Plano: gestão de incidentes de segurança

Autor: Graciela Martínez
Edição: Área de Comunicações
Área: Área de Tecnologia

Novembro 2023

lacnic
www.lacnic.net

Objetivo

O objetivo deste documento é compartilhar um breve resumo das etapas básicas que definam um plano geral para implementar a gestão de incidentes de segurança em uma organização. Ter este plano definido ajuda na resposta eficaz perante a ocorrência de um incidente de segurança.

Etapa de preparação

- Estabelecer o CSIRT
- Desenvolver um plano de resposta a incidentes de segurança: identificar, assessorar, mitigar e recuperar
- Estabelecer um mecanismo para denunciar incidentes de segurança, tanto para a comunidade alvo quanto para outras partes interessadas.
- Definir a taxonomia dos incidentes e seu nível de gravidade
- Definir o procedimento para a triagem das denúncias recebidas
- Definir um plano de comunicação para as partes interessadas internas e externas que inclua porta-vozes autorizados e leve em conta a imagem da organização
- Capacitar a equipe para que saiba como identificar possíveis ameaças e como denunciar incidentes de segurança
- Criar um inventário de ativos críticos

Etapa de identificação

- Detectar eventos e incidentes: implementar sistema de monitoramento, centralizar logs, implementar sistemas de detecção de intrusos

Etapa de contenção e erradicação

- Identificar o(s) sistema(s) afetado(s) e tomar medidas eficazes o mais rápido possível para evitar danos maiores
- Analisar se corresponde fazer notificações legais
- Iniciar a documentação correspondente, mantendo a ordem dos fatos em uma linha do tempo
- Preparar as comunicações, divulgar aos possíveis afetados e a qualquer pessoa que corresponder
- Investigar o incidente de segurança para determinar as causas que permitiram o ataque, a extensão dos danos causados, avaliar possível comprometimento de outros sistemas e analisar possíveis vulnerabilidades não detectadas até o momento
- Erradicar a causa do incidente (Exemplo: remover malware, aplicar patches, alterar senhas, avaliar a eficácia da rastreabilidade de eventos, realizar análises forenses onde e quando for apropriado, procurar artefatos para sua análise posterior, etc.)
- Documentar os motivos do incidente, as ações tomadas e quaisquer fatos que sejam relevantes para o correto entendimento deste.

Etapa de recuperação

- Restaurar os sistemas afetados à medida que forem corrigidos
- Restaurar dados de backups de acordo com o plano da organização (se necessário)
- Implementar novos controles e medidas que tenham sido identificados no processo de investigação

Etapa de avaliação pós-incidente

- Revisar a documentação gerada nas etapas prévias e completar com as informações que julgar necessárias para que sirvam de futura referência.
- Documentar as lições aprendidas:
    - Forças e fraquezas da gestão de incidentes
    - Avaliar se corresponde elaborar um plano de capacitação de acordo com as características do incidente analisado
    - Avaliar se corresponde uma atualização do plano de gestão

Plano de comunicação

É muito importante ter um plano de comunicação definido e acordado na organização. Durante a gestão de um incidente é necessário realizar as comunicações pertinentes em função deste.

Em termos gerais, os seguintes aspectos devem ser levados em consideração:

- Comunicar internamente à organização durante todas as etapas da gestão de incidentes, de acordo com a necessidade de conhecimento de cada função
- Comunicar a todas as partes interessadas externas à organização de acordo com as normas vigentes e a necessidade de saber sobre elas
- Definir como será gerenciada a intervenção da imprensa, se necessário
- Se for o caso, realizar:
    - As notificações legais
    - As denúncias perante as autoridades responsáveis pela aplicação da lei

- Uma vez concluída a gestão do incidente de segurança, preparar um relatório executivo sobre este para elevar à Direção da organização e à Diretoria, se for o caso. Este relatório é independente das comunicações que foram feitas durante as diferentes etapas da sua gestão.