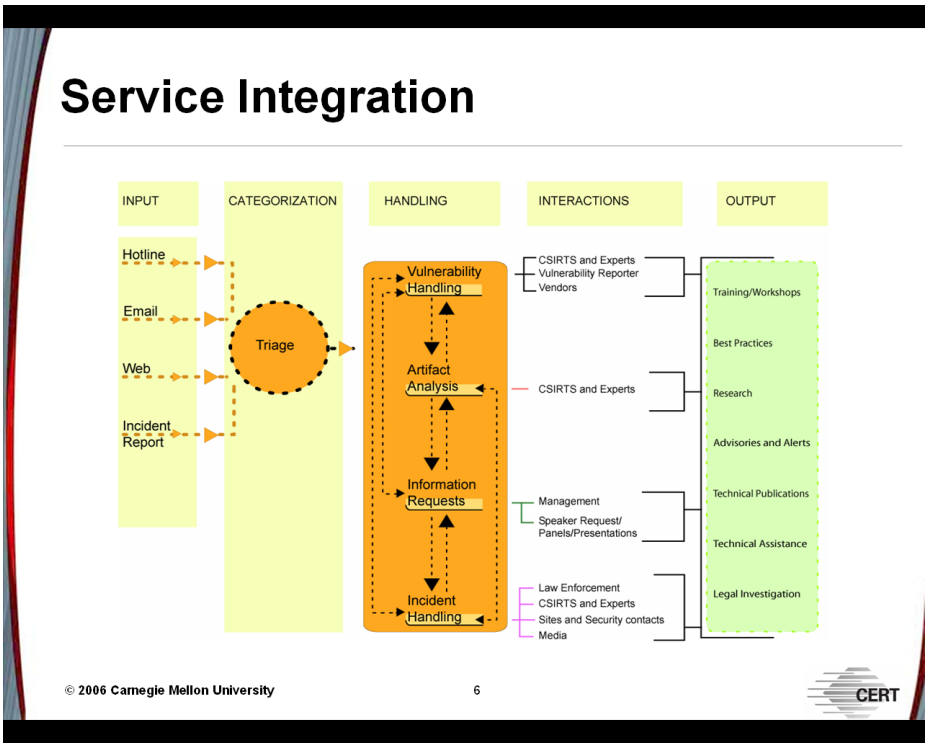
Uit de CERT/CC-trainingscursus: beste praktijken voor incidentenbeheer



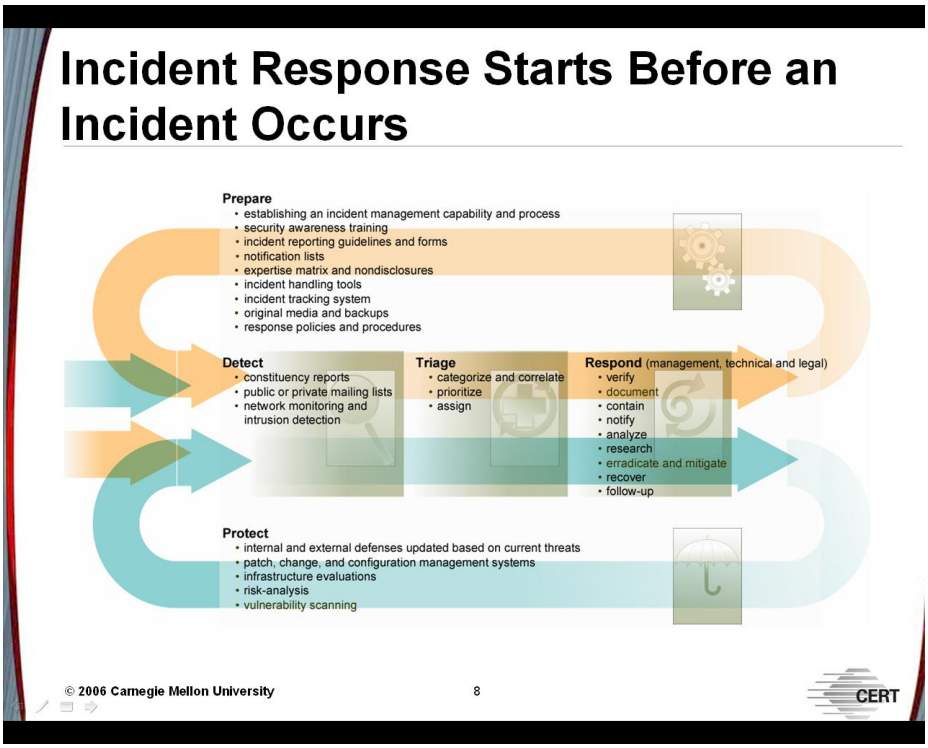
Uit de CERT/CC-trainingscursus: stappen bij het opzetten van een CSIRT



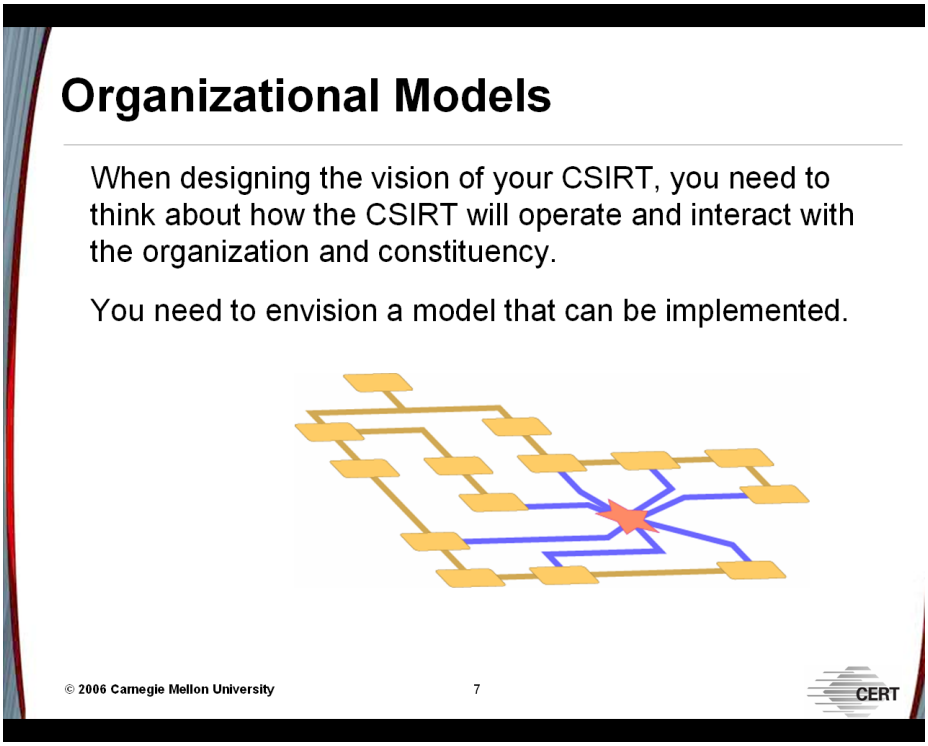
Uit de CERT/CC-trainingscursus: de diensten die een CSIRT kan verlenen



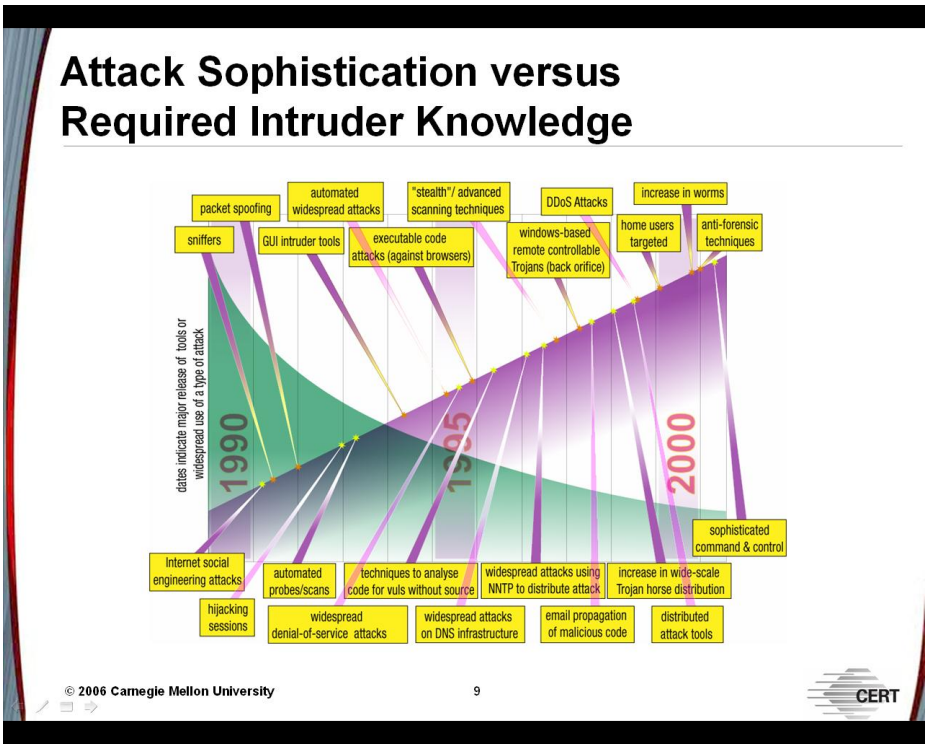
Uit de CERT/CC-trainingscursus: de werkstroom voor incidentenbeheer



Uit de CERT/CC-trainingscursus: reageren op incidenten



Uit de CERT/CC-trainingscursus: hoe wordt het CSIRT georganiseerd?



Uit de CERT/CC-trainingscursus: minder kennis, meer schade