Gerenciamento de Incidentes: o Papel do CSIRT no Aumento da Segurança das Corporações

Cristine Hoepers

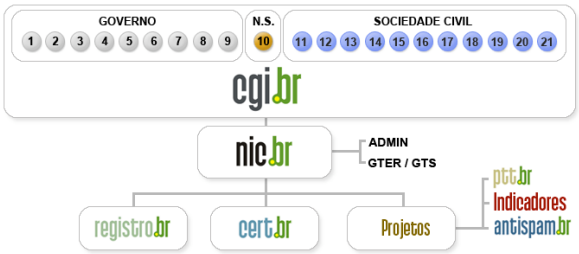
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br
http://www.cert.br/

Comitê Gestor da Internet no Brasil - CGI.br
http://www.cgi.br/

Agenda

- Sobre o CGI.br e o CERT.br
- Gerenciamento de Incidentes
  - Conceitos
  - Como integrar com a estrutura de segurança existente
  - O papel do CSIRT: reativo e proativo
- CSIRTs no Brasil
- CSIRTs no Mundo
- Treinamento
- Referências

Comitê Gestor da Internet no Brasil



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

Atividades do CERT.br

- Articulação das ações para resposta a incidentes envolvendo redes brasileiras, por exemplo:
  - Combate a fraudes: contato com sites envolvidos para remoção de códigos maliciosos; envio de novos exemplares para fabricantes de antivírus; troca de informações técnicas com instituições financeiras
- Manutenção de estatísticas sobre incidentes de segurança
- Desenvolvimento de documentos de Boas Práticas para usuários e administradores de redes
- Fomento à criação de novos Grupos de Segurança e Resposta a Incidentes (CSIRTs) no Brasil
- Oferecimento de cursos oficiais do CERT®/CC
- Coordenação do Consórcio Brasileiro de Honeypots

Parcerias do CERT.br

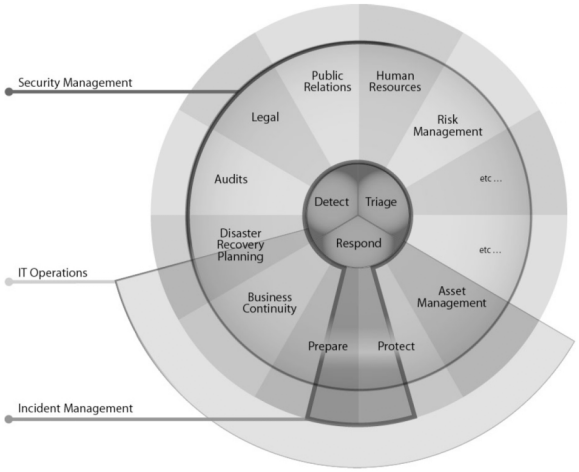
- Forum of Incident Response and Security Teams (FIRST) Full member
  http://www.first.org/membership/
- Anti-Phishing Working Group (APWG) Research Partner
  http://www.antiphishing.org/
- Honeynet Research Alliance Member
  http://honeynet.org/alliance/

Gerenciamento de Incidentes

O que é Gerenciamento de Incidentes?

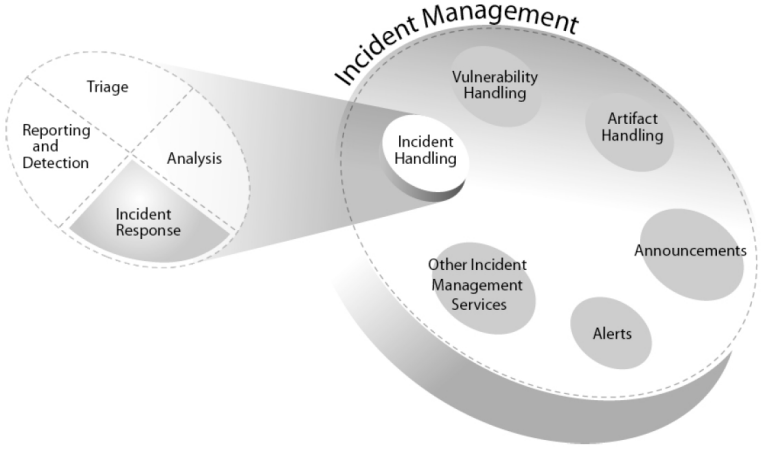
- Conjunto de processos necessários para controlar ou administrar as tarefas associadas com o tratamento de incidentes de segurança
- Realização de serviços proativos e reativos, que auxiliam o processo de tratamento de incidentes de segurança
- Normalmente envolve os seguintes processos: Preparação, Proteção, Detecção, Triagem e Resposta

Processos de Segurança e de TI



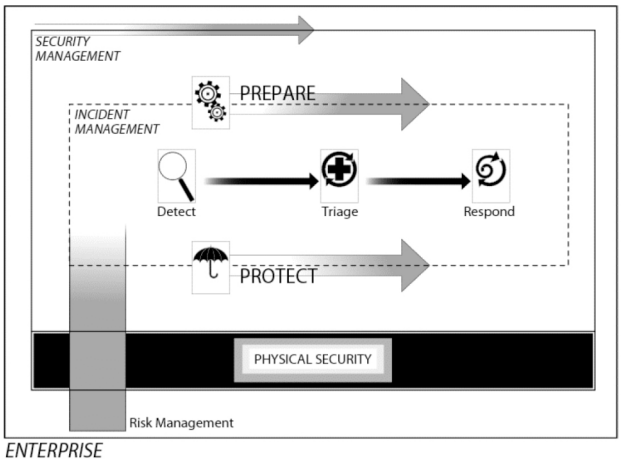
Fonte: "*Defining Incident Management Processes for CSIRTs: A Work in Progress*"
http://www.cert.org/archive/pdf/04tr015.pdf
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.

O Gerenciamento de Incidentes



Fonte: "*Defining Incident Management Processes for CSIRTs: A Work in Progress*"
http://www.cert.org/archive/pdf/04tr015.pdf
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.

Processos que Habilitam o Efetivo Gerenciamento de Incidentes



Fonte: "*Defining Incident Management Processes for CSIRTs: A Work in Progress*"
http://www.cert.org/archive/pdf/04tr015.pdf
Figura utilizada com permissão do CERT®/CC e do SEI/CMU.

O que é um CSIRT?

Um "*Computer Security Incident Response Team* (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança, é uma organização ou grupo responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

Serviços proativos: auxiliam os processos de Preparação e Proteção, auxiliando o público alvo a manter-se seguro, antecipando-se a problemas de segurança ou ataques.

Serviços reativos: são iniciados na ocorrência de eventos de segurança ou a pedido do público alvo.

Outros serviços: o CSIRT pode auxiliar a instituição em diversos serviços de segurança, normalmente executados por outras partes da organização.

Serviços de um CSIRT

Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling Incident analysis Incident response on site Incident response support Incident response coordination Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination Artifact Handling Artifact analysis Artifact response Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Fonte: "*CSIRT Services*"
http://www.cert.org/services/services.html

Histórico dos CSIRTs no Brasil

- Agosto/1996: o CGI.br divulgou o documento: "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil."
  - Ser uma organização neutra
  - Atuar como ponto focal para tratamento de incidentes no Brasil
  - Facilitar o contato e a troca de informações entre as redes envolvidas em incidentes de segurança;
  - Manter estatísticas públicas sobre a natureza dos incidentes ocorridos no Brasil.
- Junho/1997: o CGI.br cria o CERT.br (naquela ocasião chamado NBSO - NIC BR Security Office), com base nas recomendações do relatório.

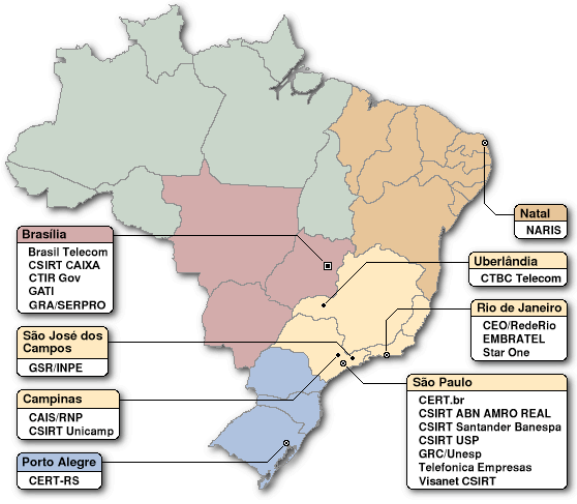
http://www.nic.br/grupo/historico-gts.htm

Histórico dos CSIRTs no Brasil (cont)

- Agosto/1997: a RNP cria o CAIS/RNP[1], seguida pela criação do CERT-RS[2], que atende às redes acadêmicas do Estado do Rio Grande do Sul;
- 1999: outras instituições, incluindo Universidades e empresas de Telecomunicações, anunciaram seus CSIRTs;
- 2003: mais de 20 CSIRTs formados no Brasil;
- 2004: criado o CTIR Gov, para atender a redes pertencentes à Administração Pública Federal[3].

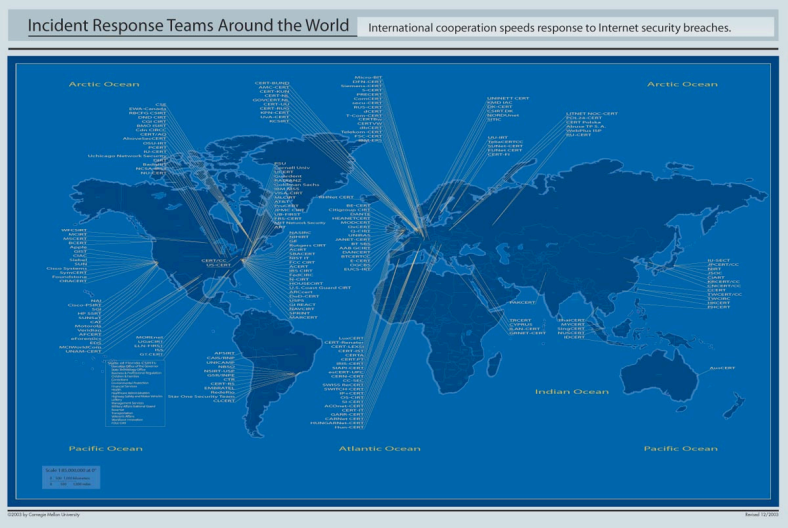
[1] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[2] http://www.cert-rs.tche.br/cert-rs.html
[3] http://www.ctir.gov.br

CSIRTs no Brasil



http://www.cert.br/contato-br.html

CSIRTs no Mundo



http://www.cert.org/csirts/

Onde Obter Treinamento

Cursos do AusCERT

- Oferecidos na Austrália

Cursos do CERT®/CC

- Oferecidos nos Estados Unidos no Software Engineering Institute, Carnegie Mellon University (SEI/CMU)
- Oferecidos no Brasil pelo CERT.br (SEI Partner):
  - Creating a CSIRT e Managing CSIRTs
  - Fundamentals of Incident Handling
  - Advanced Incident Handling for Technical Staff
- Mais de 160 pessoas treinadas
- A partir do 4º trimestre o CERT.br passará a oferecer no Brasil todos os cursos para obtenção da Certificação "*CERT® Certified Computer Security Incident Handler*"

Referências

- Esta palestra
  http://www.cert.br/docs/palestras/
- Documentos de apoio para CSIRTs
  http://www.cert.br/csirts/
- Criando um Grupo de Resposta a Incidentes de Segurança em Computaroes: Um Processo para Iniciar a Implantação
  http://www.cert.br/certcc/csirts/Creating-A-CSIRT-br.html
- Cartilha de Segurança para Internet
  http://cartilha.cert.br/
- Cursos Oficiais do CERT®/CC ministrados pelo CERT.br
  http://www.cert.br/cursos/