GvIB Expertbrief – Januari 2006
ISSN 1872-4876, Jaargang 2 – Nr. 1

CERT in de organisatie

Ron Tolido

Patrick Borsoi

Henk Bronk

Ben Elsinga

Rob Greuter

Wim Hafkamp

Aart Jochem

Martijn van der Heide

Kelvin Rorive

Thom Schiltmans

Jacques Schuurman

Roeland Reijers

Deze expertbrief behandelt het sterk aan belangstelling winnende fenomeen van bedrijfsinterne Computer Emergency Response Teams (CERTs). Het aantal interne CERTs bij grotere, commerciële organisaties is de laatste jaren flink toegenomen. Dit is vooral een reactie op de pijnlijke beveiligingsincidenten die zich de afgelopen jaren op het Internet – haarscherp waargenomen door een miljoenenpubliek – hebben voltrokken. Rond een CERT binnen een organisatie kleven vraagstukken met betrekking tot de benodigde competenties, de te volgen procedures, de beschikbaarheid en de te gebruiken hulpmiddelen. Maar de grootste uitdaging lijkt te liggen in de relatie met de bestaande IT-organisatie, zowel in termen van taakverdeling als van verantwoordelijkheden en mandaat. De uiteindelijke vraag die moet worden beantwoord is die van de levenscyclus: zullen CERTs altijd nodig blijven of gaat een CERT uiteindelijk op in de staande IT-organisatie? Met andere woorden: maakt het ultieme CERT zichzelf overbodig?

http://www.gvib.nl/

expertbrief@gvib.nl

1. ACHTERGROND

In de afgelopen jaren is het aantal interne Computer Emergency Response Teams (CERTs) bij grotere, vaak commercieel opererende organisaties sterk toegenomen. Het eerste CERT dateert van 1988. Dit werd opgericht naar aanleiding van een zogenaamd *malicious code* incident. Het Morris 'worm-programma', genoemd naar zijn infame maker, zorgde er toentertijd voor dat 10 procent van alle wereldwijd op het Internet aangesloten computers werd uitgeschakeld. Zelfs met de op dat moment nog veel beperktere omvang van het Internet werden de gevolgen als schokkend ervaren. Het beveiligingsincident leidde in Amerika tot de oprichting van het CERT© Coordination Center (CERT/CC) door de Defense Advanced Research Projects Agency (DARPA).
Enkele jaren daarna, in 1991, werd tijdens een SURFnet klantenrelatiedag besloten tot de oprichting van het eerste officiële Nederlandse computer emergency response team, CERT-NL, een CERT voor klanten en gebruikers van SURFnet.

De term CERT is een gedeponeerd handelsmerk van het CERT/CC van de Carnegie Mellon University. Zie de website www.cert.org voor meer informatie als u overweegt de term 'CERT' te gebruiken voor commerciële of niet-commerciële doeleinden.

De opkomst van bedrijfsinterne CERTs kan rechtstreeks worden teruggevoerd naar het toenemende aantal aan het Internet gerelateerde beveiligingsincidenten van de afgelopen jaren en daarmee – potentieel – de steeds grotere kans op substantiële bedrijfsschade. De incidenten, voornamelijk *spam*, *malicious code* en *hacking*, vereisen een directe, gecoördineerde aanpak door uitstekend getrainde specialisten. Aangezien er een steeds grotere claim wordt gelegd op de staande IT-beheerorganisatie, besluiten veel organisaties om hier aparte teams voor in te richten: bedrijfsinterne CERTs zijn daarmee een feit. De teams bestaan vooral uit diep gespecialiseerde IT-experts, die zich richten op onderwerpen als *besturingssystemen*, *netwerkprotocollen* en *vulnerability management tools*.

Elke CERT werkt voor een zogenaamde *gebruikergemeenschap* ('constituency'). In de meeste gevallen gaat het om de business- en IT afdelingen van de eigen organisatie. Bij (IT) dienstverlenende organisaties behoren soms ook klantgroepen tot de gebruikersgemeenschap, maar dat beschouwen we in de context van deze expertbrief als een uitzonderingsgeval.

Het inrichten van een CERT is geen eenvoudige klus. Het vinden en behouden van deskundige, gemotiveerde medewerkers is een eerste uitdaging. Het CERT moet daarnaast voortdurend de toegevoegde waarde blijven bewijzen, vooral in relatie tot de noodzakelijke investeringen in mensen, apparatuur en accommodatie. Ook moet worden geopereerd in een lastig, in de loop van de tijd bovendien verschuivend spanningsveld met de IT beheerorganisatie(s) en de afnemers van IT-diensten.

2. ONDERZOEKSVRAGEN

De hoofdvraag die de expertbrief werkgroep zich oorspronkelijk stelt, is er een met een hoog prozaïsch gehalt
Hoe wordt een CERT binnen een organisatie effectief en efficiënt ingericht?

Om die vraag goed te kunnen beantwoorden, moeten op zijn minst de volgende onderwerpen aan bod komen:

1. Wat zijn de hoofd- en neventaken van de CERT?
2. Wat is de gewenste kwaliteit en omvang van de CERT bij een 7*24 uurs dienstverlening (aantal FTE's, opleidingsniveau, ervaring, consignatierooster, et cetera.)?
3. Welke procedures hanteert de CERT (Operational Framework)?
4. Welke hulpmiddelen gebruikt de CERT?
5. Hoe is de CERT organisatorisch opgehangen?
6. Welk mandaat/bevoegdheden heeft de CERT (en welke NIET)?
7. Welke relaties hebben de CERT-activiteiten met de ITIL beheerorganisatie (in het bijzonder met Incident Management, BCM, Change Management en Security Management)?

Tijdens de werksessie wordt het duidelijk dat de eerste vier vraagstukken relatief gemakkelijk kunnen worden geadresseerd: er zijn veel bruikbare bronnen beschikbaar en er is in toenemende mate sprake van standaardisatie. Opvallend daarbij is dat in de praktijk de inrichting en het functioneren van een CERT vaak wel degelijk als problematisch wordt ervaren: waarom gaat dit zo moeilijk, terwijl er in feite al zoveel bekend is?

De laatste drie vragen – die allen betrekking hebben op de relatie van het CERT met de staande organisatie – geven verder aanleiding tot een fundamentele discussie over de levenscyclus van een CERT. Het speciale karakter van een CERT (immers gericht op het reageren op onvoorspelbare gebeurtenissen en het omgaan met crises) zorgt ervoor dat het team in de vroege fasen van zijn bestaan een vaak aparte positie in de organisatie zal innemen. Naarmate het CERT echter beter verweven raakt met de bestaande structuren en processen, lijkt de *status aparte* steeds minder gewenst. Een frequente toetsing van het eigen functioneren en de positionering binnen de organisatie is daarom noodzaak. Dat leidt tot een interessante, existentiële vervolgvraag:

Wat is de levenscyclus van een bedrijfsintern CERT?

Als eenmaal het nut en de positie van een bedrijfsinterne CERT ter discussie wordt gesteld, kan het ook geen kwaad het vizier te richten op mogelijke (goedkopere) alternatieven. Zo raadt het *UK National Infrastructure Security Coordination Center* (NISCC) het implementeren van een *Warning, Advice and Reporting Point* (WARP) aan. Daarin worden met behulp van een speciaal ingerichte toolbox allerlei diensten en producten geleverd die verwant zijn aan die van een CERT. Ook blijken er organisaties te zijn die zich met alle effectiviteit hebben voorbereid op beveiligingsincidenten zonder dat daarvoor een apart CERT binnen de organisatie is opgericht.

4

3. TAKEN EN ROLLEN: GOEDE DEFINITIES BESCHIKBAAR

Een Computer Emergency Response Team (CERT) is een team dat reageert op IT-gerelateerde beveiligingsincidenten via het bieden van diensten waarmee incidenten worden opgelost of waarmee wordt bijgedragen aan de oplossing. Ook wordt gewerkt aan de preventie van beveiligingsincidenten binnen de bij het CERT behorende gebruikersgemeenschap, dit alles conform de toegekende verantwoordelijkheden.
De primaire focus van een CERT ligt dus op het adequaat reageren op beveiligingsincidenten die met IT te maken hebben en die mogelijk impact hebben op de gebruikergemeenschap ('consituency'). De secundaire focus op preventieve activiteiten – bijvoorbeeld het adviseren rond zwakke plekken in systemen en het gevaar van virussen - moet ervoor zorgen dat de potentiële risico's worden beperkt en dat het CERT zo weinig mogelijk daadwerkelijk in actie hoeft te komen.
De volgende, onderling vergelijkbare termen worden ook wel gebruikt om een CERT aan te duiden:

- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- IRC (Incident Response Capability)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)
- SIRT (Security Incident Response Team)

Soorten CERTs

Naast het type CERT waar deze expertbrief zich op richt – een bedrijfsintern CERT – kunnen er nog andere typen CERTs worden onderscheiden. Een greep:

- Small & Medium Enterprises CERT
  - Dit is een CERT dat meerdere kleine en middelgrote bedrijven tot zijn gebruikergemeenschap rekent, doorgaans omdat de betreffende bedrijven zélf te klein zijn om een eigen team in te richten.
- Academic CERT
  - Dit is een CERT dat zich richt op de gebruikersgemeenschap van universiteiten, hogescholen, laboratoria en onderzoeksinstituten. Het verschijnsel CERT is lange tijd vooral geassocieerd met de academische wereld, niet in het minst omdat het Internet in die context is groot geworden.
- Military CERT
  - Een CERT dat zich richt op de gebruikersgemeenschap binnen defensie, inclusief gelieerde administratieve instituten.
- Commercial CERT
  - Commerciële CERTs bieden hun gespecialiseerde diensten aan aan elk bedrijf dat om wat voor reden dan ook niet zelf een CERT wil of kan inrichten.

Standaards voor inrichting en besturing

In de loop van de jaren is veel ervaring opgedaan met het inrichten en besturen van CERTs. Er zijn uitputtende, zeer volledige standaards gepubliceerd die zich richten op het takenpakket, de rollen, de organisatorische invulling en de te gebruiken tools.

GOVCERT.NL, het CERT voor de Nederlandse overheid heeft zelfs een ‘CERT-in-a-box’ gepubliceerd: een CD met daarop alle informatie, checklists en tools die nodig zijn om een CERT in te richten.

Cruciaal voor elke organisatie die zich verdiept in het verschijnsel CERT is Request For Comments (RFC) 2350 van de Internet Engineering Task Force (IETF). De IETF is een groot, internationaal opererend network van belanghebbenden rond de architectuur van het Internet en het soepel opereren daarvan. RFC 2350 is al in 1998 uitgebracht en zou als basis moeten functioneren voor het inrichten van elk CERT: het geeft richtlijnen voor het beschrijven van diensten, gebruikersgemeenschappen, werkwijzen, verwachtingspatronen, et cetera. RFC 2350 wordt zodanig erkend, dat er zelfs accreditatiemodellen zijn op basis van dit document: organisaties kunnen met RFC 2350 in de hand hun CERT formeel laten certificeren.

Het is met dit alles duidelijk dat organisaties die een eigen, bedrijfsintern CERT willen opzetten, daarmee het beste de RFC 2350 template kunnen volgen. Deze bestaat globaal uit de volgende onderdelen:

- Contactinformatie
  - Namen, adressen, telefoonnummers, e-mail, et cetera.
- Charter
  - Beschrijft de missie van het CERT, de gebruikersgemeenschap, de manier waarop het sponsorschap van het team belegd is en het toegekende mandaat
- Policies
  - Bevat een beschrijving van het soort incidenten waarop gereageerd zal worden, het niveau van ondersteuning dat zal worden geboden en de beleidslijnen die zullen worden gevolgd bij het communiceren, samenwerken en het voeren van interactie binnen en buiten de organisatie.
- Services
  - Beschrijft in meer detail welke dienstverlening zal worden geboden rond het reageren op beveiligincidenten, zowel in termen van het opvangen en analyseren van incidenten, het coördineren van uit te voeren taken en het feitelijk oplossen van incidenten. Ook wordt hier aandacht besteed aan het beschrijven van preventieve dienstverlening.
- Formulieren
  - Een overzicht van de elektronische en handmatige manieren waarop incidenten kunnen worden gemeld en vastgelegd.

4. SUCCES EN FALEN BIJ INRICHTING

Er is al met al veel bekend over het inrichten en besturen van een CERT. En dat mag ook wel, nu het fenomeen al zo'n 18 jaar bekend is. Toch blijkt het in de praktijk moeilijk om een CERT effectief en succesvol te laten opereren. Diezelfde praktijk levert dan wel een aantal *best practices* op waarvan een ieder kan profiteren:

Luister naar de doelgroep: het CERT USP

Ook al opereren CERTs vanuit hun specifieke expertisegebied vaak in een isolement, het is zaak om te allen tijde binding te houden met de gebruikersgemeenschap waar het uiteindelijk allemaal om was begonnen. Een te mechanistische checklistbenadering kan er nou net voor zorgen dat de finesses in de behoeften van de constiguency worden gemist. En dat kan weer het verschil bepalen tussen succes en falen, vooral als het gaat om de perceptie van succes vanuit de gebruikersgemeenschap.

Het gaat dus om goed luisteren naar de wensen en noden van die gebruikersgemeenschap. Daarbij moet gerealiseerd worden dat de behoeften per organisatie sterk kunnen variëren. Een CERT binnen een universiteit heeft bijvoorbeeld te maken met een doelgroep die bij uitstek eigen uitdagingen met zich meebrengt. De gebruikersgemeenschap bestaat uit slimme, 'avant-gardistische' jongens (en een enkel meisje) die vaak uitstekend op de hoogte zijn van de nieuwste ontwikkelingen en mogelijkheden. Het is niet verwonderlijk dat in zo'n context een relatief nieuw fenomeen als 'phishing' al jaren genoegzaam bekend is.

Eigenlijk zou elk CERT voor de eigen organisatie een *Unique Selling Point* (USP) moeten vaststellen: een 'bestaansreden' die zó goed past bij de missie en karakteristieken van de organisatie dat deze onmiddellijk herkend wordt door alle geledingen heen. Zo'n USP helpt bij de adoptie en erkenning door de eigen organisatie maar geeft ook het CERT de rode draad die nodig is bij de inrichting en uitvoering. Een CERT dat het niet goed lukt om een USP op te stellen, zou zich nog eens achter de oren moeten krabben over het nut van het team en de mate waarin de eigen organisatie wordt begrepen. Zeker in een tijd waarin het bijna hip (ja, zelfs 'cool') lijkt om een CERT op te richten – of er onderdeel van uit te maken – is het nodig om de existentiële vraag gelijk aan het begin te stellen.

Het beste is om de missie van het CERT op te laten stellen door vertegenwoordigers van de business zelf. Dit geeft de meeste garantie dat de doelstellingen ook werkelijk worden onderschreven en herkend. Een gezamenlijke actie om een missie op te stellen geeft niet alleen richting, maar helpt ook om de allerhoogste prioriteiten vast te stellen: het CERT krijgt zo een helder beeld van de maatregelen die het eerst moeten worden genomen.

Wees flexibel

Om goed te kunnen functioneren, moet een CERT grote nadruk leggen op het definiëren en naleven van procedures. Echter, omdat het werkgebied per definitie onverwachte, slecht voorspelbare crises omvat, is flexibiliteit een nog groter goed: met vaste procedures kan op zijn allerbest 70% van de optredende incidenten worden bestreken. Inflexibiliteit en het verschijnsel CERT zouden elkaar daarom moeten uitsluiten.

Flexibiliteit betekent ook dat het CERT voortdurend bereid moet zijn buiten de eigen bedrijfsmuren te opereren: daar ontstaan immers de potentiële crises, maar evenzeer bevindt

zich daar de kennis en de ervaring die nodig is om problemen het hoofd te bieden. Eén van de redenen waarom CERTs – zelfs na 18 jaar – niet altijd slagen of goed functioneren is het onvermogen om werkelijk kennis te delen, zowel binnen een organisatie maar vooral ook tússen organisaties.

Een grote uitdaging kan liggen in de kloof tussen de adaptiviteit van een CERT en het veel meer rigide karakter van de beheerorganisatie. Botsingen liggen voor de hand.

Vind de juiste plaats in de organisatie

Zoals de organisatieleer ons vertelt, is er niet één ideale manier om een organisatie in te richten. En als die er al zou zijn, is hij zeker binnen korte tijd alweer verouderd. De randvoorwaarden blijven immers voortdurend verschuiven en 'behaalde successen in het verleden bieden geen garantie voor de toekomst'. Daarom zijn er verschillende *best practices* rond de plaats van een CERT in de organisatie, onder andere beïnvloed door de omvang van de organisatie, de volwassenheid en ervaring van de lokale IT-afdelingen, de mate van inbedding in de bedrijfsvoering, het sóórt bedrijfsvoering en de mogelijkheden om de impact van een verstoring al dan niet lokaal te kunnen vaststellen.

Met name als de organisatie groot en gedistribueerd is, zal één centraal CERT niet afdoende blijken te zijn. Omdat de relatie met de gebruikersgemeenschap allesbepalend is, is het zaak om zo dicht mogelijk bij de werkvloer te opereren: daar immers zal de impact van mogelijk crises werkelijk worden gevoeld. Het is nodig om aan de ene kant snel en praktisch te kunnen opereren en daarnaast het vermogen te hebben om – waar nodig – werkelijk invloed te kunnen uitoefenen op de bedrijfsvoering.

Er zijn succesvolle CERTs bekend waarin elke business unit een eigen 'CERT light' heeft, gecoördineerd door een overkoepelende CERT. Dit laatste aspect is alleen al vanuit de noodzaak van kennisdeling cruciaal.

Verder zijn er diverse grotere organisaties die één centraal CERT hebben en daarnaast binnen de diverse IT-afdelingen (niet te verwarren met business units) kleinere 'CERTs light'. In dat geval moet goed worden bekeken in welke mate er sowieso al binnen de IT-afdelingen sprake is van lokaal incidentmanagement. Dit raakt opnieuw aan het interessante onderwerp van de relatie tussen het CERT en de IT-organisatie.

Een andere optie die wordt genoemd is die van een echte netwerkorganisatie. Daarin opereren verschillende, relatief zelfstandige CERTs (vaak dichtbij of in de business units) en worden de onderlinge lijnen in een losser matrixverband onderhouden.

Soms lijkt het slim om een 'virtueel team' te creëren. Er is dan niet sprake van een feitelijke organisatorische eenheid, maar deze is opgebouwd uit vertegenwoordigers van andere eenheden. Deze optie lijkt vooral voor de hand te liggen als er belemmeringen of vraagstukken zijn rond het veranderen van de organisatie. Ook kan het een bruikbare strategie zijn om tot een betere borging in de bedrijfsvoering te komen.

In een tijdperk waarin steeds meer (IT)activiteiten worden uitbesteed, wekt het geen verwondering dat er ondertussen ook organisaties zijn die een deel van de taken van een CERT uitbesteden aan een externe leverancier. Vaak zal de externe, gespecialiseerde leverancier dan 'alerts' afgeven op bij dreigende of daadwerkelijke optredende

beveiligingsincidenten. Het is vervolgens de taak voor een klein, intern team om zorg te dragen voor interne communicatie en het coördineren van de activiteiten van de IT-afdelingen. Niet zelden zullen ook die IT-afdelingen weer uitbesteed blijken te zijn. Het *managen* van alle betrokken partijen – waar dan ook – wordt zo een kunst op zich en de vraagstukken rond mandaat worden nog meer gevoeld dan normaal.

Hoewel RFC 2350 in een grote mate van detail de taken en relaties van een CERT beschrijft, doet deze geen expliciete uitspraken over de organisatorische inbedding. De werkgroep constateert dat dit op zich aanleiding zou kunnen geven tot het ontwikkelen van *organisatorische 'patterns'* die – gekoppeld aan een beschrijving van typerende omgevingsfactoren – een basis zouden kunnen vormen voor besluitvorming rond organisatorische inrichting. Dit onderwerp is weliswaar te gespecialiseerd om in deze expertbrief dieper te adresseren, maar zal mogelijk in een vervolgsessie kunnen worden geadresseerd. En anders zou er een fraai afstudeeronderwerp in de academische wereld aan gewijd kunnen worden.

Kweek vertrouwen

Vertrouwen is een noodzakelijke basis voor elk CERT om bestendig te kunnen opereren. Daartoe moet tot op het hoogste niveau van de organisatie mandaat worden verkregen, niet door dat zomaar te claimen, maar door in de praktijk vertrouwen te winnen.

Het moet voor alle betrokkenen – binnen en buiten het CERT – volstrekt helder zijn wanneer het CERT in actie komt en wat dan vervolgens de speelruimte is. De metafoor van het trekken aan de noodrem is dan nog niet zo gek, evenals die van het bellen van de brandweer: je doet het álleen als er écht gegronde redenen zijn. En vergissingen zijn duur; als het CERT eenmaal een keer ten onrechte in actie is gekomen (en bedrijfsbreed zijn bijvoorbeeld alle computersystemen voor de zekerheid een paar uur stilgelegd), dan zal het bij een volgende keer veel moeilijker worden om de organisatie te overtuigen dat actie noodzakelijk is. 'Misbruik' wordt in dit geval letterlijk gestraft en het is daarom nodig om het hoofd koel te houden in een omgeving waarin soms té hysterisch zou kunnen worden gereageerd op mogelijke verstoringen.

De uiteindelijke beslissing over 'wel of niet de stekker eruit' is en blijft overigens een business-overweging. Als de systemen van ProRail worden stilgelegd, zouden er wel eens 100.000 man op de stations kunnen stranden. In zo'n situatie is het volstrekt cruciaal om over de juiste informatie te beschikken, maar nog belangrijker is dat er vertrouwen is tussen de betrokkenen, door alle geledingen van de organisatie heen. Alleen als het CERT weet te opereren in een zelf gekoesterd *Trust Ecosystem* is er sprake van werkelijk mandaat.

Het 'stekkermandaat' zal vanuit praktische overwegingen uiteindelijk toch vaak komen te liggen in de operationele beheerorganisatie. Bij ernstige, werkelijk acute bedreigingen zou er immers te weinig tijd kunnen zijn om eerst eens bedachtzaam op managementniveau te overleggen. *Eerst schieten, dan vragen stellen*, wordt dan de onvermijdelijke gedragslijn.

Overigens helpt moderne technologie wel degelijk om de impact van een mogelijke verstoring beter in te kunnen schatten, zeker als we dat vergelijken met de situatie van 18 jaar terug. Verregaande standaardisatie en *business intelligence tools* (zoals bijvoorbeeld HP's Open View en IBM's Tivoli) stellen een CERT in staat om de consequenties van problemen in de infrastructuur rechtstreeks te herleiden naar de gevolgen voor de bedrijfsvoering, tot op

het niveau van specifieke processen, business units en zelfs klantenrelaties. Binnen zulke moderne beheeromgevingen kunnen met zogenaamde “business process views” instantaan de consequenties van een (potentieel) incident op het niveau van de bedrijfsprocessen inzichtelijk worden gemaakt. Zo is er een Europees telecombedrijf dat door middel van een “cashflow assurance” systeem de gevolgen van een incident voor de basale bedrijfsvoering van het bedrijf heeft gekwantificeerd.

Maar zelfs in zulke gevallen kan de meest gedetailleerde *pie-chart* niet op tegen gegrond, wederzijds vertrouwen. Het gaat immers over mensen en – zoals in de werkgroep vol overtuiging wordt vastgesteld – ‘soms is bier het beste smeermiddel’.

5. DE RELATIE TOT DE IT-ORGANISATIE

De relatie tussen de IT-afdeling(en) en het CERT is er een die verwant is aan het bredere onderwerp van organisatorische inbedding. Een goede relatie met de IT-organisatie is vanuit het CERT cruciaal voor succes, evenals de relatie met de bedrijfsvoering. Vraagstukken die daarbij spelen hebben onder andere betrekking op mandaat, flexibiliteit, kennisdeling en de volwassenheid van processen. Ook hier geldt dat een organisatorische ophanging per definitie situationeel bepaald is en bovendien in de loop van de tijd zijn geldigheid en effectiviteit kan verliezen.

In veel gevallen is het CERT eenvoudigweg onderdeel van de IT-organisatie, alleen al om ervoor te zorgen dat de nodige acties ook werkelijk onmiddellijk worden genomen (‘stel je anders voor dat het CERT zegt “gij zult niet patchen” en de op ITIL gebaseerde IT-afdeling doet het gewoon toch’).
Maar vaak wordt toch ook juist expliciet gekozen om de twee werelden gescheiden te houden. Dit heeft onder andere te maken met het verschil in dynamiek: een CERT moet snel en ‘oningehouden’ kunnen reageren waar een IT-afdeling – mogelijk gestandaardiseerd op ITIL – vooral een focus lijkt te leggen op voorspelbaarheid en herhaalbaarheid. Het snel kunnen reageren op onverwachte incidenten is een duidelijke specialisatie die zich bovendien mogelijk uitstrekt over meerdere platformen, organisatie-eenheden en belanghebbenden heen. Een CERT zal bovendien meestal veel meer operationeel bezig zijn met het oplossen van plotseling optredende crises, waar de IT-afdeling zich typisch meer zal richten op het duurzaam inrichten van zaken als *securitymanagement, incidentmanagement* en *changemanagement*.

Toch is er – uit de aard der zaak – veel overlap tussen beide werkgebieden. En de één kan de ander beïnvloeden. Vooral als de kwestie van *mandaat* ter sprake komt (‘als die stekker er uit moet, dan zál hij er ook uit gaan’), kan dit aanleiding zijn tot het beter definiëren van processen en interfaces: met de oprichting van een CERT kan daarmee van de weeromstuit de volwassenheid van de IT-afdeling een flinke duw voorwaarts krijgen. Ook de discussie rond wat ‘incidenteel’ is en wat duurzaam zou moeten zijn ingericht, kan ertoe leiden dat binnen de IT-afdeling verbeterslagen worden doorgevoerd; zaken die noodgedwongen in eerste instantie door het CERT worden opgepakt vloeien dan vanzelf over in de richting van de staande IT-organisatie.

Dat inzicht leidt tot een belangrijke conclusie: een goed functionerend CERT gedijt pas goed in combinatie met een wérkelijk volwassen IT-afdeling. En veel IT-afdelingen zijn nog niet volwassen genoeg. Dit wordt vaak pas manifest bij het inrichten van het CERT. Een verbeterproces zou het logische vervolg moeten zijn, waarbij de positie en het functioneren van het CERT in de loop van dat traject zouden moeten veranderen in de richting van zijn oorspronkelijke missie: het hoofd bieden aan onverwachte beveiligingscrises.

Afhankelijk van het stadium van volwassenheid en andere omgevingsfactoren kan een ‘Incident Response’ organisatie dan alsnog allerlei verschillende vormen aannemen.
Het *UK National Infrastructure Security Coordination Center* (NISCC) raadt bijvoorbeeld het implementeren van een *Warning, Advice and Reporting Point* (WARP) aan. Daarin worden met behulp van een speciaal ingerichte toolbox allerlei diensten en producten geleverd die verwant zijn aan die van een CERT. Het center heeft dan echter veel meer een coördinerende, kennisdelende rol in plaats van de operationele gerichtheid die je bij een CERT verwacht. Het operationele aspect wordt dan geacht op een

volwassen niveau in de IT-organisatie te zijn ingebed. In een zelfde context functioneren de zogenaamde ‘ISA’ centers, die voornamelijk op het verzamelen en delen van kennis zijn gericht: in de praktijk immers een van dé succesfactoren rond het tijdig kunnen reageren op nieuwe verstoringen.

Ook blijken er al genoeg organisaties te zijn – ook in Nederland - die zich met alle effectiviteit hebben voorbereid op beveiligingsincidenten zonder dat daarvoor een apart CERT binnen de organisatie is opgericht. Er is dan blijkbaar een volwassenheidsniveau binnen de eigen IT-afdeling bereikt waarin standaardisatie en herhaalbaarheid zich goed verdragen met de flexibiliteit die nodig is om plotseling optredende beveiligingscrises het hoofd te bieden.

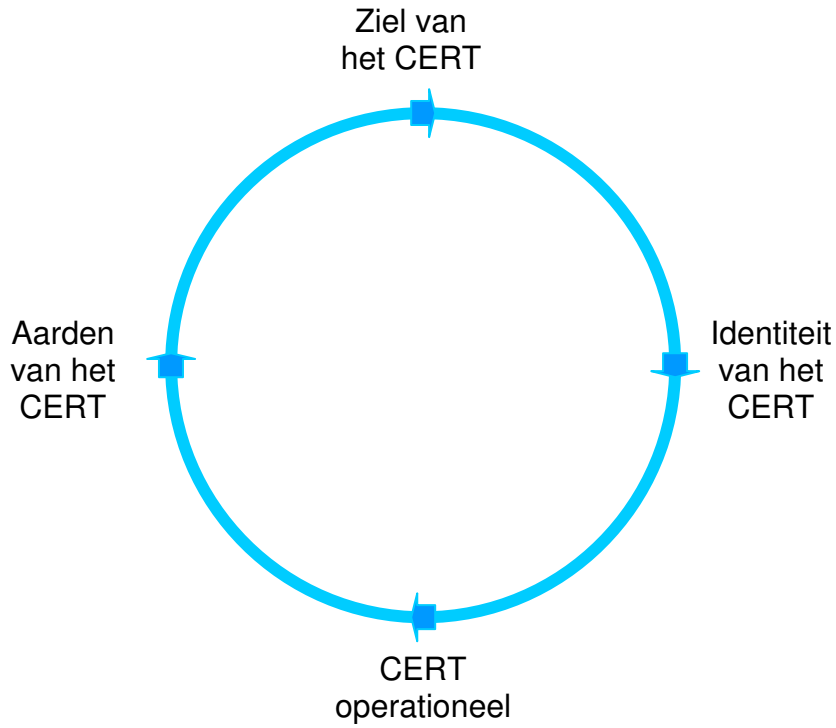
In alle gevallen geldt dat de lokale situatie ook nog eens uiteindelijk bepaalt wat de zwaarte moet zijn van de te nemen maatregelen: er worden immers niet altijd dezelfde eisen gesteld aan tijdigheid, snelheid en effectiviteit.

6. LEVENSCYCLUS VAN EEN CERT

Een CERT beweegt in een raderwerk of zelfs ‘ecosysteem’ van interne en externe omstandigheden. Dit raderwerk komt nooit tot stilstand en zoals al eerder werd gesteld, er is geen ideale toestand waarin niets meer hoeft te veranderen.

Wel zou je kunnen stellen dat elk CERT een levenscyclus doorloopt, die bovendien zichzelf kalibreert: als de hele cyclus is doorlopen kan dat aanleiding geven tot een verandering in de missie waardoor de gehele of gedeeltelijke cyclus opnieuw zal moeten worden doorlopen. Het aantal iteraties van zo’n cyclus is daarmee in potentie onbeperkt, want het ecosysteem blijft immers altijd in beweging.

De levenscyclus bestaat uit 4 duidelijke stappen:



Stap 1: **Het vaststellen waarom de organisatie een CERT nodig heeft**. Dit is het creëren van de ‘ziel’ van het CERT. Zonder een ziel geen succes, daarom is deze stap allesbepalend voor het uiteindelijke slagen van het CERT. Er dient vooral goed gekeken te worden naar de missie en de omgeving van de organisatie en de relatie van mogelijke verstoringen met de bedrijfsvoering. Doorgaans zal de ‘ziel’ pas echt worden herkend door de organisatie als diezelfde organisatie vanaf het begin betrokken is geweest bij het opstellen van de missie en doelen van het CERT. Een business case voor het CERT helpt om de benodigde investeringen en inspanningen in het juiste perspectief te plaatsen.

Stap 2: **Het invullen van het identiteitsdocument van het CERT**. Dit kan het beste gebeuren op basis van het zeer volledige RFC 2350. Het identiteitsdocument fungeert als een ‘geboorteakte’ of charter naar de staande organisatie. CERTs hoeven hier gelukkig niet zelf het wiel uit te vinden en in een tijd van ‘CERT-in-a-box’, voorgedefinieerde templates en de

eerste tekenen van ‘patterns’ hoeft deze stap minder tijd te kosten dan misschien wordt gedacht.

Stap 3: **Het werkelijk uitvoeren van de noodzakelijke activiteiten**. Hier is het CERT volledig operationeel, in een mix van pro-actieve en reactieve activiteiten.

Stap 4: **Het aarden van het CERT in de organisatie.** Dit is een adaptief proces waarin het creëren en inregelen van standaards, richtlijnen en processen hand in hand gaat met het kweken van het cruciale wederzijdse vertrouwen. In feite is dit een transformatie, waarin alle betrokken partijen in meerdere of mindere mate leren en veranderen.

Zoals gezegd, na het doorlopen van deze cyclus zou frequent getoetst moeten worden of de omgevingsfactoren nog steeds hetzelfde zijn. Zowel binnen als buiten de organisatie vinden veranderingen plaats en we constateerden al eerder dat het inrichten en daadwerkelijk operationaliseren van een CERT bovendien rechtstreeks effecten kan hebben op de volwassenheid van de IT-afdelingen. De ‘ziel’ van het CERT zou daarmee in de loop van de tijd zomaar eens kunnen veranderen, evenals de manier waarop het team in de organisatie zou moeten zijn verankerd. Dit kan aanleiding geven tot een veranderd identiteitsdocument, op basis waarvan de resterende stappen in de levenscyclus opnieuw moeten worden doorlopen.

Het is duidelijk dat de werkgroep niet voor niets spreekt van een levenscyclus, waarin de benodigde stappen in de juiste volgorde moeten worden gezet. Een CERT dat zich plompverloren stort in de activiteiten van stap3, mist elke basis voor succes. Toch gebeurt dit vaak, niet in het minst gedreven door trends en de waan van dag, en het verklaart voor een belangrijk waarom zelfs na 18 jaar het oprichten en in stand houden van een CERT niet vanzelfsprekend lukt. Evenzeer zou uit het voorgaande helder moeten worden dat een goed functionerend CERT dat niet per definitie blíjft doen: dat zal alleen het geval zijn als de rest van de wereld onveranderd blijft. En die kans is klein, naar het schijnt.

7. HET ULTIEME CERT: OVERBODIG?

Als we eenmaal op een dergelijk hoog niveau van zelfbespiegeling zijn aangeland, resteert de ultieme vraag: bestaat er een *stap 5* waarin het CERT zichzelf overbodig heeft gemaakt en er dus tot opheffing kan worden overgegaan? En áls dat werkelijk het geval zal blijken te zijn, zal het fanatieke, overtuigde CERT-lid zich zonder (onbewust) verzet aan deze realiteit overgeven?

Eén ding is zeker: in het geval van een werkelijk volwassen IT-organisatie, waarin standaardisatie en herhaalbaarheid gekoppeld zijn aan flexibiliteit en adaptiviteit, zal een CERT minder te doen hebben dan misschien oorspronkelijk wordt gedacht. De werkgroep is van mening dat een zeer drukbezet CERT met een overvolle plank aan nog uit te voeren activiteiten over het algemeen een indicatie is van een slecht functionerende, of in ieder geval onvolwassen, IT-organisatie (dit wordt overigens gestaafd door managementtheorie: een écht effectieve manager zal over het algemeen een zee van ruimte in zijn agenda hebben).

Een CERT zou zich daarom per direct kunnen opheffen als álle noodzakelijke maatregelen met succes kunnen worden genomen door de staande organisatie. Ook is het mogelijk dat alle cruciale processen bij een externe dienstverlener zijn belegd (via outsourcing) waardoor er eenvoudigweg geen noodzaak meer is voor een bedrijfsintern CERT. Door veranderende externe of interne omstandigheden kan de scope ook zó klein zijn geworden dat de business case van een apart CERT niet meer aanwezig is.

8. TOT SLOT

De werkgroep stelt vast dat er nog genoeg interessante onderwerpen zijn om een toekomstige expertbrief aan te wijden. '*Patterns*' voor organisatorische inbedding, bijvoorbeeld. Maar ook het gebruik van geavanceerde *business intelligence* om de impact van verstoringen beter in beeld te krijgen. Voorts ontstaat de vraag of er in de vele jaren van het bestaan van CERT standaards als RFC 2350 ondertussen niet zoveel is veranderd in de omgeving (denk aan sterk toenemende wet- en regelgeving, open source, transparantie, de schaalgrootte van het Internet) dat een herijking van de standaards gerechtvaardig zou zijn.

Hoe dan ook, we hebben geconstateerd dat door het voortdurend blijven doorlopen van de CERT levenscyclus, inclusief het hertoetsen van missie en ziel, het vanzelf duidelijk zal worden wanneer een CERT overbodig is of – beter nog – zichzelf overbodig heeft gemaakt. Dat dit voor de betrokkenen in het CERT een pijnlijke, finale stap zou kunnen zijn is niets meer dan menselijk. Aan de andere kant: een eenvoudige boeddhistische wijsheid leert ons dat pijn veroorzaakt wordt door het vastklampen aan de illusie van stabiliteit in een wereld waarin nu juist alles, altijd zal veranderen. En dat lijken de juiste, bespiegelende woorden ter afsluiting van deze expertbrief.

U kunt uw reactie op dit artikel sturen naar expertbrief@gvib.nl

Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

16

LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief over CERT in de organisatie heeft de werkgroep de volgende literatuur geraadpleegd:

[1] Patrick Borsoi, *CERT-functionaliteit bij een grote overheidsorganisatie*, juli 2005

[2] Chris Alberts e.a., *Defining Incident Management Processes for CSIRTS: a work in progress,* oktober 2000

[3] Moira West-Brown, *Avoiding the Trial-by-Fire Approach to Security Incidents*, Crosstalk oktober 2000

[4] Stanford White Paper, *International Coordination for Cyber Crime and Terrorism in the 21st Century Version 6*

[5] Bart Bokhorst en Jan Schapink, *PI-Studie Basisnormen Beveiliging en Beheer ICT-infrastructuur*, EDP Auditor 2003-4

[6] *Coatings team Incident Response Conclusions*, AKZO Nobel presentatie 17 september 2003

[7] *ISF SoGP - Incident Management,* Parts taken from the ISF Standard of Good Practice

[8] *CERT-in-a-box*, uitgave van GOVCERT.NL

[9] Kevin Rorive, *ITIL is een zegen voor Patch Management*, Informatiebeveiliging Jaarboek 2004/2005

[10] Moira J. West-Brown, *Handbook for Computer Security Incident ResponseTeams (CSIRTs),* CMU/SEI April 2003

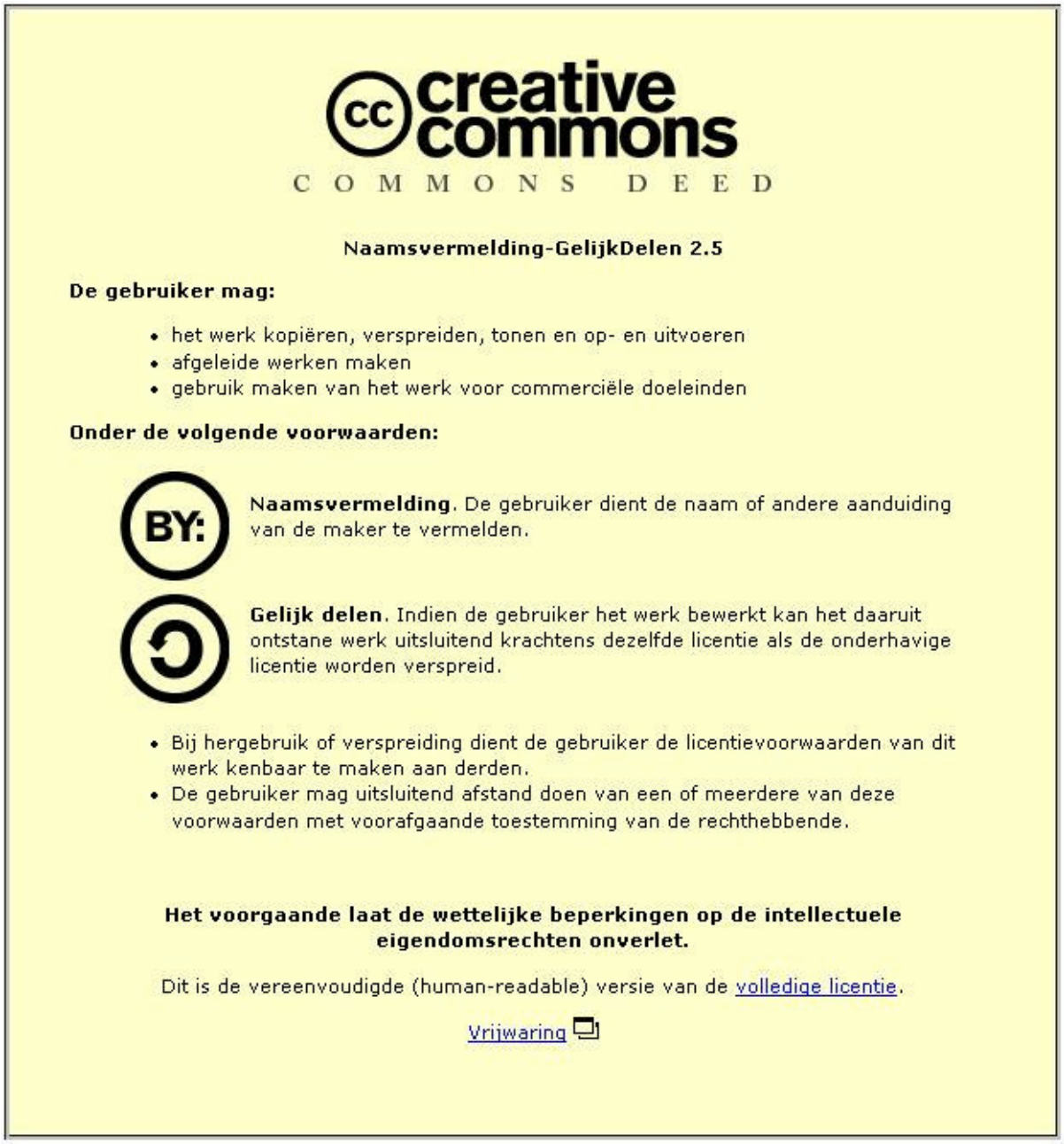
[11] Linda Kelver, *Incident Response in A Global Environment*, GSEC Version 1.2b, SANS Institute 2000-2002

[12] N. Brownlee, E. Guttman, *Request for Comments (RFC) 2350*

Met dank aan *Ton van Gessel* voor zijn waardevolle inbreng tijdens de voorbereiding van de expertbrief sessie.

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/



creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

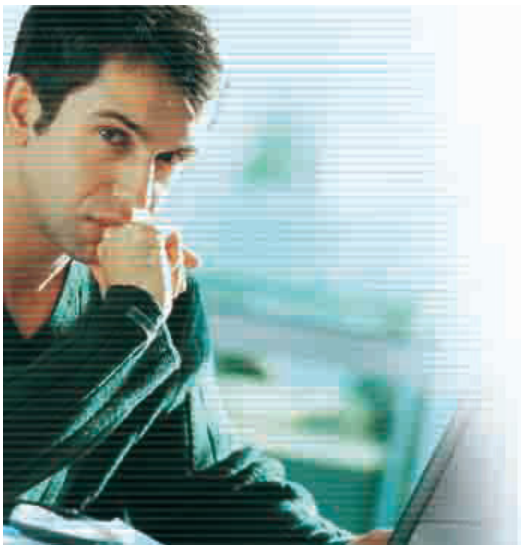
Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

18

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is al jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm