P E P

Auditoria e Segurança de Redes de Computadores

Jacson R. C. Silva
<jeiks@doctum.edu.br>

Conteúdo

- Introdução
- Políticas de Segurança
- Arquitetura:
  - Plano de segurança
  - Proteção de serviços
- Serviços de Segurança e Procedimentos
  - Serviços e procedimentos seguros
  - Autenticação
  - Confiança
  - Integridade
  - Autorização
  - Acesso
  - Auditoria
  - Protegendo Backups

Introdução

- Vamos discutir sobre Segurança em Redes de Computadores...

Introdução

- Um plano de segurança inclui os seguintes passos:
  - Identificar o que está tentando proteger;
  - Determinar o que está tentando se proteger;
  - Determina o quanto provável são as ameaças;
  - Implementar as medidas de proteção dos recursos importantes de maneira efetiva;
  - Revisar o processo continuamente e fazer melhorias cada vez que uma fraqueza for encontrada.

Provérbio...

- Provérbio
  - “o custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir”
- Sendo custo, as perdas:
  - expressadas em moeda corrente real;
  - reputação;
  - confiança e outras medidas menos óbvias.
- Sem conhecimento razoável do que está protegendo e o que são as ameaças prováveis, proteger sua rede pode ser impossível.

Discussão Geral

- Razão importantes de criar uma política de segurança de computador:
  - assegurar que esforços dispendidos em segurança renderão benefícios efetivos
- Pode parecer óbvio, mas

  é possível se enganar sobre *onde* os esforços são necessários.

Análise do risco

- É preciso determinar
  - o você precisa proteger,
  - do que você precisa proteger,
  - e como proteger.
- Deve-se
  - examinar todos os riscos,
  - e ordená-los por nível de severidade.

Identificando os recursos

- Para análise de risco, é necessário identificar tudo que precisa ser protegido
- Algumas categorias são:
  - **Hardware**: CPUs, teclados, estações de trabalho, discos;
  - **Software**: programas fonte e objeto, utilitários, programas de diagnóstico, sistemas operacionais e programas de comunicação;
  - **Dados**: durante execução, armazenados on-line e off-line, backups, logs;
  - **Pessoas**: usuários, administradores e suporte de hardware.
  - **Documentação**: programas, hardware, sistemas, local, procedimentos administrativos.
  - **Materiais**: papel, formulários, fitas e mídia magnética.

Identificando as ameaças

- Identificando os recursos, torna-se necessário identificar as ameaças a esses recursos
- As ameaças podem ser examinadas para determinar o potencial de perda existente
- Dentre as ameaças, encontram-se:
  - Acesso sem autorização a informações e/ou recursos
  - Revelação de informação sem intenção e/ou sem autorização
  - *Denial of Service*

Políticas de Segurança

- O que é e por que ter?
  - As decisões tomadas ou não quanto à segurança, irão determinar:
    - quão segura ou insegura é a sua rede,
    - quantas funcionalidades ela irá oferecer, e
    - qual será a facilidade de utilizá-la.
- Para tomar boas decisões sobre segurança, necessita-se determinar quais são as metas de segurança
- Não poderá utilizar qualquer coleção de ferramentas de segurança enquanto não souber o que checar e quais restrições impor

Políticas de Segurança

- Estabelecer objetivos através determinantes:
  - Serviços oferecidos versus Segurança fornecida
    - Cada serviço oferecido para os usuários carrega seu próprios riscos de segurança.
    - Para alguns serviços, o risco é superior que o benefício do mesmo, optando-se por eliminar o serviço ao invés de tentar torná-lo menos inseguro.
  - Facilidade de uso versus Segurança
    - O sistema mais fácil de usar deveria permitir acesso a qualquer usuário e não exigir senha, ou seja, sem segurança.
    - Solicitar senhas torna o sistema um pouco menos conveniente, mas mais seguro.
    - Requerer senhas de momento geradas por dispositivos, torna o sistema ainda mais difícil de utilizar, mas bastante mais seguro.

Políticas de Segurança

- Custo da segurança versus o Risco da perda
  - Custos diferentes para segurança:
    - monetário (o custo da aquisição de hardware e software como firewalls, e geradores de senha de momento),
    - performance (tempo cifragem e decifragem), e
    - facilidade de uso.
  - Níveis de risco:
    - perda de privacidade (a leitura de uma informação por indivíduos não autorizados),
    - perda de dados (corrupção ou deleção de informações), e
    - a perda de serviços (ocupar todo o espaço disponível em disco, impossibilidade de acesso à rede).
  - Cada tipo de custo deve ser contra-balançado ao tipo de perda.

Políticas de Segurança

- Conjunto de regras de segurança que regem sobre a rede de computadores
- Devem ser comunicadas a todos os usuários, pessoal operacional e gerentes da empresa

Uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

Propósitos...

- Informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação
- Especificar os mecanismos através dos quais estes requisitos podem ser alcançados.
- Oferecer um ponto de referência, a partir do qual se possa
  - adquirir, configurar e auditar sistemas computacionais e redes,
  - para que sejam adequados aos requisitos propostos.
- Uma política de uso apropriado (*Appropriate* - ou *Acceptable* - *Use Policy – AUP*) pode também ser parte de uma política de segurança
  - Ela deveria expressar o que os usuários devem e não devem fazer, incluindo o tipo de tráfego permitido nas redes
  - Deve ser explícita, evitando ambigüidades e maus entendimentos

Quem deve ser envolvido?

- Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização.
- Deve envolver:
  - O administrador de segurança do site
  - O pessoal técnico de tecnologia da informação
  - Os Administradores de grandes grupos de usuários dentro da organização
  - A equipe de reação a incidentes de segurança
  - Os Representantes de grupos de usuários afetados pela política de segurança
  - O Conselho Legal

Boa Política de Segurança

- As características de uma boa política de segurança são:
  - deve ser implementável através de
    - procedimentos de administração,
    - publicação das regras de uso aceitáveis, ou
    - outros métodos apropriados.
  - Ela deve ser exigida com
    - ferramentas de segurança, onde apropriado, e
    - sanções onde a prevenção efetiva não seja tecnicamente possível.
  - Ela deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

Boa Política de Segurança

- Seus Componentes:
  - Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir.
  - Uma política de privacidade que defina
    - expectativas razoáveis de privacidade relacionadas a aspectos como a monitoração de correio eletrônico,
    - logs de atividades, e
    - acesso aos arquivos dos usuários.
  - Uma política de acesso que defina os direitos e os privilégios para proteger a organização de danos, através da especificação de linhas de conduta dos usuários, pessoal e gerentes.

Boa Política de Segurança

- Seus Componentes:
  - Uma política de contabilidade que defina as responsabilidades dos usuários.
    - deve especificar a capacidade de auditoria e
    - oferecer a conduta no caso de incidentes.
  - Uma política de autenticação que estabeleça confiança através de
    - uma política de senhas efetiva e
    - através da linha de conduta para autenticação de acessos remotos e o uso de dispositivos de autenticação.

Boa Política de Segurança

- Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos
  - endereçando aspectos como redundância e recuperação,
  - especificando horários de operação e de manutenção,
  - com informações para contato para relatar falhas de sistema e de rede.
- Um sistema de tecnologia de informação e política de manutenção de rede que descreva como tanto o pessoal de manutenção interno como externo devem manipular e acessar a tecnologia
- Uma política de relatório de violações que indique quais os tipos de violações devem ser relatados e a quem estes relatos devem ser feitos

Boa Política de Segurança

- Suporte a informação
  - que ofereça aos usuários informações para contato para cada tipo de violação
  - Linha de conduta sobre como gerenciar consultas externas sobre um incidente de segurança
  - Referências cruzadas para procedimentos de segurança e informações relacionadas

Confirmação dos participantes

Uma vez que a política tenha sido estabelecida, deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concordaram com a política estabelecida

Finalmente, a política deve ser revisada regularmente para verificar seu funcionamento e possíveis melhorias

Manter a política flexível

- Uma política deve ser largamente independente de *hardware* e *softwares* específicos
- Os mecanismos para a atualização da política devem estar claros
- Deve-se explicitar o processo e as pessoas envolvidas na atualização da política

Arquitetura

- Objetivos
- Planos de Segurança Completamente Definidos
  - Separação de Serviços
  - Bloquear tudo / Permitir tudo
  - Identificação das Reais Necessidades de Serviços

Definição de planos de segurança

- Cada instituição deve definir um amplo plano de segurança
  - de mais alto nível
  - projetado como um *framework* de objetivos amplos nos quais políticas específicas se enquadrarão.

Plano de Segurança

- Um plano de segurança deve definir:
  - a lista de serviços de rede que serão providos;
  - quais áreas da organização proverão os serviços;
  - quem terá acesso aos serviços;
  - como o acesso será provido;
  - quem administrará esses serviços;
  - Como os incidentes serão tratados;
  - etc.

Separação de Serviços

- Isolar os serviços em hosts dedicados;
- níveis diferentes de acesso e modelos de confiança
- distinguir entre hosts que operam em diferentes modelos e confiança
- Se possível, cada serviço deve estar sendo executado em máquinas diferentes que têm como o único objetivo prover aquele serviço
  - fica mais fácil isolar intrusos e limitar falhas potenciais

Bloquear tudo / Permitir tudo

- Existem 2 filosofias diametricamente opostas que podem ser adotadas quando se define um plano de segurança
- Ambas as alternativas são modelos legítimos a se adotar
- A escolha entre uma ou outra depende do local e suas necessidades de segurança

Bloquear tudo / Permitir tudo

- A primeira opção é:
  - retirar todos os serviços e então habilitá-los seletivamente, considerando-os caso a caso.
- Isto pode ser feito no nível de host ou rede
- É mais seguro do que o outro
- Porém, a configuração requer mais trabalho e compreensão dos serviços

Bloquear tudo / Permitir tudo

- A segunda opção é:
  - permitir tudo na rede ou host
- É mais fácil de implementar
- É menos segura que a outra
- Simplesmente ligar todos os serviços (*a nível de host*) e permitir a todos os protocolos que trafeguem na rede (*a nível de roteador*)
- Os buracos de segurança ficam aparentes no host ou rede

Pode-se misturar as duas filosofias

- Pode-se usar "permitir tudo" quando se trata de estações de uso geral, mas "bloquear tudo" quando se trata de servidores de informações, como servidores de email
- Pode-se também "permitir tudo" para o tráfego entre subredes internas, mas "bloquear tudo" para comunicação com a Internet.

Reais necessidades de Serviços

- Novos serviços disponibilizados
- Deve-se avaliar cada novo serviço em relação à sua necessidade real
- Geralmente, mais serviços, mais insegurança

Configuração de Serviços e Rede

- Proteção da Infra-Estrutura
- Proteção da Rede
- Proteção dos Serviços
- Proteção da Proteção

Protegendo a Infra-estrutura

- administradores de rede costumam
  - proteger bem seus hosts
  - deixar de proteger a rede
- Pensa-se que os atacantes não tirarão proveito atacando os dados da rede
  - Mas um ataque comum nos dados da rede é a procura por *senhas* de *logins* alheios
- A infra-estrutura também pede proteção dos erros humanos
- Quando um administrador não configura bem um *host*, ele pode oferecer um mau serviço

Proteção da Rede

- Existem muitos ataques nos quais as redes se tornam vulneráveis
- O ataque clássico é o "denial of service"
  - a rede é levada a um estado no qual não consegue mais transmitir dados de usuários legítimos
  - Há duas maneiras de como isso pode ser feito:
    - atacando os roteadores e
    - enchendo a rede com tráfego estranho

Proteção dos Serviços

- Proteção diferenciada dos serviços fornecidos no host
- Utilização de Intranet
- Proteção de acesso anônimo, ou guest
- Acessos isolados de *hosts* e sistemas de arquivos que não devem ser vistos por usuários externos.
- Acesso anônimo com permissão de escrita
  - informações colocadas por anônimos devem ser monitoradas.

Proteção de Serviços

- Servidores de Nomes (DNS e NIS(+))
- Servidores de Senha/Chave (NIS(+) e KDC)
- Servidores de Autenticação/Proxy (SOCKS, FWTK)
- Correio Eletrônico
- World Wide Web (WWW)
- Transferência de Arquivo (FTP, TFTP)
- NFS

Arquitetura

- Firewalls
- Sistemas de Detecção de Intrusos
- Sistemas de Prevenção de Intrusos

Serviços e Procedimentos Seguros

- Autenticação
  - Senhas de Acesso Único
  - Kerberos
  - Escolhendo e Protegendo Tokens e Indentificadores Pessoais Numéricos Secretos
  - Garantia da Senha
    - Senhas robustas
    - Troca de senhas padrão
    - Restringindo acesso ao arquivo de senhas
    - Envelhecimento de Senhas
    - Bloqueio de contas e senhas

Propriedades para a segurança dos dados

- Confidencialidade
  - Guardar grandes segredos da empresa
- Integridade
  - Informações destruídas ou alteradas
- Disponibilidade
  - Conseguir acessar externamente e seguramente as informações importantes de uma empresa

Confidencialidade

- Proteger da revelação à entidades não autorizadas
- Proteção de arquivos através de permissões
- Utilização de criptografia

Integridade

- Prover alguma garantia sobre a integridade da informação em seus sistemas
- Realizar *checksum* de arquivos e manter *offline*
- Alguns *sums* não são de confiança

Autorização

- Conceder privilégios para processos e, em última análise, para usuários
- Uma vez identificados (seguramente), os privilégios, direitos, propriedade e ações permissíveis do usuário são determinados através da autorização
- Uma abordagem, popularizada em sistemas de UNIX, é associar a cada objeto três classes de usuário:

  proprietário, grupo e mundo
- Outra forma é através de Lista de Controle de Acesso (ACL)

Acesso

- Acesso Físico
- Conexões de Rede Wireless
- Outras Tecnologias de Rede com comutação
- Modems
  - Linhas gerenciadas
  - Usuários de discagem autenticados
  - Capacidade de chamada reversa
  - Logins registrados no log

Acesso

- Modems
  - Mensagem de abertura
  - Autenticação Dial-Out
  - Programação forte da configuração dos modems

Acesso Físico

- Restringir o acesso físico aos *hosts*, permitindo acesso somente a aquelas pessoas que devem usá-los
- Manter cópias originais e *backup* de programas e dados seguras
  - Além de mantê-las em boas condições para fins de *backup*, elas devem ser protegidas contra furtos
- *Hosts* portáteis
  - Certificar que não causarão problemas se um computador portátil de seu pessoal for roubado
  - espécies de dados permitidos em discos de computadores portáteis
  - e maneira pela qual os dados devem ser protegidos

Conexões de Rede Wireless

- Permite a qualquer usuário conectar um host não autorizado a sua rede
- Política de autenticação
- Fornecer o serviço somente em locais necessários
- *Warchalking*

Modems

- Linhas de Modem devem ser Gerenciadas
  - Cuidado ao acesso conveniente a um local para todos seus usuários
    - elas podem também fornecer um desvio efetivo dos firewalls do local
  - Não permite aos usuários instalar uma linha de modem sem uma autorização apropriada
  - Tenha um registro de todas as suas linhas de modem e mantenha-o atualizado

Modems

- Usuários de Discagem devem ser Autenticados
  - A verificação do código de usuário e da senha antes que o usuário possa ter acesso a qualquer coisa na sua rede
  - Estabelecer um intervalo curto após o primeiro e o segundo "*login*" falho, e force uma desconexão após o terceiro

Modems

- Capacidade de Chamada Reversa
  - Alguns servidores "dial-in" oferecem facilidades de chamada reversa
  - o usuário disca e é autenticado, então o sistema desconecta a chamada e chama de volta no número específico do usuário

Modems

- Registrar *Logins* em *Log*
  - todos os *logins* bem-sucedidos ou não deveriam ser registrados no *log*
  - não guardar senhas corretas no *log*
  - registre-as como uma simples tentativa de *login* bem-sucedida

Modems

- Banner de abertura correto
  - Muitos locais usam um "default" do sistema contido em um arquivo de mensagem do dia para seu "banner" de abertura
  - Infelizmente, isto frequentemente inclui o tipo de hardware e sistema operacional do host
  - Isto pode fornecer informações valiosas para um possível intruso
  - O Ideal é um banner curto e sem nomes convidativos

Modems

- Autenticação "Dial-Out"
  - Usuários "dial-out" deveriam ser autenticados

    particularmente porque seu local terá de pagar pelas despesas telefônicas
  - Jamais permitir a discagem de saída a partir de uma chamada de entrada não autenticada
  - Estabelecer se será permitida a discagem de saídaà partir de uma entrada autenticada

Modems

- Configuração Eficaz
  - Certificar que os modems não podem ser reprogramados enquanto estiverem em serviço
  - O ideal é programa os modems para "*resetarem*" sua configuração padrão no início de cada chamada

Auditoria

- O que coletar
  - Processo de Coleta
- Carga de Coleta
- Manipulando e Preservando os dados de auditoria
- Condições legais

O que coletar

- Incluir qualquer tentativa de obter um nível de segurança diferente por qualquer pessoa, processo, ou outra entidade da rede
  - "login" e "logout"
  - acesso de super-usuário
  - qualquer outra mudança de acesso ou estado
  - é especialmente importante notar o acesso "anonymous" ou "guest" a servidores públicos
- Nota muito importante: não coletar senhas

Processo de Coleta

- Ordenado pelo host ou recurso sendo acessado
- Manter os dados localmente ou em outros hosts
- Três formas de armazenar registros de auditoria:
  - em um arquivo de leitura e escrita em um host,
  - em um dispositivo do tipo escreva uma vez, leia várias
  - em um dispositivo somente de escrita
- Deve-se tornar seguro o caminho entre o dispositivo que gera o registro e o que realmente armazena o registro
- Se o caminho está comprometido, o registro pode ser parado, ou adulterado, ou ambos

Carga da Coleta

- Deve-se considerar a disponibilidade de armazenamento para os dados coletados
- Compactação de dados
- Armazenamento de dados durante um período de tempo
- Apagar *logs* antigos

Manipulando e Preservando os Dados de Auditoria

- Devem estar entre aqueles mais protegidos no local e nos backups
- Se um intruso tiver acesso aos registros de auditoria, não só os dados, mas também os próprios sistemas correriam riscos
- Dados de auditoria podem também se tornar chaves para a investigação, apreensão e acusação do autor de um incidente
- Estabelecimento de manipulação dos dados pela equipe jurídica

Considerações Legais

- O conteúdo dos dados de auditoria
  - atenção da sua equipe jurídica
- Ao coletar e salvar dados de auditoria
  - deve-se preparar para as conseqüências resultantes tanto da sua existência como do seu conteúdo
- A investigação nos dado poderia representar uma invasão de privacidade

Protegendo Backups

- Certificar que os backups estão sendo criados
- Certificar que está utilizando armazenamento secundário para os backups
  - A localização deve ser cuidadosamente selecionada
- Criptografar os backups para proporcionar proteção
- Não assumir que os backups sempre estão bons
- Periodicamente verifique a correção e a completude de seus backups.

Tratamento de incidentes de Segurança

- Se a brecha é o resultado de
  - um ataque de intruso externo,
  - dano não intencional,
  - um estudante testando algum programa novo para explorar uma vulnerabilidade de software,
  - ou um empregado com más intensões
- Deve-se reagir conforme o plano, que já deveria ter sido previsto com antecedência

Preparando e Planejando o Tratamento de Incidentes

- Estar preparado para responder a um incidente antes dele acontecer
- Preparar diretrizes de tratamento de incidentes como parte de um plano de contingência para sua organização ou site

Preparando e Planejando o Tratamento de Incidentes

- Aprender a responder eficazmente a um incidente para
  - proteger os recursos que poderiam ser comprometidos
  - proteger os recursos que poderiam ser utilizados mais eficientemente se um incidente não requeresse seus serviços
  - seguir os regulamentos (do governo ou outros)
  - prevenir o uso de seus sistemas em ataques contra outros sistemas (que poderia implicar em obrigações legais)
  - minimizar o potencial para exposição negativa

Preparando e Planejando o Tratamento de Incidentes

- Um conjunto específico de objetivos poderia ser:
  - descobrir como aconteceu
  - descobrir como evitar exploração adicional da mesma vulnerabilidade
  - evitar a expansão e incidentes adicionais
  - avaliar o impacto e dano do incidente
  - recuperar-se do incidente
  - atualizar políticas e procedimentos conforme necessário
  - descobrir quem fez isto (se apropriado e possível)

Preparando e Planejando o Tratamento de Incidentes

- É importante priorizar as ações a serem tomadas durante um incidente com bastante antecedência antes do incidente acontecer
- Sugestões de prioridade são:
  1. proteger vida humana e segurança das pessoas

     vida humana sempre tem precedência sobre outras considerações
  2. proteger dados importantes

     Previna exploração sistemas, redes ou locais importantes.

     Informe sistemas, redes ou locais importantes que tenham sido afetados sobre invasões acontecidas

Preparando e Planejando o Tratamento de Incidentes

3. proteger outros dados incluindo dados proprietários, científicos, administrativos e outros, pois perda de dados é cara em termos de recursos.
   - Previna explorações de outros sistemas, redes ou locais e informe os sistemas, redes ou locais afetados sobre invasões bem sucedidas
4. prevenir dano para sistemas
   - Danos em sistemas pode resultar em custo de recuperação alto.

Preparando e Planejando o Tratamento de Incidentes

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

Notificação e Pontos de Contato

- Gerentes locais e Pessoal
  - quem está encarregado de coordenar a atividade dos diversos jogadores
- Agências de Investigação e de Execução da Lei
- Grupos de Tratamento de Incidentes de Segurança de Computadores
- Sites Afetados e Envolvidos
- Comunicações internas
- Relações públicas - *Press Releases*

Relações Públicas

- Algumas ações importantes
  - manter o nível de detalhes técnicos baixo
  - manter a especulação fora de declarações de imprensa
  - trabalhar com profissionais da lei para assegurar que a evidência é protegida
  - não dar uma entrevista de imprensa antes de estar preparado
  - não permitir que a atenção de imprensa diminua o tratamento do evento

Identificando um Incidente

- É Real?
- Tipos e Escopo de Incidentes
- Avaliando Dano e Extensão

O Incidente é Real?

- Esta fase envolve determinar se um problema realmente existe
- Naturalmente muitos são anomalias tal como falhas de *hardware* ou comportamento de suspeito de sistema/usuário
- Há sintomas que merecem mais atenção

“Sintomas”

- Quedas (*Crashes*) de sistemas.
- Novas contas de usuário (a conta sysadmin2 foi criada inesperadamente),

  ou atividade alta em uma conta previamente pouco usada.
- arquivos novos (normalmente com nomes de arquivo estranhos)
- discrepâncias de contabilidade (ex: lastlog)
- mudanças em tamanho ou data de arquivo
- tentativas de escrever em pastas de sistema
- modificação de dados ou apagamento

“Sintomas”

- negação de serviço (usuários impedidos de entrar no sistema)
- desempenho de sistema inexplicavelmente baixo
- anomalias (mensagens no monitor e inexplicáveis "*beeps*")
- numerosas tentativas de *login* sem sucesso de outro nodo
- alguém se torna um usuário *root* em um sistema UNIX e acessa arquivos arquivo após arquivo em contas de muitos usuários
- inabilidade de um usuário para se *logar* devido a modificações em sua conta.
- Estes são apenas alguns dos sintomas maliciosos

Tipos e Escopo de Incidentes

- Avaliação do âmbito e impacto do problema
- É importante identificar os limites do incidente corretamente para
  - lidar efetivamente e
  - priorizar respostas
- Olhar pontos, como por exemplo:
  - é este um incidente multi-site?
  - muitos computadores foram afetados?
  - a imprensa está envolvida?

Avaliando Dano e Extensão

- A análise do dano e extensão do incidente pode consumir muito tempo
  - mas deve conduzir a alguma idéia sobre a natureza do incidente e ajudar na investigação e prossecução
- Assim que a brecha tenha acontecido, o sistema inteiro e todos seus componentes devem ser considerado suspeitos

Avaliando Dano e Extensão

- Deve-se verificar
  - A integridade dos arquivos
  - Os backups de sistema
  - Os logs centralizados
    - procura por anormalidades
    - procura por caminhos percorridos por usuários

Tratando um Incidente

- Tipos de Notificação e Troca de Informação
- Protegendo as Evidências e Logs de Atividade
- Retenção
- Erradicação
- Recuperação
- Acompanhamento

Tratando um Incidente

- Seguir políticas existentes para não perder o enfoque
- Restabelecer controle dos sistemas afetados e limitar o impacto e dano
  - No pior caso, fechando o sistema, ou desconectando o sistema da rede
- Ajuda quanto necessário para agilizar o trabalho
  - danos reais podem acontecer devido a demoras ou a informações perdidas

Tipos de Notificação e Troca de Informação

- O pessoal apropriado deve ser notificado
- As circunstâncias devem ser descritas em tantos detalhes quanto possível
  - facilitar o pronto reconhecimento e entender o problema
- Cuidado ao determinar quais grupos técnicos a informação será enviada na notificação

Tipos de Notificação e Troca de Informação

- A escolha da fala usada quando notificar as pessoas sobre o incidente pode ter um efeito profundo no modo que informação é recebida
  - Quando você usa termos emocionais ou inflamatórios, você eleva o potencial para dano e resultados negativos do incidente
  - É importante permanecer tranqüilo ambos as comunicações escrita e falada
- Também requer cuidado de idiomas, *timezone*, etc.

Protegendo as Evidências e Logs de Atividade

- Deve-se documentar todos os detalhes relacionados ao incidente
- Isto proverá valiosa informação para desvendar o curso dos eventos
- Detalhes armazenados também proverão evidências para esforços de prossecução e proverão os movimentos naquela direção

Protegendo as Evidências e Logs de Atividade

- Como mínimo, deve-se registrar:
  - todos os eventos de sistemas
    - registros de auditoria
  - todas as ações feitas
    - tempo usado
  - todas as conversações externas
    - inclusive a pessoa com quem falou, a data e tempo, e o conteúdo da conversa

Protegendo as Evidências e Logs de Atividade

- O modo mais direto para manter documentação é mantendo um livro de log
- Seguindo, por exemplo, os passos
  - Fazer cópias rotineiras assinadas de seus *logs* para um administrador de documentos
  - O administrador deve armazenar estas páginas copiadas em um lugar seguro
  - Ao submeter a informação para armazenamento, um recibo datado e assinado pelo administrador do documento deve ser emitido

Retenção

- O propósito de retenção é limitar a extensão de um ataque
- Uma parte essencial de retenção é decisão do que fazer
  - por exemplo: determinando desligar um sistema; desconectar da rede; monitorar sistemas ou atividades de rede; etc.
- A organização ou site deve, por exemplo, definir riscos aceitáveis lidando com um incidente
  - estabelecendo ações específicas e
  - estratégias adequadas;
  - Isso é importante quando uma decisão rápida é necessária.

Erradicação

- Uma vez que o incidente foi contido, é tempo para erradicar a causa
- Softwares podem estar disponíveis para ajudar no processo de erradicação
- Deve-se tomar cuidado com os backups, pois pode existir uma cópia dos problemas
- Depois de erradicação, deveria ser feito um novo backup

Erradicação

- Removendo todas as vulnerabilidades uma vez um incidente aconteceu é difícil
- A chave para remover vulnerabilidades é conhecimento e entendimento da brecha atacada
- Pode ser necessário voltar para as mídia de distribuição originais e ré-customizar o sistema

Recuperação

- Uma vez que a causa de um incidente foi erradicada, a fase de recuperação define a próxima fase de ação
- A meta de recuperação é retornar o sistema ao normal
- Em geral, expondo serviços na ordem de demanda

Acompanhamento

- Uma vez que você acredita que o sistema foi restabelecido a um "estado seguro", ainda é possível que buracos, e até mesmo armadilhas
- Uma das fases mais importantes de respostas a incidentes é a fase de acompanhamento
-

Resultados de um Incidente

- Ações posteriores ao incidente
  - Criação de um inventário dos recursos dos sistemas
  - Criar um novo plano de segurança revisado com as lições aprendidas para impedir o incidente de ré-acontecer
  - Desenvolver uma análise de risco nova levando em conta o incidente
  - Uma investigação e prossecução dos indivíduos que causaram o incidente, se julgada desejável

Responsabilidades

- Proteja a sua própria rede e não as dos outros
- À partir do conhecimento, você conhecerá a falha de outras redes
- Não caia na tentação de fazer como seu intruso

Endereços interessantes

- CAIS (Centro de Atendimento à Incidentes de Segurança)

  http://www.rnp.br/cais
- NBSO (NIC BR Security Office)

  http://www.nbso.nic.br/
- CERT (Computer Emergence Response Team)

  http://www.cert.org
- Ferramentas de Monitoramento

  http://tools.netsa.cert.org/
- Cartilha do CERT

  http://cartilha.cert.br/download/
- Apostila CERT

  http://www.cert.br/docs/seg-adm-redes/