**GUIA PARA UMA POLÍTICA DE TRATAMENTO DE INCIDENTES**

Este documento é um guia a ser usado antes, durante, e depois de um incidente de segurança de computador que aconteça na empresa.

As seções abaixo são um esboço inicial para a criação da política de sua empresa para tratamento de incidentes de segurança. As seções são:

1. **Preparando e planejando** (quais são as metas e objetivos no tratamento de um incidente).

Parte do tratamento de um incidente é estar preparado para responder a um incidente antes dele acontecer. Proteção inclui preparar diretrizes de tratamento de incidentes como parte de um plano de contingência para sua empresa.

Ter planos escritos elimina conduzirá a um conjunto mais apropriado e completo de respostas. É vitalmente importante testar o plano proposto antes de um incidente acontecer. Um grupo poderia considerar a contratação de um grupo-tigre, que é um grupo de especialistas que tentam penetrar a segurança de um sistema.

Devido à natureza do incidente, pode haver um conflito entre analisar a fonte original de um problema e restabelecer sistemas e serviços. Metas globais (como assegurar a integridade de sistemas críticos) pode ser uma razão para não analisar um incidente. É claro, esta é uma decisão de administração importante; mas todas as partes envolvidas devem estar conscientes que sem análise pode o mesmo incidente acontecer novamente.

Também é importante priorizar as ações a serem tomadas durante um incidente antes do incidente acontecer. Às vezes um incidente pode ser tão complexo que é impossível fazer tudo ao mesmo tempo para responder a ele; prioridades são essenciais. Embora prioridades variem de instituição para instituição, as seguintes sugestões de prioridades podem servir como ponto de partida para definir a resposta de sua organização:

Prioridade 1 --proteja vida humana e segurança das pessoas; vida humana sempre tem precedência sobre outras considerações.

Prioridade 2 -- proteger dados importantes. Previna exploração sistemas, redes ou locais importantes. Informe sistemas, redes ou locais importantes que tenham sido afetados sobre invasões acontecidas.

Prioridade 3--proteja outros dados incluindo dados proprietários, científicos, administrativos e outros, pois perda de dados é cara em termos de recursos.

Prioridade 4--previna dano para sistemas (por exemplo, perda ou alteração de arquivos de sistemas, danos a unidades de disco, etc.). Danos em sistemas pode resultar em custo de recuperação alto.

Prioridade 5--minimize a interrupção dos recursos de computação (inclusive processos). É melhor em muitos casos desligar um sistema ou desconecta-lo de uma rede que arriscar dano para dados ou sistemas.

2. **Notificação** (quem deveria ser contatado no caso de um incidente).

\* Os gerentes locais e pessoal;

\* Agências investigativas e executoras da lei;

\* Equipes CERT;

\* Locais afetados e envolvidos;

\* Comunicações internas;

\* Relações públicas e imprensa;

3. **Identificando um incidente** (verificar se a suspeita de um incidente se confirma e qual a sua criticidade).

4. **Tratamento** (ações a serem tomadas no caso de um incidente).

\* Notificação (quem deveria ser notificado sobre o incidente);

\* Protegendo evidências e logs de atividades (que registros deveriam ser mantidos de antes, durante, e depois do incidente);

\* Contenção (como o dano pode ser limitado);

\* Erradicação (como eliminar as causas do incidente);

\* Recuperação (como restabelecer serviço e sistemas);

\* Sequência (que ação devem ser tomadas depois do incidente).

5. **Consequências** (quais as implicações de incidentes passados).

6. **Resposta administrativa para incidentes**.