



ABORDAGEM GRADUAL DE CRIAÇÃO DE UMA CSIRT

Versão WP2006/5.1 (CERT-D1/D2)

Índice

1	Síntese.....	2
2	Advertência	2
3	Agradecimentos	2
4	Introdução	3
4.1	PÚBLICO-ALVO.....	5
4.2	COMO UTILIZAR O PRESENTE DOCUMENTO.....	5
4.3	CONVENÇÕES UTILIZADAS NO PRESENTE DOCUMENTO	6
5	Estratégia global para planear e criar uma CSIRT	7
5.1	O QUE É UMA CSIRT?	7
5.2	EVENTUAIS SERVIÇOS QUE UMA CSIRT PODE PRESTAR	12
5.3	ANÁLISE DA COMUNIDADE UTILIZADORA E DEFINIÇÃO DA MISSÃO	15
6	Desenvolvimento do Plano de Actividades	22
6.1	DEFINIÇÃO DO MODELO FINANCEIRO	22
6.2	DEFINIÇÃO DA ESTRUTURA ORGANIZATIVA	24
6.3	CONTRATAÇÃO DO PESSOAL ADEQUADO	29
6.4	UTILIZAÇÃO E EQUIPAMENTO DAS INSTALAÇÕES	32
6.5	FORMULAÇÃO DE UMA POLÍTICA DE SEGURANÇA INFORMÁTICA	35
6.6	BUSCA DA COOPERAÇÃO ENTRE OUTRAS CSIRT E POSSÍVEIS INICIATIVAS NACIONAIS	36
7	Promoção do Plano de Actividades	39
7.1	DESCRIÇÃO DOS PLANOS DE ACTIVIDADES E DOS FACTORES DE MOTIVAÇÃO DA ADMINISTRAÇÃO	42
8	Exemplos de procedimentos operacionais e técnicos (fluxos de trabalho).....	46
8.1	AVALIAR AS INSTALAÇÕES EXISTENTES NA COMUNIDADE UTILIZADORA	47
8.2	PRODUZIR ALERTAS, AVISOS E COMUNICAÇÕES	48
8.3	PROCEDIMENTO DE GESTÃO DE INCIDENTES.....	57
8.4	EXEMPLO DE UMA ESCALA HORÁRIA DE RESPOSTA.....	64
8.5	FERRAMENTAS CSIRT DISPONÍVEIS	65
9	Formação CSIRT	67
9.1	TRANSITS.....	67
9.2	CERT/CC.....	68
10	Exercício: produção de um aviso.....	70
11	Conclusão	76
12	Descrição do plano de projecto.....	77
ANEXO.....		82
A.1	OUTRAS LEITURAS.....	82
A.2	SERVIÇOS CSIRT	83
A.3	EXEMPLOS	96
A.4	MATERIAL DOS CURSOS PARA CSIRT.....	100

1 Síntese

O presente documento descreve o processo de criação de uma Equipa de Resposta a Incidentes de Segurança Informática (Computer Security and Incident Response Team - (CSIRT)) de todas as perspectivas pertinentes, como as de gestão empresarial, processual e técnica. Com ele se concretizam dois dos produtos mencionados no capítulo 5.1 do Programa de Trabalho 2006 da ENISA:

- Presente documento: *Relatório escrito sobre uma abordagem gradual de criação de uma CERT ou recursos similares, incluindo exemplos. (CERT-D1)*
- Capítulo 12 e ficheiros externos: *Excerto de um roteiro discriminado por pontos para possibilitar a sua fácil aplicação na prática. (CERT-D2)*

2 Advertência

Advertimos que a presente publicação corresponde aos pontos de vista e interpretações dos seus autores e editores, salvo indicação em contrário. Não deverá considerar-se que se trata de uma acção da ENISA nem dos seus órgãos, a menos que seja aprovada nos termos do Regulamento ENISA (CE) N.º 460/2004. A presente publicação não apresenta, necessariamente, a informação mais actual, podendo ser actualizada de vez em quando.

As fontes de terceiros são citadas na medida do necessário. A ENISA não é responsável pelo conteúdo das fontes externas, incluindo *websites* externos, mencionados na presente publicação.

Os fins desta publicação são meramente pedagógicos e informativos. Nem a ENISA nem qualquer pessoa que haja em seu nome é responsável pelo uso que possa ser dado ao seu conteúdo informativo.

Todos os direitos reservados. Nenhuma parte da presente publicação pode ser reproduzida, armazenada num sistema de pesquisa de informação ou transmitida de qualquer outra forma ou por qualquer meio, electrónico, mecânico, por fotocópia, gravação ou outro, sem a autorização prévia e por escrito da ENISA, ou ainda tal como é expressamente permitido por lei ou nos termos acordados com os organismos competentes em matéria de direitos. A fonte deve ser sempre mencionada. Os pedidos de reprodução podem ser enviados para o endereço mencionado na presente publicação.

© Agência Europeia para a Segurança das Redes e da Informação (ENISA), 2006

3 Agradecimentos

A ENISA deseja agradecer a todas as instituições e pessoas que contribuíram para o presente documento, com especial menção das seguintes:

- A Henk Bronk, que enquanto consultor produziu a primeira versão do documento.

- Ao CERT/CC e, em especial, à equipa de desenvolvimento da CSIRT, que forneceu materiais extremamente úteis e o exemplo de material didáctico apresentado no anexo.
- À GovCERT.NL por fornecer o “*CERT-in-a-box*”
- À equipa TRANSITS que forneceu o exemplo de material didáctico apresentado no anexo.
- Aos colegas da secção Políticas de Segurança do Departamento Técnico, que elaboraram o capítulo 6.6
- Às inúmeras pessoas que reviram o documento.

4 Introdução

As redes de comunicações e os sistemas informáticos tornaram-se um factor essencial do desenvolvimento económico e social. A informática e as redes estão a tornar-se serviços de utilidade pública omnipresentes, como já o são os serviços de abastecimento de electricidade e água.

A segurança das redes de comunicações e dos sistemas informáticos, em particular a sua disponibilidade, ganha, por conseguinte, uma importância crescente para a sociedade, decorrente do risco de problemas nos sistemas informáticos essenciais, devido à complexidade dos sistemas, aos acidentes, erros e ataques que podem ter consequências para as infra-estruturas físicas que prestam serviços críticos para o bem-estar dos cidadãos da União Europeia.

Em 10 de Março de 2004, foi criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA)¹, com o objectivo de garantir um nível de segurança das redes e da informação elevado e eficaz, dentro da Comunidade, e desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público na União Europeia, contribuindo, assim, para o normal funcionamento do mercado interno.

Há já vários anos que várias comunidades de segurança da Europa, como as CERT/CSIRT, Abuse Teams (equipas anti-abuso) e WARP, colaboram para melhorar a segurança da Internet. A ENISA tenciona apoiar os esforços destas comunidades fornecendo informações sobre as medidas a tomar para garantir um nível de qualidade de serviço satisfatório. Além disso, a ENISA tenciona reforçar a sua capacidade de aconselhamento aos Estados-Membros da UE e aos organismos da União no que respeita à cobertura de grupos específicos de utilizadores de TI com serviços de segurança adequados. Desenvolvendo as conclusões do Grupo de Trabalho *ad-hoc* “Cooperação e Apoio CERT”, criado em 2005, este novo grupo de trabalho irá ocupar-se, assim, de questões relacionadas com a prestação de serviços de segurança adequados (serviços “CERT”) a (categorias ou grupos de) utilizadores específicos.

¹ Regulamento (CE) N.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação. Uma “agência da Comunidade Europeia” é um organismo criado pela UE para realizar uma tarefa técnica, científica ou de gestão muito específica no “domínio comunitário” (“primeiro pilar”) da UE.



A ENISA apoia a criação de novas CSIRT através da publicação do presente relatório *“Abordagem gradual de criação de uma CSIRT, com uma lista de verificação suplementar”*, que auxiliará o leitor a criar a sua própria CSIRT.

4.1 Público-alvo

Os principais grupos-alvo do presente relatório são as instituições governamentais e outras que decidam criar uma CSIRT para proteger a sua própria infra-estrutura informática ou a dos seus parceiros.

4.2 Como utilizar o presente documento

O presente documento informá-lo-á sobre o que é uma CSIRT, os serviços que ela pode prestar e que passos é necessário dar para iniciar as actividades. Ele deverá proporcionar-lhe uma perspectiva clara e pragmática da abordagem, da estrutura e dos conteúdos relativos à criação de uma CSIRT.

Capítulo 4 “Introdução”

Introdução ao presente relatório

Capítulo 5 “Estratégia global para planejar e criar uma CSIRT”

A primeira secção descreve o que é uma CSIRT, além de fornecer informações sobre os diferentes ambientes em que as CSIRT podem funcionar e os serviços que podem prestar.

Capítulo 6 “Desenvolvimento do Plano de Actividades”

Este capítulo descreve a abordagem de gestão empresarial ao processo de constituição da equipa.

Capítulo 7 “Promoção do Plano de Actividades”

Este capítulo trata das questões económicas e de financiamento.

Capítulo 8 “Exemplos de procedimentos operacionais e técnicos”

Este capítulo descreve o procedimento de obtenção de informações e sua tradução num boletim de segurança. Faz também uma descrição de um fluxo de trabalho relativo à gestão de um incidente.

Capítulo 9 “Formação CSIRT”

Este capítulo apresenta um resumo da formação CSIRT disponível, ilustrado com exemplos de matérias dos cursos apresentados no anexo.

Capítulo 10 “Exercício: produção de um aviso”

Este capítulo inclui um exercício sobre o modo de desempenhar um dos serviços básicos (ou essenciais) da CSIRT: a produção de um boletim de segurança (ou aviso).

Capítulo 12 “Descrição do plano de projecto”

Este capítulo indica o plano de projecto suplementar (lista de verificação) fornecido juntamente com o presente guia e que pretende ser uma ferramenta simples de utilizar para a aplicação do mesmo.

4.3 Convenções utilizadas no presente documento

Para orientar o leitor, cada capítulo principia com as etapas já transpostas no processo de criação de uma CSIRT. Esses resumos são apresentados em caixas como a seguinte:

Demos o primeiro passo

Cada capítulo terminará com um exemplo prático das etapas analisadas. No presente documento, a “CSIRT fictícia” será uma pequena CSIRT independente para uma empresa ou instituição de dimensões médias. No anexo, poderá encontrar uma síntese.

CSIRT fictícia

5 Estratégia global para planear e criar uma CSIRT

Para iniciar adequadamente o processo de criação de uma CSIRT é importante ter uma visão clara dos eventuais serviços que ela pode prestar aos seus clientes, geralmente denominados no “mundo CSIRT” por “comunidade utilizadora”. Importa compreender, portanto, quais são as necessidades dos utilizadores para lhes prestar os serviços adequados, no momento certo e com a qualidade apropriada.

5.1 O que é uma CSIRT?

A abreviatura CSIRT significa “Computer Security Incident Response Team” (Equipa de Resposta a Incidentes de Segurança Informática). Trata-se de um termo predominantemente utilizado na Europa e que corresponde ao termo protegido CERT, registado nos EUA pelo CERT Coordination Center (CERT/CC) [Centro de Coordenação CERT].

Existem várias abreviaturas para o mesmo tipo de equipas:

- CERT ou CERT/CC (Computer Emergency Response Team / Coordination Center – Equipa de Resposta a Emergências Informáticas / Centro de Coordenação)
- CSIRT (Computer Security Incident Response Team - Equipa de Resposta a Incidentes de Segurança Informática)
- IRT (Incident Response Team – Equipa de Resposta a Incidentes)
- CIRT (Computer Incident Response Team – Equipa de Resposta a Incidentes Informáticos)
- SERT (Security Emergency Response Team – Equipa de Resposta a Emergências de Segurança)

O primeiro grande ataque de um “verme” (*worm*) na infra-estrutura informática mundial verificou-se no final da década de 1980. O verme foi denominado Morris² e disseminou-se rapidamente, tendo contaminado um grande número de sistemas informáticos em todo o mundo.

Este incidente funcionou como um sinal de alerta: de repente, as pessoas tomaram consciência de que a cooperação e a coordenação entre administradores de sistemas e gestores informáticos eram extremamente necessárias para resolver casos como este. Como o tempo era um factor decisivo, impunha-se criar uma abordagem mais organizada e estrutural à gestão de incidentes de segurança informática e, por isso, poucos dias após o “incidente Morris” a Agência de Projectos de Pesquisa Avançada do Departamento de Defesa (Defence Advanced Research Projects Agency (DARPA)) criou a primeira CSIRT: o Centro de Coordenação CERT (CERT/CC³), localizado na Carnegie Mellon University, em Pittsburgh (Pensilvânia).

Este modelo depressa foi adoptado na Europa e, em 1992, a fornecedora académica holandesa SURFnet lançou a primeira CSIRT na Europa, denominada SURFnet-CERT⁴. Muitas outras equipas se seguiram e, presentemente, o *Inventory of CERT activities in*

² Para mais informações sobre o verme Morris, ver http://en.wikipedia.org/wiki/Morris_worm

³ CERT-CC <http://www.cert.org>

⁴ SURFnet-CERT: <http://cert.surfnet.nl/>

*Europe*⁵ (Inventário de actividades de CERT na Europa) da ENISA contém mais de cem equipas conhecidas localizadas na Europa.

Ao longo dos anos, as CERT foram ampliando as suas capacidades e deixaram de ser uma simples força reactiva, passando a fornecer serviços de segurança completos, incluindo serviços preventivos, como alertas e recomendações de segurança, formação e serviços de gestão de segurança. O termo “CERT” depressa foi considerado insuficiente, o que levou à criação do novo termo “CSIRT”, no final da década de 1990. Actualmente, ambos os termos (CERT e CSIRT) são usados como sinónimos, sendo CSIRT o termo mais exacto.

5.1.1 O termo *Comunidade utilizadora*

Daqui em diante, o termo “comunidade utilizadora”, solidamente implantado (nas comunidades CSIRT), será utilizado para designar a base de clientes de uma CSIRT. Um cliente individual será denominado “utilizador” e um grupo de clientes “utilizadores”.

5.1.2 Definição de CSIRT

Uma CSIRT é uma equipa de peritos de segurança informática que tem como principal actividade responder aos incidentes de segurança informática. Presta os serviços necessários para os gerir e ajudar os seus utilizadores a recuperarem das violações da segurança.

A fim de atenuar os riscos e minimizar o número de respostas necessárias, a maioria das CSIRT também presta serviços preventivos e pedagógicos à sua comunidade utilizadora. Emite avisos sobre as vulnerabilidades dos *softwares* e *hardwares* em utilização e informa os utilizadores acerca dos aproveitamentos e dos vírus que tiram partido destas falhas. Deste modo, os utilizadores podem proteger e actualizar rapidamente os seus sistemas. Ver no capítulo 5.2 *Eventuais serviços* uma lista completa dos serviços possíveis.

5.1.3 Os benefícios de possuir uma CSIRT

Dispor de uma equipa de segurança informática dedicada ajuda as organizações a atenuarem e prevenirem os incidentes graves, bem como a proteger os seus valiosos recursos.

Outros benefícios possíveis são os seguintes:

- Ter uma coordenação centralizada para as questões de segurança informática na organização (Ponto de Contacto, PoC).
- Gestão e resposta centralizadas e especializadas em matéria de incidentes informáticos.
- Contar com peritos disponíveis para apoiarem e ajudarem os utilizadores a recuperarem rapidamente dos incidentes de segurança.
- Tratar das questões jurídicas e preservar as provas em caso de acção judicial.
- Acompanhar a evolução no domínio da segurança.

⁵ Inventário ENISA http://www.enisa.europa.eu/cert_inventory/

- Estimular a cooperação em matéria de segurança informática no seio da comunidade utilizadora (sensibilização).

CSIRT fictícia (etapa 0)**Compreender o que é uma CSIRT:**

Este exemplo de CSIRT terá de servir uma instituição de dimensão média, com 200 efectivos. A instituição possui o seu próprio departamento de informática e duas outras sucursais no mesmo país. A informática desempenha um papel fundamental para a empresa, porque é utilizada na comunicação interna, numa rede de dados e num cibernegócio que funciona permanentemente. A instituição tem uma rede própria e dispõe de uma ligação suplementar à Internet através de dois fornecedores de serviços Internet diferentes.

5.1.4 Descrição dos diferentes tipos de ambientes CSIRT

Demos o primeiro passo

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.

>> A próxima etapa é responder à pergunta: “A que sector serão os serviços da CSIRT prestados?”

Ao lançar uma CSIRT (tal como com qualquer outra actividade) é muito importante adquirir rapidamente uma perspectiva clara de quem são os seus utilizadores e do tipo de ambiente para o qual os serviços da CSIRT serão desenvolvidos. Neste momento, distinguimos os seguintes “sectores”, enumerados por ordem alfabética:

- CSIRT do Sector Académico
- CSIRT Comercial
- CSIRT do Sector PIC/PIIC (Protecção de informações críticas/protecção de informações e infra-estruturas críticas)
- CSIRT do Sector Governamental
- CSIRT Interna
- CSIRT do Sector Militar
- CSIRT Nacional
- CSIRT do Sector das Pequenas e Médias Empresas (PME)
- CSIRT de fornecedores

CSIRT do Sector Académico

Enfoque

Uma CSIRT do sector académico presta serviços CSIRT a instituições académicas e educativas, como universidades e centros de investigação, bem como aos ambientes Internet dos respectivos *campi* universitários.

Utilizadores

Os utilizadores habituais deste tipo de CSIRT são o pessoal e os estudantes das universidades.

CSIRT Comercial

Enfoque

Uma CSIRT comercial presta serviços CSIRT comercialmente aos seus utilizadores. No caso de um fornecedor de serviços Internet, a CSIRT presta sobretudo serviços anti-abuso aos clientes finais (Dial-in, ADSL) e serviços CSIRT aos seus clientes profissionais.

Utilizadores

As CSIRT comerciais prestam normalmente serviços a utilizadores que os pagam.

CSIRT do Sector PIC/PIIC*Enfoque*

As CSIRT deste sector concentram-se principalmente na Protecção de Informações Críticas e/ ou de Informações e Infra-estruturas Críticas. Na maioria dos casos, esta CSIRT especializada coopera intimamente com um serviço governamental nesta última área. Abrange todos os sectores informáticos críticos do país e protege os seus cidadãos.

Utilizadores

Governo; empresas em que a informática desempenha um papel crítico; cidadãos

CSIRT do Sector Governamental*Enfoque*

Uma CSIRT governamental presta serviços às agências governamentais e, em alguns países, aos cidadãos.

Utilizadores

Governo e agências conexas; em alguns países também são prestados serviços de alerta aos cidadãos (por exemplo na Bélgica, Hungria, Países Baixos, Reino Unido ou Alemanha).

CSIRT Interna*Enfoque*

Uma CSIRT interna apenas presta serviços à organização em que está instalada, sendo mais uma função do que um sector propriamente dito. Muitas organizações de telecomunicações e bancos, por exemplo, possuem as suas próprias CSIRT internas. Normalmente não mantêm um *website* público.

Utilizadores

Pessoal interno e departamento informático da organização de acolhimento.

CSIRT do Sector Militar*Enfoque*

Uma CSIRT deste sector presta serviços às organizações militares responsáveis pela infra-estrutura informática necessária para fins de defesa.

Utilizadores

Pessoal das instituições militares ou de entidades intimamente relacionadas com estas, por exemplo o Departamento de Defesa.

CSIRT Nacional*Enfoque*

É uma CSIRT centrada no nível nacional e considerada como um ponto de contacto de segurança para o país. Em alguns casos, a CSIRT governamental também funciona como ponto de contacto nacional (como a UNIRAS no Reino Unido).

Utilizadores

Este tipo de CSIRT normalmente não tem utilizadores directos, uma vez que a CSIRT nacional desempenha apenas um papel de intermediário para todo o país.

CSIRT do Sector das Pequenas e Médias Empresas (PME)

Enfoque

Trata-se de uma CSIRT auto-organizada, que presta os seus serviços à sua própria sucursal ou a um grupo de utilizadores semelhante.

Utilizadores

Os utilizadores destas CSIRT podem ser PME e o seu pessoal, ou grupos de interesses especiais como a “Associação de Cidades e Municípios” de um país.

CSIRT de Fornecedores

Enfoque

Uma CSIRT de fornecedores concentra-se no apoio aos produtos específicos dos fornecedores. Normalmente, tem por objectivo desenvolver e apresentar soluções para eliminar as vulnerabilidades e atenuar os potenciais efeitos negativos das falhas.

Utilizadores

Proprietários de produtos

Tal como se afirma no parágrafo sobre as CSIRT nacionais, é possível que uma equipa sirva mais de um sector. Este facto afecta, por exemplo, a análise da comunidade utilizadora e das suas necessidades.

CSIRT fictícia (etapa 1)

Fase de arranque

Na fase inicial, a nova CSIRT é planeada como uma CSIRT Interna, prestando os seus serviços à empresa de acolhimento, ao departamento informático local e ao pessoal. Também apoia e coordena a gestão dos incidentes de segurança informática entre as diversas sucursais.

5.2 Eventuais serviços que uma CSIRT pode prestar

Demos os primeiros dois passos

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?

>> A próxima etapa consiste em responder à pergunta, *que serviços prestar aos utilizadores?*

Uma CSIRT pode prestar muitos serviços, mas até agora nenhuma CSIRT existente os presta todos. Em consequência, a selecção do conjunto de serviços adequado é uma decisão crucial. Encontrará, a seguir, uma breve panorâmica de todos os serviços



CSIRT conhecidos, definidos no “Handbook for CSIRTs” [Manual das CSIRT] publicado pelo CERT/CC⁶.

⁶ CERT/CC CSIRT handbook <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

<u>Serviços reactivos</u>	<u>Serviços proactivos</u>	<u>Gestão de artefactos</u>
<ul style="list-style-type: none"> • Alertas e avisos • Gestão de incidentes • Análise de incidentes • Apoio na resposta a incidentes • Coordenação da resposta a incidentes • Resposta a incidentes no local • Gestão das vulnerabilidades • Análise das vulnerabilidades • Resposta às vulnerabilidades • Coordenação da resposta às vulnerabilidades 	<ul style="list-style-type: none"> • Comunicações • Vigilância tecnológica • Auditorias ou avaliações de segurança • Configuração e manutenção da segurança • Desenvolvimento de ferramentas de segurança • Serviços de detecção de intrusão • Difusão de informações relacionadas com a segurança 	<ul style="list-style-type: none"> • <u>Análise de artefactos</u> • <u>Resposta aos artefactos</u> • <u>Coordenação da resposta aos artefactos</u>
		<u>Gestão de qualidade da segurança</u> <ul style="list-style-type: none"> • <u>Análise dos riscos</u> • <u>Continuidade da actividade e recuperação de emergências</u> • <u>Consultoria de segurança</u> • <u>Sensibilização</u> • <u>Educação/Formação</u> • <u>Avaliação ou certificação dos produtos</u>

Fig. 1 Lista de serviços CSIRT do CERT/CC⁷

Serviços essenciais (a negro): É feita uma distinção entre serviços reactivos e proactivos. Os serviços proactivos visam prevenir os incidentes através da sensibilização e da formação, ao passo que os serviços reactivos procuram gerir os incidentes e atenuar os danos deles resultantes.

A gestão de artefactos inclui a análise de qualquer ficheiro ou objecto encontrado num sistema e que possa estar envolvido em acções malévolas, como é o caso dos resíduos de vírus, “vermes”, roteiros, “cavalos de Tróia”, etc. Também inclui a gestão e a distribuição das informações resultantes a fornecedores e outras partes interessadas, a fim de evitar que o *malware* (software maligno) continue a disseminar-se e para mitigar os riscos.

Os serviços de gestão de qualidade da segurança têm objectivos a longo prazo e incluem consultoria e medidas pedagógicas.

Ver no anexo uma explicação pormenorizada dos serviços CSIRT.

A escolha dos serviços adequados para a sua comunidade utilizadora é uma etapa importante e voltará a ser focada no capítulo 6.1 *Definição do modelo financeiro*.

A maioria das CSIRT começa por distribuir “alertas e avisos”, faz “comunicações” e assegura a “gestão de incidentes” ao serviço da sua comunidade utilizadora. Estes serviços essenciais costumam proporcionar uma boa visibilidade e chamar a atenção da

⁷ Lista de serviços CSIRT do CERT/CC: <http://www.cert.org/csirts/services.html>

comunidade utilizadora, sendo geralmente considerados como uma verdadeira “maívalia”.

É uma boa prática começar com um pequeno número de utilizadores “piloto”, prestar os serviços essenciais por um período experimental e solicitar-lhes, seguidamente, que forneçam *feedback*.

Os utilizadores-piloto interessados fornecem, normalmente, um *feedback* construtivo e ajudam a desenvolver serviços adaptados às suas necessidades.

CSIRT fictícia (etapa 2)

Escolha dos serviços adequados

Na fase inicial, decide-se que a nova CSIRT se concentrará, sobretudo, na prestação de alguns serviços essenciais aos funcionários.

É decidido que, após uma fase-piloto, se poderá ponderar o alargamento da carteira de serviços prestados e a adição de alguns “Serviços de Gestão da Segurança”. Essa decisão será tomada com base no *feedback* recebido dos utilizadores-piloto e em íntima colaboração com o departamento de garantia da qualidade.

5.3 Análise da comunidade utilizadora e definição da missão

Demos os primeiros três passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora?

>> A próxima etapa consiste em responder à pergunta, *que tipo de abordagem deverá ser utilizada no arranque da CSIRT?*

A próxima etapa implica um exame mais profundo da comunidade utilizadora, com o objectivo principal de escolher os canais de comunicação correctos:

- Definição da abordagem de comunicação com os utilizadores
- Definição da missão
- Elaborar um plano de execução ou de projecto realista
- Definição dos serviços CSIRT
- Definição da estrutura organizativa
- Definição da política de segurança da informação
- Contratação do pessoal adequado
- Utilização das instalações da CSIRT
- Busca de cooperação entre outras CSIRT e possíveis iniciativas nacionais

Estas etapas serão descritas em pormenor nos parágrafos seguintes e podem ser usadas como contributos para os planos de actividades e de projecto.

5.3.1 Abordagem de comunicação com a comunidade utilizadora

Como já foi dito, é muito importante que o leitor conheça as necessidades da comunidade utilizadora, bem como a sua própria estratégia de comunicação, incluindo os canais de comunicação mais adequados para lhe fazer chegar a informação.

A teoria da gestão inclui várias abordagens possíveis a este problema da análise de um grupo-alvo. No presente documento, descrevemos duas delas: a análise SWOT e a análise PEST.

Análise SWOT

Uma Análise SWOT é um instrumento de planeamento estratégico utilizado para avaliar os **Pontos fortes** (**Strengths**), os **Pontos fracos** (**Weaknesses**), as **Oportunidades** (**Opportunities**) e as **Ameaças** (**Threats**) envolvidos num projecto ou numa actividade, bem como em qualquer outra situação que exija uma tomada de decisões. A técnica é atribuída a Albert Humphrey, que liderou um projecto de investigação na Stanford University, nas décadas de 1960 e 1970, utilizando dados da revista Fortune das 500 maiores empresas.⁸

Pontos fortes	Pontos fracos
Oportunidades	Ameaças

Fig. 2 Análise SWOT

⁸ Análise SWOT na Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Análise PEST

A análise PEST é outro instrumento importante e muito utilizado para analisar a comunidade utilizadora com o objectivo de compreender as circunstâncias **Políticas**, **Económicas**, **Socioculturais** e **Tecnológicas** do ambiente em que uma CSIRT opera. Ela ajudará a determinar se o planeamento ainda está em harmonia com o ambiente e, provavelmente, a evitar que as acções sejam decididas com base em pressupostos errados.

Políticas <ul style="list-style-type: none"> • Questões ecológicas/ambientais • Legislação actual do mercado interno • Legislação futura • Legislação europeia/internacional • Entidades e processos reguladores • Políticas governamentais • Mandato e alteração do governo • Políticas comerciais • Financiamento, subvenções e iniciativas • Grupos de interesses/de pressão presentes no mercado interno • Grupos de pressão internacionais 	Económicas <ul style="list-style-type: none"> • Situação económica interna • Tendências económicas internas • Economias e tendências internacionais • Questões fiscais gerais • Tributação específica de produtos/serviços • Questões de sazonalidade/meteorológicas • Ciclos de mercado e comerciais • Factores industriais específicos • Rotas e tendências de distribuição do mercado • Motivações dos clientes/utilizadores finais • Taxas de juros e de câmbios
Sociais <ul style="list-style-type: none"> • Tendências de estilo de vida • Demografia • Atitudes e opiniões dos consumidores • Pontos de vista da comunicação social • Mudanças legislativas que afectam os factores sociais • Imagem de marca, empresarial, tecnológica • Padrões de compra dos consumidores • Moda e modelos positivos • Acontecimentos e influências importantes • Acesso e tendências de compra • Factores étnicos/religiosos • Publicidade e divulgação 	Tecnológicas <ul style="list-style-type: none"> • Desenvolvimento tecnológico concorrencial • Financiamento da investigação • Tecnologias associadas/dependentes • Tecnologia/soluções de substituição • Maturidade da tecnologia • Maturidade e capacidade de produção • Informação e comunicações • Mecanismos de compra/tecnológicos dos consumidores • Legislação tecnológica • Potencial de inovação • Acesso à tecnologia, licenças, patentes • Questões de propriedade intelectual

Fig. 3 Modelo de análise PEST

Pode encontrar uma descrição pormenorizada da análise PEST na Wikipedia⁹.

Ambos os instrumentos oferecem uma perspectiva ampla e estruturada das necessidades da comunidade utilizadora. Os resultados complementarão a proposta empresarial e ajudarão, assim, a obter financiamento para a criação da CSIRT.

Canais de comunicação

Um tema importante a incluir na análise é o dos possíveis métodos de comunicação e distribuição de informação (“Como comunicar com a comunidade utilizadora?”)

⁹ Análise PEST na Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Se possível, deverá ponderar-se a hipótese de realizar visitas pessoais regulares aos utilizadores. Está provado que os encontros pessoais facilitam a cooperação e, se ambas as partes estiverem dispostas a colaborar, eles permitirão estabelecer uma relação mais aberta.

Normalmente, as CSIRT usam um conjunto de canais de comunicação. Os seguintes provaram a sua utilidade na prática e vale a pena considerá-los:

- Website público
- Área do *website* reservada a membros
- Formulários-web para a notificação de incidentes
- Sistemas de lista de distribuição
- Correio electrónico personalizado
- Telefone / Fax
- SMS
- Cartas em papel “à moda antiga”
- Relatórios mensais ou anuais

Para além de utilizar o correio electrónico, formulários-web de notificação, o telefone ou o fax para facilitar a gestão de incidentes (receber notificações de incidentes enviadas pela comunidade utilizadora, coordenar com outras equipas ou dar *feedback* e apoio à vítima), a maioria das CSIRT publica as suas recomendações de segurança num *website* acessível ao público e através de sistemas de lista de distribuição.

! Se possível, as informações devem ser distribuídas de forma segura. As mensagens de correio electrónico, por exemplo, podem ser assinadas digitalmente com uma aplicação PGP e os dados sensíveis relativos a incidentes devem ser sempre enviados em linguagem cifrada.

Para mais informações, ver o capítulo 8.5 *Ferramentas de CSIRT disponíveis*. Ver também o capítulo 2.3 do RFC2350¹⁰.

CSIRT fictícia (etapa 3a)

Fazer uma análise da comunidade utilizadora e dos canais de comunicação adequados

Uma sessão de reflexão com alguns dos principais membros da administração e da comunidade utilizadora produziu elementos suficientes para uma análise SWOT. Esta permite concluir que são necessários os seguintes serviços essenciais:

- Alertas e avisos
- Gestão de incidentes (análise, apoio à resposta e coordenação da resposta)
- Comunicações

Importa garantir que as informações são distribuídas de forma bem organizada para chegarem à maior parcela possível da comunidade utilizadora. Decidiu-se, por isso,

¹⁰ <http://www.ietf.org/rfc/rfc2350.txt>

publicar os alertas, avisos e comunicações sob a forma de recomendações de segurança num *website* específico e disseminá-las através de um sistema de lista de distribuição. A CSIRT facilita o correio electrónico, o telefone e o fax para a recepção das notificações de incidentes. Para a próxima etapa está previsto um formulário-web unificado.

Ver, na próxima página, um exemplo de análise SWOT.

Pontos fortes <ul style="list-style-type: none"> • A empresa dispõe de alguns conhecimentos. • Gostam do plano e estão dispostos a cooperar • Apoio e financiamento por parte do Conselho de Administração 	Pontos fracos <ul style="list-style-type: none"> • Comunicação insuficiente entre os diversos departamentos e sucursais. • Falta de coordenação com os incidentes informáticos • Grande número de “pequenos departamentos”
Oportunidades <ul style="list-style-type: none"> • Grande afluxo de informações não estruturadas sobre as vulnerabilidades • Grande necessidade de coordenação • Redução das perdas causadas por incidentes • Muitos pontos em aberto em matéria de segurança informática • Educar o pessoal em matéria de segurança informática 	Ameaças <ul style="list-style-type: none"> • Poucas verbas disponíveis • Pessoal insuficiente • Expectativas elevadas • Cultura

Fig. 4 Exemplo de análise SWOT

5.3.2 Definição da missão

Depois de analisar as necessidades e os desejos da comunidade utilizadora no que respeita aos serviços CSIRT, deverá formular-se, na etapa seguinte, uma definição da missão.

Esta definição descreve a função básica da organização na sociedade, em termos dos produtos e serviços que fornece aos membros da sua comunidade utilizadora, e permite comunicar claramente a existência e a função da nova CSIRT.

É uma boa prática definir a missão de forma concisa, mas sem excessiva rigidez, porque normalmente essa definição permanecerá inalterada durante alguns anos.

Eis alguns exemplos de definições da missão de CSIRT que estão em actividade:

“<Nome da CSIRT> fornece informações e assistência aos seus <utilizadores (defina quem são)> na aplicação de medidas proactivas para reduzir os riscos de incidentes informáticos e responder a tais incidentes, quando se verificarem.”

*"Oferecer apoio aos <utilizadores> em matéria de prevenção e de resposta a incidentes de segurança informática"*¹¹

A definição da missão é uma etapa muito importante e necessária para o arranque. Consulte no capítulo 2.1 do RFC2350¹² uma descrição mais pormenorizada das informações que uma CSIRT deverá publicar.

CSIRT fictícia (etapa 3b)

A gestão da CSIRT fictícia elaborou a seguinte definição da missão:

"A CSIRT fictícia fornece informação e assistência ao pessoal da sua empresa de acolhimento para reduzir os riscos de incidentes de segurança informática e responder a tais incidentes, quando se verificam."

A CSIRT fictícia esclarece, assim, que se trata de uma CSIRT interna e que a sua actividade essencial é tratar de questões de segurança informática.

¹¹ Definição de missão da Govcert.nl: <http://www.govcert.nl>

¹² <http://www.ietf.org/rfc/rfc2350.txt>

6 Desenvolvimento do Plano de Actividades

Demos os seguintes passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora.
4. Análise do ambiente e dos utilizadores.
5. Definição da missão

>> A próxima etapa é definir o plano de actividades

Os resultados da análise dão-lhe uma boa panorâmica das necessidades e dos (supostos) pontos fracos da comunidade utilizadora, por isso são usados como um contributo para a próxima etapa.

6.1 Definição do modelo financeiro

Após a análise, foram escolhidos alguns serviços essenciais para começar. A próxima etapa consiste em pensar acerca do modelo financeiro: que parâmetros de prestação de serviços são simultaneamente adequados e economicamente compensadores.

Num mundo perfeito, o financiamento estaria adaptado às necessidades da comunidade utilizadora, mas, na realidade, o conjunto de serviços que podem ser prestados tem de se adaptar a um dado orçamento. Por isso, é mais realista começar por planear as questões monetárias.

6.1.1 Modelo de custos

Os dois principais factores que influenciam os custos são a determinação do horário de serviço e do número (e qualidade) de efectivos a empregar. Haverá necessidade de fornecer resposta a incidentes e apoio técnico 24 horas por dia, sete dias por semana, ou estes serviços apenas serão prestados nas horas de expediente?

Dependendo da disponibilidade desejada e dos equipamentos de escritório (será, por exemplo, possível trabalhar a partir de casa?) poderá ser benéfico trabalhar com um sistema de piquete ou com uma escala de turnos programados.

Um cenário admissível será prestar serviços proactivos e reactivos durante as horas de expediente e, fora desse horário, prestar apenas serviços limitados, por exemplo só em caso de grandes desastres e incidentes, por um funcionário de piquete.

Outra opção é procurar a cooperação internacional existente entre outras equipas CSIRT. Já há exemplos de cooperação funcional em que equipas localizadas em diferentes fusos horários se vão revezando (cooperação "Following the Sun"). Por exemplo, a cooperação entre equipas europeias e americanas revelou ser benéfica e

constituir uma boa forma de partilhar as capacidades umas das outras. A CSIRT Sun Microsystems, por exemplo, que tem várias sucursais em diversos fusos horários de todo o mundo (mas todas incluídas na mesma equipa CSIRT), assegura serviços permanentes graças à constante rotação entre as equipas das várias regiões do mundo. Esta prática limita muito os custos, porque todas as equipas só trabalham nas horas normais de expediente prestando também serviços à parte do mundo que está “a dormir”.

É uma boa prática analisar, especificamente, a necessidade de serviços permanentes de forma aprofundada com a comunidade utilizadora. Os alertas e avisos fornecidos durante a noite não fazem muito sentido quando o receptor apenas os lê na manhã seguinte. Uma linha estreita separa “necessitar de um serviço” de “querer um serviço”, mas o horário de trabalho faz uma diferença particularmente grande no número de funcionários e nas instalações necessários, afectando, por isso, fortemente o modelo de custos.

6.1.2 Modelo de receitas

Quando se conhecem os custos, convém pensar seguidamente nos possíveis modelos das receitas: como financiar os serviços previstos. Eis alguns cenários a avaliar:

Utilização dos recursos existentes

É sempre benéfico avaliar os recursos já presentes noutras secções da empresa. Esta já emprega pessoal adequado (por exemplo no departamento informático existente), dotado da experiência e das competências necessárias? Provavelmente, pode combinar-se com a administração que este pessoal seja destacado para a CSIRT, na fase inicial, ou que preste apoio à equipa pontualmente.

Cotização

Outra possibilidade é vender os seus serviços à comunidade utilizadora, por uma cotização anual/trimestral. Os serviços adicionais poderão ser pagos consoante a sua utilização, por exemplo, serviços de consultoria ou auditorias de segurança.

Outro cenário possível: os serviços à comunidade utilizadora (interna) são prestados a título gratuito, mas os serviços prestados a clientes externos podem ter de ser pagos. Outra ideia é publicar avisos e boletins informativos no *website* público e ter uma secção “Reservada a membros” com informações específicas, mais pormenorizadas ou individualizadas.

Provou-se, na prática, que a “Assinatura por serviço CSIRT” tem pouca utilidade para obter o financiamento suficiente, sobretudo na fase de arranque. Há, por exemplo, custos básicos fixos relativos à equipa e ao equipamento que têm de ser pagos antecipadamente. O financiamento destes custos com a venda de serviços CSIRT é difícil e exige uma análise financeira muito pormenorizada para encontrar o equilíbrio financeiro.

Subsídio

Outra possibilidade que vale a pena considerar poderá ser a de requerer um subsídio para projectos concedido pelo governo, ou por um organismo do Estado, uma vez que,

actualmente, a maioria dos países tem fundos disponíveis para projectos de segurança informática. Contactar o Ministério do Interior poderá ser um bom ponto de partida.

Evidentemente que será possível conjugar vários modelos.

6.2 Definição da estrutura organizativa

A estrutura organizativa adequada para uma CSIRT depende muito da estrutura existente na organização de acolhimento e na comunidade utilizadora. Depende também do acesso a peritos competentes que possam ser contratados permanentemente ou de forma pontual.

Uma CSIRT normal define as seguintes funções dentro da equipa:

Geral

- Director geral

Pessoal

- Director de departamento
- Contabilista
- Consultor de comunicação
- Consultor jurídico

Equipa técnica operacional

- Chefe da equipa técnica
- Técnicos de CSIRT, que prestam os serviços CSIRT
- Investigadores

Consultores externos

- Contratados quando necessário

É extremamente útil ter um jurista na equipa, sobretudo na fase inicial da CSIRT. Irá aumentar os custos mas, no final, poupará tempo e problemas jurídicos.

Em função da diversidade de conhecimentos especializados existentes na comunidade utilizadora, e quando a CSIRT tem grande visibilidade nos meios de comunicação social, também se revelou muito útil ter um perito de comunicação na equipa. Estes peritos podem centrar-se na tradução de questões técnicas difíceis para mensagens que os utilizadores ou os seus parceiros dos meios de comunicação social possam compreender melhor. O perito de comunicação também transmitirá o *feedback* da comunidade utilizadora aos peritos técnicos, podendo funcionar, assim, como “tradutor” e “facilitador” entre estes dois grupos.

Seguem-se alguns exemplos de modelos organizativos presentemente utilizados pelas CSIRT operacionais.

6.2.1 O modelo empresarial independente

A CSIRT é estabelecida e actua como uma organização independente, com a sua própria gestão e os seus próprios funcionários.

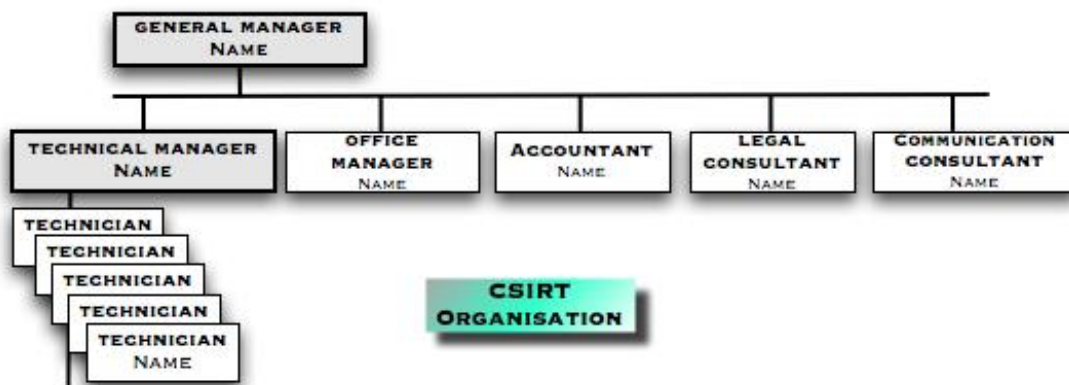


Fig. 5 Modelo empresarial independente

	Director-geral Nome			
Director técnico Nome	Director de Departamento Nome	Contabilista Nome	Consultor Jurídico Nome	Consultor de Comunicação Nome
Técnico Técnico Técnico Nome		Organização da CSIRT		

6.2.2 O modelo integrado

Este modelo pode ser utilizado se uma CSIRT for criada no âmbito de uma organização existente, com base num departamento informático já existente, por exemplo. A CSIRT é chefiada por um chefe de equipa e este é responsável pelas actividades CSIRT. O chefe de equipa reúne os técnicos necessários para resolver incidentes ou trabalhar nas ditas actividades, podendo solicitar a ajuda de especialistas pertencentes à organização.

Este modelo também pode ser adaptado a situações específicas, à medida que estas vão surgindo. Neste caso, é atribuído à equipa um número fixo de funcionários ou um equivalente a tempo inteiro (FTE). A assistência anti-abusos num fornecedor de serviços Internet, por exemplo, constitui certamente um emprego a tempo inteiro para um ou (na maioria dos casos) mais de um FTE.

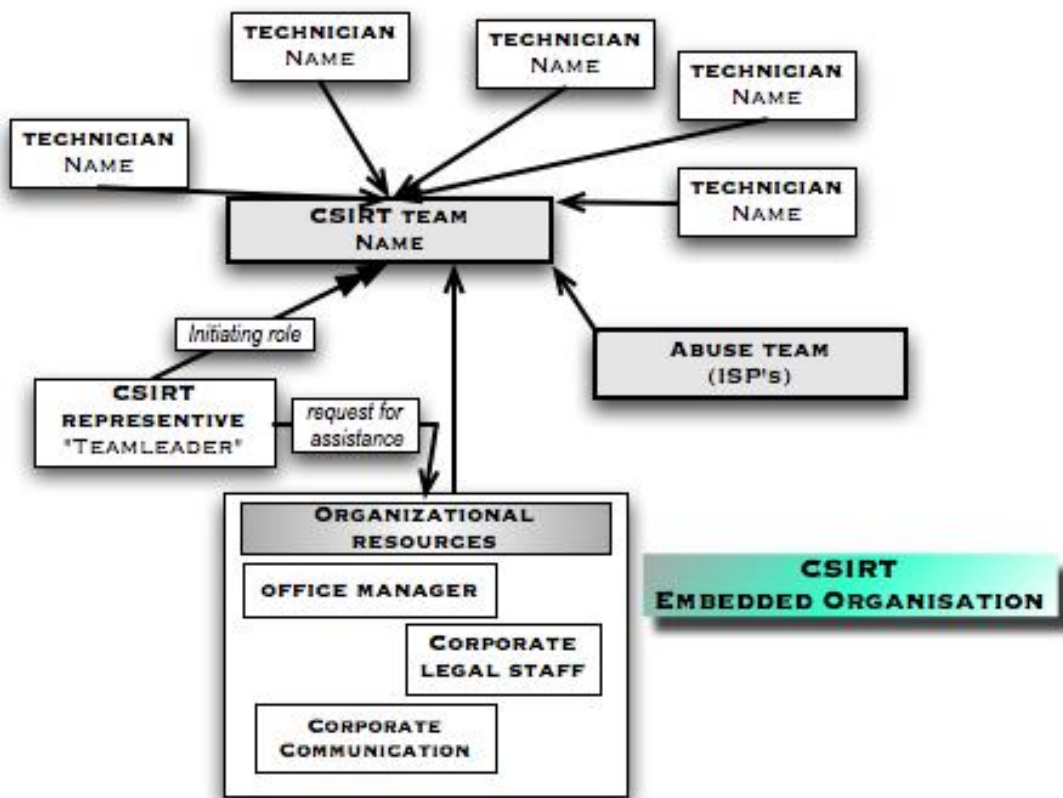


Fig. 6 Modelo organizativo integrado

	Técnico Nome	Técnico Nome	Técnico Nome	Técnico Nome
Técnico Nome		Equipa CSIRT Nome		Técnico Nome

	Papel de dinamização		Equipa Anti-Abusos (Prestadores Serviços Internet)	
Representante da CSIRT "Chefe de equipa"	Pedido de assistência	Recursos organizativos Director de departamento Pessoal jurídico da organização Comunicação institucional		CSIRT Organização integrada

6.2.3 O modelo “campus”

O modelo “campus”, como o nome indica, é sobretudo adoptado pelas CSIRT académicas e de investigação. A maioria das organizações académicas e de investigação é constituída por várias universidades e centros académicos localizados em diversos sítios, dispersos por uma região ou até pelo país inteiro (como no caso das NREN, National Research Networks – Redes de Investigação Nacionais). Normalmente, estas organizações são independentes umas das outras e possuem, frequentemente, a sua própria CSIRT. Estas CSIRT estão habitualmente organizadas sob a coordenação da CSIRT “mãe” ou central, que coordena e é o ponto de contacto único para o mundo exterior. Na maior parte dos casos, a CSIRT central também presta os serviços CSIRT essenciais, além de distribuir informações sobre os incidentes à CSIRT do campus adequado.

Algumas CSIRT fazem circular os seus serviços CSIRT essenciais com as outras CSIRT do género, o que permite baixar as despesas gerais da CSIRT central.

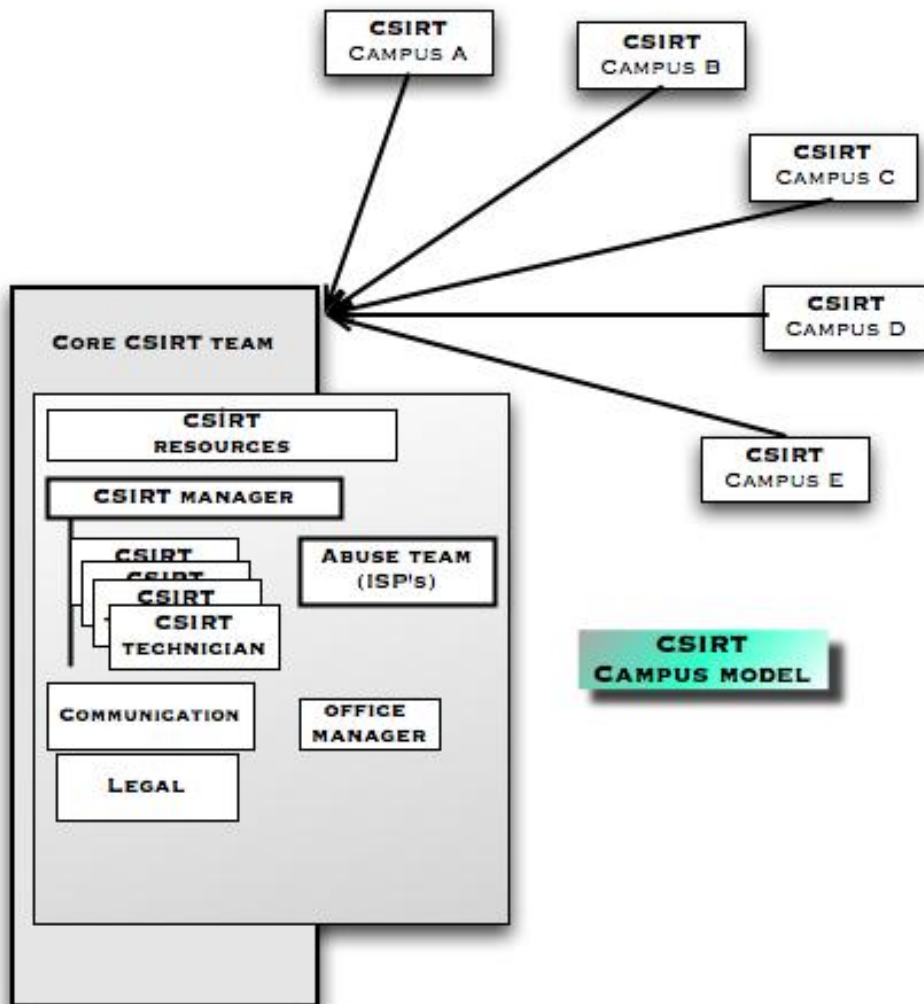


Fig. 7 Modelo “campus”

	CSIRT Campus A	CSIRT Campus B		CSIRT Campus C
Equipa CSIRT central				CSIRT Campus D
	Recursos CSIRT Director CSIRT Técnico CSIRT Técnico CSIRT Técnico CSIRT Técnico CSIRT Comunicação Jurídico	Equipa Anti- abusos (Fornecedores Serviços Internet) Director de departamento	CSIRT Campus E	

6.2.4 O modelo voluntário

Este modelo organizativo descreve um grupo de pessoas (especialistas) que se reúnem para fornecer aconselhamento e apoio mútuos (e a outros) de forma voluntária. É uma comunidade pouco estável e está muito dependente da motivação dos participantes.

Este modelo é adoptado, por exemplo, pela comunidade WARP¹³.

6.3 Contratação do pessoal adequado

Tendo decidido os serviços e o nível de apoio a prestar, e depois de escolher um modelo organizativo, a etapa seguinte consiste em encontrar a quantidade correcta de pessoas competentes para o trabalho.

¹³ Iniciativa WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

É quase impossível indicar um número concreto para o pessoal técnico necessário deste ponto de vista, mas os seguintes valores-chave provaram ser uma boa abordagem:

- Para prestar dois serviços essenciais de distribuição de boletins de aviso e de gestão de incidentes: no mínimo **4 FTE**.
- Para uma CSIRT que preste serviços completos durante as horas de expediente, e assegure a manutenção dos sistemas: no mínimo, **6 a 8 FTE**.
- Para um serviço por turnos permanente com o pessoal completo (2 turnos fora das horas de expediente), são necessários, no mínimo, cerca de **12 FTE**.

Estes valores também incluem pessoal suplementar para substituições em caso de doença, férias, etc. É igualmente necessário verificar os contratos colectivos de trabalho locais. O facto de as pessoas trabalharem fora das horas de expediente poderá implicar custos adicionais sob a forma de subsídios extraordinários que tenham de ser pagos.

Segue-se uma breve síntese das principais competências exigidas aos peritos técnicos de uma CSIRT

Aspectos gerais da descrição de funções do pessoal técnico:

Competências pessoais

- Flexibilidade, criatividade e bom espírito de equipa
- Boas capacidades analíticas
- Aptidão para explicar questões técnicas difíceis com termos fáceis de entender
- Sensibilidade no que respeita à confidencialidade e ao trabalho em questões processuais
- Boas competências organizativas
- Resistência ao stresse
- Boas competências de comunicação e de escrita
- Abertura de espírito e vontade de aprender

Competências técnicas

- Amplos conhecimentos da tecnologia e dos protocolos Internet
- Conhecimento dos sistemas Linux e Unix (dependendo dos equipamentos da comunidade utilizadora)
- Conhecimento dos sistemas Windows (dependendo dos equipamentos da comunidade utilizadora)
- Conhecimento dos equipamentos da infra-estrutura da rede (encaminhador (*router*), comutadores, DNS [Sistema de Nomes de Domínio], *Proxy*, *Correio*, etc.)
- Conhecimento das aplicações Internet (SMTP, HTTP(s), FTP, TELNET, SSH, etc.)
- Conhecimento das ameaças à segurança (DdoS (*Distributed denials of service* – negações de serviço), *Phishing* [apropriação da identidade de alguém através de correio electrónico], *Defacing* [alteração ilícita de páginas web], *sniffing* [Intercepção das comunicações], etc.)
- Conhecimento da avaliação dos riscos e das suas aplicações práticas

Competências suplementares

- Disponibilidade para trabalhar em turnos a qualquer hora do dia ou em qualquer dia da semana ou para estar de piquete (consoante o modelo de serviço)
- Máximo de distância de viagem (em caso de emergência, disponibilidade no escritório; tempo máximo de viagem)
- Nível de habilitações
- Experiência de trabalho no domínio da segurança informática

CSIRT fictícia (etapa 4)

Definição do Plano de Actividades

Modelo financeiro

Dado que a empresa tem um cibernegócio permanente e também um departamento informático que funciona 24 horas por dia e sete dias por semana, foi decidido que se prestaria um serviço completo durante as horas de expediente e um serviço de piquete fora desse horário. Os serviços à comunidade utilizadora serão prestados a título

gratuito, mas a possibilidade de prestar serviços a clientes externos será avaliada durante a fase piloto e a fase de avaliação.

Modelo de receitas

Durante a fase de arranque e a fase-piloto, a CSIRT será financiada através da empresa de acolhimento. Na fase-piloto e na fase de avaliação, debater-se-á um financiamento adicional, incluindo a possibilidade de vender serviços a clientes externos.

Modelo organizativo

A organização de acolhimento é uma pequena empresa, por isso é escolhido o modelo integrado.

Durante as horas de expediente, os serviços básicos (distribuição de recomendações de segurança e gestão/coordenação de incidentes) serão prestados por três pessoas.

O departamento informático da empresa já dispõe de pessoal com as competências adequadas. É celebrado um acordo com esse departamento para que a nova CSIRT possa pedir apoio pontualmente, quando for necessário. Também é possível recorrer à segunda linha dos seus técnicos em serviço de piquete.

Haverá uma equipa CSIRT de base, composta por quatro elementos a tempo inteiro e cinco elementos suplementares. Um destes também estará disponível em turnos rotativos.

Pessoal

O chefe de equipa CSIRT tem experiência profissional no domínio da segurança e do apoio de 1º e 2º nível, tendo trabalhado no domínio da gestão e recuperação de crises. Os outros três membros da equipa são especialistas de segurança. Os membros da equipa CSIRT a tempo parcial provenientes do departamento informático são especializados no seu sector da infra-estrutura da empresa.

6.4 Utilização e equipamento das instalações

O equipamento e a utilização do espaço de escritórios, bem como a segurança física, são temas muito vastos, não se podendo fazer uma descrição exaustiva dos mesmos no presente documento. Este capítulo pretende dar uma breve perspectiva do tema.

É possível encontrar mais informações sobre segurança física nos endereços:

http://en.wikipedia.org/wiki/Physical_security

http://www.sans.org/reading_room/whitepapers/physcial/

<http://www.infosyssec.net/infosyssec/physfac1.htm>

“Blindar o edifício”

Dado que as CSIRT gerem normalmente informações muito sensíveis, é boa prática permitir que a equipa assuma o controlo da segurança física do escritório. Isto dependerá muito das instalações e infra-estruturas existentes, bem como da política de segurança informática da empresa de acolhimento.

Os governos, por exemplo, trabalham com sistemas de classificação e são muito rigorosos quanto ao modo como as informações confidenciais devem ser tratadas. Verifique com a sua própria empresa ou instituição as regras e políticas locais.

Normalmente, uma nova CSIRT está dependente da cooperação da organização de acolhimento para conhecer as regras, as políticas e outras questões jurídicas locais.

Fazer uma descrição exaustiva de todos os equipamentos e medidas de segurança necessários está fora do âmbito do presente documento. No entanto, poderá encontrar seguidamente uma lista sucinta dos recursos básicos para a sua CSIRT:

Regras gerais para o edifício

- Utilizar controlos de acesso
- Apenas permitir o acesso aos escritórios CSIRT, pelo menos, ao pessoal da equipa.
- Vigiar os gabinetes e entradas com câmaras de vídeo.
- Arquivar as informações confidenciais em armários com chave ou num cofre.
- Utilizar sistemas informáticos seguros.

Regras gerais para os equipamentos informáticos

- Utilizar equipamentos que possam ser assistidos pelo pessoal
- “Blindar” todos os sistemas
- Proteger e actualizar todos os sistemas antes de os ligar à Internet
- Utilizar *software* de segurança (Firewalls, múltiplos *scanners* anti-vírus, *anti-spyware*, etc.)

Manter os canais de comunicação

- *Website* público
- Área reservada aos membros no *website*
- Formulários-web de notificação de incidentes
- Correio electrónico (apoio PGP / GPG / S/MIME)
- *Software* de sistema de lista de distribuição
- Ter um número de telefone exclusivo à disposição da comunidade utilizadora:
 - Telefone
 - Fax
 - SMS

Sistema(s) de acompanhamento de registos

- Base de contactos com informações dos membros da equipa, de outras equipas, etc.
- Ferramentas CRM (gestão de relacionamento com o cliente)
- Sistema de talões para a gestão de incidentes

Utilizar o “estilo institucional” desde o início para

- A estrutura normal das mensagens de correio electrónico e dos boletins de aviso
- As cartas “à moda antiga” em papel
- Os relatórios mensais ou anuais
- Os formulários de notificação de incidentes

Outras questões

- Prever comunicação fora da banda em caso de ataque
- Prever um sistema suplementar de ligação à Internet

Para mais informações sobre ferramentas CSIRT específicas, ver o capítulo 8.5 *Ferramentas CSIRT disponíveis*.

6.5 *Formulação de uma política de segurança informática*

A política de segurança da informação dependerá do seu tipo de CSIRT. Para além de descrever o estado desejado dos processos e procedimentos operacionais e administrativos, essa política deve estar conforme com a legislação e as normas, em especial no que respeita à responsabilidade da CSIRT. Esta última está normalmente vinculada por leis e regulamentos nacionais, que são muitas vezes aplicados no contexto de legislação europeia (normalmente directivas) e outros acordos internacionais. As normas não são necessariamente vinculativas, de forma directa, mas podem ser impostas ou recomendadas por leis e regulamentos.

Segue-se uma breve lista de possíveis leis e políticas:

Nacionais

- Várias leis sobre informática, telecomunicações, meios de comunicação social
- Leis sobre a protecção de dados e a privacidade
- Leis e regulamentos sobre a conservação dos dados
- Legislação sobre finanças, contabilidade e gestão das sociedades
- Códigos de conduta para a governação das sociedades e a governação no domínio da informática

Europeias

- Directiva relativa às assinaturas electrónicas (1999/93/CE)
- Directivas relativas à protecção de dados (1995/46/CE) e à privacidade das comunicações electrónicas (2002/58/CE)
- Directivas relativas às redes e serviços de comunicação electrónicas (2002/19/CE – 2002/22/CE)
- Directivas relativas ao direito das sociedades (por exemplo, 8ª Directiva sobre direito das sociedades)

Internacionais

- Acordo Basileia II (especialmente no que respeita à gestão dos riscos operacionais)
- Convenção sobre Cibercriminalidade do Conselho da Europa
- Convenção sobre Direitos Humanos do Conselho da Europa (artigo 8.º sobre privacidade)
- Normas internacionais de contabilidade (IAS; mandatam em alguma medida os controlos informáticos)

Normas

- Normas britânicas BS 7799 (Segurança da Informação)
- Normas internacionais ISO2700x (Sistema de gestão da segurança da informação)
- IT-Grundschutzbuch alemã, EBIOS francesa e outras variações nacionais.

Para determinar se a sua CSIRT está a agir em conformidade com a legislação nacional e internacional, consulte o seu consultor jurídico.

As perguntas mais básicas que devem ser respondidas nas suas políticas de gestão da informação são as seguintes:

- Como é a informação de entrada "etiquetada" ou "classificada"?
- Como é a informação gerida, em especial no que respeita à exclusividade?
- Que critérios são adoptados para a divulgação de informações, nomeadamente se são transmitidas informações relativas a incidentes a outras equipas ou *sites*?
- Há considerações jurídicas a ter em conta em relação à gestão da informação?
- Tem uma política relativa ao uso de criptografia para proteger a exclusividade e a integridade nos arquivos e/ou na comunicação de dados, especialmente por correio electrónico?
- Esta política inclui eventuais condições limitativas de ordem jurídica como o depósito de chaves ou a obrigatoriedade de decifragem em caso de processo judicial?

CSIRT fictícia (etapa 5)

Equipamento e localização das instalações

Em virtude de a empresa de acolhimento já ter uma segurança física eficiente instalada, a nova CSIRT está bem protegida nesse aspecto. Existe uma "sala de guerra" para assegurar a coordenação em caso de emergência. Foi adquirido um cofre para o material de cifragem e para os documentos sensíveis. Instalou-se uma linha telefónica separada, incluindo uma central telefónica para assegurar a linha directa durante as horas de expediente e o telefone móvel de serviço "por chamada" no período fora desse horário, com o mesmo número de telefone.

Os equipamentos existentes e o *website* da organização também podem ser utilizados para comunicar informações relacionadas com a CSIRT. Há um sistema de lista de distribuição, de manutenção assegurada, com uma parte reservada à comunicação entre os membros da equipa e com outras equipas. Todos os contactos dos membros do pessoal estão armazenados numa base de dados, guardando-se uma listagem impressa dos mesmos no cofre.

Regulamentação

Como a CSIRT está integrada numa empresa com políticas de segurança informática em vigor, as políticas correspondentes aplicáveis à CSIRT foram estabelecidas com o auxílio do consultor jurídico da empresa.

6.6 Busca da cooperação entre outras CSIRT e possíveis iniciativas nacionais

A existência de outras iniciativas CSIRT e a forte necessidade de cooperação entre elas já foi mencionada algumas vezes no presente documento. É uma boa prática contactar outras CSIRT, o mais cedo possível, para obter o contacto necessário com as comunidades CISRT. Normalmente, as outras CSIRT estão muito abertas a ajudar as equipas recém-constituídas no início da sua actividade.

O *Inventory of CERT activities in Europe*¹⁴ [Inventário das actividades CERT na Europa] da ENISA é um ponto de partida muito útil para procurar outras CSIRT existentes no país, ou actividades de cooperação nacional por elas realizadas.

Para obter apoio na busca de uma fonte de informações adequada sobre as CSIRT, contacte os peritos CSIRT da ENISA:

CERT-Relations@enisa.europa.eu

¹⁴ Inventário da ENISA: http://www.enisa.europa.eu/cert_inventory/

Apresenta-se, seguidamente, uma panorâmica das actividades da comunidade CSIRT. Consulte o *Inventário* para obter uma descrição mais completa e informações suplementares.

Iniciativa CSIRT Europeia

TF-CSIRT¹⁵

A *Task Force* TF-CSIRT promove a colaboração entre Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) na Europa. Os objectivos principais desta *Task Force* são oferecer um fórum para o intercâmbio de experiências e conhecimentos, criar serviços-piloto para a comunidade de CSIRT europeias e ajudar a constituir novas CSIRT.

A *Task Force* tem como principais objectivos:

- Oferecer um fórum para o intercâmbio de experiências e conhecimentos
- Criar serviços-piloto para a comunidade de CSIRT europeias
- Promover normas e procedimentos comuns para responder aos incidentes de segurança
- Ajudar a constituir novas CSIRT e a dar formação ao seu pessoal.
- As actividades da TF-CSIRT estão centradas na Europa e nos países vizinhos, em conformidade com o mandato aprovado pelo comité técnico TERENA, em 15 de Setembro de 2004.

Iniciativa CSIRT Global

FIRST¹⁶

A FIRST é a organização principal e a líder mundial reconhecida no domínio da resposta a incidentes. A adesão à FIRST permite que as equipas de resposta a incidentes reajam aos incidentes de segurança de forma mais eficaz – tanto reactiva como pró-activa.

A FIRST congrega várias equipas de resposta a incidentes de segurança informática pertencentes a organizações governamentais, comerciais e educativas. Tem o intuito de fomentar a cooperação e a coordenação na prevenção de incidentes, estimular uma reacção rápida a estes últimos e promover a partilha de informações entre os seus membros e a comunidade em geral.

Para além da rede por si constituída na comunidade mundial de resposta a incidentes, a FIRST também presta serviços de valor acrescentado.

CSIRT fictícia (etapa 6)

Busca de cooperação

Utilizando o Inventário da ENISA, depressa se encontraram e contactaram algumas CSIRT do mesmo país. Combinou-se uma visita do chefe de equipa recém-contratado às instalações de uma delas, onde foi informado a respeito das iniciativas das CSIRT nacionais e participou numa reunião.

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

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

Esta reunião foi extremamente útil para recolher exemplos de métodos de trabalho e obter apoio de outras equipas.

7 Promoção do Plano de Actividades

Até agora, demos os seguintes passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora.
4. Análise do ambiente e dos utilizadores.
5. Definição da missão.
6. Desenvolvimento do Plano de Actividades.
 - a. Definição do modelo financeiro
 - b. Definição da estrutura organizativa
 - c. Início da contratação de pessoal
 - d. Utilização e equipamento das instalações
 - e. Formulação de uma política de segurança informática
 - f. Busca de parceiros de cooperação

>> A etapa seguinte é traduzir os passos anteriores num plano de projecto e começar!

Uma boa forma de começar a definir o seu projecto é formular uma fundamentação empresarial, que servirá de base ao plano de projecto, bem como para pedir o apoio da administração e obter recursos orçamentais ou de outro tipo.

É conveniente manter a administração permanentemente informada para que a sua sensibilização para os problemas de segurança informática não diminua e, consequentemente, continue a apoiar a própria CSIRT.

A fundamentação empresarial começa pela análise dos problemas e oportunidades, com base num modelo de análise descrito no capítulo *5.3 Análise da Comunidade Utilizadora*, e pela busca de um estreito contacto com os potenciais utilizadores.

Como já foi referido, há muitos aspectos a considerar quando se cria uma CSIRT. É melhor ajustar os materiais atrás mencionados às necessidades das CSIRT, à medida que estas se desenvolvem.

Ao informar a administração, é aconselhável apresentar argumentos tão actualizados quanto possível, recorrendo a artigos recentemente publicados na imprensa ou na Internet, e explicar por que razão o serviço da CSIRT e a coordenação interna dos incidentes são cruciais para proteger os activos da empresa. É igualmente necessário esclarecer que, em questões de segurança informática, só um apoio contínuo pode assegurar a estabilidade, sobretudo no caso de empresas ou instituições dependentes da informática.

(Uma frase notável de Bruce Schneier sintetiza bem esta questão: “A segurança não é um produto, mas sim um processo”¹⁷!)

Um conhecido instrumento para ilustrar os problemas de segurança é o gráfico seguinte, fornecido pelo CERT/CC:

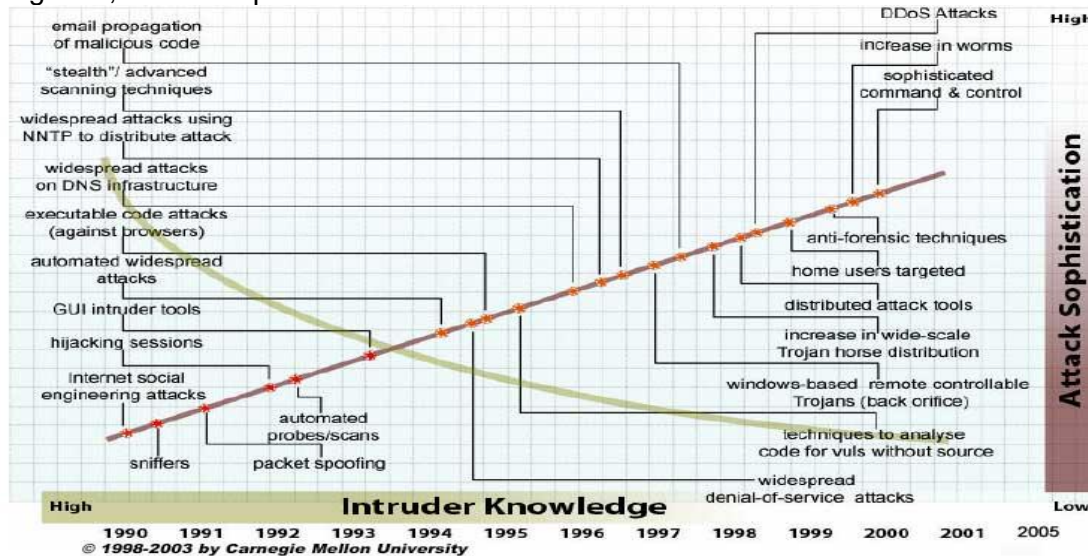


Fig. 8 Conhecimentos do intruso versus sofisticação do ataque (fonte CERT-CC¹⁸)

Propagação de código malévolo por correio electrónico			Ataques DDOS	Elevada
Ataque furtivo/técnicas de exploração avançadas			Aumento dos "vermes"	Sofisticação do ataque
Ataques generalizados utilizando o NNTP (Network News Transfer Protocol) para os distribuir			Comando e controlo sofisticado	Baixa
Ataques generalizados na infra-estrutura DNS			Técnicas anti-forenses	
Ataques de código executável (contra programas de navegação)			Utilizadores residenciais tomados como alvo	
Ataques generalizados automáticos			Ferramentas de ataque distribuído	
Ferramentas de intrusão GUI			Aumento da distribuição de cavalos de Tróia em larga escala	
Sessões de pirataria			Cavalos de Tróia	

¹⁷ Bruce Schneier: <http://www.schneier.com/>

¹⁸ <http://www.cert.org/archive/pdf/info-sec-ip.pdf>

			baseados no Windows e controlados remotamente	
Ataques de engenharia social pela Internet	Sondas/exploradores automáticos		Técnicas para analisar código para vulnerabilidades sem fonte	
<i>Sniffers</i> (interceptores de comunicações)	<i>Spoofing</i> (adopção da identidade de outrem) por pacotes		Ataques generalizados de negação de serviço	
Elevados		Conhecimentos do intruso		Baixos

Este gráfico permite visualizar as tendências em matéria de segurança informática, designadamente a diminuição das competências necessárias para levar a cabo ataques cada vez mais sofisticados.

Outro aspecto a mencionar é o período cada vez mais curto entre a disponibilização de actualizações do *software* para corrigir as vulnerabilidades e o início dos ataques contra elas:

Correcção	->	Ritmo de propagação	
Exploração			
Nimda:	11 meses	Code red:	Dias
Slammer:	6 meses	Nimda:	Horas
Nachi:	5 meses	Slammer:	Minutos
Blaster:	3 semanas		
Witty:	1 dia (!)		

Os dados recolhidos sobre os incidentes, as eventuais melhorias e as lições aprendidas também podem servir de base a uma boa apresentação.

7.1 Descrição dos planos de actividades e dos factores de motivação da administração

Uma apresentação que se limite a promover a CSIRT não basta como fundamentação empresarial, mas, se for realizada da forma adequada, suscitará, na maioria dos casos, o apoio da administração à CSIRT. A fundamentação empresarial, em contrapartida, não deve ser apenas encarada como um exercício de gestão, mas sim igualmente utilizada na comunicação com a equipa e a comunidade utilizadora. O termo “fundamentação empresarial” pode parecer muito comercial e alheado da prática quotidiana da CSIRT, mas permite centrar e direccionar bem os esforços no processo de constituição de uma CSIRT.

As respostas às seguintes perguntas podem ser usadas para formular uma boa fundamentação empresarial (os exemplos apresentados são hipotéticos e apenas usados a título ilustrativo). As “verdadeiras” respostas dependem muito das circunstâncias “reais”).

- Qual é o problema?
- Que objectivos gostaria de atingir com a sua comunidade utilizadora?
- O que acontecerá se não fizer nada?
- O que acontecerá se tomar medidas?
- Quanto irá custar?
- O que se irá ganhar?
- Quando irá começar e quanto estará concluído?

Qual é o problema?

De um modo geral, a ideia de criar uma CSIRT surge quando a segurança informática se tornou uma parte essencial da actividade principal de uma empresa ou instituição e quando os incidentes de segurança começam a constituir um risco empresarial, tornando as actividades de segurança numa operação normal da empresa.

A maioria das empresas ou instituições dispõe de um departamento de apoio regular ou de um serviço de assistência, mas geralmente os incidentes de segurança são geridos de forma insuficiente e menos estruturada do que deviam. Normalmente, a área dos incidentes de segurança exige competências e atenção especiais. Dispor de uma abordagem mais estruturada também é benéfico e diminuirá os riscos e prejuízos para a empresa.

O problema, na maior parte dos casos, é a falta de coordenação e a não utilização dos conhecimentos existentes para gerir os incidentes, o que poderia impedi-los de voltar a acontecer e evitaria eventuais perdas financeiras e/ou danos para a reputação de uma instituição.

Quais os objectivos a alcançar em relação à comunidade utilizadora?

Como já foi dito, a sua CSIRT servirá a respectiva comunidade utilizadora e ajudá-la-á a resolver incidentes e problemas de segurança informática. Aumentar o nível de conhecimentos nesta matéria e implantar uma cultura sensível às questões de segurança são objectivos adicionais.

Trata-se de uma cultura que procura adoptar medidas proactivas e preventivas desde o início e reduzir, assim, os custos operacionais.

A introdução desta cultura de cooperação e assistência numa empresa ou instituição poderá, na maioria dos casos, estimular a eficiência em geral.

O que acontecerá se nada se fizer?

Gerir a segurança informática de forma não estruturada pode causar maiores prejuízos, nomeadamente à reputação da instituição. Perdas financeiras e consequências legais podem ser outros resultados.

O que acontecerá se forem tomadas medidas?

A sensibilização para a ocorrência de problemas de segurança aumenta, o que ajuda a resolvê-los com mais eficiência e a evitar perdas futuras.

Quanto irá custar?

Consoante o modelo organizativo, implicará custos com as remunerações dos membros da equipa CSIRT e com a organização, os equipamentos, as ferramentas e as licenças de software.

O que se irá ganhar?

Dependendo da empresa e das perdas sofridas no passado, ganhar-se-á maior transparência nos procedimentos e nas práticas de segurança, protegendo deste modos activos essenciais da empresa.

Quanto tempo demora?

Ver no capítulo 12. *Descrição do Plano de Projecto* um exemplo deste tipo de plano.

Exemplos de casos e abordagens existentes

Eis alguns exemplos de projectos empresariais CSIRT que merecem ser estudados:

- http://www.cert.org/csirts/AFI_case-study.html
Criação de uma CSIRT de Instituição Financeira: Um estudo de caso

Este documento pretende partilhar as lições aprendidas por uma instituição financeira (denominada AFI no documento), à medida que se foi desenvolvendo e implementando um plano para solucionar as preocupações de segurança e uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT).
- <http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>
Resumo do caso da CERT POLSKA (apresentação de diapositivos em formato PDF).
- <http://www.auscert.org.au/render.html?it=2252>
A constituição de uma Equipa de Resposta a Incidentes, na década de 1990, pode ser uma tarefa arrojada, já que muitas das pessoas que a formam não têm qualquer experiência neste campo. Este documento examina o papel que uma equipa de resposta a incidentes pode desempenhar na comunidade e as questões a abordar

quer durante a sua formação, quer depois de iniciar as operações. Poderá ser útil às equipas de resposta a incidentes existentes, chamando eventualmente a atenção para questões que não tenham sido abordadas anteriormente.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
Estudo de caso sobre segurança informática, proteger a empresa (Case Study in Information Security, Securing the Enterprise), de Roger Benton

Trata-se de um estudo de caso prático da migração de uma companhia de seguros para um sistema de segurança a nível de toda a empresa. Este documento pretende indicar um caminho a seguir quando se cria ou migra para um sistema de segurança. Inicialmente, o único mecanismo de controlo do acesso aos dados da companhia era um sistema primitivo de segurança em linha. A exposição ao risco era grave pois não existiam controlos da integridade fora do ambiente em linha. Qualquer pessoa com competências básicas de programação podia acrescentar, mudar e/ou apagar dados de produção.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
Marriott's e-security strategy: business-IT collaboration (Estratégia de segurança electrónica da Marriott: colaboração informática empresarial)

A experiência da Marriott International, Inc.'s Chris Zoladz em matéria de segurança do comércio electrónico é um processo, não um projecto. Foi esta a mensagem que Zoladz transmitiu nas recentes conferência e exposição sobre segurança electrónica realizadas em Boston com o patrocínio do Intermedia Group. Enquanto vice-presidente para a protecção da informação da Marriott, Zoladz apresenta os seus relatórios através do departamento jurídico, embora não seja jurista. A sua função é identificar onde estão armazenadas as informações empresariais mais valiosas da Marriott e como entram e saem da empresa. A Marriott estabeleceu uma responsabilidade distinta em relação à infra-estrutura técnica em que a segurança assenta, confiando-a ao arquitecto de segurança informática.

CSIRT fictícia (etapa 7)

Promoção do Plano de Actividades

Decidiu-se recolher factos e números sobre a história da empresa, que são extremamente úteis para obter uma perspectiva estatística do estado da segurança informática. Esta recolha deverá prosseguir quando a CSIRT estiver estabelecida e a funcionar, a fim de manter as estatísticas actualizadas.

Outras CSIRT nacionais foram contactadas e entrevistadas a respeito dos seus casos, tendo dado apoio mediante a compilação de diapositivos com informações sobre os incidentes de segurança informática mais recentes e os respectivos custos.

Neste exemplo de CSIRT fictícia, não havia uma necessidade premente de convencer a administração da importância da actividade informática e, por isso, não foi difícil obter luz verde para a primeira fase. Procedeu-se à elaboração da fundamentação empresarial e do plano de projecto, incluindo uma estimativa dos custos de arranque e dos custos de funcionamento.

8 Exemplos de procedimentos operacionais e técnicos (fluxos de trabalho)

Até agora, demos os seguintes passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora.
4. Análise do ambiente e dos utilizadores.
5. Definição da missão.
6. Desenvolvimento do Plano de Actividades.
 - a. Definição do modelo financeiro.
 - b. Definição da estrutura organizativa.
 - c. Início da contratação de pessoal.
 - d. Utilização e equipamento das instalações.
 - e. Formulação de uma política de segurança informática.
 - f. Busca de parceiros de cooperação.
7. Promoção do Plano de Actividades.
 - a. Fazer aprovar a fundamentação empresarial.
 - b. Inserir tudo num plano de projecto.

>> A próxima etapa é: tornar a CSIRT operacional

Uma boa definição dos fluxos de trabalho irá melhorar a qualidade e o tempo necessário para cada incidente ou caso de vulnerabilidade.

Como foi descrito nas caixas de exemplos, a CSIRT fictícia prestará os serviços CSIRT básicos essenciais:

- Alertas e avisos
- Gestão de incidentes
- Comunicações

O presente capítulo apresenta exemplos de fluxos de trabalho que descrevem os serviços essenciais de uma CSIRT. Contém também informações sobre a recolha de informações a partir de diversas fontes, a verificação da sua pertinência e autenticidade, e a sua redistribuição para a comunidade utilizadora. Por último, inclui exemplos dos procedimentos mais básicos e das ferramentas CSIRT específicas.

8.1 Avaliar as instalações existentes na comunidade utilizadora

A primeira etapa consiste em fazer um inventário dos sistemas informáticos instalados na sua comunidade utilizadora. Deste modo, a CSIRT pode avaliar a pertinência da informação que chega e filtrá-la antes de a redistribuir, para que os utilizadores não fiquem submersos em informações que lhes são basicamente inúteis.

É conveniente começar de forma simples, por exemplo utilizando uma folha Excel como a seguinte:

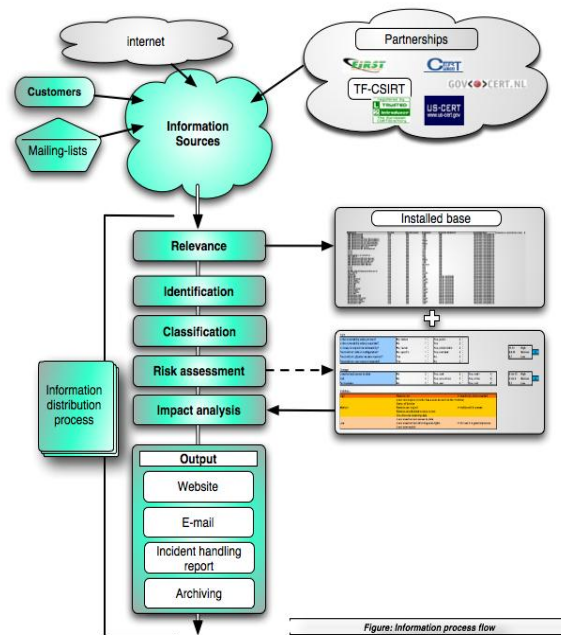
Categoria	Aplicação	Produto de Software	Versão	SO	Versão SO	Utilizador
Computador	Office	Excel	x-x-x	Microsoft	XP-prof	A
Computador	Navegador	IE	x-x-	Microsoft	XP-prof	A
Rede	Encaminha dor	CISCO	x-x-x	CISCO	x-x-x-	B
Servidor	Servidor	Linux	x-x-x	L-distro	x-x-x	B
Serviços	Servidor Web	Apache		Unix	x-x-x	B

Com a função de filtro em Excel é muito fácil escolher o *software* adequado e ver que tipo de *software* utiliza cada um dos utilizadores.

8.2 Produzir Alertas, Avisos e Comunicações

A produção de alertas, avisos e comunicações segue os mesmos fluxos de trabalho:

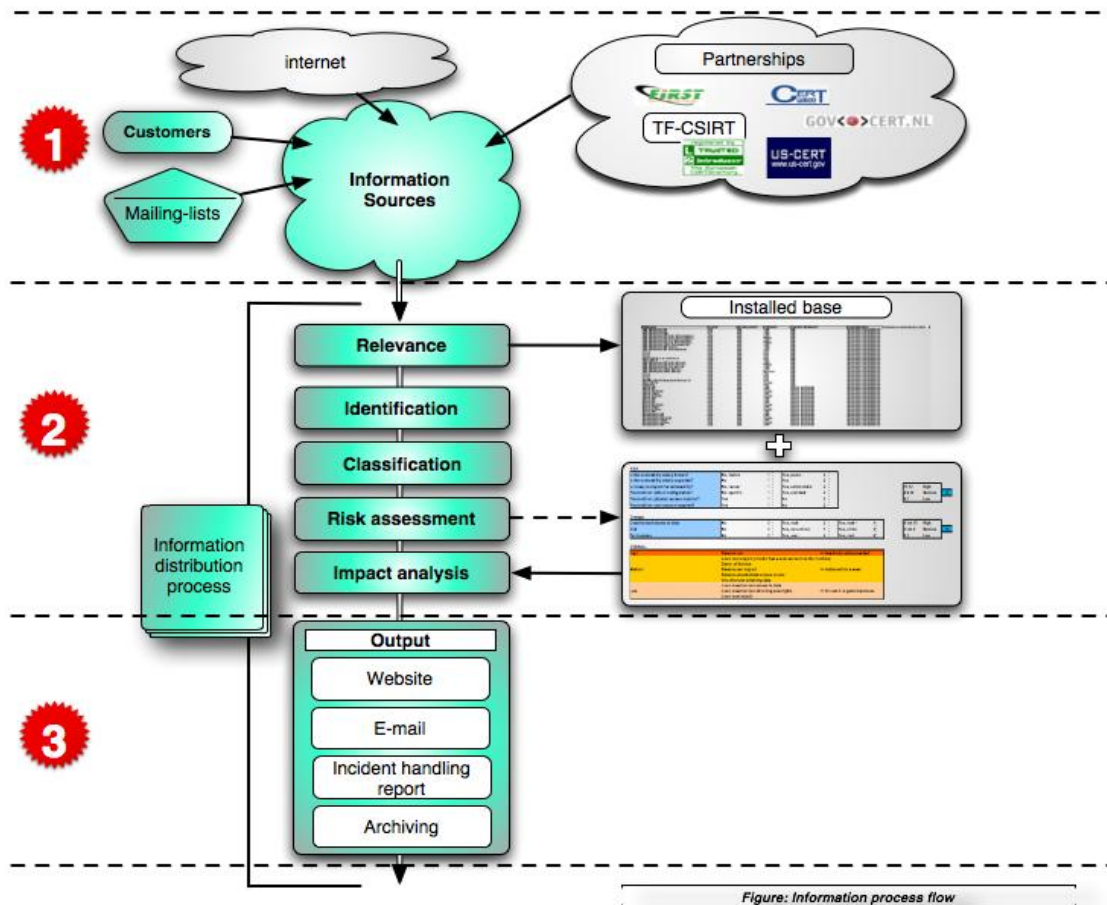
- Recolha de informação
- Avaliação da pertinência da informação e da sua fonte
- Avaliação dos riscos com base nas informações recolhidas
- Distribuição da informação



	Internet	Parcerias
Cientes	Fontes de informação	
Sistemas de lista de distribuição	Pertinência	Base instalada
	Identificação	
	Classificação	
Processo de distribuição da informação	Avaliação dos riscos	
	Análise do impacto	
	Produtos	
	Website	
	Correio electrónico	
	Relatório de gestão do incidente	
	Arquivo	Figura: Fluxo do processo de informação

Fig. 9 : Fluxo do processo de informação

Nos parágrafos seguintes, este fluxo de trabalho será descrito em mais pormenor.



1 Etapa 1: Recolha de informações sobre as vulnerabilidades.

Normalmente, existem dois tipos principais de fontes de informação que fornecem informações úteis para os serviços:

- Informações relativas à vulnerabilidade dos (seus) sistemas informáticos
- Notificações de incidentes

Dependendo do tipo de empresa e de infra-estrutura informática, há muitas fontes públicas e fechadas de informações sobre as vulnerabilidades:

- Sistemas de lista de distribuição públicos e fechados
- Informações sobre a vulnerabilidade dos produtos provenientes das empresas que os vendem
- Websites
- Informações publicadas na Internet (Google, etc...)

- Parcerias públicas e privadas que fornecem informações sobre as vulnerabilidades (FIRST, TF-CSIRT, CERT-CC, US-CERT....)

Todas estas informações aumentam o nível de conhecimento sobre as vulnerabilidades específicas dos sistemas informáticos.

Como se disse, há muitas fontes de informações de segurança úteis e de fácil acesso disponíveis na Internet. O grupo de trabalho ad-hoc da ENISA “Serviços CERT” para 2006 está a elaborar, no momento da redacção do presente documento, uma lista mais completa que deverá estar pronta no final de 2006¹⁹.



Etapa 2: Análise da informação e avaliação do risco

Esta etapa produzirá uma análise do impacto de uma vulnerabilidade específica para a infra-estrutura informática da comunidade utilizadora.

Identificação

As informações sobre vulnerabilidades recebidas têm de ser sempre identificadas pela sua fonte, sendo necessário determinar se esta é fiável antes de transmitir quaisquer informações à comunidade utilizadora. De outro modo, as pessoas poderiam receber alertas falsos, que perturbariam desnecessariamente o funcionamento das empresas e acabariam por prejudicar a reputação das CSIRT.

¹⁹ GT ad-hoc Serviços CERT: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Apresenta-se, seguidamente, um exemplo de identificação da autenticidade de uma mensagem:

Procedimento para identificar a autenticidade de uma mensagem e a sua fonte

Lista de verificação geral

1. A fonte é conhecida e está registada como tal?
2. A informação chega através de um canal normal?
3. Há algum conteúdo informativo “estranho” que “soe a falso”?
4. Siga a sua intuição, em caso de dúvida sobre uma informação, não aja sem a verificar novamente!

Correio electrónico – Fontes

1. O endereço da fonte é conhecido da organização e consta da lista de fontes?
2. A assinatura PGP está correcta?
3. Em caso de dúvida verifique os cabeçalhos completos de uma mensagem.
4. Em caso de dúvida, utilize “nslookup” ou “dig” para verificar o domínio do remetente²⁰.

WWW – Fontes

1. Verifique os certificados do programa de navegação quando se ligar a um *website* protegido (https://).
2. Verifique o conteúdo e a validade (técnica) da fonte.
3. Em caso de dúvida, não clique em nenhuma ligação nem descarregue qualquer software.
4. Em caso de dúvida, faça “lookup” e “dig” no domínio e efectue um “traceroute” (localizar determinado IP).

Telefone

1. Escute atentamente o nome.
2. Reconhece a voz?
3. Em caso de dúvida, peça o número de telefone e diga à pessoa que lhe telefonou que lhe ligará de volta.

Fig. 10 Exemplo de um procedimento de identificação da informação

Pertinência

O inventário, já realizado, do *hardware* e do *software* instalados pode ser usado para filtrar a informação de vulnerabilidade recebida no que respeita à pertinência, com o objectivo de encontrar resposta para as perguntas: “A comunidade utilizadora usa este *software*?”; “Esta informação será pertinente para ela?”

Classificação

Algumas informações recebidas podem ser classificadas ou etiquetadas como reservadas (por exemplo, as notificações de incidentes enviadas por outras equipas). Todas as informações devem ser tratadas de acordo com o pedido do remetente e com

²⁰ Ferramentas para verificar as identificações no CHIHT:

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

a sua própria política de segurança informática. Uma boa regra básica é: *“Não distribua informações se não tiver a certeza de que elas devem ser distribuídas; em caso de dúvida, peça autorização ao remetente para o fazer.”*

Avaliação dos riscos e análise do impacto

Há vários métodos para determinar o risco e o impacto de uma (potencial) vulnerabilidade.

Entende-se por risco a possibilidade de a vulnerabilidade vir a ser explorada. Há vários factores importantes (entre outros):

- A vulnerabilidade é muito conhecida?
- A vulnerabilidade é generalizada?
- É fácil explorar a vulnerabilidade?
- É uma vulnerabilidade susceptível de ser explorada remotamente?

Todas estas perguntas dão uma boa indicação da gravidade da vulnerabilidade. Um método muito simples para calcular o risco é a fórmula seguinte:

$\text{Impacto} = \text{Risco} \times \text{Dano potencial}$
--

O dano potencial poderá ser

- O acesso não autorizado aos dados
- A negação de serviço (DOS)
- A obtenção ou extensão de autorizações

(Ver sistemas de classificação mais elaborados no fim do capítulo).

Uma vez respondidas estas perguntas, pode acrescentar-se uma classificação global ao aviso, informando acerca dos riscos e danos potenciais. São frequentemente usados termos simples como BAIXO, MÉDIO e ELEVADO.

Outros sistemas de avaliação dos riscos mais exaustivos são os seguintes:

Sistema de classificação da GOVCERT.NL²¹

A CSIRT governamental neerlandesa GOVCERT.NL, na sua fase inicial, desenvolveu uma matriz para a avaliação dos riscos que se mantém actualizada segundo as tendências mais recentes.

RISK					
Is the vulnerability widely known?	No, limited	1	Yes, public	2	
Is the vulnerability widely exploited?	No	1	Yes	2	
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2	
Precondition: default configuration?	No, specific	1	Yes, standard	2	
Precondition: physical access required?	Yes	1	No	2	
Precondition: user account required?	Yes	1	No	2	

11,12	High
8,9,10	Medium
6,7	Low

0

Damage						
Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4
DoS	No	0	Yes, non-critical	1	Yes, critical	5
Permissions	No	0	Yes, user	4	Yes, root	6

6 t/m 15	High
2 t/m 5	Medium
0,1	Low

0

OVERALL		
High	Remote root	>> Immediately action needed!
	Local root exploit (attacker has a user account on the machine)	
	Denial of Service	
Medium	Remote user exploit	>> Action within a week
	Remote unauthorized access to data	
	Unauthorized obtaining data	
	Local unauthorized access to data	
Low	Local unauthorized obtaining user-rights	>> Include it in general process
	Local user exploit	

Fig. 11 Sistema de classificação da GOVCERT.NL

RISCO			11, 12 8, 9, 10 6,7	Elevado Médio Baixo
A vulnerabilidade é muito conhecida?	Não, pouco	Sim, pública		
A vulnerabilidade é muito explorada?	Não	Sim		
É fácil explorar a vulnerabilidade?	Não, pirata	Sim, <i>script kiddie</i>		
Pré-condição: configuração por defeito?	Não, específica	Não, normal		
Pré-condição: é necessário acesso físico?	Sim	Não		
Pré-condição: é necessária conta de utilizador?	Sim	Não		
DANOS				
Acesso não autorizado a dados	Não	Sim, ler		Sim, ler
Negação de serviço	Não	Sim, não crítico		Sim, crítico
Autorizações	Não	Sim, utilizador		Sim, raiz
GLOBAL				
Alto	Raiz remota	São necessárias medidas imediatas!		
Médio	Exploração da raiz local (o atacante tem uma conta de utilizador na máquina)	Medidas dentro de uma semana		
	Negação de serviço			
	Exploração de utilizador remoto			
	Acesso remoto não autorizado aos dados			
	Obtenção não autorizada de dados			
Baixo	Acesso local não autorizado a dados	Incluir no processo geral		
	Obtenção local não autorizada de direitos de utilizador			
	Exploração de utilizador local			

²¹ Matriz de vulnerabilidade: <http://www.govcert.nl/download.html?f=33>

Descrição do Formato de Aviso Comum do EISPP (Common Advisory Format Description)²²

O Programa Europeu de Promoção de Segurança Informática (European Information Security Promotion Programme - EISPP) é um projecto co-financiado pela Comunidade Europeia no âmbito do Quinto Programa-Quadro. O projecto EISPP pretende desenvolver um quadro europeu, não só para partilhar conhecimentos de segurança mas também para definir o conteúdo e as formas de difundir informações de segurança junto das PME. Se às PME europeias forem fornecidos os serviços de segurança informática necessários, elas sentir-se-ão estimuladas a desenvolver a sua confiança e a utilizar mais intensamente o comércio electrónico, o que aumentará e melhorará as oportunidades de negócio. O EISPP é pioneiro na visão da Comissão Europeia de formar uma rede europeia de peritos na União Europeia.

Formato de aviso DAF (Deutsches Advisory Format)²³

O DAF é uma iniciativa da CERT-Verbund alemã e um componente essencial da infraestrutura de produção e intercâmbio de recomendações de segurança por diversas equipas. Especialmente adaptado às necessidades das CERT alemãs; a norma é desenvolvida e mantida pela CERT-Bund, a DFN-CERT, a PRESECURE e a Siemens-CERT.

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

3**Etapa 3: Distribuição da informação**

Uma CSIRT pode escolher entre vários métodos de distribuição, consoante os desejos dos utilizadores e a sua estratégia de comunicação.

- Website
- Correio electrónico
- Notificações
- Arquivo e pesquisa

A recomendações de segurança divulgadas por uma CSIRT devem respeitar sempre a mesma estrutura. Isto aumentará a sua legibilidade e o leitor encontrará rapidamente todas as informações pertinentes.

Um aviso deverá conter, no mínimo, as seguintes informações:

Título do aviso
Número de referência
Sistemas afectados - -
SO associado + versão
Risco (Elevado-Médio-Baixo)
Impacto/dano potencial (Elevado-Médio-Baixo)
Identificação externa: (CVE, Identificação do boletim de vulnerabilidade)
Síntese da vulnerabilidade
Impacto
Solução
Descrição (detalhes)
Anexo

Fig. 12 Exemplo de esquema de aviso

Ver no capítulo 10. *Exercício* um exemplo completo de aviso de segurança.

8.3 Procedimento de gestão de incidentes

Como foi dito na introdução do presente capítulo, o processo de gestão da informação durante a gestão de um incidente é muito semelhante ao utilizado na compilação de alertas, avisos e comunicações. Porém, a parte de recolha de informação é habitualmente diferente, visto que os dados relativos a incidentes são normalmente obtidos por meio de notificações de incidentes enviadas pela comunidade utilizadora ou por outras equipas, ou da recepção de *feedback* das partes envolvidas no processo de gestão do incidente. As informações circulam geralmente por correio electrónico (cifrado); por vezes, é necessário utilizar o telefone ou o fax.

Quando se recebem informações pelo telefone, é conveniente tomar imediatamente nota dos mais ínfimos pormenores, recorrendo a uma ferramenta de gestão/notificação de incidentes ou elaborando um memorando. É necessário atribuir logo (antes de a chamada terminar) um número ao incidente (se ainda não existir nenhum para este incidente) e comunicá-lo à pessoa que está em linha (podendo também fazê-lo numa mensagem de correio electrónico posterior, a resumir o incidente) como referência para posteriores contactos.

O resto do presente capítulo descreve o processo básico de gestão de incidentes. Na documentação do CERT/CC *Definição de processos de gestão de incidentes para as CSIRT²⁴* poderá encontrar uma análise muito aprofundada de todo o processo, bem como dos fluxos e subfluxos de trabalho envolvidos.

²⁴ Defining Incident Management Processes: <http://www.cert.org/archive/pdf/04tr015.pdf>

Essencialmente, a gestão de incidentes obedece ao seguinte fluxo de trabalho:

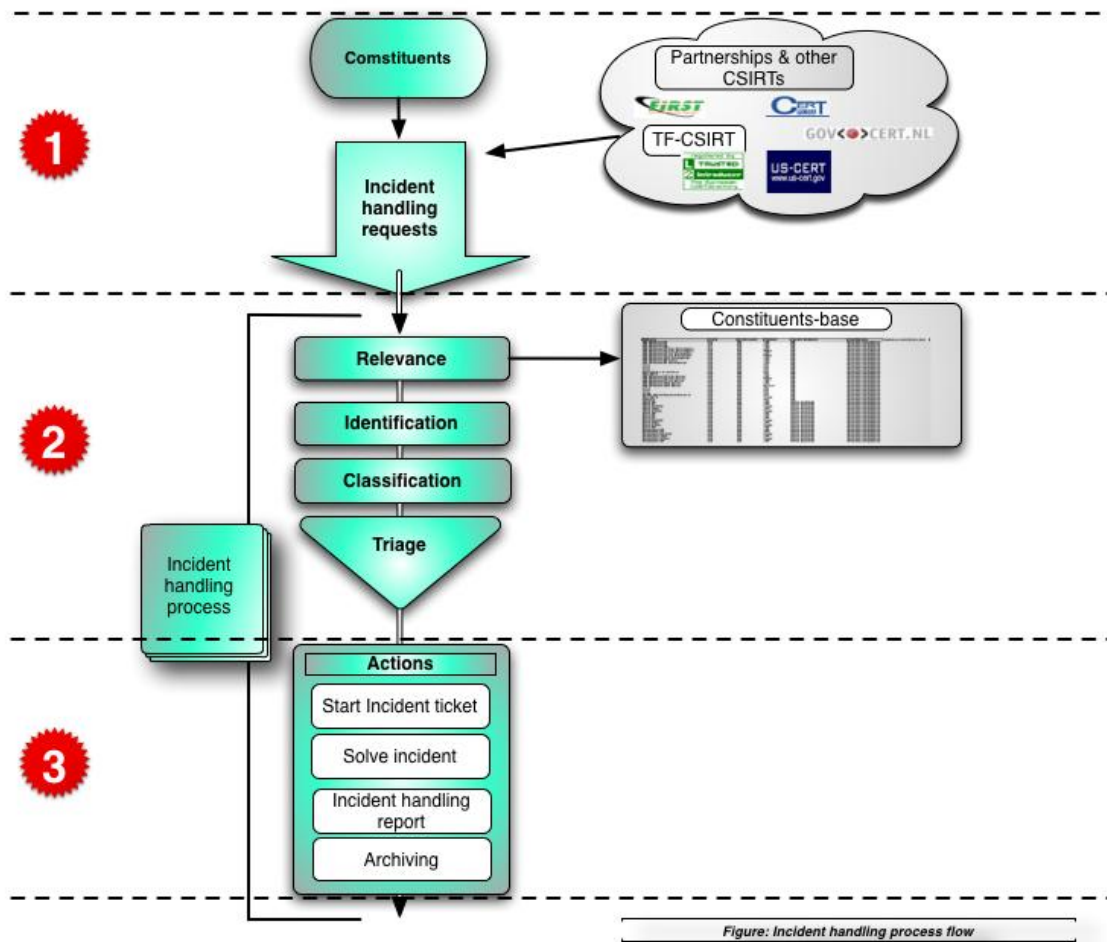


Fig. 13 Fluxo processual dos incidentes

	Utilizadores	Parcerias e outras CSIRT
	Pedidos de gestão de incidentes	
	Pertinência	Base de utilizadores
	Identificação	
	Classificação	
Processo de gestão de incidentes	Triagem	
	Ações	
	Iniciar talão de incidente Resolver o incidente Relatório de gestão do incidente Arquivo	Figura: Fluxo processual dos incidentes

1**Etapa 1: Recepção de notificações de incidentes**

Como já foi dito, as notificações de incidentes chegam a uma CSIRT através de vários canais, sobretudo por correio electrónico, mas também por telefone ou por fax.

Como foi mencionado, é boa prática tomar nota de todos os pormenores, em formato uniforme, quando recebe a notificação de um incidente, para garantir que não são esquecidas informações cruciais. Encontrará, seguidamente, um esquema exemplificativo:

FORMULÁRIO DE NOTIFICAÇÃO DE INCIDENTES	
<i>Preencha este formulário e envie-o por Fax ou correio electrónico para:</i> <i>As linhas assinaladas com asterisco * são de preenchimento obrigatório.</i>	
<i>Nome e Organização</i>	
1.	Nome*:
2.	Nome da Organização*:
3.	Tipo de sector:
4.	País*:
5.	Cidade:
6.	Endereço de correio electrónico*:
7.	Número de telefone*:
8.	Outros:
<i>Computadores centrais afectados</i>	
9.	Número de computadores centrais:
10.	Nome e IP do computador central*:
11.	Função do computador central*:
12.	Fuso horário:
13.	<i>Hardware:</i>
14.	Sistema operativo:
15.	<i>Software</i> afectado:
16.	Ficheiros afectados:
17.	Segurança:
18.	Nome e IP do computador central:
19.	Protocolo/porta:
<i>Incidente</i>	
20.	Número de referência ref #:
21.	Tipo de incidente:
22.	Início do incidente:
23.	Trata-se de um incidente contínuo: SIM NÃO
24.	Hora e método de detecção:
25.	Vulnerabilidades conhecidas:
26.	Ficheiros suspeitos:
27.	Contra-medidas:
28.	Descrição detalhada*:

Fig. 14 Conteúdo de uma notificação de incidente

2

Etapa 2: Avaliação do incidente

Durante esta etapa, a autenticidade e a pertinência de um incidente notificado são verificadas e o incidente classificado.

Identificação

Para evitar qualquer acção desnecessária, é bom hábito verificar se o autor da notificação é digno de confiança e se faz parte da sua comunidade utilizadora ou da comunidade utilizadora de outras CSIRT. São aplicáveis regras semelhantes às descritas no capítulo 8.2 *Produção de alertas*.

Pertinência

Nesta etapa, verifica-se se o pedido de gestão de incidente tem origem na comunidade utilizadora da CSIRT, ou se o incidente notificado envolve sistemas informáticos da comunidade utilizadora. Se nenhum dos casos for aplicável, o relatório é geralmente reencaminhado para a CSIRT certa²⁵.

Classificação

Nesta etapa, a triagem é preparada mediante a classificação da gravidade do incidente. A descrição pormenorizada da classificação de incidentes está fora do âmbito do presente documento. Um bom começo é utilizar o sistema de Classificação de Casos CSIRT (Exemplo para a CSIRT empresarial):

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	<ul style="list-style-type: none"> DOS or DDOS attack.
Forensics	S1	<ul style="list-style-type: none"> Any forensic work to be done by CSIRT.
Compromised Information	S1	<ul style="list-style-type: none"> Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	<ul style="list-style-type: none"> Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	<ul style="list-style-type: none"> Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	<ul style="list-style-type: none"> 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.

²⁵ Ferramentas para verificar as identificações no CHIHT:

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

Fig. 15 Sistema de classificação de incidentes (fonte: FIRST)²⁶

Categorias de Incidente

Todos os incidentes geridos pela CSIRT devem ser classificados numa das categorias enumeradas no quadro seguinte.

Categoria de incidente	Sensibilidade*	Descrição
Negação de serviço	S3	Ataque DOS ou DDOS.
Forense	S1	Qualquer trabalho forense a efectuar pela CSIRT.
Informação comprometida	S1	Destruição, corrupção ou divulgação de informações empresariais sensíveis ou de propriedade intelectual, tentadas ou concretizadas
Activo comprometido	S1, S2	Computador central comprometido (conta raiz, cavalo de Tróia, <i>rootkit</i>), dispositivo de rede, aplicação, conta de utilizador. Isto inclui computadores centrais infectados com <i>malware</i> em que um atacante controla activamente o computador central.
Actividade ilegal	S1	Roubo/ Fraude/ Segurança Humana /Pornografia infantil. Incidentes informáticos de natureza criminosa, susceptíveis de infringir a lei, investigações globais ou prevenção de perdas.
Pirataria interna	S1,S2,S3	Acção de reconhecimento ou actividade suspeita com origem no interior da rede da empresa, excluindo <i>malware</i> .
Pirataria externa	S1,S2,S3	Acção de reconhecimento ou actividade suspeita com origem no exterior da rede da empresa (rede de parceiros, Internet), excluindo <i>malware</i> .
<i>Malware</i>	S3	Um vírus ou verme que afecta normalmente múltiplos dispositivos empresariais. Não inclui computadores centrais comprometidos alvos de controlo activo por um atacante através de <i>backdoor</i> ou cavalo de Tróia (ver Activo comprometido).
Correio electrónico	S3	Correio electrónico com identidade alterada, SPAM e outros eventos relacionados com a segurança do correio electrónico.
Consultoria	S1,S2,S3	Consultoria de segurança não relacionada com nenhum incidente confirmado.
Violações de política	S1,S2,S3	Partilha de material ofensivo, partilha/posse de material sujeito a direitos de autor. Violação deliberada da política Infosec. Utilização inadequada de um activo da empresa, como um computador, uma rede ou uma aplicação. Escalada não autorizada de privilégios ou tentativa deliberada de subverter os controlos de acesso.

* A sensibilidade varia em função das circunstâncias. São fornecidas orientações.

Triagem

A triagem é um sistema utilizado pelo pessoal médico ou das urgências para racionar recursos médicos limitados, quando o número de feridos necessitados de cuidados excede os recursos disponíveis para prestar assistência, de modo a tratar o maior número de doentes possível²⁷.

O CERT/CC apresenta a seguinte descrição:

²⁶ Classificação de Casos CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

²⁷ Triagem na Wikipedia: <http://en.wikipedia.org/wiki/Triage>

A triagem é um elemento essencial de qualquer capacidade de gestão de incidentes, em especial para qualquer CSIRT estabelecida. A triagem é essencial para compreender o que está a ser notificado em toda a organização. Serve de veículo para fazer fluir todas as informações para um ponto de contacto único, permitindo uma visão empresarial da actividade em curso e uma correlação global de todos os dados comunicados. A triagem permite fazer a avaliação inicial de uma notificação recebida e coloca-a em lista de espera para tratamento futuro. Também constitui um meio para iniciar a documentação e a introdução de dados de uma notificação ou pedido, se tal não tiver já sido feito no processo de detecção.

A função triagem dá uma imagem imediata do estado actual de todas as actividades notificadas — que notificações são abertas ou fechadas, que acções estão pendentes, e quantas notificações de cada tipo foram recebidas. Este processo pode ajudar a identificar eventuais problemas de segurança e definir prioridades no volume de trabalho. As informações reunidas durante a triagem também podem ser usadas para gerar tendências em matéria de vulnerabilidade e incidentes, bem como estatísticas destinadas à administração²⁸.

A triagem só deverá ser feita pelos membros mais experientes da equipa, porque exige uma compreensão profunda dos potenciais impactos dos incidentes em parcelas específicas da comunidade utilizadora e a capacidade de decidir quem será o melhor membro da equipa para resolver esse incidente.

²⁸ Defining Incident Management Processes [Definição de processos de gestão de incidentes]:

<http://www.cert.org/archive/pdf/04tr015.pdf>



Etapa 3: Acções

Depois da triagem, os incidentes vão para uma fila de espera de pedidos, numa ferramenta de gestão de incidentes usada por um ou mais gestores de incidentes, que seguem essencialmente as etapas seguintes.

Iniciar o talão de incidente

O número do talão de incidente poderá já ter sido gerado numa fase anterior (por exemplo, quando o incidente foi comunicado por via telefónica). Caso contrário, a primeira etapa consiste em criar esse número, que será usado em todos os contactos posteriores respeitantes ao incidente.

Ciclo de vida do incidente

Gerir um incidente não corresponde a uma sucessão de medidas conducentes a uma solução, mas a sim um círculo de medidas que são repetidamente aplicadas até o incidente ficar finalmente resolvido e todas as partes envolvidas terem todas as informações necessárias. Este círculo, também denominado, frequentemente, “ciclo de vida do incidente”, inclui os seguintes processos:

- Análise:* Todos os detalhes do incidente notificado são analisados.
- Obter informação de contacto:* Para poder transmitir outras informações relativas ao incidente a todas as partes envolvidas, designadamente a outras CSIRT, às vítimas e, provavelmente, aos proprietários dos sistemas eventualmente utilizados de forma abusiva para desencadear um ataque.
- Fornecer assistência técnica:* Ajudar as vítimas a recuperarem rapidamente dos resultados do incidente e recolher mais informações sobre o ataque.
- Coordenação:* Informar as outras partes envolvidas, como a CSIRT responsável pelo sistema informático usado num ataque, ou outras vítimas.

Esta estrutura é denominada “ciclo de vida”, porque uma das etapas leva a outra e a última, a parte de coordenação, poderá conduzir a uma nova análise, recomeçando o ciclo. O processo termina quando todas as partes envolvidas tiverem recebido e comunicado todas as informações necessárias.

Veja no manual CSIRT do CERT/CC uma descrição mais pormenorizada do ciclo de vida dos incidentes²⁹.

Relatório da gestão do incidente

Prepare-se para responder a perguntas da administração sobre o incidente compilando um relatório. É sempre aconselhável escrever um documento (apenas para uso interno) sobre as “lições aprendidas” para ensinar o pessoal e evitar que se cometam erros em futuros processos de gestão de incidentes.

²⁹ Manual CSIRT: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Arquivo

Consulte as normas de arquivo anteriormente descritas no capítulo 6.5 *Formulação de uma política de segurança informática*.

Veja na secção A.1 *Outras leituras* do anexo guias exaustivos sobre a gestão de incidentes e o ciclo de vida dos incidentes.

8.4 Exemplo de uma escala horária de resposta

A definição dos tempos de resposta é frequentemente negligenciada, mas deve fazer parte de qualquer Acordo de Nível de Serviço (SLA) correctamente formulado entre uma CSIRT e a sua comunidade utilizadora. Dar um *feedback* oportuno aos utilizadores durante a gestão de um incidente é crucial, tanto para as responsabilidades dos próprios utilizadores como para a reputação da equipa.

Os tempos de resposta devem ser claramente comunicados à comunidade utilizadora para evitar expectativas incorrectas. A escala horária muito básica que apresentamos a seguir pode ser usada como ponto de partida para um Acordo de Nível de Serviço mais pormenorizado com a comunidade utilizadora de uma CSIRT.

Eis o exemplo de uma escala horária de resposta prática, a partir do momento em que é recebido um pedido de assistência:

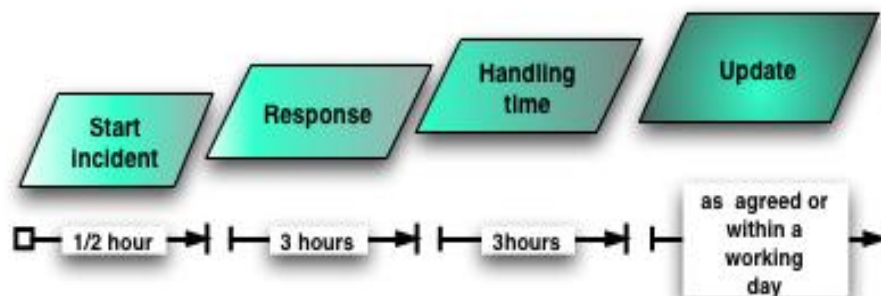


Fig. 16 Exemplo de escala horário de resposta

Iniciar incidente	Resposta	Tempo de gestão	Actualização
½ hora	3 horas	3 horas	Conforme o combinado ou no espaço de um dia útil

Também é uma boa prática instruir a comunidade utilizadora a respeito dos seus próprios tempos de resposta, em especial quando deve contactar a CSIRT em caso de emergência. Na maior parte dos casos, é melhor contactar a respectiva CSIRT numa fase inicial, sendo boa prática incentivar a comunidade utilizadora a fazê-lo em caso de dúvida.

8.5 Ferramentas CSIRT disponíveis

Este capítulo fornece algumas indicações de ferramentas comuns usadas pelas CSIRT. Dá apenas alguns exemplos, podendo encontrar-se mais indicações no *Clearinghouse of Incident Handling Tools*³⁰ (CHIHT).

Software de correio electrónico e cifragem de mensagens

- GNUPG <http://www.gnupg.org/>
O GnuPG é a aplicação completa e gratuita da norma OpenPGP do projecto GNU, definida pelo RFC2440. O GnuPG permite-lhe cifrar e assinar os seus dados e comunicações.
- PGP <http://www.pgp.com/>
Variante comercial

Ferramenta de gestão de incidentes

Administrar os incidentes e o seu acompanhamento, mantendo um registo das acções.

- RTIR <http://www.bestpractical.com/rtir/>
O RTIR é um sistema de gestão de incidentes de fonte aberta, concebido para satisfazer as necessidades das equipas CERT e de outras equipas de resposta a incidentes.

Equipas CRM

Quando tem muitos utilizadores diferentes e necessita de localizar todos os compromissos e informações, é útil dispor de uma base de dados CRM. Há muitas variantes; eis alguns exemplos:

- SugarCRM <http://www.sugarcrm.com/crm/>
- Sugarforce (Versão fonte aberta gratuita) <http://www.sugarforge.org/>

Verificação das informações

- Website watcher <http://www.aignes.com/index.htm>
Este programa vigia as actualizações e alterações introduzidas nos *websites*.
- Watch that page <http://www.watchthatpage.com/>
O serviço envia informações sobre as alterações introduzidas nos *websites* por correio electrónico (a título gratuito e comercialmente).

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

Procurar informações de contacto

Encontrar o contacto correcto para notificar os incidentes não é tarefa simples. É possível recorrer a algumas fontes de informação:

- RIPE³¹
- IRT-object³²
- TI³³

Além disso, o CHIHT enumera algumas ferramentas para procurar informações relativas a contactos³⁴.

CSIRT fictícia (etapa 8)**Criar fluxos processuais e procedimentos operacionais e técnicos**

A CSIRT fictícia concentra esforços na prestação de serviços CSIRT essenciais:

- Alertas e Avisos
- Comunicações
- Gestão de incidentes

A equipa desenvolveu procedimentos que funcionam bem e são fáceis de compreender por todos os membros da equipa. A CSIRT fictícia também contratou um jurista para tratar das responsabilidades e da política de segurança da informação. A equipa adoptou algumas ferramentas eficientes e obteve informações úteis sobre as questões operacionais debatendo-as com outras CSIRT.

Foi elaborado um modelo uniforme para as recomendações de segurança e as notificações de incidentes. A equipa utiliza o RTIR para a gestão de incidentes.

³¹ RIPE whois: <http://www.ripe.net/whois>

³² IRT-object na base de dados RIPE: 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 Ferramentas para verificar as identidades no CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Formação CSIRT

Até agora, demos os seguintes passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora.
4. Análise do ambiente e dos utilizadores.
5. Definição da missão.
6. Desenvolvimento do Plano de Actividades.
 - a. Definição do modelo financeiro.
 - b. Definição da estrutura organizativa.
 - c. Início da contratação de pessoal.
 - d. Utilização e equipamento das instalações.
 - e. Formulação de uma política de segurança informática
 - f. Busca de parceiros de cooperação.
7. Promoção do Plano de Actividades.
 - a. Fazer aprovar a fundamentação empresarial.
 - b. Inserir tudo num plano de projecto.
8. Tornar a CSIRT operacional.
 - a. Criar fluxos de trabalho
 - b. Aplicar as ferramentas CSIRT.

>> A próxima etapa é: dar formação ao pessoal

Este capítulo descreve as duas principais fontes para a formação CSIRT específica: os cursos TRANSITS e CERT/CC.

9.1 TRANSITS

O TRANSITS é um projecto europeu destinado a promover a criação de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) e o reforço das já existentes, através da resolução do problema da falta de pessoal competente. Para isso, ofereceu cursos de formação especializados para o pessoal das (novas) CSIRT que abordam as questões organizativas, operacionais, técnicas, comerciais e jurídicas envolvidas na prestação de serviços CSIRT.

Em particular, o TRANSITS

- desenvolveu, actualizou e reviu regularmente as matérias que compõem os módulos de formação
- organizou *workshops* de formação, em que essas matérias foram administradas
- permitiu que membros do pessoal das (novas) CSIRT participassem nestes *workshops* de formação, com especial destaque para a participação dos novos Estados-Membros da UE

- difundiu os materiais do curso de formação e assegurou a exploração dos resultados³⁵.

A ENISA está a facilitar e a apoiar os cursos TRANSITS. Se quiser saber como se pode candidatar à frequência dos mesmos, bem como os seus requisitos e custos, contacte os peritos CSIRT da ENISA:

CERT-Relations@enisa.europa.eu

Consulte os exemplos de matérias dos cursos no anexo do presente documento!

9.2 CERT/CC

A complexidade das infra-estruturas informáticas e de rede e o desafio colocado pela administração dificultam a gestão adequada da segurança das redes. Os administradores de redes e sistemas não dispõem de pessoal nem de práticas de segurança suficientes para se defenderem dos ataques e minimizarem os danos. Em consequência, há um número crescente de incidentes de segurança informática.

Quando estes incidentes se verificarem, as organizações devem responder de forma rápida e eficaz. Quanto mais depressa uma organização reconhece, analisa e responde a um incidente, melhor pode limitar os danos e diminuir os custos de recuperação. Criar uma equipa de resposta a incidentes de segurança informática (CSIRT) é uma boa forma de assegurar esta capacidade de resposta rápida e ajudar a prevenir futuros incidentes.

O CERT-CC oferece cursos para gestores e pessoal técnico em áreas como a criação e a gestão de equipas de resposta a incidentes de segurança informática (CSIRT), a resposta e a análise de incidentes de segurança, e a melhoria da segurança das redes. Salvo indicação em contrário, todos os cursos são realizados em Pittsburgh, PA. Os membros do nosso pessoal também administram cursos sobre segurança na Universidade Carnegie Mellon.

Cursos CERT/CC disponíveis³⁶ dedicados às CSIRT

Criação de uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT)
Gestão de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT)
Princípios Básicos da Gestão de Incidentes
Gestão Avançada de Incidentes para o Pessoal Técnico

Consulte os exemplos de matérias dos cursos no anexo do presente documento!

CSIRT fictícia (etapa 9)
Formação do pessoal

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

³⁶ Cursos CERT/CC : <http://www.sei.cmu.edu/products/courses>

A CSIRT fictícia decide enviar todo o seu pessoal técnico para os próximos cursos TRANSITS disponíveis. O chefe de equipa frequenta, complementarmente, o curso de *Gestão de CSIRT* do CERT/CC.

10 Exercício: produção de um aviso

Até agora, demos os seguintes passos:

1. Compreender o que é uma CSIRT e que benefícios pode proporcionar.
2. A que sector prestará a nova equipa os seus serviços?
3. Que tipo de serviços pode uma CSIRT prestar à sua comunidade utilizadora.
4. Análise do ambiente e dos utilizadores.
5. Definição da missão.
6. Desenvolvimento do Plano de Actividades.
 - a. Definição do modelo financeiro.
 - b. Definição da estrutura organizativa.
 - c. Início da contratação de pessoal.
 - d. Utilização e equipamento das instalações.
 - e. Formulação de uma política de segurança informática.
 - f. Busca de parceiros de cooperação.
7. Promoção do Plano de Actividades.
 - a. Fazer aprovar a fundamentação empresarial.
 - b. Inserir tudo num plano de projecto.
8. Tornar a CSIRT operacional.
 - a. Criar fluxos de trabalho.
 - b. Aplicar as ferramentas CSIRT.
9. Formação do seu pessoal.

>> A fase seguinte consiste em exercitar-se e preparar-se para o trabalho a sério!

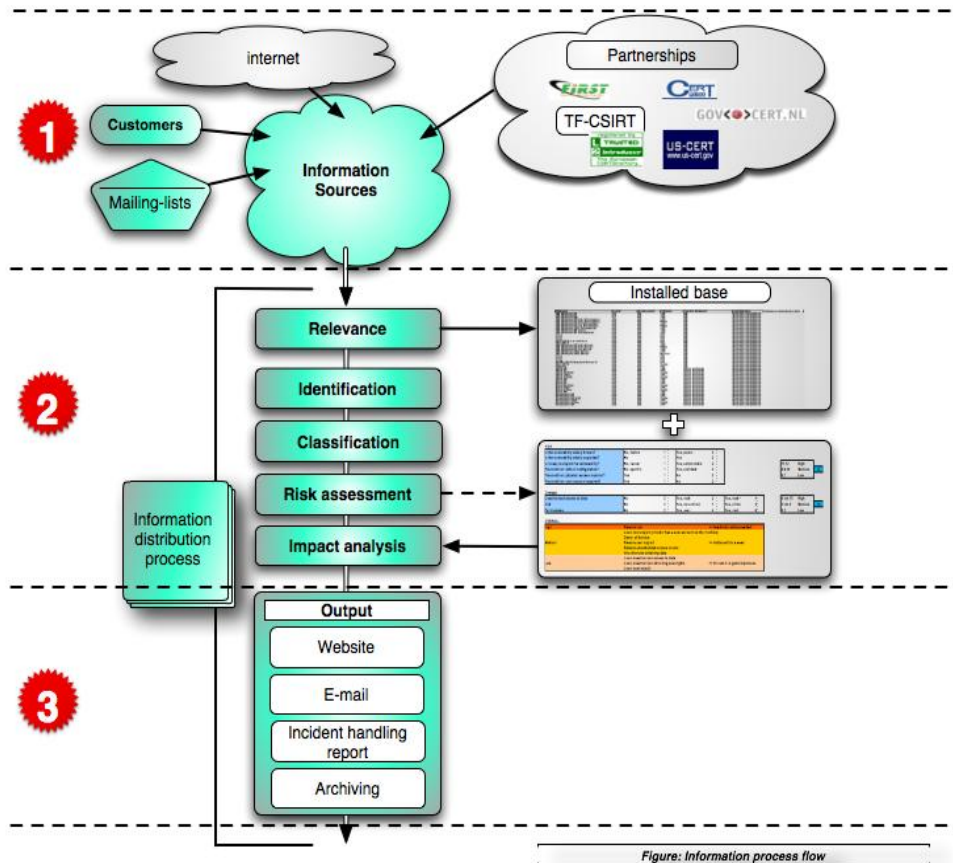
A título ilustrativo, este capítulo descreve um exemplo de exercício relativo a uma tarefa CSIRT quotidiana: criar um aviso de segurança.

Na sua origem, esteve o seguinte aviso de segurança inicialmente enviado pela Microsoft:

Identificador do Boletim	Boletim de Segurança da Microsoft MS06-042
Título do Boletim	Actualização de Segurança Cumulativa para o Internet Explorer (918899)
Resumo	A presente actualização serve para corrigir várias vulnerabilidades existentes no Internet Explorer que poderiam permitir uma execução de código remoto.
Classificação de Gravidade Máxima	Crítica
Impacto da Vulnerabilidade	Execução de Código Remoto
Software Afetado	Windows, Internet Explorer. Para mais informações, ver a secção <i>Software Afetado e Locais de Descarregamento</i> .

Este boletim do fornecedor refere-se a uma vulnerabilidade recentemente detectada no Internet Explorer. O fornecedor publica múltiplas correcções deste *software* para várias versões do Microsoft Windows.

A CSIRT fictícia, depois de receber esta informação de vulnerabilidade através de um sistema de lista de distribuição, dá início ao fluxo de trabalho descrito no capítulo 8.2



Produzir Alertas, Avisos e Comunicações.

	Internet	Parcerias
Cientes	Fontes de informação	
Sistemas de lista de distribuição	Pertinência	Base instalada
	Identificação	
	Classificação	
Processo de distribuição de informação	Avaliação dos riscos	
	Análise do impacto	
	Produtos	
	Website	
	Correio electrónico	
	Relatório de gestão do incidente	
	Arquivo	Figura: Fluxo do processo de informação

A red circular icon with a white number "1" inside, indicating the first step in a process.**Etapa 1: Recolha de informações sobre as vulnerabilidades.**

A primeira etapa é navegar até ao *website* do fornecedor. Aí a CSIRT fictícia verifica a autenticidade da informação e recolhe mais detalhes acerca da vulnerabilidade e dos sistemas informáticos afectados.

2**Etapa 2: Análise da informação e avaliação do risco****Identificação**

A informação já foi verificada mediante a comparação da informação de vulnerabilidade recebida por correio electrónico com o texto publicado no *website* do fornecedor.

Pertinência

A CSIRT fictícia verifica a lista dos sistemas afectados divulgada no *website* comparando-a com a lista dos sistemas usados na comunidade utilizadora. Conclui que um dos seus utilizadores, pelo menos, usa o Internet Explorer, pelo que a informação relativa à vulnerabilidade é efectivamente pertinente.

Categoria	Aplicação	Produto de Software	Versão	SO	Versão SO	Utilizador
Computador	Navegador	IE	x-x-	Microsoft	XP-prof	A

Classificação

A informação é pública, por isso pode ser usada e redistribuída.

Avaliação dos riscos e análise de impacto

A resposta às perguntas mostra que o risco e o impacto são *elevados* (classificado como *crítico* pela Microsoft).

RISCO

A vulnerabilidade é muito conhecida?	Sim
A vulnerabilidade é generalizada?	Sim
É fácil explorar a vulnerabilidade?	Sim
É uma vulnerabilidade que pode ser explorada remotamente?	Sim

DANOS

Os impactos possíveis são a acessibilidade remota e a potencial execução de código remoto. Esta vulnerabilidade contém muitos problemas, o que torna *elevado* o risco de danos.



Etapa 3: Distribuição

A CSIRT fictícia é uma CSIRT interna. Tem um correio electrónico, um telefone e um *website* interno como canais de comunicação disponíveis. A CSIRT produz este aviso, derivado do modelo do capítulo 8.2 *Produzir Alertas, Avisos e Comunicações*.

Título do aviso Múltiplas vulnerabilidades detectadas no Internet Explorer	
Número de referência 082006-1	
Sistemas afectados <ul style="list-style-type: none">• Todos os sistemas de computador que utilizam a Microsoft	
SO associado + versão <ul style="list-style-type: none">• Microsoft Windows 2000 Service Pack 4• Microsoft Windows XP Service Pack 1 e Microsoft Windows XP Service Pack 2• Microsoft Windows XP Professional x64 Edition• Microsoft Windows Server 2003 e Microsoft Windows Server 2003 Service Pack 1• Microsoft Windows Server 2003 for Itanium-based Systems e Microsoft Windows Server 2003 com SP1 for Itanium-based Systems• Microsoft Windows Server 2003 x64 Edition	
Risco	(Elevado-Médio-Baixo)
ELEVADO	
Impacto/dano potencial	(Elevado-Médio-Baixo)
ELEVADO	
Identificações externas:	(CVE, Identificação do Boletim de vulnerabilidade)
MS-06-42	
Síntese da vulnerabilidade <p>A Microsoft detectou várias vulnerabilidades críticas no Internet Explorer que podem levar à execução de código remoto.</p>	
Impacto <p>Um atacante poderá controlar completamente o sistema, instalando programas, acrescentando utilizadores e vias de acesso, alterando ou apagando dados. Um factor atenuante é o facto de isso apenas ser possível se o utilizador estiver registado com direitos de administrador. Os utilizadores registados com menos direitos poderão sofrer um impacto menor.</p>	
Solução <p>Proteja o seu IE imediatamente</p>	
Descrição (detalhes) <p>Ver mais informações em ms06-042.mspcx</p>	
Anexo <p>Ver mais informações em ms06-042.mspcx</p>	

Este produto já está pronto para distribuição. Como se trata de um boletim crítico é aconselhável telefonar também aos utilizadores, sempre que possível.

CSIRT fictícia (etapa 10)**Exercícios**

Nas primeiras semanas de funcionamento, a CSIRT fictícia utilizou vários casos fictícios (facultados a título de exemplo por outras CSIRT) como exercício. Além disso, emitiu algumas recomendações de segurança baseadas em informações reais sobre vulnerabilidades, distribuídas por fornecedores de *hardware* e de *software*, depois de as aperfeiçoar e ajustar às necessidades da comunidade utilizadora.

11 Conclusão

O guia termina aqui. O presente documento visa apresentar uma panorâmica muito concisa dos vários processos necessários para criar uma CSIRT, sem pretensões de ser completo e sem entrar muito em pormenores específicos. Consulte a secção *A.1 Outras leituras* no anexo, onde encontrará literatura sobre esse tema que vale a pena ler.

As etapas importantes seguintes para a CSIRT Fictícia serão agora:

- Receber *feedback* da comunidade utilizadora para aperfeiçoar os serviços prestados
- Estabelecer uma rotina para o trabalho quotidiano
- Realizar exercícios de treino para situações de emergência
- Manter um contacto estreito com as diversas comunidades CSIRT, no intuito de vir a contribuir um dia para o trabalho voluntário que elas desenvolvem.

12 Descrição do plano de projecto

NOTA: O plano de projecto constitui uma primeira estimativa do tempo necessário. Contudo, a duração real do projecto pode variar em função dos recursos disponíveis.

O plano de projecto encontra-se disponível em diferentes formatos em CD e no sítio Web da ENISA, e cobre todos os processos descritos neste documento.

O principal formato será o Microsoft Project, pelo que pode ser directamente utilizado nesta ferramenta de gestão de projecto

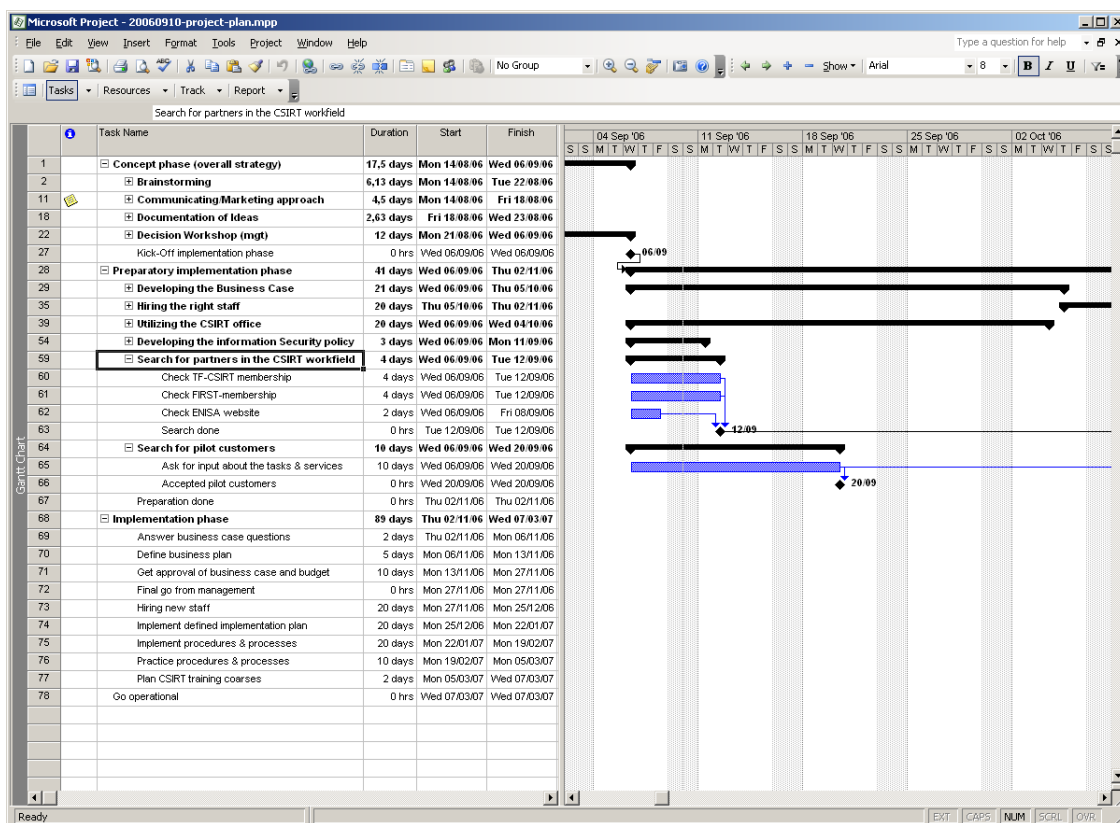


Fig. 17 Plano de projecto

Designação da tarefa	Duração	Início	Termo
Fase de concepção (estratégia global)	17,5 dias		
Reflexão	6,13 dias		
Comunicação / abordagem de <i>marketing</i>	4,5 dias		
Documentação de ideias	2,63 dias		
<i>Workshop</i> de decisão (admin.)	12 dias		
Arranque da fase de implementação	0 horas		
Fase preparatória da implementação			
Desenvolvimento da fundamentação empresarial	41 dias		
Recrutamento do pessoal adequado	21 dias		

Utilização do gabinete da CSIRT	20 dias
Desenvolvimento da política de segurança informática	20 dias
Procura de parceiros no domínio de actividade da CSIRT	3 dias
Verificação dos membros da TF-CSIRT	4 dias
Verificação dos membros de FIRST	4 dias
Verificação do sítio Web da ENISA	2 dias
Pesquisa efectuada	0 horas
Procura de clientes-piloto	10 dias
Solicitar elementos sobre tarefas e serviços	10 dias
Aceitação de clientes-pilotos	0 horas
Preparação efectuada	0 horas
Fase de implementação	89 dias
Resposta a perguntas sobre a fundamentação empresarial	2 dias
Definição do plano de investimento	5 dias
Obtenção de aprovação da fundamentação empresarial e do orçamento	10 dias
Aprovação definitiva pela administração	0 horas
Recrutamento de pessoal suplementar	20 dias
Execução do plano de implementação definido	20 dias
Implementação de procedimentos e processos	20 dias
Prática de procedimentos e processos	10 dias
Planificação de cursos de formação da CSIRT	2 dias
Entrada em funcionamento	0 horas

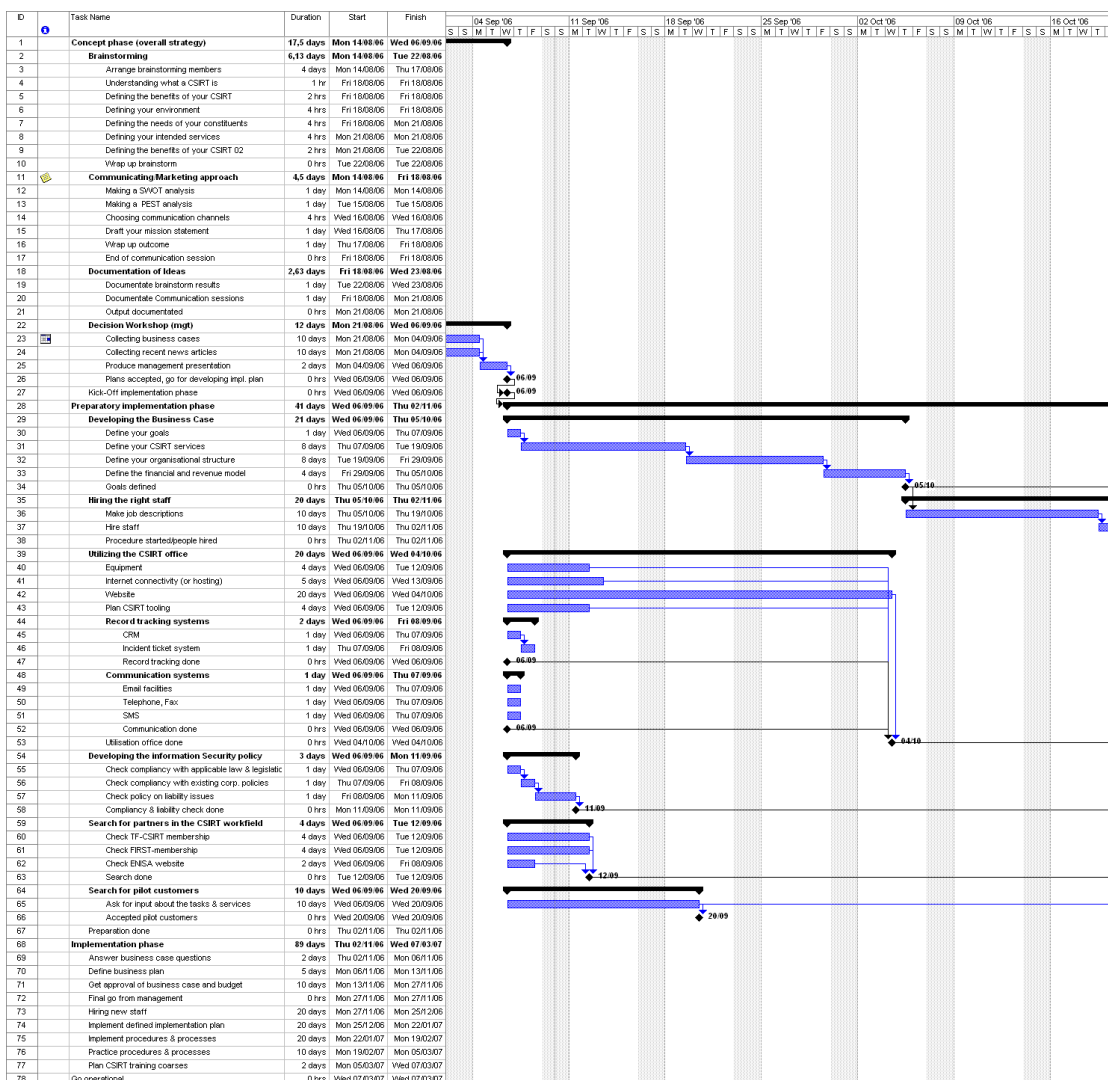


Fig. 18 Plano do projecto com todas as tarefas e uma parte do gráfico de Gant

Designação da tarefa	Duração	Início	Termo
Fase de concepção (estratégia global)	17,5 dias		
Reflexão	6,13 dias		
Seleccção dos membros do grupo de reflexão	4 dias		
Compreender o que é uma CSIRT	1 hora		
Definir as vantagens do seu CSIRT	2 horas		
Definir o seu ambiente	4 horas		
Definir as necessidades dos seus utilizadores	4 horas		
Definir os serviços que pretende prestar	4 horas		
Definir as vantagens do seu CSIRT 02	2 horas		
Conclusão da reflexão	0 horas		
Comunicação / abordagem de marketing	4,5 dias		
Realização de análise SWOT	1 dia		
Realização de análise PEST	1 dia		
Escolha de canais de comunicação	4 horas		

Elaboração da definição de missão	1 dia		
Integração dos resultados	1 dia		
Fim da sessão de comunicação	0 horas		
Documentação de ideias	2,63 dias		
Documentação dos resultados da reflexão	1 dia		
Documentação das sessões de comunicação	1 dia		
Documentação dos resultados	0 horas		
Workshop de decisão (admin.)	12 dias		
Recolha de fundamentações empresariais	10 dias		
Recolha de artigos publicados recentemente	10 dias		
Apresentação à administração	2 dias		
Aceitação dos planos, luz verde ao desenvolvimento do plano de implementação	0 horas		
Arranque da fase de implementação	0 horas		
Fase de implementação preparatória	41 dias		
Desenvolvimento da fundamentação empresarial	21 dias		
Definição de objectivos	1 dia		
Definição dos serviços da CSIRT	8 dias		
Definição da estrutura da organização	8 dias		
Definição do modelo financeiro e de receitas	4 dias		
Objectivos definidos	0 horas		
Recrutamento do pessoal adequado	20 dias		
Descrição de funções	10 dias		
Recrutamento de pessoal	10 dias		
Processo iniciado/pessoal recrutado	0 horas		
Utilização do gabinete da CSIRT	20 dias		
Equipamento	4 dias		
Ligação à Internet (ou acolhimento)	5 dias		
Sítio Web	20 dias		
Planificação das ferramentas da CSIRT	4 dias		
Sistemas de acompanhamento de registos	2 dias		
CRM	1 dia		
Sistema de registo de incidentes	1 dia		
Acompanhamento de registos concluído	0 horas		
Sistemas de comunicação	1 dia		
E-mail	1 dia		
Telefone, fax	1 dia		
SMS	1 dia		
Comunicação concluída	0 horas		
Utilização do gabinete concluída	0 horas		
Desenvolvimento da política de segurança informática	3 dias		
Verificação da conformidade com a legislação aplicável	1 dia		
Verificação da conformidade com as políticas empresariais em vigor	1 dia		
Verificação da política em matéria de responsabilidade	1 dia		
Verificação da conformidade e da responsabilidade concluída	0 horas		

Procura de parceiros no domínio de actividade da CSIRT	4 dias		
Verificação dos membros da TF-CSIRT	4 dias		
Verificação dos membros de FIRST	4 dias		
Verificação do sítio Web da ENISA	2 dias		
Pesquisa efectuada	0 horas		
Procura de clientes-piloto	10 dias		
Solicitar elementos sobre tarefas e serviços	10 dias		
Clientes-piloto aceites	0 horas		
Preparação efectuada	0 horas		
Fase de implementação	89 dias		
Resposta a perguntas sobre o plano de investimento	2 dias		
Definição do plano de actividades	5 dias		
Obtenção da aprovação do plano de actividades e do orçamento	10 dias		
Aprovação definitiva pela administração	0 horas		
Recrutamento de pessoal suplementar	20 dias		
Execução do plano de implementação definido	20 dias		
Implementação de procedimentos e processos	20 dias		
Prática de procedimentos e processos	10 dias		
Planificação de cursos de formação da CSIRT	2 dias		
Entrada em funcionamento	0 horas		

O plano de projecto encontra-se igualmente disponível nos formatos CVS e XML.
Outras utilizações podem ser solicitadas aos peritos em CSIRT da ENISA:

CERT-Relations@enisa.europa.eu

ANEXO

A.1 Outras leituras***Handbook for CSIRTs (CERT/CC) [Manual para CSIRT (CERT/CC)]***

Uma obra de referência, muito exaustiva, para todos os tópicos importantes para o trabalho de uma CSIRT.

Fonte: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Defining Incident Management Processes for CSIRTs: A Work in Progress [Definição de processos de gestão de incidentes para CSIRT: um trabalho em curso]

Uma análise aprofundada da gestão de incidentes.

Fonte: <http://www.cert.org/archive/pdf/04tr015.pdf>

State of the Practice of Computer Security Incident Response Teams (CSIRTs) [Situação actual das Equipas de Resposta a Incidentes de Segurança Informática]

Uma análise aprofundada da situação actual das CSIRT em todo o mundo, incluindo história, estatísticas e muito mais.

Fonte: <http://www.cert.org/archive/pdf/03tr001.pdf>

CERT-in-a-box

Uma descrição exaustiva dos ensinamentos extraídos da criação da GOVCERT.NL e do 'De Waarschuwingsdienst', o serviço nacional de alerta neerlandês.

Fonte: <http://www.govcert.nl/render.html?it=69>

RFC 2350: Expectations for Computer Security Incident Response [RFC 2350: Expectativas em matéria de Resposta a Incidentes de Segurança Informática].

Fonte: <http://www.ietf.org/rfc/rfc2350.txt>

NIST³⁷ Computer Security Incident Handling Guide [Guia NIST para a Gestão dos Incidentes de Segurança Informática]

Fonte: <http://www.securityunit.com/publications/sp800-61.pdf>

ENISA Inventory of CERT activities in Europe [Inventário das actividades de CERT na Europa (ENISA)]

Uma obra de referência, que reúne informações sobre os CSIRT existentes na Europa e as suas diferentes actividades.

Fonte: <http://www.enisa.europa.eu/ENISA%20CERT/index.htm>

³⁷ NIST: Instituto Nacional de Normalização e Tecnologias.

A.2 Serviços CSIRT

Um agradecimento especial ao CERT/CC, que forneceu esta lista.

Serviços reactivos	Serviços proactivos	Gestão de artefactos
<ul style="list-style-type: none"> • Serviços reactivos • Gestão de incidentes • Análise de incidentes • Resposta a incidentes no local • Assistência na resposta a incidentes • Coordenação da resposta a incidentes • Gestão da vulnerabilidade • Análise da vulnerabilidade • Resposta à vulnerabilidade • Coordenação da resposta à vulnerabilidade 	<ul style="list-style-type: none"> • Avisos • Vigilância tecnológica • Auditorias ou avaliações de segurança • Configuração e manutenção de segurança • Desenvolvimento de ferramentas de segurança • Serviços de detecção de intrusões • Difusão de informações relativas à segurança 	<ul style="list-style-type: none"> • Análise de artefactos • Resposta a artefactos • Coordenação de resposta a artefactos
		Gestão da qualidade da segurança
		<ul style="list-style-type: none"> • Análise dos riscos • Planificação da continuidade da actividade e da recuperação de emergência • Consultoria de segurança • Sensibilização • Educação/Formação • Avaliação ou certificação dos produtos

Fig. 19 Lista de serviços CSIRT do CERT/CC

Descrições dos serviços

Serviços reactivos

Os serviços reactivos são concebidos para responder a pedidos de assistência, a notificações de incidentes na comunidade utilizadora CSIRT e a quaisquer ameaças ou ataques contra os sistemas CSIRT. Alguns serviços podem ser desencadeados por notificação de terceiros ou por monitorização e visualização ou por registos e alertas dos IDS (sistemas de detecção de intrusões).

Alertas e avisos

Este serviço envolve a divulgação de informações que descrevem ataques de intrusos, vulnerabilidades de segurança, alertas de intrusão, vírus informáticos ou falsos alarmes (*hoax*), e a rápida divulgação de recomendações para enfrentar os problemas. O alerta, aviso ou recomendação é enviado como reacção ao problema em causa, a fim de informar os utilizadores da actividade e de os ajudar a proteger os seus sistemas ou a recuperar os sistemas eventualmente afectados. As informações podem ser produzidas pela CSIRT e divulgadas pelos fornecedores, por outros CSIRT ou por peritos em segurança ou ainda por outras partes da comunidade utilizadora.

Gestão de incidentes

A gestão de incidentes inclui a recepção, triagem e resposta a solicitações e notificações, bem como a análise de incidentes e ocorrências. Em determinados casos, as actividades de resposta podem incluir:

- a tomada de medidas tendentes a proteger sistemas e redes afectados ou ameaçados pela actividade de intrusos
- a apresentação de soluções e de estratégias de atenuação a partir das recomendações ou alertas pertinentes
- a busca de actividade de intrusos noutras partes da rede
- a filtragem do tráfego da rede
- a reconstrução de sistemas
- a correcção ou a reparação de sistemas
- o desenvolvimento de alternativas ou de estratégias de solução provisória

Dado que as actividades de gestão de incidentes são executadas de diversas formas por diferentes tipos de CSIRT, este serviço é classificado, principalmente, em função do tipo de actividades desenvolvidas e do tipo de assistência prestado, do seguinte modo:

Análise de incidentes

Existem muitos níveis de análises de incidentes e muitos subserviços. Essencialmente, a análise de um incidente consiste no exame de todas as informações disponíveis e das provas ou artefactos de apoio relacionados com um incidente ou ocorrência. A análise tem por objectivo identificar o âmbito do incidente, a extensão dos danos causados pelo incidente, a natureza do incidente e estratégias de resposta ou soluções provisórias. A CSIRT pode utilizar os resultados das análises de vulnerabilidade e dos artefactos (descritas *infra*) para compreender e, em consequência, fornecer uma análise tão completa e actualizada quanto possível do que aconteceu num dado sistema.

A CSIRT compara a actividade dos diferentes incidentes, a fim de determinar eventuais inter-relações, tendências, padrões ou assinaturas de intrusos.

Dois subserviços que podem ser prestados no âmbito da análise de incidentes, em função da missão, dos objectivos e dos processos da CSIRT, são:

Recolha de provas forenses

A recolha, preservação, documentação e análise de provas num sistema informático comprometido, a fim de determinar alterações ao sistema e apoiar a reconstrução das ocorrências conducentes a essa situação. Esta recolha de informações e de provas deve ser efectuada de forma que documente uma cadeia de custódia susceptível de ser provada de forma admissível em tribunal de acordo com as normas de prova. As tarefas inerentes à recolha de provas forenses incluem (embora não se limitem) a realização de cópias de imagens digitais do disco duro do sistema afectado, a verificação de mudanças no sistema, como novos programas, ficheiros, serviços e utilizadores, a observação de processos em curso e de portas abertas e a procura de programas e ferramentas troianos ou “cavalos de Tróia”. O pessoal da CSIRT que executa esta função pode igualmente ter de estar preparado para agir na qualidade de peritos ou de testemunhas em processos judiciais.

Rastreio ou localização

A localização da origem de um intruso ou a identificação de sistemas a que o intruso teve acesso. Esta actividade pode incluir o rastreio ou a localização da forma como o

intruso invadiu os sistemas afectados e as redes conexas, quais os sistemas utilizados para conseguir esse acesso, qual o ponto de origem do ataque e que outros sistemas e redes foram utilizados no quadro do ataque. Pode igualmente incluir a tentativa de identificação do intruso. Este trabalho pode ser realizado isoladamente, mas, normalmente, decorre em colaboração com autoridades responsáveis pela execução da lei, fornecedores de serviços de Internet ou outras organizações envolvidas.

Resposta a incidentes no local

A CSIRT assegura apoio directo, no local, para ajudar os utilizadores a recuperar do incidente. A própria CSIRT analisa fisicamente os sistemas afectados e dirige a reparação e a recuperação dos sistemas, não se limitando a assegurar um apoio de resposta ao incidente por telefone ou por correio electrónico (ver *infra*). Este serviço inclui todas as medidas de nível local necessárias em caso de suspeita ou de ocorrência de incidente. Se a CSIRT não se localizar na zona afectada, deverá fazer deslocar membros da equipa e assegurar a resposta. Noutros casos, poderá já encontrar-se na zona uma equipa local que assegure a resposta ao incidente no âmbito do seu trabalho de rotina. Tal verifica-se especialmente quando a gestão do incidente é assegurada no âmbito das tarefas normais dos administradores do sistema, da rede ou da segurança e não por uma CSIRT estabelecida.

Apoio na resposta a incidentes

A CSIRT assiste e orienta a(s) vítima(s) do ataque na recuperação de um incidente, por telefone, e-mail, fax ou documentação. Isto pode implicar a prestação de assistência técnica na interpretação dos dados recolhidos, o fornecimento de contactos ou a emissão de orientações sobre estratégias de atenuação e de recuperação. Não implica acções directas, no local, de resposta a incidentes, como as acima descritas. A CSIRT limita-se a prestar orientação à distância, de modo a permitir que o pessoal no local proceda à recuperação.

Coordenação da resposta a incidentes

A CSIRT coordena o esforço de resposta das partes envolvidas no incidente, que são, em princípio, a vítima do ataque, outros sítios envolvidos no ataques e quaisquer sítios que requeiram assistência na análise do ataque. Podem incluir igualmente as partes que prestam apoio em TI à vítima, como prestadores de serviços Internet, outras CSIRT e os administradores de sistema e de rede no local. O trabalho de coordenação pode implicar a recolha de contactos, a notificação de sítios sobre o seu potencial envolvimento (enquanto vítima ou fonte de um ataque), a recolha de dados estatísticos sobre o número de sítios envolvidos e a facilitação do intercâmbio e da análise de informações. Parte do trabalho de coordenação pode implicar a notificação e a colaboração com o consultor jurídico e com os departamentos de recursos humanos e de relações públicas de uma organização, bem como coordenação com entidades responsáveis pela aplicação da legislação. Este serviço não inclui resposta directa a incidentes, no local.

Gestão das vulnerabilidades

A gestão das vulnerabilidades inclui a recepção de informações e relatórios sobre as vulnerabilidades do *hardware* e do *software*, a análise da natureza, mecânica e efeitos das vulnerabilidades e o desenvolvimento de estratégias de resposta para detecção e reparação de vulnerabilidades. Atendendo a que as actividades de gestão das vulnerabilidades são executadas de diversas formas por diferentes tipos de CSIRT, este serviço é classificado, principalmente, em função do tipo de actividade executada e do tipo de assistência prestada, do seguinte modo:

Análise das vulnerabilidades

A CSIRT procede a análises técnicas e a exames de vulnerabilidades de *hardware* ou de *software*, que incluem a verificação de suspeitas de vulnerabilidades e o exame técnico da vulnerabilidade do *hardware* ou do *software*, com vista a determinar onde se situa e de que modo pode ser explorada. A análise pode incluir a verificação do código-fonte, com recurso a um programa de correcção (*debugger*), a fim de determinar onde ocorre a vulnerabilidade, ou a tentativa de reproduzir o problema num sistema de teste.

Resposta às vulnerabilidades

Este serviço consiste em determinar a resposta adequada para atenuar ou reparar a vulnerabilidade. Esta actividade pode incluir o desenvolvimento ou a pesquisa de correcções, reparações e soluções provisórias. Pode ainda incluir a notificação da estratégia de atenuação a terceiros, nomeadamente através da formulação e difusão de recomendações ou alertas. A resposta deste serviço pode ser dada através da instalação de correcções, reparações ou soluções provisórias.

Coordenação da resposta às vulnerabilidades

A CSIRT notifica as diferentes partes da empresa ou da comunidade de utilizadores acerca da vulnerabilidade e partilha informação sobre a forma de solucionar ou atenuar a vulnerabilidade. A CSIRT certifica-se de que a estratégia de resposta à vulnerabilidade foi aplicada com êxito. O serviço pode implicar comunicação com fornecedores, outras CSIRT, peritos técnicos, utilizadores e com os primeiros indivíduos ou grupos que detectaram ou notificaram a vulnerabilidade. As actividades incluem a facilitação da análise de uma vulnerabilidade ou do relatório de vulnerabilidade, a coordenação dos calendários de lançamento dos documentos e das correcções ou soluções provisórias correspondentes, e a síntese da análise técnica realizada por diferentes partes. Este serviço pode ainda incluir a manutenção de um arquivo ou base de conhecimentos, pública ou privada, de informações sobre as vulnerabilidades e as estratégias de resposta correspondentes.

Gestão de artefactos

Um artefacto é qualquer ficheiro ou objecto encontrado num sistema susceptível de estar relacionado com a exploração ou o ataque de sistemas e redes, ou que esteja a ser utilizado para contornar medidas de segurança. São artefactos, entre outros, os vírus informáticos, os programas cavalos de Tróia, os vermes, os roteiros de exploração e os conjuntos de ferramentas.

A gestão dos artefactos implica a recepção de informações sobre os artefactos utilizados em ataques de intrusão, reconhecimento e noutras actividades não autorizadas ou perturbadoras, e de cópias dos mesmos. Depois de recebidos, os artefactos são analisados. Essa análise incide na natureza, mecânica, versão e utilização do artefacto em causa, sendo em seguida desenvolvidas (ou sugeridas) estratégias de resposta para a detecção, remoção ou defesa contra o artefacto. Atendendo a que as actividades de gestão de artefactos são executadas de diversas formas por diferentes tipos de CSIRT, este serviço é classificado, principalmente, em função do tipo de actividade executada e do tipo de assistência prestada, do seguinte modo:

Análise de artefactos

A CSIRT procede ao exame e análise técnicos de todos os artefactos encontrados num sistema. A análise efectuada pode incluir a identificação do tipo de ficheiro e da estrutura do artefacto, a comparação de um novo artefacto com artefactos existentes ou com outras versões do mesmo artefacto, a fim de detectar a semelhanças e as diferenças, ou ainda a engenharia inversa ou a desmontagem do código, para determinar a finalidade e a função do artefacto.

Resposta aos artefactos

Este serviço inclui a determinação das medidas adequadas para detectar e remover artefactos de um sistema, bem como medidas para impedir a instalação de artefactos, o que pode implicar a criação de assinaturas adicionáveis ao *software* antivírus ou ao sistema de detecção de intrusão (IDS).

Coordenação da resposta aos artefactos

Este serviço implicar partilhar e sintetizar os resultados das análises e as estratégias de resposta adequadas a um artefacto com outros investigadores, CSIRT, fornecedores e outros peritos em segurança. As actividades incluem a notificação de terceiros e a síntese de análises técnicas de diversas fontes. Podem ainda incluir a manutenção de um arquivo, público ou reservado aos utilizadores, de artefactos conhecidos, do seu impacto e das estratégias de resposta correspondentes.

Serviços proactivos

Os serviços proactivos são concebidos para melhorar a infra-estrutura e os processos de segurança da comunidade de utilizadores antes de se registar ou de ser detectado qualquer incidente ou ocorrência. Os seus principais objectivos consistem em evitar incidentes e reduzir o seu impacto e extensão quando se registam.

Comunicações

As comunicações incluem, nomeadamente, alertas de intrusão, avisos de vulnerabilidade e recomendações de segurança, destinados a informar os utilizadores sobre novas evoluções com impacto de médio a longo prazo, como vulnerabilidades recém-detectadas ou novas ferramentas de intrusão. As comunicações permitem aos utilizadores proteger os seus sistemas e redes contra problemas novos, antes de serem afectados.

Vigilância tecnológica

A CSIRT acompanha e observa novos progressos técnicos, actividades de intrusão e tendências conexas, a fim de contribuir para a identificação de ameaças futuras. Os tópicos analisados podem ser alargados de modo a ter em conta medidas legais e legislativas, ameaças sociais ou políticas e tecnologias emergentes. Este serviço implica a leitura de listas de endereços securizadas, sítios Web dedicados à segurança, bem como notícias e artigos de imprensa nos domínios da ciência, tecnologia, política e governação, a fim de extrair informações pertinentes para a segurança dos sistemas e redes dos utilizadores. Pode ainda requerer a comunicação com outras partes que sejam autoridades nestes domínios, de modo a garantir a obtenção das melhores e mais rigorosas informações e a sua correcta interpretação. Deste trabalho pode resultar algum tipo de comunicação, directrizes ou recomendações sobre questões de segurança de médio a longo prazo.

Auditorias ou avaliações de segurança

Este serviço assegura a verificação e a análise aprofundadas da infra-estrutura de segurança de uma organização, com base nos requisitos definidos pela mesma ou por outras normas sectoriais aplicáveis. Pode ainda incluir uma avaliação das práticas de

segurança das organizações. Podem ser executados muitos tipos diferentes de auditorias ou avaliações, incluindo:

Verificação da infra-estrutura

Verificação manual das configurações de *hardware* e *software*, *routers*, *firewalls*, servidores e dispositivos de *desktop*, no intuito de garantir que estes correspondem às melhores práticas das políticas de segurança da organização ou do sector e às configurações-tipo.

Verificação das melhores práticas

Entrevista de empregados e de administradores de sistemas e redes, para determinar se as suas práticas de segurança correspondem à política de segurança definida pela organização ou a normas sectoriais específicas.

Exame

Com recurso a *scanners* de vulnerabilidade ou de vírus, a fim de identificar sistemas e redes vulneráveis.

Testes de penetração

Testes à segurança de um sítio através de ataques intencionais aos seus sistemas e redes.

É necessária a aprovação prévia da administração para a realização de auditorias ou avaliações deste tipo. Algumas destas abordagens podem ser proibidas pela política da organização. A prestação deste serviço pode incluir o desenvolvimento de um conjunto comum de práticas contra as quais os testes ou avaliações são conduzidos, a par do desenvolvimento de um conjunto de aptidões requeridas ou de requisitos de certificação para o pessoal que executa os testes, avaliações, auditorias ou análises. Este serviço pode ser confiado a um terceiro contratante ou a um prestador de serviços de segurança que possua a proficiência adequada na condução de auditorias e avaliações.

Configuração e manutenção de ferramentas de segurança, aplicações, infra-estruturas e serviços

Este serviço identifica e fornece orientações sobre a forma de configurar e manter em segurança ferramentas, aplicações e a infra-estrutura informática geral utilizada pela comunidade de utilizadores da CSIRT ou pela própria CSIRT. Para além de fornecer orientações, as CSIRT podem proceder a actualizações das configurações e à manutenção das ferramentas e serviços de segurança, como sistemas de detecção de intrusões (IDS), exploração da rede ou sistemas de acompanhamento, filtros, *wrappers*, *firewalls*, redes virtuais privadas (VPN) ou mecanismos de autenticação. As CSIRT podem também fornecer estes serviços no âmbito da sua função principal. As CSIRT podem igualmente configurar ou assegurar a manutenção de servidores, computadores de secretária e portáteis, agendas pessoais digitais (PDA) e outros dispositivos sem fios, de acordo com directrizes de segurança. Este serviço inclui a colocação à consideração da administração de quaisquer questões ou problemas relacionados com configurações ou com a utilização de ferramentas e aplicações que a CSIRT considere susceptíveis de tornar o sistema vulnerável a ataques.

Desenvolvimento de ferramentas de segurança

Este serviço inclui o desenvolvimento de ferramentas novas e destinadas exclusivamente aos utilizadores que sejam solicitadas ou desejadas pela comunidade de utilizadores ou pela própria CSIRT. Podem, nomeadamente, ser desenvolvidas correcções de segurança para *software* adaptado utilizado pela comunidade de utilizadores ou distribuições securizadas de *software* para reconstrução de sistemas centrais comprometidos. Podem igualmente desenvolver ferramentas ou roteiros que aumentem o número de funcionalidades das ferramentas de segurança existentes, como uma nova ligação a um *scanner* de vulnerabilidades ou da rede, a roteiros que facilitem a utilização de tecnologia de cifragem ou a mecanismos automatizados de distribuição de correcções.

Serviços de detecção de intrusão

As CSIRT que prestam este serviço revêem os registos IDS existentes, analisam e iniciam respostas para todas as ocorrências que correspondam ao limiar que definiram, ou reencaminham os alertas de acordo com um acordo de nível de serviços predefinido ou com uma estratégia em escalada. A detecção de intrusos e a análise dos registos de segurança conexos pode constituir uma tarefa desencorajadora – não apenas no que se refere à determinação da localização mais adequada para os sensores, mas também no que respeita à recolha e subsequente análise da enorme quantidade de dados coligidos. Em muitos casos, são necessárias ferramentas ou proficiência especializadas para sintetizar e interpretar as informações de modo a identificar alarmes falsos, ataques ou ocorrências na rede e para executar estratégias tendentes a eliminar ou minimizar tais ocorrências. Algumas organizações optam por confiar esta actividade a terceiros mais preparados para assegurar estes serviços, como é o caso dos fornecedores de serviços de segurança.

Difusão de informações relacionadas com a segurança

Este serviço fornece aos utilizadores uma recolha exaustiva e de fácil consulta de informações úteis para os ajudar a melhorar a segurança. Essas informações podem incluir:

- directrizes de notificação e contactos da CSIRT
- arquivos de alerta, avisos e outras comunicações
- documentação sobre as melhores práticas actuais
- orientações gerais de segurança informática
- políticas, procedimentos e listas de verificação
- desenvolvimento de protecções e informações de distribuição
- ligações a fornecedores
- estatísticas e tendências actuais em matéria de notificação de incidentes
- outras informações susceptíveis de melhorar as práticas de segurança geral.

Estas informações podem ser produzidas e publicadas pela CSIRT ou por outra parte da organização (TI, recursos humanos ou relações públicas) e podem incluir informações de recursos externos, como outras CSIRT, fornecedores e peritos em segurança.

Serviços de gestão da qualidade da segurança

Os serviços que se inserem nesta categoria não se esgotam na gestão de incidentes ou nas CSIRT. Trata-se de serviços bem conhecidos e estabelecidos, que visam melhorar a segurança geral de uma organização. Graças à experiência adquirida com a prestação dos serviços reactivos e proactivos acima descritos, uma CSIRT pode trazer a estes serviços de gestão da qualidade perspectivas únicas que de outro modo não estariam disponíveis. Estes serviços visam a tomada em consideração do *feedback* e dos ensinamentos adquiridos com a resposta a incidentes, vulnerabilidades e ataques. A integração destas experiências nos serviços tradicionais existentes (adiante descritos), no quadro de um processo de gestão da qualidade da segurança, pode melhorar os esforços de segurança a longo prazo numa organização. Consoante as estruturas e responsabilidades organizacionais, uma CSIRT pode prestar estes serviços ou participar num esforço organizacional de equipa mais vasto.

As descrições que se seguem explicam de que forma a proficiência das CSIRT pode beneficiar cada um destes serviços de gestão da qualidade.

Análise dos riscos

Os CSIRT podem estar em condições de acrescentar valor às análises e avaliações dos riscos, o que pode melhorar a capacidade das organizações para avaliar as ameaças reais, efectuar avaliações realistas, qualitativas e quantitativas, dos riscos para os recursos de informação e para avaliar as estratégias de protecção e de resposta. As CSIRT que asseguram este serviço desenvolvem ou assistem actividades de análise dos riscos para a segurança da informação relativamente a novos sistemas e processos empresariais ou avaliam ameaças e ataques contra recursos e sistemas de utilizadores.

Planificação da continuidade da actividade e da recuperação de emergência

Tendo em conta as ocorrências do passado e as previsões de incidentes emergentes ou as tendências de segurança, é crescente o número de incidentes com potencial para afectar gravemente as actividades empresariais. Em consequência, a planificação dos esforços deve ter em conta a experiência e as recomendações das CSIRT na determinação da melhor forma de responder a incidentes tendo em vista a continuidade da actividade empresarial. As CSIRT que prestam este serviço participam na planificação da continuidade da actividade e da recuperação de emergência na sequência de ocorrências relacionadas com ameaças e ataques à segurança informática.

Consultoria de segurança

As CSIRT podem ser utilizadas para prestar aconselhamento e orientação quanto às melhores práticas de segurança a observar pelos utilizadores nas suas actividades. As CSIRT que prestam este serviço formulam igualmente recomendações ou identificam requisitos a observar na aquisição, instalação ou securização de novos sistemas, dispositivos de rede, aplicações de *software* ou processos empresariais que afectem toda a actividade. Este serviço inclui a prestação de orientação e assistência no desenvolvimento de políticas de segurança à escala da organização ou da comunidade de utilizadores. Pode incluir igualmente a prestação de testemunho ou aconselhamento a órgãos legislativos ou a outros órgãos governamentais.

Sensibilização

As CSIRT podem conseguir detectar quando os seus utilizadores necessitam de mais informação e orientação para melhor se conformarem a práticas de segurança aceites e a políticas de segurança organizacional. Cada vez mais, a sensibilização da população de utilizadores para as questões de segurança geral não só aumenta a sua compreensão das questões de segurança como os ajuda a executar as suas operações quotidianas de forma mais segura. A sensibilização pode reduzir a ocorrência de ataques bem-sucedidos e aumentar a probabilidade de os utilizadores detectarem e notificarem ataques, diminuindo, desta forma, o tempo de recuperação e eliminando ou minimizando perdas.

As CSIRT que asseguram este serviço procuram aumentar a sensibilização para a segurança através da criação de artigos, cartazes, boletins informativos, sítios Web ou outros recursos de informação que expliquem as melhores práticas de segurança e aconselhem acerca das precauções a tomar. As actividades podem ainda incluir a organização de reuniões e seminários destinados a manter os utilizadores actualizados

quanto aos procedimentos de segurança e às potenciais ameaças para os sistemas organizacionais.

Educação/Formação

Este serviço consiste no fornecimento aos utilizadores de informações sobre questões relacionadas com a segurança informática no âmbito de seminários, *workshops*, cursos e outras acções de formação. Os tópicos podem incluir directrizes de notificação de incidentes, métodos de resposta adequados, ferramentas de resposta a incidentes, métodos de prevenção de incidentes e outras informações necessárias para proteger, detectar, notificar e responder a incidentes de segurança informática.

Avaliação ou certificação dos produtos

Para este serviço, a CSIRT pode proceder a avaliações de produto relativamente a ferramentas, aplicações ou outros serviços, a fim de se certificar da segurança dos produtos e da sua conformidade com práticas de segurança da CSIRT ou com práticas organizacionais aceitáveis. As ferramentas e aplicações avaliadas podem ser de fonte aberta ou produtos comerciais. Este serviço pode ser prestado como avaliação ou no quadro de um programa de certificação, consoante as normas aplicadas pela organização ou pela CSIRT.

A.3 Exemplos

CSIRT fictícia

Etapas 0 - Compreender o que é uma CSIRT:

Este exemplo de CSIRT serve uma instituição de dimensão média, com 200 efectivos. A instituição possui o seu próprio departamento de informática e duas outras sucursais no mesmo país. A informática desempenha um papel fundamental para a empresa, porque é utilizada na comunicação interna, numa rede de dados e num cibernegócio que funciona permanentemente. A instituição tem uma rede própria e dispõe de uma ligação suplementar à Internet através de dois prestadores de serviços Internet distintos.

Etapas 1: Fase de arranque

Na fase de arranque, a nova CSIRT é planeada como uma CSIRT interna, prestando os seus serviços à empresa de acolhimento, ao departamento informático local e ao pessoal. Também apoia e coordena a gestão dos incidentes de segurança informática entre as diversas sucursais.

Passo 2: Escolha dos serviços adequados

Na fase inicial, decide-se que a nova CSIRT se concentrará, sobretudo, na prestação de alguns serviços essenciais aos funcionários.

É decidido que, após uma fase-piloto, se poderá ponderar o alargamento da carteira de serviços prestados e a adição de alguns serviços de gestão da segurança. Essa decisão será tomada com base no *feedback* recebido dos utilizadores-piloto e em estreita cooperação com o departamento de garantia da qualidade.

Etapas 3: Análise da comunidade utilizadora e dos canais de comunicação adequados

Uma sessão de reflexão com alguns dos principais membros da administração e da comunidade utilizadora produziu elementos suficientes para uma análise SWOT. Esta permite concluir que são necessários os seguintes serviços essenciais:

- Alertas e avisos
- Gestão de incidentes (análise, apoio à resposta e coordenação da resposta)
- Comunicações

Importa garantir que as informações são distribuídas de forma bem organizada para chegarem à maior percentagem possível da comunidade utilizadora. Decidiu-se, por isso, publicar os alertas, avisos e comunicações sob a forma de recomendações de segurança num *website* específico e divulgá-las através de um sistema de lista de distribuição. A CSIRT faculta o correio electrónico, o telefone e o fax para a recepção das notificações de incidentes. Para a próxima etapa está previsto um formulário-web unificado.

Etapa 4: Definição da missão

A gestão da CSIRT fictícia elaborou a seguinte definição de missão:

“A CSIRT fictícia fornece informação e assistência ao pessoal da sua empresa de acolhimento para reduzir os riscos de incidentes de segurança informática e responder a tais incidentes, quando se verificam.”

A CSIRT fictícia esclarece, assim, que se trata de uma CSIRT interna e que a sua actividade essencial é tratar das questões de segurança informática.

Etapa 5: Definição do Plano de Actividades

Modelo financeiro

Dado que a empresa tem um cibernegócio permanente e também um departamento informático que funciona 24 horas por dia e sete dias por semana, foi decidido que se prestaria um serviço completo durante as horas de expediente e um serviço de piquete fora desse horário. Os serviços à comunidade utilizadora serão prestados a título gratuito, mas a possibilidade de prestar serviços a clientes externos será avaliada durante a fase piloto e a fase de avaliação.

Modelo de receitas

Durante a fase de arranque e a fase piloto, a CSIRT será financiada através da empresa de acolhimento. Na fase piloto e na fase de avaliação, debater-se-á um financiamento adicional, incluindo a possibilidade de vender serviços a clientes externos.

Modelo organizativo

A organização de acolhimento é uma pequena empresa, por isso é escolhido o modelo integrado.

Durante as horas de expediente, os serviços básicos (distribuição de recomendações de segurança e gestão/coordenação em caso de incidentes) serão prestados por três pessoas.

O departamento informático da empresa já dispõe de pessoal com as competências adequadas. É celebrado um acordo com esse departamento para que a nova CSIRT possa pedir apoio pontualmente, quando necessário. Também é possível recorrer à segunda linha dos seus técnicos de piquete.

Haverá uma equipa CSIRT de base, composta por quatro elementos a tempo inteiro e cinco elementos suplementares. Um destes também estará disponível em turnos rotativos.

Pessoal

O chefe de equipa CSIRT tem experiência profissional no domínio da segurança e do apoio de 1º e 2º nível, tendo trabalhado no domínio da gestão e da resistência a crises. Os outros três membros da equipa são especialistas de segurança. Os membros da equipa CSIRT a tempo parcial provenientes do departamento informático são especializados no seu sector da infra-estrutura da empresa.

Etapas 6: Utilização das instalações e política de segurança informática

Equipamento e localização das instalações

Em virtude de a empresa de acolhimento já ter uma segurança física eficiente instalada, a nova CSIRT está bem protegida nesse aspecto. Existe uma “sala de guerra” para assegurar a coordenação em caso de emergência. Foi adquirido um cofre para o material de cifragem e para os documentos sensíveis. Instalou-se uma linha telefónica separada, incluindo uma central telefónica para assegurar a linha directa durante as horas de expediente e um telefone móvel de serviço “por chamada” no período fora desse horário, com o mesmo número de telefone.

Os equipamentos existentes e o *website* da organização também podem ser utilizados para comunicar informações relacionadas com a CSIRT. É instalado um *software* de lista de distribuição, cuja manutenção é assegurada, com uma parte reservada à comunicação entre os membros da equipa e com outras equipas. Todos os contactos dos membros do pessoal estão armazenados numa base de dados, estando uma listagem impressa dos mesmos guardada no cofre.

Regulamentação

Como a CSIRT está integrada numa empresa com políticas de segurança informática em vigor, as políticas correspondentes aplicáveis à CSIRT foram estabelecidas com o auxílio do consultor jurídico da empresa.

Etapas 7: Procurar cooperação

Utilizando o Inventário da ENISA, seria rápido encontrar e contactar algumas CSIRT do mesmo país. Combinou-se uma visita do chefe de equipa recém-contratado às instalações de uma delas, onde foi informado sobre as actividades das CSIRT nacionais e participou numa reunião.

Esta reunião foi extremamente útil para recolher exemplos de métodos de trabalho e obter apoio de outras equipas.

Etapas 8: Promoção do Plano de Actividades

É decidido proceder à recolha de factos e números da história da empresa, de grande utilidade para uma perspectiva estatística da situação de segurança informática. A recolha deve ser prosseguida quando a CSIRT estiver a funcionar, de modo a manter as estatísticas actualizadas.

Foram contactadas outras CSIRT nacionais, que foram entrevistadas sobre as suas fundamentações empresariais. As CSIRT colaboraram, compilando alguns diapositivos com informação sobre a evolução recente em matéria de incidentes de segurança informática e sobre os custos dos incidentes.

Neste exemplo de CSIRT fictícia, não foi necessário convencer a administração da importância da informática, pelo que não foi difícil obter luz verde para a primeira etapa. Foram preparados planos de investimento e de projecto, incluindo uma estimativa dos custos de estabelecimento e de funcionamento.

Etapa 9: Estabelecimento de fluxos de processos e de procedimentos operacionais e técnicos

A CSIRT fictícia concentra-se na prestação dos serviços CSIRT essenciais:

- Alertas e avisos
- Comunicações
- Gestão de incidentes

A equipa desenvolveu procedimentos que funcionam bem e são facilmente compreensíveis por todos os membros da equipa. A CSIRT fictícia contratou ainda um jurista para se ocupar das responsabilidades e da política de segurança informática da empresa. A equipa adoptou algumas ferramentas úteis e encontrou informações úteis sobre questões operacionais na sequência de debates com outras CSIRT.

Foi produzido um modelo para as recomendações de segurança e as notificações de incidentes. A equipa utiliza RTIR para a gestão de incidentes.

Etapa 10: Formação do pessoal

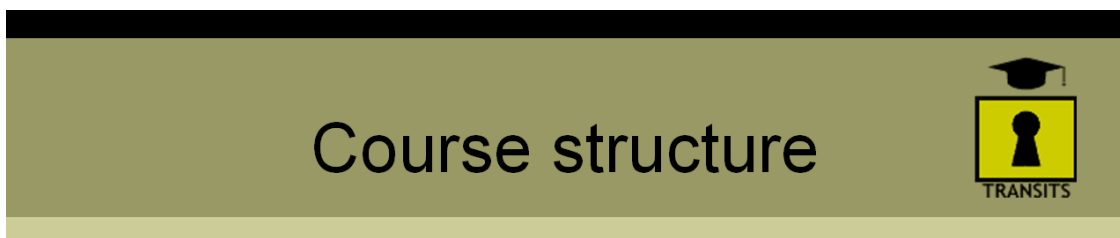
A CSIRT fictícia decide que todo o pessoal técnico frequentará os próximos cursos TRANSITS. O chefe de equipa deve ainda frequentar o curso *Managing a CSIRT* [Gerir um CSIRT] do CERT/CC.

Etapa 11: Funcionamento

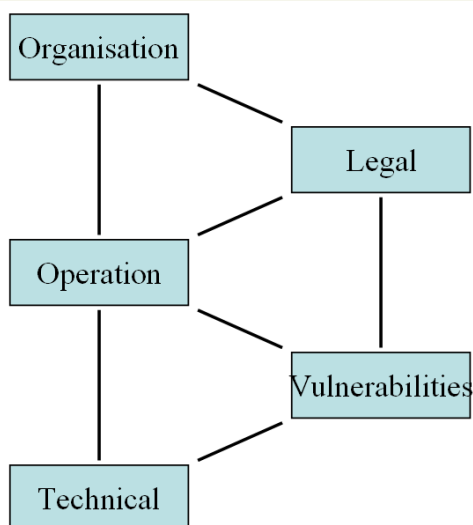
Durante as primeiras semanas de funcionamento, a CSIRT fictícia utilizou diversos casos fictícios (que foram cedidos como exemplos por outros CSIRT) como exercícios. Emitiu ainda algumas recomendações de segurança com base em informações sobre vulnerabilidades reais, distribuídas por fornecedores de *hardware* e de *software*, que considera rigorosas e ajustadas às necessidades da comunidade de utilizadores.

A.4 Material dos cursos para CSIRT

TRANSITS (gentilmente autorizados por Terena <http://www.terena.nl>)



- Five modules
- Independent, but linked
- 12-14 hours work in 2 days
- Practical exercises include
 - Analyse incidents
 - Organisational plan
 - Incident response plan



CSIRT training course

©TERENA, 2002-6

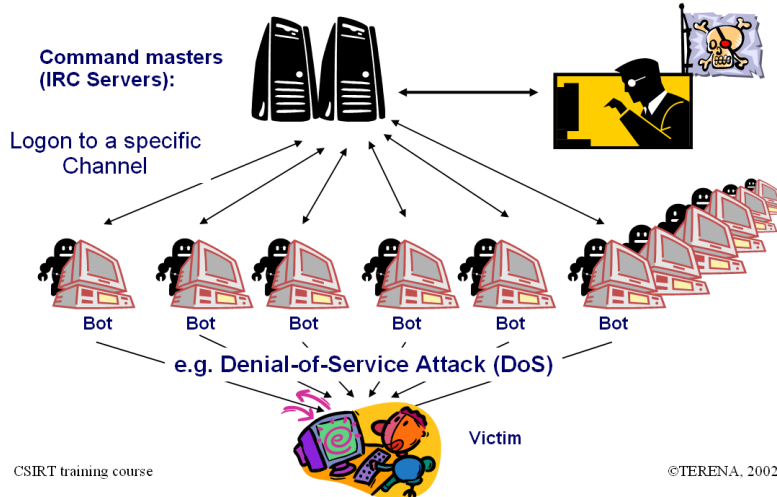
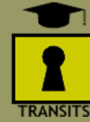


Estrutura do curso		
Cinco módulos	Organização	
Independentes, mas interligados		
12-14 horas de trabalho em dois dias		Questões jurídicas
Os exercícios práticos incluem	Funcionamento	
Análise de incidentes		
Plano organizacional		Vulnerabilidades
Plano de resposta a incidentes		
	Técnica	

Panorâmica: estrutura do curso

Malicious Code

Malicious IRC Bots - A botnet in action



Código malicioso		
<i>Bots IRC maliciosos – Uma rede de bots em acção</i>		
Commando (servidores IRC)		
Início de sessão num canal específico		
	por exemplo, ataque de negação de serviço (DoS)	
	vítima	

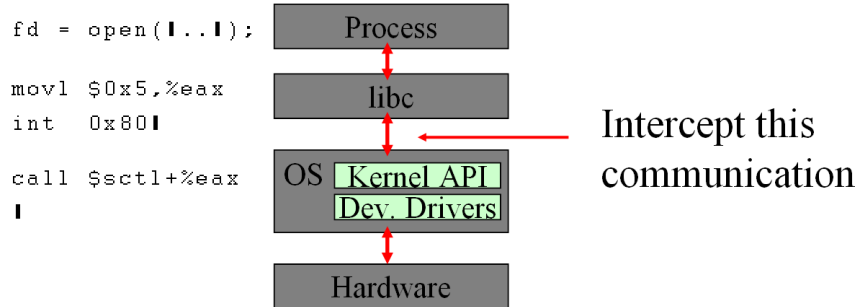
Do *Módulo técnico*: Descrição de uma *botnet*

Malicious Code

Rootkits - Basic design



- Replacing binaries is easily detected (tripwire et al).
- A more elegant approach would deliver false data to **all** processes -> Modify kernel

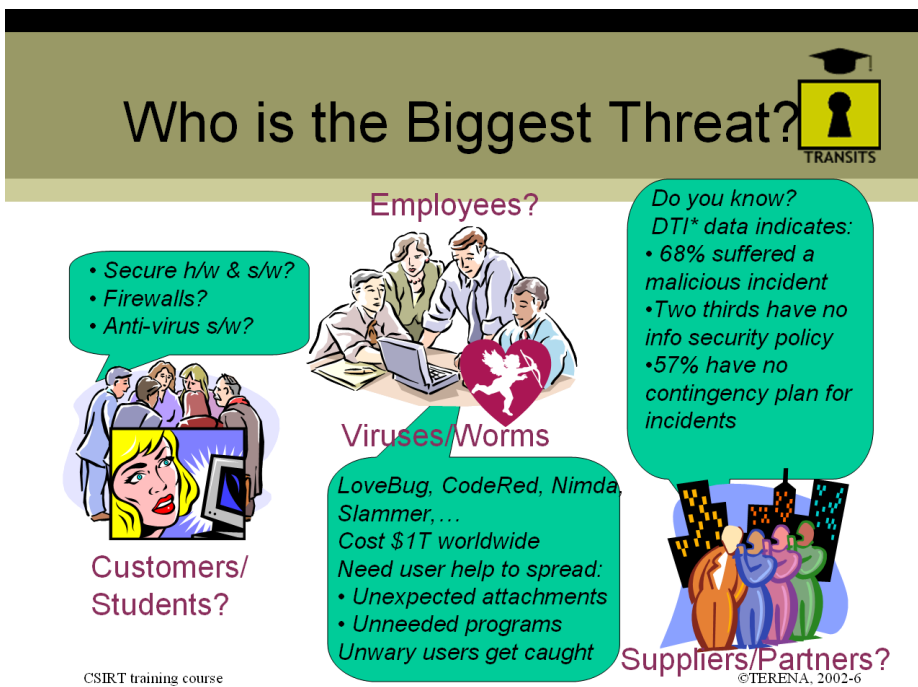


CSIRT training course

©TERENA, 2002-6

Código malicioso		
<i>Rootkits (programas de ataque à raiz) – Conceção básica</i>		
A substituição de binários é facilmente detectada (Tripware e outros programas)		
Uma abordagem mais elegante introduziria dados falsos em todos os processos -> alteração do núcleo do sistema		
	Processo	
	<i>libc</i>	
	OS, API, núcleo do sistema	Interceptar esta comunicação
	Dev, drivers	
	<i>Hardware</i>	

Do *Módulo técnico*: Conceção básica de um *rootkit*.

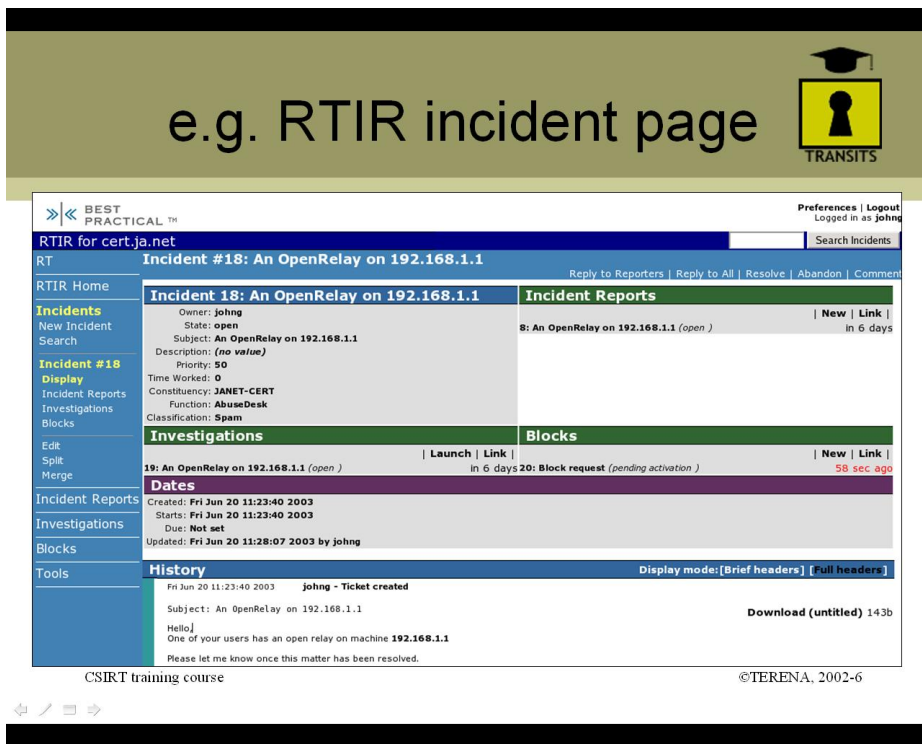


Quem constitui a maior ameaça		
	Os empregados?	Sabia? Dados do DTI* indicam que:
Hardware e software seguros? Firewalls? Software antivírus?		<ul style="list-style-type: none"> • 68% foram objecto de um incidente malicioso • dois terços não dispõem de política de segurança informática • 57% não possuem um plano de contingência para incidentes
	Vírus/vermes	
Clientes/Estudantes?	LoveBug, CodeRed, Nimda, Slammer... custam um bilião de dólares em todo o mundo É necessário que os utilizadores ajudem a difundir: <ul style="list-style-type: none"> • anexos não desejados • programas desnecessários Os utilizadores desprevenidos são	Fornecedores/Parceiros?

	as vítimas	
* Inquérito às falhas de segurança informática do Ministério do Comércio e Indústria do Reino Unido, 2004.		

Do *Módulo organizacional*: No interno ou exterior – onde está a maior ameaça?

e.g. RTIR incident page



CSIRT training course ©TERENA, 2002-6

Da *pista operacional*: Request Tracker for Incident Response (RTIR) [localizador de pedidos de resposta a incidentes]

		Exemplo de página RTIR	
Incidentes		Incidente 18: Relé aberta em	Comunicação de incidente
Novo acidente			
Procura			
Apresentação de incidente 18	de	Proprietário	Relé aberta em....
Notificação	de	Estado	
incidente		Assunto	
Investigações		Descrição	
Bloqueios		Prioridade	
		Tempo de trabalho	
		Comunidade de utilizadores	
		Função	
		Classificação	
		Investigações	Bloqueios
		Relé aberta em	Solicitação de bloqueio (activação pendente)

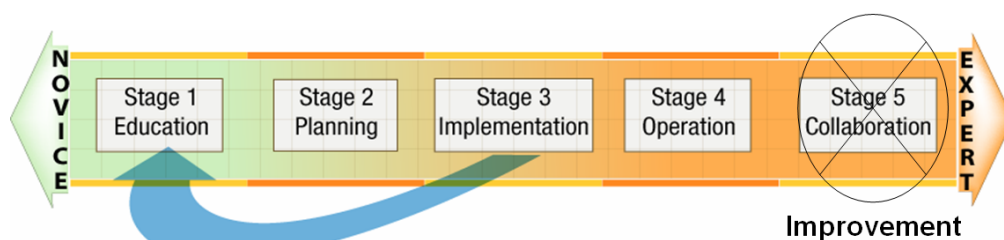
Notificação incidente Investigações Bloqueios	de	Datas	
		História Assunto: Relé aberta em Olá, um dos vossos utilizadores tem uma relé aberta em Agradeço que informem quando o problema estiver resolvido.	

“Criação de CSIRT” (gentilmente autorizado pelo CERT/CC, <http://www.cert.org>)

A ENISA agradece à equipa de desenvolvimento da CSIRT do programa CERT a autorização para utilizar conteúdos dos seus cursos de formação!

Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 ~~Peer collaboration~~ — Improvement of the CSIRT



© 2006 Carnegie Mellon University

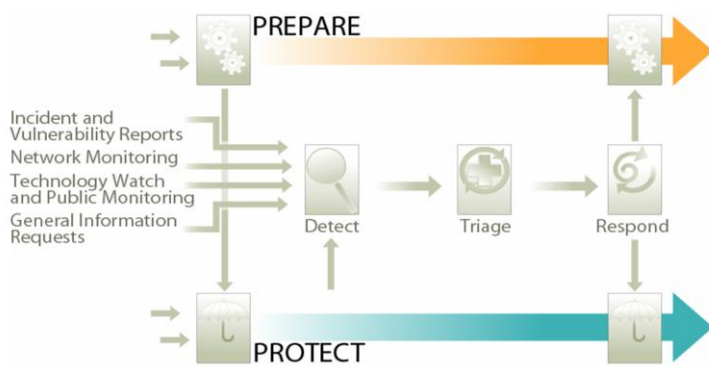
2



Fases de desenvolvimento de uma CSIRT						
Fase 1	Educação da organização					
Fase 2	Planificação do esforço					
Fase 3	Implementação inicial					
Fase 4	Fase operacional					
Fase 5	Colaboração dos pares — Melhoria da CSIRT					
Principiantes	Fase 1 Educação	Fase 2 Planificação	Fase 3 Implementação	Fase 4 Funcionamento	Fase 5 Colaboração	Peritos
					Melhoria	

Do Curso de formação do CERT/CC: Etapas da criação de CSIRT.

Incident Management Best Practice Model

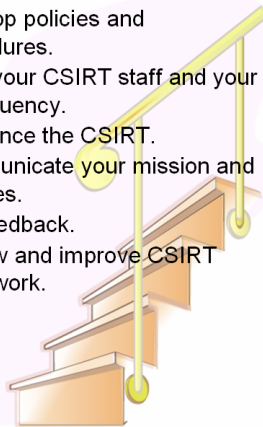


Modelo de melhores práticas de gestão de incidentes			
	PREPARAÇÃO		
Notificações de incidentes e de vulnerabilidades			
Acompanhamento de redes			
Vigilância tecnológica e acompanhamento público	Detecção	Triagem	Resposta
Pedidos de informações gerais			
	PROTECÇÃO		

Do *Curso de formação* do CERT/CC: Melhores práticas na gestão de incidentes.

Basic Implementation Steps

- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and improve CSIRT framework.



© 2006 Carnegie Mellon University

4

CERT

Etapas básicas de implementação

- | | |
|---|---|
| <ul style="list-style-type: none"> • Recolha de informações. • Identificação da comunidade de utilizadores da CSIRT. • Determinação da missão da CSIRT. • Obtenção de fundos para o funcionamento da CSIRT. • Determinação da categoria e dos níveis de serviço da CSIRT. • Determinação da estrutura de notificação da CSIRT, da autoridade e do modelo organizativo. • Identificação de interacções com partes importantes da comunidade de utilizadores. • Definição de papéis e de responsabilidades para interacções. • Criação de um plano, obtenção de <i>feedback</i> sobre o plano. | <ul style="list-style-type: none"> • Identificação e aquisição de recursos humanos, equipamento e infra-estruturas. • Definição de políticas e procedimentos. • Formação do pessoal da CSIRT e da comunidade de utilizadores. • Divulgação da CSIRT. • Comunicação da missão e dos serviços • Obtenção de <i>feedback</i> • Avaliação e melhoramento do quadro da CSIRT. |
|---|---|

Do *Curso de formação* do CERT/CC: Etapas a seguir na criação de CSIRT.

Range of CSIRT Services



© 2006 Carnegie Mellon University

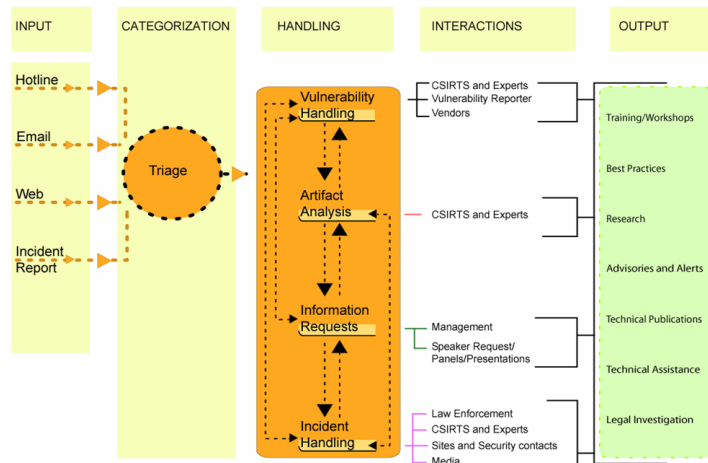
5



Gama de serviços da CSIRT		
Serviços reactivos	Serviços proactivos	Serviços de gestão da qualidade da segurança
<ul style="list-style-type: none"> • Alertas e avisos • Gestão de incidentes <ul style="list-style-type: none"> - Análise de incidentes - Resposta a incidentes no local - Apoio à resposta a incidentes - Coordenação da resposta a incidentes • Gestão das vulnerabilidades <ul style="list-style-type: none"> - Análise da vulnerabilidade - Resposta à vulnerabilidade - Coordenação da resposta à vulnerabilidade • Gestão de artefactos <ul style="list-style-type: none"> - Análise de artefactos - Resposta a artefactos - Coordenação da resposta a artefactos 	<ul style="list-style-type: none"> ❖ Recomendações ❖ Vigilância tecnológica ❖ Auditorias ou avaliações de segurança ❖ Configuração e manutenção de ferramentas de segurança, aplicações e infra-estruturas ❖ Desenvolvimento de ferramentas de segurança ❖ Serviços de detecção de intrusões ❖ Divulgação de informações relacionadas com segurança 	<ul style="list-style-type: none"> ✓ Análise dos riscos ✓ Continuidade da actividade e planificação da recuperação de emergência ✓ Consultoria de segurança ✓ Sensibilização ✓ Educação/Formação ✓ Avaliação ou certificação de produtos

Do Curso de formação do CERT/CC: Os serviços que uma CSIRT pode prestar

Service Integration



© 2006 Carnegie Mellon University

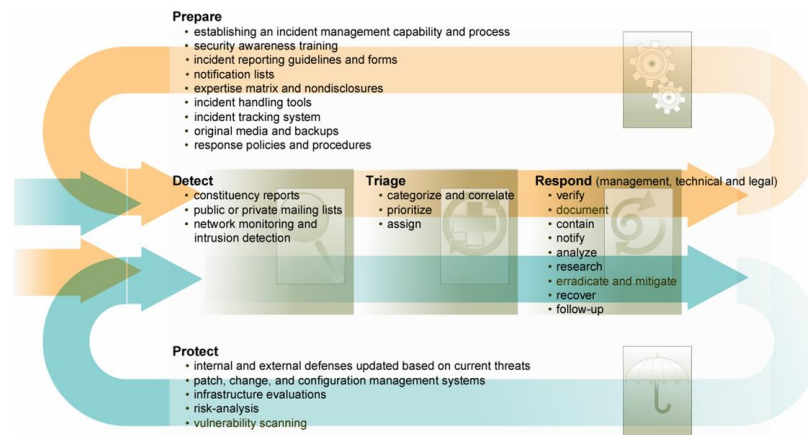
6



Integração do serviço				
ENTRADA	CLASSIFICAÇÃO	GESTÃO	INTERACÇÕES	RESULTADOS
Linha directa	Triagem	Gestão de vulnerabilidade	CSIRT e peritos Notificante da vulnerabilidade Fornecedores	Formação/ <i>Workshops</i>
E-mail				Melhores práticas
Web		Análise De artefacto	CSIRT e peritos	Investigação Recomendações e alertas
Notificação do incidente		Pedidos De informação	Administração Representante/ painéis/apresentações	Publicações técnicas Assistência técnica
		Gestão de incidentes	Aplicação da legislação CSIRT e peritos Sítios e contactos de segurança Comunicação social	Investigação judicial

Do Curso de formação do CERT/CC: O fluxo de trabalho da gestão de incidentes.

Incident Response Starts Before an Incident Occurs



© 2006 Carnegie Mellon University

8



A resposta a incidentes começa antes de estes ocorrerem

Preparação

- Criação de capacidade e processos de gestão de incidentes
- Formação em sensibilização para a segurança
- Directrizes e formulários para a notificação de incidentes
- Listas de notificação
- Matriz de competência e confidencialidade
- Ferramentas de gestão de incidentes
- Sistema de acompanhamento de incidentes
- Suporte original e cópias de segurança
- Políticas e procedimentos de resposta

Deteção

- Relatórios da comunidade de utilizadores
- Listas de distribuição públicas ou privadas
- Acompanhamento de redes e detecção de intrusões

Triagem

- Classificação e correlacionamento
- Estabelecimento de prioridades
- Atribuição

Resposta (de gestão, técnica e judicial)

- Verificar
- Documentar
- Conter
- Notificar
- Analisar
- Investigar
- Erradicar e atenuar
- Recuperar
- Acompanhar

Protecção

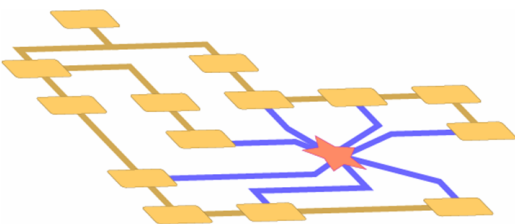
- Defesas internas e externas actualizadas com base nas ameaças actuais
- Correção, alteração e configuração dos sistemas de gestão
- Avaliações das infra-estruturas
- Análise dos riscos
- Exploração de vulnerabilidades

Do *Curso de formação* do CERT/CC: Resposta a incidentes

Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

You need to envision a model that can be implemented.



© 2006 Carnegie Mellon University

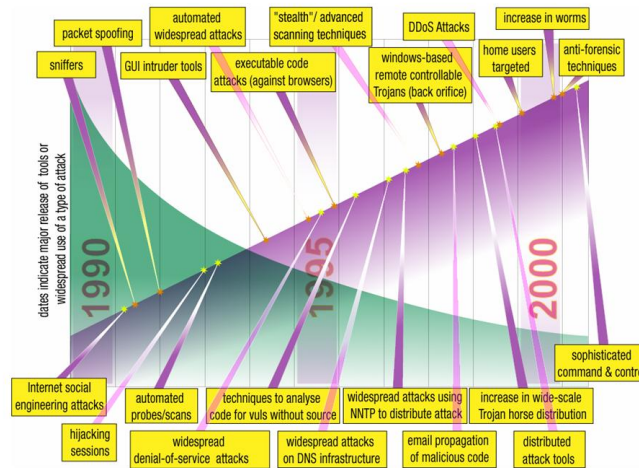
7

CERT

Modelos de organização
<p>Ao conceber uma CSIRT, é necessário pensar de que forma esta vai funcionar e interagir com a organização e a comunidade de utilizadores.</p> <p>É importante antever um modelo que seja exequível.</p>

Do *Curso de formação* do CERT/CC: Como organizar o CSIRT

Attack Sophistication versus Required Intruder Knowledge



© 2006 Carnegie Mellon University

9



Sofisticação dos ataques *versus* conhecimento necessário em matéria de intrusão

Pacote de spoofing		Ataques de disseminação automática		"Vírus furtivos"/técnicas avançadas de exploração	Ataques DDoS	Aumento do número de vermes	
S nif fer s	Ferramentas de intrusão GUI	Ataques com código executável (contra programas de navegação)		Cavalos de Tróia localizados no Windows controláveis à distância (<i>back office</i>)	Utilizadores domésticos como alvo	Técnicas anti-forenses	
As datas indicam uma forte saída de ferramentas de recurso maciço a um tipo de ataque							Comando e controlo sofisticados
		Ataques de engenharia social via Internet	Sondagem/exploração automatizada	Técnicas para analisar código para <i>vuls</i> sem fonte	Ataques maciços com recurso a NNTP para distribuir o ataque	Aumento da distribuição em grande escala de cavalos de Tróia	
		Sessões de pirataria	Ataques maciços de negação de serviço	Ataques maciços a infra-estruturas DNS	Propagação de e-mails de código malicioso	Ferramentas de ataque distribuídas	

Do Curso de formação do CERT/CC: Menos conhecimentos, mais danos.