questera REPORT

QR20040604PR

4 de Junho de 2004

# Equipes de Resposta a Emergências Computacionais, Um Cenário de Excelência

**Phil Rosch – Old Harbour Consulting**

## Sumário



## Resumo Executivo

Equipes de Resposta à Emergências Computacionais (Computer Emergency Response Teams - CERT).

A composição de uma CERT pode variar desde uma pessoa “que sabe muito sobre PCs” até uma bem coordenada, multidisciplinar e experiente equipe policial tática. Irei pormenorizar a minha visão de como organizar uma equipe em companhias prestadoras de serviços financeiros de médio e grande porte, e comentar sobre alguns dos fatores críticos para o sucesso.

# Estabelecendo o Caso de Negócio

Mesmo grandes companhias não podem se dar ao luxo de manter uma CERT em tempo integral. Logo, a prioridade é estruturar as necessidades em termos de gerenciamento de riscos. Recomendo o "modelo de corpo de bombeiros voluntário" para a maioria das companhias. Quando o alarme toca, agentes-chave param o que estão fazendo para responder ao chamado. Os elementos de um caso de negócio bem pensado são:

- uma avaliação-base das atuais capacidades de resposta,
- discussões com áreas de negócios para definir as necessidades emergentes,
- sondagens ambientais internas para avaliar a presente experiência real com incidentes,
- sondagens externas para comparar a experiência interna com a da indústria,
- a experiência da indústria em casos legais
- um paradigma de "situação desejada", baseado nos itens acima, e articulando:
  - Os objetivos da equipe
  - As implicações organizacionais e as relações de comando
  - Os critérios de candidatos
  - A métrica
  - Os requisitos iniciais de financiamento
  - Os requisitos contínuos de financiamento

Uma vez que o caso de negócio esteja completo, é necessário comunicá-lo e vendê-lo aos stakeholders, de maneira a conseguir a sua aprovação e estabelecer o nível geral de risco a ser aceito, designado ou mitigado.

# Formando a equipe

Quem deve ser recrutado e por quê? Aqui estão alguns candidatos e porque eles devem ser considerados:

- Engenharia de Redes — essa é óbvia. Essas são as pessoas que mantém a infra-estrutura disponível.
- Engenharia de Firewall — geralmente é um braço da equipe de rede, mas está se separando organizacionalmente em muitas companhias.
- Administração de Segurança — Direitos e privilégios
- Meios — HVAC e ambientes
- Engenharia de Correio Eletrônico — uma organização distinta em muitas companhias
- Departamento Legal — para aconselhar sobre conservação de evidências e problemas legais
- Comunicação Corporativa — para lidar com "controle de danos" e coreografar conferências com a imprensa
- Suporte Técnico de Segurança — "administradores-chefe" e tecnólogos de segurança dando suporte à arquitetura e aos padrões globais de segurança

- Segurança Física — às vezes, terceirizada, normalmente é parte do Gerenciamento de Meios, se for da casa
- Auditoria Interna — para aconselhamento
- Unidade de Fraude — se houver uma equipe desse tipo na sua companhia
- Acesso de Fornecedores — Disponibilidade de pessoal de suporte dos fornecedores na área de Gerenciamento de Vírus e Detecção de Intrusão

Todas essas habilidades devem estar disponíveis para o líder da CERT, que geralmente é o Chefe da Segurança (CSO) ou um assessor direto. Nem todos os incidentes necessitarão da presença da equipe inteira, mas todos os recursos devem estar disponíveis rapidamente e treinados para atuar efetivamente.

## Implicações

A maioria dos fatores críticos para o sucesso envolvem uma dedicação contínua para financiar e exercitar a equipe. Por exemplo:

- A equipe precisa ter acesso a um “laboratório de interoperabilidade”, o qual reflita a estrutura atual do fluxo de produção. Eles precisam de um “parque” onde possam introduzir um vírus e otimizar os manuais de resposta.
- Já que ninguém estará presente em tempo integral, com exceção do CSO, tempo para treinamento, que requer que o participante não esteja atuando na sua função principal, terá que ser negociado com cada área de suporte.
- Hardware especial e licenças de software adicionais serão necessários e devem ser orçados pela organização do CSO de maneira a reduzir a complexidade.
- A equipe tem que ser guiada por um manual ou mapa processual. Eu recomendaria a metodologia, baseada em cenários, de Backup de Desastre e Recuperação (DBAR), na qual alocam-se recursos para cobrir riscos de DBAR em ordem de prioridade (do mais provável ao menos provável). Muitas companhias se atrofiam ao se preocupar com o holocausto e são derrubadas pelo mau-funcionamento de uma bomba d’água em um arranha-céu.

Resumindo, as equipes mais bem sucedidas são bem treinadas, bem exercitadas, bem capitalizadas e bem lideradas.

## Sobre o Autor

Phil Rosch é um veterano com mais de 35 anos de experiência em TI. Antes de fundar a Old Harbour Consulting, ele dirigiu a equipe de Estabelecimento de Direção em TI da Aetna, a qual criou, alinhou e dirigiu a visão de tecnologia de empreendimentos da companhia, incluindo sua estratégia, arquitetura, política e seus padrões. Antes disso, ele dirigiu o Suporte Técnico Corporativo da Aetna, responsável não só pela extensa pasta de hardware e software, bem como por todos os trabalhos de consultoria técnica sênior. Phil também atuou como diretor de pesquisa da Giga Information Group para a área de segurança e risco.

Phil é um trabalhador multidisciplinar com experiência real e prática em implementar arquitetura e padrões de TI, e em reengenharia de segurança. Seu histórico também inclui experiência com uma vasta gama de operações e suporte técnico, incluindo o posto de chefe de segurança por nove anos.

Phil cursou a Universidade de Connecticut, o Instituto de Marketing Ford, e recebeu certificados em gerenciamento de projeto, da Universidade de Boston, e gerenciamento de processo, da IBM.