Políticas de Segurança

Neste documento há uma série de referências para políticas de segurança. Seguidamente, estas referências incluirão recomendações para políticas específicas.

Introdução:

2.1 - O que é uma política de segurança? Pôr que ter uma?

As decisões que você como administrador toma ou deixa de tomar, relacionadas 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. No entanto, você não consegue tomar boas decisões sobre segurança, sem antes determinar quais são as suas metas de segurança. Até que você determine quais sejam elas, você não poderá fazer uso efetivo de qualquer coleção de ferramentas de segurança pois você simplesmente não saberá o que checar e quais restrições impor.
Pôr exemplo, seus objetivos provavelmente serão muito diferentes dos que são definidos pôr um vendedor de produto. Os vendedores procuram deixar a configuração e a operação de seus produtos o mais simplificado possível, o que implica que as configurações default normalmente serão bastante tão abertas (e pôr conseguinte inseguras) quanto possível. Se pôr uma lado isto torna o processo de instalação de novos produtos mais simples, também deixa acessos abertos, para qualquer usuário.
Seus objetivos devem ser determinados a partir das seguintes determinantes:

1. *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, e o administrador deve optar pôr eliminar o serviço ao invés de tentar torná-lo menos inseguro.
2. *Facilidade de uso* ***versus*** *Segurança* - O sistema mais fácil de usar deveria permitir acesso a qualquer usuário e não exigir senha, isto é, não haveria segurança. Solicitar senhas torna o sistema um pouco menos conveniente, mas mais seguro. Requerer senhas "one-time" geradas pôr dispositivos, torna o sistema ainda mais difícil de utilizar, mas bastante mais seguro.
3. *Custo da segurança* ***versus*** *o Risco da perda* - Há muitos custos diferentes para segurança: monetário (o custo da aquisição de hardware e software como firewalls, e geradores de senha "one-time"), performance (tempo cifragem e decifragem), e facilidade de uso. Há também muitos níveis de risco: perda de privacidade (a leitura de uma informação pôr 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.

Seus objetivos devem ser comunicados a todos os usuários, pessoal operacional, e gerentes através de um conjunto de regras de segurança, chamado de "política de segurança". Nós utilizamos este termo ao invés de "política de segurança computacional", uma vez que o escopo inclui todos os tipos de tecnologias de informação e informações armazenadas e manipuladas pela tecnologia.

2.1.1 - Definição de uma política de segurança

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

2.1.2 - Propósitos de um política de segurança

O principal propósito de uma política de segurança é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançado. Outro propósito é 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. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.
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 em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes. A AUP deve ser tão explícita quanto possível para evitar ambiguidades ou maus entendimentos. Pôr exemplo, uma AUP pode lista newsgroups USENET proibidos.

2.1.3 - Quem deve ser envolvido na formulação da política?

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. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance que ela tenha o impacto desejado. A seguinte lista de indivíduos deveria estar envolvida na criação e revisão dos documentos da política de segurança:

- 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

A lista acima é representativa para muitas organizações que tem controle acionário, mas não necessariamente para todas. A idéia é trazer representações dos membros, gerentes com autoridade sobre o orçamento e política, pessoal técnico que saiba o que pode e o que não pode ser suportado, e o conselho legal que conheça as decorrências legais das várias políticas. Em algumas organizações, pode ser apropriado incluir pessoal de auditoria. Envolver este grupo é importante se as política resultante deverá alcançar a maior aceitabilidade possível. Também é importante mencionar que o papel do conselho legal irá variar de país para país.

2.2 O que faz uma boa política de segurança?

As características de uma boa política de segurança são:

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

Os componentes de uma boa política de segurança incluem:

1. Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir.
2. 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.
3. Uma política de acesso que define os direitos e os privilégios para proteger a organização de danos, através da especificação de linhas de conduta dos usuários, pessoal e gerentes. Ela deve oferecer linhas de condutas para conexões externas, comunicação de dados, conexão de dispositivos a uma rede, adição de novos softwares, etc. Também deve especificar quaisquer mensagens de notificação requeridas (pôr exemplo, mensagens de conexão devem oferecer aviso sobre o uso autorizado, e monitoração de linha, e não simplesmente "welcome".

4. Uma política de contabilidade que defina as responsabilidades dos usuários. Deve especificar a capacidade de auditoria, e oferecer a conduta no caso de incidentes (pôr exemplo, o que fazer e a quem contactar se for detectada uma possível intromissão.
5. 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.
6. Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos. Ele deve endereçar aspectos como redundância e recuperação, bem como especificar horários de operação e de manutenção. Ele também deve incluir informações para contato para relatar falhas de sistema e de rede.
7. 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. Um tópico importante a ser tratado aqui é como a manutenção remota é permitida e como tal acesso é controlado. Outra área para considerar aqui é a terceirização e como ele é gerenciada.
8. Uma política de relatório de violações que indique quais os tipos de violações devem ser relatados e a quem estes relatos devem ser feitos. Uma atmosfera de não ameaça e a possibilidade de denúncias anônimas irá resultar uma grande probabilidade que uma violação seja relatada.
9. 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, ou informação que seja considerada confidencial ou proprietária; referências cruzadas para procedimentos de segurança e informações relacionadas, tais como as políticas da companhia e leis e regulamentações governamentais.

Pode haver requisitos regulatórios que afetem alguns aspectos de sua política de segurança (como a monitoração). Os criadores da política de segurança devem considerar a busca de assistência legal na criação da mesma. No mínimo, a política deve ser revisada pôr um conselho legal.

Uma vez que a política tenha sido estabelecida ela deve ser claramente comunicada aos usuários, pessoal e gerentes. Deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concordaram com a política estabelecida. Esta é uma parte importante do processo. Finalmente sua política deve ser revisada regularmente para verificar se ela está suportando com sucesso suas necessidades de segurança.

2.3 - Mantendo a política flexível

No intuito de tornar a política viável a longo prazo, é necessário bastante flexibilidade baseada no conceito de segurança arquitetural. Uma política deve ser largamente independente de hardware e softwares específicos. Os mecanismos para a atualização da política devem estar claros. Isto inclui o processo e as pessoas envolvidas.

Também é importante reconhecer que há expectativas para cada regra. Sempre que possível a política deve expressar quais expectativas foram determinadas para a sua existência. Pôr exemplo, sob que condições um administrador de sistema tem direito a pesquisar nos arquivos do usuário. Também pode haver casos em que múltiplos usuários terão acesso à mesma userid. Pôr exemplo, em sistemas com um usuário root, múltiplos administradores de sistema talvez conheçam a senha e utilizem a conta.

Outra consideração é chamada a "Síndrome do Caminhão de Lixo". Isto se refere a o que pode acontecer ao um site se uma pessoa chave repentinamente não esteja mais disponível para sua função (ficou doente ou deixou a companhia). Enquanto a grande segurança reside na mínima disseminação de informação, o risco de perder informação crítica cresce quando a informação não é compartilhada. É importante determinar qual o peso ideal desta medida em seu site.

3. Arquitetura

3.1 Objetivos

3.1.1 Planos de Segurança Completamente Definidos

Todos os sites devem definir um amplo plano de segurança, que deve ser de mais alto nível que as políticas discutidas no capítulo 2, e deve ser projetado como um framework de objetivos amplos nos quais políticas específicas se enquadrarão.
É importante ter esse framework de tal maneira que políticas individuais possam ser consistentes dentro de todo o contexto da arquitetura de segurança do site. Pôr exemplo, ter uma política forte em relação ao acesso pela Internet e ter baixas restrições no uso do modem é inconsistente dentro de uma filosofia de fortes restrições no que diz respeito ao acesso externo.
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; etc.
O plano também deve indicar como incidentes serão tratados. Capítulo 5 provê uma discussão profunda neste tópico, mas é importante que cada site defina classes de incidentes e reações correspondentes. Pôr exemplo, sites com firewalls devem setar um número de tentativas de ataque suportado antes de tomar uma ação? Níveis de ação devem ser definidos para todos os ataques e respostas. Sites com firewalls devem determinar se uma simples tentativa de conexão a um host constitui um incidente ou não. E em relação à procura sistemática de sistemas?
Para sites conectados à Internet, o número significativo de incidentes relatados em relação à segurança pode se fazer esquecer dos incidentes internos à rede. Da mesma maneira, organizações não conectadas à Internet devem ter planos fortes e bem definidos de política de segurança interna.

3.1.2 Separação de Serviços

Existem muitos serviços que um site deve prover para seus usuários, alguns dos quais podem ser externos. Há uma variedade de razões para isolar os serviços em hosts dedicados. Há também razões de performance em muitos casos, e uma discussão detalhada será feita neste documento.
Os serviços que um site deve prover terão, em muitos casos, níveis diferentes de acesso e modelos de confiança. É melhor colocar serviços que são essenciais à segurança ou operação do site em máquinas dedicadas com acesso limitado do que em uma máquina que provê serviço(s) menos seguro(s), ou que requer acesso pôr parte dos usuários, que podem acidentalmente burlar a segurança.
É também relevante distinguir entre hosts que operam em diferentes modelos e confiança (isto é, todos os hosts da rede interna versus hosts da rede externa).
Alguns dos serviços que são potencialmente separáveis são discutidos na sessão é importante lembrar que segurança é tão forte quanto a corrente é em relação ao menor elo. Muitos dos
ataques conhecidos nos anos recentes têm sido feitos pôr exploração de vulnerabilidades nos sistemas de correio eletrônico. Os intrusos não querem acesso ao correio eletrônico, mas usar as suas vulnerabilidades para ganhar acesso a outros sistemas.
Se possível, cada serviço deve estar sendo executado em máquinas diferentes que têm como o único objetivo prover aquele serviço. Assim, fica mais fácil isolar intrusos e limitar falhas potenciais.

3.1.3 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, e a escolha entre uma ou outra depende do site e suas necessidades de segurança.

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, o mais apropriado. Este modelo, referenciando como "bloquear tudo", é geralmente mais seguro do que o outro, descrito no próximo parágrafo. Porém, a configuração requer mais trabalho e compreensão dos serviços. Permitir somente serviços conhecidos para uma melhor análise de um particular serviço/protocolo e o projeto de um mecanismo de segurança cabem no nível de segurança do site.
O outro modelo, referenciado como "permitir tudo", é mais fácil de implementar, mas é geralmente menos seguro que o outro. Simplesmente ligar todos os serviços (a nível de host) e permitir a todos os protocolos que trafeguem na rede (a nível de roteador). Como os buracos de segurança ficam aparentes, eles são restritos aos níveis de host e rede.
Cada um dos modelos pode ser aplicado a diferentes porções do site, dependendo dos requerimentos das funcionalidades, do controle administrativo, da política de segurança, etc. Pôr exemplo, a política pode ser 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. Da mesma forma, "permitir tudo" pode ser empregado no tráfego entre subredes internas, mas "bloquear tudo" pode ser adotado na comunicação com a Internet.
Deve-se tomar cuidados quando se mistura as duas filosofias. Tomar cuidado somente com usuários externos pode não ser a melhor filosofia, pois usuários internos à rede podem não ser confiáveis. E a partir do momento que um usuário externo entra na rede (passando pôr um firewall) ele tem acesso a tudo, pois não há isolamento interno.

3.1.4 Identificação das Reais Necessidades de Serviços

Há uma grande variedade de serviços que podem ser providos, tanto internamente quanto na Internet. Gerenciar segurança é, em muitos casos, gerenciar o acesso a serviços internos ao site e como o acesso interno a serviços externos se dará.
Os serviços tendem a se disseminar como ondas na Internet. Através dos anos muitos sites criaram servidores de: FTP anônimos, gopher, wais, WWW, etc, seguindo a moda quando eles se tornaram populares, mas sem levar em conta a necessidade real deles. Deve-se avaliar cada novo serviço em relação à sua necessidade real, esquecendo-se do modismo.
É bom ter-se em mente que a complexidade de segurança pode crescer exponencialmente com o número de serviços providos. Roteadores-filtros precisam ser modificados para suportar novos protocolos. Alguns protocolos são inerentemente difíceis de se filtrar seguramente (como RPC e UDP), assim abrindo-se novas portas ao mundo interno. Serviços providos pela mesma máquina podem interagir de modos catastróficos, pôr exemplo, FTP anônimo com WWW permite que um atacante coloque um arquivo na área de FTP e faça com que o servidor HTTP o execute.

3.2 Configuração de Serviços e Rede

3.2.1 Proteção da Infra-estrutura

Muitos administradores de rede protegem bem seus hosts, mas poucos são os que fazem a tarefa de proteger a rede. Existe razão para isso. Geralmente o objetivo são dados de servidores, pois os atacantes não tirarão proveito atacando os dados da rede, embora isso não desmereça a necessidade de sua proteção, pois um ataque comum nos dados da rede é a procura pôr senhas de logins alheios. Mas a proteção da infra-estrutura também diz respeito à gerência de rede (SNMP), serviços (DNS, NFS, NTP, WWW, ...) e segurança propriamente dita (autenticação e restrições de acesso).
A infra-estrutura também pede proteção dos erros humanos. Quando um administrador não configura bem um host, ele pode oferecer um mau serviço. Isto pode afetar somente os usuários daquele host, e ao menos que seja um servidor primário daquele serviço, o número de usuários afetados será limitado. Entretanto, se um roteador está mal configurado, todos os usuários que usarem a rede serão afetados.

3.2.2 Proteção da Rede

Existem muitos ataques nos quais as redes se tornam vulneráveis. O ataque clássico é o "denial of service". Neste caso, 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. Note-se que o termo roteador é usado para representar toda a classe de equipamentos de interconexão, nos quais se incluem firewalls. servidores-proxy, etc.

Um ataque num roteador é feito para impedi-lo de transmitir pacotes adiante, ou transmiti-los de forma errada. Isso pode ser feito devido a uma má configuração, a injeção de atualização daninha de informação de roteamento, ou através de um "flood atack" , ou seja, o roteador é bombardeado com pacotes não roteáveis, fazendo sua performance decair. Um "flood atack" em uma rede é similar em relação a um roteador, exceto que os pacotes são broadcast. Um ataque ideal deste tipo seria a injeção de um único pacote que requeresse que todas as estações o retransmitisse, ou gerar pacotes de erro, cada um também repetido pelas outras estações. Um ataque deste tipo bem feito pode sempre gerar uma explosão exponencial de transmissões.

Um outro ataque é o "spoofing". Neste caso, pacotes maléficos com informações erradas sobre roteamento são enviados a um ou mais roteadores fazendo com que eles roteem errado. Este ataque difere do primeiro somente no propósito do roteamento. No ataque anterior, o objetivo era deixar o roteador inutilizável, um estado facilmente detectado pelos usuários da rede. No "spoofing" os pacotes são enviados a algum host onde eles podem ser monitorados e depois reenviados a seu destino correto, tendo seu conteúdo alterado ou não.

A solução para a maioria desses casos é proteger os pacotes de atualização de roteamento de protocolos como RIP-2 e OSPF. Existem 3 níveis de proteção: senha textual, checksum criptografado e criptografia. Senhas oferecem a mínima proteção contra intrusos que não têm acesso à rede física. Também protegem roteadores mal configurados (ou seja, roteadores que não deveriam rotear pacotes). A vantagem de senhas é que elas têm um baixo overhead, tanto em tempo de transmissão como de CPU. Checksums protegem contra a injeção de pacotes daninhos, até mesmo se o intruso tem acesso à rede física. Combinado com um número de seqüência, ou outro identificador único, o checksum pode também detectar ataques de retransmissão, onde uma informação mais antiga está sendo retransmitida, seja pôr um intruso ou roteador mal configurado. O melhor é prover criptografia completa das seqüências, ou unicamente identificadas, tabelas de roteamento. Isso impede um intruso de determinar a topologia da rede. A desvantagem da criptografia é o overhead envolvido no processamento.

Tanto RIP-2 (RFC 1723) como OSPF (RFC 1583) suportam senhas textuais nas suas especificações básicas de projeto. E existem extensões para cada protocolo suportar o algoritmo de criptografia MD5.

Infelizmente não há proteção adequada a um ataque "flooding" , mas felizmente esse ataque é óbvio quando ocorre e geralmente pode ser terminado de forma relativamente fácil.

3.2.3 Proteção dos Serviços

Existem muitos tipos de serviços e cada um tem seus próprios requerimentos de segurança, que vão variar baseado no uso do serviço. Pôr exemplo, um serviço que poderia ser usado dentro de um site (NFS) requer mecanismos de proteção diferentes de outros serviços usados externamente à rede. Pode ser suficiente proteger o servidor de acesso externo, mas um servidor WWW, que provê documentos que devem ser vistos pôr usuários da Internet, requer uma forte proteção, para impedir que se modifique o banco de dados da Web pôr pessoas externas à rede.

Serviços internos (usados pelos usuários do site) e serviços externos (deliberadamente permitidos para uso pôr usuários da internet) terão, de uma maneira geral, requerimentos de proteção diferentes dos já descritos. É bom isolar os serviços internos em um conjunto de servidores diferente do conjunto de servidores de serviços externos, ou seja, é bom não se deixar todos os serviços no mesmo(s) host(s). Na realidade, muitos sites vão além e têm um conjunto de subredes (ou até redes diferentes) que são acessíveis de fora do site e outro conjunto acessível somente de dentro do site. Claro, há usualmente

firewalls conectando estes conjuntos. Um grande cuidado deve-se tomar a fim de garantir o funcionamento correto da firewall.
Há um grande interesse em se usar intranets na conexão com diferentes partes da organização (divisões da companhia). Enquanto este documento diferencia rede interna de rede externa (privada e pública), sites com intranets devem estar atentos que eles precisarão considerar 3 separações e tomar ações apropriadas quando projetando e oferecendo serviços. Um serviço provido a uma intranet não deve se tornar público, nem completamente privado como um serviço de uma sub-unidade da organização. Entretanto, o serviço pode precisar de um suporte próprio, separadamente tanto dos serviços e rede internos e externos.
Uma forma de serviço externo que merece uma atenção especial é o acesso anônimo, ou guest. Ele pode ser tanto pôr FTP ou pôr login guest (não autenticado). É importante manter esses acessos isolados de hosts e sistemas de arquivos que não devem ser vistos pôr usuários externos. Outro cuidado especial diz respeito ao acesso anônimo com permissão de escrita. Um site deve ser legalmente responsável pela informação pôr ele tornada pública, portanto informações colocadas pôr anônimos devem ser monitoradas.
Agora iremos considerar alguns dos mais populares serviços: servidor de nomes, servidor de senhas, servidor de proxy/autenticação, correio eletrônico, WWW, transferência de arquivos e NFS. Considerando que são os serviços mais freqüentemente usados, são os principais alvos de ataques. E um ataque em um destes serviços pode produzir um desastre além das proporções do serviço básico.

3.3 Firewalls

Uma das medidas de segurança mais amplamente empregada e publicada em uso na Internet é um "firewall". Firewalls tem sido determinados a reputação de uma panacéia geral para muitas, senão todas, questões de segurança da Internet. Eles não são. Firewalls são apenas outra ferramenta em questão para segurança de sistema. Eles fornecem um certo nível de proteção e são, em geral, uma maneira de implementar a política de segurança no nível de rede. O nível de segurança que um firewall fornece pode variar tanto quanto o nível de segurança em uma máquina particular. Existe o tradicional "trade-off" entre segurança, facilidade de uso, custo, complexidade, etc.
Um firewall é qualquer um dos vários mecanismos usados para controlar e observar o acesso de e para uma rede com a finalidade de protegê-la. Um firewall atua como um gateway através do qual todo o tráfego de e para a rede ou sistemas protegidos passa. Firewalls ajudam a colocar limitações na quantidade e tipo de comunicação que ocorre entre a rede protegida e a outra rede (pôr exemplo, a Internet, ou outra parte da rede de um site).
Um firewall geralmente é uma maneira de construir uma parede entre uma parte de uma rede, uma rede interna de uma empresa, pôr exemplo, e outra parte, a Internet global, pôr exemplo. A única característica sobre esta parede é que precisam existir maneiras para algum tráfego com características particulares passarem através de portas cuidadosamente monitoradas ("gateways"). A parte difícil é estabelecer o critério pelo qual os pacotes são permitidos ou negados acesso pelas portas. Livros escritos sobre firewall usam terminologia diferente para descrever as várias formas de firewalls. Isto pode ser confuso para administradores de sistemas que não são familiares com firewalls. O ponto a observar aqui é que não existe nenhuma terminologia fixa para a descrição de firewalls.
Firewalls não são sempre, ou mesmo tipicamente, uma única máquina. Preferivelmente, firewalls são freqüentemente uma combinação de roteadores, segmentos de rede, e computadores host. Portanto, para o propósito desta discussão, o termo "firewall" pode consistir em mais de um dispositivo físico. Firewalls são tipicamente construídos usando dois diferentes componentes, roteadores de filtragem e servidores proxy.

Roteadores de filtragem são o componente mais fácil de conceituar em um firewall. Um roteador move dados de um lado para outro entre duas (ou mais) redes diferentes. Um roteador "normal" pega um pacote da rede A e encaminha-o para seu destino na rede B. Um roteador de filtragem faz a mesma coisa mas

decide não apenas como rotear o pacote mas se deveria rotear o pacote. Isto é feito instalando uma série de filtros pelos quais o roteador decide o que fazer com qualquer pacote de dados.
Uma discussão referente a capacidades de uma marca particular de roteador, executando uma versão de software específica está fora do escopo deste documento. Porém, quando avaliando um roteador para ser usado para filtragem de pacotes , o seguinte critério pode ser importante quando da implementação de uma política de filtragem: endereço IP origem e destino, números de porta TCP origem e destino, estado do bit "ACK" no pacote TCP, números de porta UDP origem e destino, e direção do fluxo de pacotes (i.e., A->B ou B->A). Outra informação necessária para construir um esquema de filtragem seguro é se o roteador reordena instruções de filtro (projetada para otimizar filtros, isto algumas vezes pode mudar o significado e causar acesso não pretendido), e se é possível aplicar filtros para pacotes que chegam e que saem em cada interface (se o roteador filtra somente pacotes que saem então o roteador é externo aos seus filtros e pode ser mais vulnerável para atacar). Além do roteador ser vulnerável, esta distinção entre aplicar filtros em pacotes que chegam ou que saem é especialmente relevante para roteadores com mais de duas interfaces. Outras questões importantes são a capacidade de criar filtros baseado nas opções do cabeçalho IP e o fragmento de estado do pacote. Construir um bom filtro pode ser muito difícil e requer um bom entendimento do tipo de serviços (protocolos) que serão filtrados.
Para melhor segurança, os filtros geralmente restringem acesso entre as duas redes conectadas a apenas um host, o bastion host. Só é possível ter acesso para a outra rede através deste bastion host. Como somente este host, em lugar de algumas centenas de host´s, pode ser atacado, é mais fácil manter um certo nível de segurança pois somente este host tem que ser muito cuidadosamente protegido. Para tornar disponível recursos para legitimar usuários através deste firewall, serviços tem que ser passados adiante pelo bastion host. Alguns servidores tem esta capacidade embutida (como servidores DNS ou servidores SMTP), para outros serviços (pôr exemplo, Telnet, FTP, etc.), servidores proxy podem ser usados para permitir acesso aos recursos através do firewall de modo seguro.
Um servidor proxy é um modo para concentrar serviços de aplicação através de uma única máquina. Tipicamente existe uma única máquina (o bastion host) que atua como um servidor proxy para uma variedade de protocolos (Telnet, SMTP, TFP, HTTP, etc.) mas podem existir computadores host individuais para cada serviço. Ao invés de conectar diretamente um servidor externo, o cliente conecta para o servidor proxy que em troca inicia uma conexão para o servidor externo solicitado. Dependendo do tipo de servidor proxy usado, é possível configurar clientes internos para realizar este redirecionamento automaticamente, sem conhecimento para o usuário, outros podem requerer que o usuário conecte diretamente para o servidor proxy e então iniciar a conexão através de um formato específico.
Existem significantes benefícios de segurança que podem ser obtidos pelo uso de servidores proxy. É possível adicionar listas de controle de acesso para protocolos, exigir que usuários ou sistemas forneçam algum nível de autenticação antes do acesso ser concedido. Servidores proxy mais espertos, algumas vezes chamados Gateways da Camada de Aplicação, podem ser escritos de modo que entendam protocolos específicos e podem ser configurados para bloquear somente subseções do protocolo. Pôr exemplo, um Gateway de Aplicação para FTP pode reconhecer a diferença entre o comando "put" e o comando "get"; uma organização pode desejar permitir aos usuários realizar "get" de arquivos da Internet, mas não permitir "put" de arquivos internos no servidor remoto. Em contraste, um roteador de filtragem poderia ou bloquear todo acesso ao FTP, ou não, mas não um subconjunto.
Servidores proxy também podem ser configurados para encriptar fluxos de dados baseado em uma variedade de parâmetros. Uma organização pode usar esta característica para permitir conexões encriptadas entre duas localizações cujos únicos pontos de acesso estão na Internet.
Firewalls são pensados como uma maneira de manter intrusos do lado de fora, mas eles são usados geralmente como uma maneira de legitimar usuários em um site. Existem muitos exemplos onde um usuário válido poderia precisar acessar regularmente o site "home" durante viagens para apresentações e conferências, etc. Acesso à Internet geralmente é disponível mas pode ser através de uma máquina ou rede não confiável. Um servidor proxy configurado corretamente pode permitir os usuários corretos no site enquanto bloqueia acesso para outros usuários.

O maior esforço atual em técnicas de firewall é encontrar uma combinação de um par de roteadores de filtragem com um ou mais servidores proxy na rede entre os dois roteadores. Esta configuração permite ao roteador externo bloquear qualquer tentativa de usar a camada IP subjacente para quebrar a segurança (IP spoofing, roteamento pela origem, fragmentos de pacotes), enquanto permite ao servidor proxy tratar potenciais furos de segurança nos protocolo das camadas superiores. A finalidade do roteador interno é bloquear todo tráfego exceto para o servidor proxy. Se esta configuração é implementada rigorosamente, pode ser obtido um alto nível de segurança.
Muitos firewalls fornecem capacidade de log que pode ser adequado para fazer administração mais conveniente da segurança da rede. A função de log pode ser centralizada e o sistema pode ser configurado para enviar alertas para condições anormais. É importante monitorar regularmente estes logs para qualquer sinal de intrusões ou tentativas de arrombamento. Desde que alguns intrusos tentarão encobrir seus ataques pela edição dos logs, é desejável proteger esses logs. Uma variedade de métodos está disponível, incluindo: escreva uma vez, leia muitos (WORM) drives; logs em papel; e logs centralizados através do utilitário "syslog". Outra técnica é usar um impressora serial falsa, mas ter uma porta serial conectada para uma máquina isolada ou PC que mantêm os logs.
Firewalls estão disponíveis em uma ampla faixa de qualidade e intensidade. Pacotes comerciais iniciam em aproximadamente $10,000US e alcançam mais de $250,000US. Firewalls desenvolvidos pelo próprio site podem ser construídos para quantias menores de capital. Deve-se lembrar que a configuração correta de um firewall (comercial ou "caseiro") requer uma significante habilidade e conhecimento do TCP/IP. Ambos os tipos requerem manutenção regular, instalação de patches de softwares e atualizações, e monitoração regular. Quando realiza-se o orçamento de um firewall, estes custos adicionais deveriam ser considerados além do custo dos elementos físicos do firewall.
Como um aparte, construir uma solução "caseira" para um firewall requer significante habilidade e conhecimento do TCP/IP. Isto não deveria ser tentado trivialmente pois a sensação de segurança percebida é pior ao longo da execução do que saber que não existe nenhuma segurança. Como com todas as medidas de segurança, é importante decidir na ameaça, o valor do recurso a ser protegido, e os custos para implementar segurança.
Uma nota final sobre firewalls. Eles podem ser uma grande ajuda quando implementando segurança para um site e protegem contra uma grande variedade de ataques. Mas é importante ter em mente que eles são apenas uma parte da solução. Eles não podem proteger seu site contra todos os tipos de ataque.
O que é e como funciona o principal dispositivo de segurança na Internet.
Segurança ainda é o ponto mais discutido na Internet, mas, em grande parte dos casos, a discussão se resume a problemas como violação de correspondência e dificuldades para se enviar número de cartão de credito. À medida que a maior parte das empresas conecta suas redes privadas à grande rede, entretanto, a questão fundamental passa a ser como impedir que usuários não autorizados ganhem acesso livre a dados sensíveis. O principal meio de proteger as redes privadas são os chamados firewalls.
Um firewall é um sistema ou grupo de sistemas através do qual flui o trafego de dados entre duas redes distintas de computadores, permitindo que se implemente uma política de segurança que determine o que pode ou não passar de uma rede para outra. A aplicação mais comum de um firewall é proteger uma rede contra acesso dos inúmeros usuários mal-intencionados (chamados crackers) que povoam a Internet.
Mais especificamente, o firewall é um dispositivo de hardware dotado de duas placas de rede (uma ligada a rede corporativa e a outra ligada à Internet) rodando software especifico de analise e roteamento de pacotes. Como todo pacote enviado de uma rede a outra passa obrigatoriamente pelo sistema, o firewall tem a chance de analisá-lo, determinar se ele representa algum risco e, se for o caso, descartá-lo antes que ele possa alcançar seu destino.
Os critérios utilizados para decidir se determinado pacote de dados oferece ou não risco fazem parte a política de segurança praticada pela entidade proprietária do firewall. Existem firewalls que operam na camada de rede – analisando pacotes IP – e outros que operam na camada de aplicação – analisando os dados dentro dos pacotes IP. Alguns firewalls são tão restritos que deixam passar apenas mensagens de correio, enquanto outros são bem permissivos. Como seria de se esperar, quanto mais diligente e rigoroso for o firewall, mais difícil será penetrar um ataque e mais facial será investigá-lo posteriormente.

Firewall no nível de rede

Firewalls de rede se restringem ao nível do IP, decidindo que pacotes devem passar e que pacotes devem ser descartados com base nos dados constantes do cabeçalho do pacote – informações como endereço de remetente, endereço de destinatário e a porta IP utilizada. A porta é um campo de dois bytes contendo um número inteiro que indica a máquina destinatária qual é o programa que deve manipular o pacote recebido (o SMTP, protocolo de correio da Internet, pôr exemplo, usa a porta 25).
Até um roteador comum pode ser configurado para agir como um firewall de rede – se bem que será um firewall simples, já que roteadores tradicionais não costumam ser muito sofisticados e freqüentemente não conseguem determinar de onde um pacote efetivamente veio ou que tipo de informação ele está carregando. Um roteador comum, que se preocupa apenas em enviar os pacotes a seus destinatários, pode ser presa de alguns ataques clássicos, como o "IP spoofing".
Máquinas bem configuradas só concedem acesso a computadores conhecidos, em geral localizados numa mesma rede privada. Assim, para obter acesso a uma maquina bem configurada, é necessário introduzi-la a crer que a máquina do invasor é de confiança – um processo denominado spoofing. Para isso, o invasor precisa descobrir o endereço legitimo de uma maquina da rede interna e enviar à vitima pacotes que apresentam tal endereço como origem. A vitima, crendo ser o atacante uma maquina de confiança, responderá enviando pacotes para o endereço do remetente.
Para o esquema funcionar, entretanto o cracker precisa tomar duas providencias. A primeira é impedir que a maquina legitima responda aos pacotes enviados pela vitima; em geral, isso é feito garantindo-se que a maquina legitima esteja fora do ar (pode-se efetuar o ataque num momento em que se saiba que a maquina esta desligada, ou derrubá-la de algum método mais hostil).
A segunda é garantir que o pacote seja ecoado para fora da rede interna. Em geral, o pacote apenas diz para onde quer ir e os roteadores no caminho decidem qual a melhor rota a seguir. Desta forma, os pacotes enviados pela vítima não seriam passados para a Internet, porque o endereço de destino (que pertence a maquina que esta fora do ar) encontra-se dentro da rede interna. Para evitar isso, o invasor recorre ao "source-routing", uma técnica criada para testes e depuração que permite que a maquina que inicia a comunicação (no caso, o invasor) especifique qual a rota a ser utilizada pôr todos os pacotes de uma determinada conexão, o que garante que os pacotes sejam ecoados da rede interna para a Internet.
Um firewall de rede sofisticado não se contenta em rotear os pacotes para seus destinos: ele mantém informações sobre o estado das conexões e sobre o conteúdo dos pacotes, o que lhe permite perceber que um pacote cujo endereço de origem pertence a rede interna não pode provir da Internet. Se isto ocorre, configura-se o spoofing e o firewall descarta o pacote e aciona o alarme. Similarmente, comunicações normais não devem gerar pedidos de source-routing, de modo que, se um tal pedido surge, o firewall deve considerá-lo um ataque e agir de acordo. Independente de sua sofisticação, firwalls de rede roteiam tráfego diretamente, o que os torna rápidos e transparentes mas os impede de analisar o conteúdo efetivo dos pacotes trafegados e exige que as maquinas na rede interna tenham endereços IP válidos (o que pode ser um risco em si).

Firewall no nível de aplicação

Firewalls de aplicação costumam ser computadores de uso geral que rodam programas especiais chamados "proxy servers". Cada aplicação abilitada na configuração de firewall – SMTP (correio), HTTP (Web), FTP, Telnet etc. – exige um proxy server específico que supervisione a porta IP por onde passam os pacotes referentes àquela determinada aplicação.
Este tipo de firewall não permite tráfego direto entre duas redes: toda comunicação requer o estabelecimento de duas conexões, uma entre o remetente proxy e a outra entre o proxy e o destinatário. O proxy correlaciona a duas comunicações através do número da sessão TCP (que está presente em todos os

pacotes) e ecoa os dados que vêm da conexão x para a conexão y e vice-versa. O que é importante é que todo pacote, antes de ser ecoado de uma conexão para a outra, é analisado pelo proxy server – um programa para detectar abusos de segurança no protocolo utilizado naquela porta específica - , que decide se o pacote deve passar ou ser descartado. O resultado é o firewall de aplicação consege detectar riscos que um firewall de rede não teria como perceber, alcançando um nível de segurança superior.
Um exemplo clássico do tipo de informação que um proxy pode filtrar é o comando DEBUG do SMTP, usado para solicitar a um servidor de correio que forneça certas informações de controle e considerado arriscado pela maior parte dos administradores de rede. Como não é normal que esse tipo de comando seja emitido durante uma troca de mensagens de correio, um bom proxy SMTP descartará o pacote como o comando proibido, mudará o estado do firewall para "ataque em curso" e enviara uma mensagem (que pode até seguir para um pager ou telefone celular) para o administrador, prevenindo-o do ocorrido.
Outro exemplo são proxies FTP, que podem vedar completamente o acesso de usuários externos ás maquinas da empresa ao mesmo tempo que permite que funcionários copiem arquivos da Internet para a rede interne (comando GET), mas não o contrário (comando PUT). Todos esses exemplos estão ligados ao funcionamento dos protocolos específicos de cada aplicação e não poderiam ser implementados em firewalls de rede, que não são capazes de examinar o conteúdo dos pacote IP.
Firwalls de aplicação são bem menos transparentes do que firewalls e rede. Para começar, toda e qualquer aplicação exige a existência de um proxy; se o usuário precisa de uma aplicação para a qual não existe um proxy rodando no firewall, não há o que fazer: a aplicação simplesmente não funcionará. Em um mundo onde há novas aplicações sendo lançadas todos os dias, este tende a ser um problema considerável, e o resultado é que os fornecedores sempre têm uma nova versão (esta suporta SSL, a próxima suportará Real Áudio, a seguinte suportará SQL) de firewall no forno.
Quando é necessário usar uma aplicação para a qual o fornecedor do firewall não tem (nem terá) um proxy específico, a solução é a utilização de um proxy genérico. Criar um proxy genérico é simples: trata-se tão-somente de informar ao firewall que quaisquer pacote trafegando entre as maquinas x (internas) e as maquina y (externas)que usem a porta z são confiáveis e podem passar. Apesar de tais pacotes serem roteados sem uma análise cuidadosa (similar ao que faria um firewall de rede), trata-se de um procedimento razoavelmente seguro, porque a comunicação não monitorada é duplamente restrita: não apenas ocorre numa única porta IP, como só envolvem maquinas de confiança – afinal, se o fornecedor não fosse de confiança não seria contratado.
Como não permite comunicação direta entre o cliente e o servidor, o firewall de aplicação é consideravelmente menos transparente que o firewall de rede. É necessário que o programa cliente saiba que deve estabelecer uma conexão com o proxy e determinar ações como "conecte-se ao servidor Web da Mantel e recupere a página tal para mim". Quando o cliente sabe isso; como é a maioria dos browsers Web, basta configurá-lo corretamente. Quando os clientes são poucos sofisticados e exigem conexões diretas com o servidor (como é comum com FTP e Telnet, pôr exemplo), utiliza-se um artifício: o usuário se loga no proxy e este; m vez de solicitar nome e senha (como seria de esperar), solicita o nome do servidor com o qual se deseja a conexão; a partir daí, tudo funciona normalmente.
O firewall de aplicação oferece algumas vantagens sobre o firewall de rede. A primeira e mais importante é permitir um acompanhamento muito mais próximo e efetivo das comunicações entre duas redes, inclusive com logs e relatórios de auditoria. O fato de o DNS ser também um proxy server permite que os nomes das maquinas internas sejam preservados e que um mesmo nome possa identificar duas maquinas diferentes da origem de quem consulta, se um usuário interno ou externo.
Além disso, como toda a comunicação é ricocheteada pelo firewall, o mundo só precisa saber de um único endereço IP (o da porta externa do firewall), e os verdadeiros endereços das maquinas internas podem ser protegidos, trazendo vários benefícios. Para começar, o simples desconhecimento dos endereços reais reforça a segurança. Melhor ainda é que isso permite o uso de faixas reservadas de endereços que, pôr convenção, não podem ser utilizadas na Internet. Neste caso, é virtualmente impossível para o cracker enviar pacotes diretamente às maquinas da rede interna. E o uso de endereços protegidos também possibilita a atribuição de mais endereços do que os concedidos originalmente pelo provedor de acesso.

Na verdade, a discussão sobre qual é o melhor firewall, se o de rede ou o de aplicação, não procede, porque eles não representam soluções mutuamente excludentes. Os melhores sistemas de firewall, como seria de esperar, adotam ambas as abordagens, permitindo a definição de regras, controles e auditorias nos dois níveis.

Além do firewall

Infelizmente, não há firewall que consiga bloquear um ataque efetuado pôr fora do firewall. Apesar de isso ser óbvio, a Internet parece deter o monopólio no que se refere a difundir o terror; de modo que há muita gente que só vê perigo na grande rede, deixando de lado os outros pontos onde, com freqüência, o dano pode ser maior ou o risco mais provável. São comuns os casos empresas que instalam firewalls de primeira ao mesmo modems permitindo acesso discado sem senha. Isso eqüivale a colocar tranca de aço na portas da frente e abandonar as janelas destrancadas.
Um firewall não impede o vazamento de dados. O correio eletrônico é de fato a forma mais simples de se enviar dados para fora da empresa, mas também é a forma mais perigosa, já que o trafego de correio pode ser controlado e auditado. Um espião consciencioso preferirá uma fita, um disquete (razão pelos quais há quem defenda o banimento dos drives de disquete) ou um simples fax. E não existe apólice de seguro contra estupidez: se um funcionário fornecer sua senha de acesso a usuários não autorizados ou desconhecidos, não há firewall que resolva.
Firewalls podem ser muito eficientes para reconhecer e neutralizar ataques efetuados da utilização maliciosa de características específicas dos protocolos de comunicação utilizados na rede, mas pouco podem fazer contra ataques baseados em dados. Do ponto de vista do firewall, mensagens de correio ou arquivos copiados para algum servidor não constituem ataque. O resultado é que é possível que crackers se valha de características (ou, mais comumente, falhas) de programas específicos para executar ações nefastas. O caso mais notório deste tipo de utilização mal-intencionada foi o vírus da Internet, que se valia de uma falha do sendmail (programa de envio de correio do Unix) e derrubou 6 mil maquinas em 1988. Outros exemplos particularmente graves são os vírus e programas executáveis pelos browsers (como applets java ou controles activeX); ambos os casos são tratados pelos firewalls como dados e, em geral, trafegam de uma rede a outra sem problema algum.
A maneira correta de combater vírus é a tradicional, através da utilização de programas rodando em estações e servidores de arquivos identificar e limpar arquivos contaminados logo depois sua gravação em disco. Também já existem antivírus para servidores de correio capazes de analisar arquivos anexados a mensagens de correio, detectando e removendo vírus antes mesmo que os destinatários sejam notificados de sua chegada. A prevenção contra o código executável distribuído através da Web deve ser feita nos programas que recebem e executam. Browsers como o Netscape e Internet Explorer têm opções de configuração que permitem que tipos de objetos podem ser recebidos e em que condições podem ser executados.
Apesar de haver no mercado excelentes soluções para proteger redes privadas contra ataque de invasores inescrupulosos, o firewall não pode ser encarado como solução isolada para a questão de segurança na comunicação com a Internet. Há empresas que gastam pequenas fortunas para montar firewall inexpugnáveis mas não se preocupam em criar políticas de segurança coerentes e consistentes. Para ser eficaz, o firewall deve ser parte de uma política global de segurança – uma que seja realista o bastante para identificar e prevenir os riscos efetivos (maquinas que contêm dados mais confidenciais, pôr exemplo, não precisam de firewall: elas não devem estar ligadas à Internet), mas que, pôr outro lado, não seja paranóica a ponto de impedir as pessoas de trabalhar.

4. Serviços e Procedimentos Seguros

Este capítulo guia o leitor através de uma série de tópicos os quais deveriam ser observados para tornar um *site* seguro. Cada seção aborda um serviço ou uma capacidade de segurança que pode ser necessária para proteger a informação e os sistemas de um *site*. Os tópicos são apresentados em razoável alto-nível para a introdução de conceitos ao leitor.
Ao longo do capítulo você encontrará referências significativas à criptografia. Está fora do escopo deste documento aprofundar-se em detalhes concernentes à criptografia, mas o leitor interessado pode obter mais informações através de livros e artigos listados na seção de referência deste documento.

4.1 Autenticação

Pôr muitos anos, o método prescrito para a autenticação de usuários tem passado pelo uso de senhas padrão reutilizáveis. Originalmente, estas senhas eram usadas pôr usuários em terminais para autenticarem-se em um computador central. Na época não existiam redes (interiormente ou externamente), sendo mínimo o risco de revelação da senha de texto claro. Atualmente sistemas são conectados através de redes locais, e estas redes locais são conectadas mais adiante e à Internet. Usuários estão se *logando* de toda parte o globo; suas senhas reutilizáveis são freqüentemente transmitidas através destas mesmas redes em texto claro, no ponto para que qualquer um (que esteja na escuta) possa capturar. E, sem dúvida, o Centro de Coordenação CERT* e outras equipes de reação estão vendo um grande número de incidentes envolvendo visualizadores de pacote os quais estão capturando as senhas de texto claro.
Com o advento de tecnologias mais recentes, como senhas de uso único (pôr exemplo, *S/Key*), PGP, e dispositivos de autenticação baseados em *tokens*, as pessoas estão usando *strings* tipo senhas como *tokens* e identificadores numéricos secretos. Se estes *tokens* e identificadores numéricos secretos não forem apropriadamente selecionados e protegidos, a autenticação será facilmente subvertida.

4.1.1 Senhas de uso único

Como mencionado acima, dado os atuais ambientes de rede, é recomendado que *sites* relacionados com a segurança e a integridade de seus sistemas e redes considerem mudanças em relação às senha padrão reutilizáveis. Tem ocorrido muitos incidentes envolvendo programas de rede de Tróia (pôr exemplo, telnet e rlogin) e programas visualizadores de pacotes de rede. Estes programas capturam trios de nomes de máquina, contas e senhas em texto claro. Intrusos podem usar a informação capturada para acesso subseqüente às máquinas e contas. Isto é possível porque 1) a senha é usada várias vezes (consequentemente o termo "reutilizável") e 2) a senha passa através d rede em texto claro.
Foram desenvolvidas algumas técnicas de autenticação que dirigem-se à este problema. Entre estas técnicas estão tecnologias de desafio-resposta que provêem senhas que são uma usadas uma só vez (comumente chamadas de senhas de única vez). Há vários produtos disponíveis que *sites* deveriam considerar o uso. A decisão de usar um produto é responsabilidade de cada organização, e cada organização deveria realizar sua própria avaliação e seleção.

4.1.2 Kerberos

Kerberos é um sistema de segurança de rede distribuído que provê autenticação através de redes inseguras. Caso sejam requisitados pela aplicação, integridade e criptografia também podem ser providos. Kerberos foi desenvolvido originalmente no Instituto de Massachusetts de Tecnologia (MIT) nos anos oitenta. Há dois principais lançamentos do Kerberos, versão 4 e 5 que são, para propósitos práticos, incompatíveis.

Kerberos confia em um banco de dados de chaves simétricas, utilizando um centro de distribuição de chaves (KDC) que é conhecido como o servidor Kerberos. São concedido "ingressos" eletrônicos para usuários ou serviços (conhecidos como "principais") depois de apropriada comunicação com o KDC. Estes ingressos são usados para autenticação entre principais. Todos os ingressos incluem uma marca de tempo a qual limita o período de tempo para o qual o ingresso é válido. Portanto, os clientes e o servidor Kerberos devem possuir uma fonte de tempo segura e estarem aptos à manter o controle de tempo com precisão.
O lado prático de Kerberos é sua integração com o nível de aplicação. Aplicações típicas como FTP, telnet, POP e NFS têm sido integradas com o sistema Kerberos. Há uma variedade de implementações que possuem níveis variados de integração. Pôr favor veja o FAQ do Kerberos disponível via http://www.ov.com/misc/krb-faq.html para a mais recente informação.

4.1.3 Escolhendo e Protegendo *Tokens* e Indentificadores Numéricos Secretos

Quando da seleção de *tokens* secretos, deve-se preocupar-se em escolhe-los cuidadosamente. Como a seleção de senhas, eles devem ser robustos contra esforços de força bruta para adivinha-los. Isto é, eles não devem ser palavras únicas em qualquer idioma, qualquer acrônimo comum, industrial ou cultural, etc. Idealmente, eles devem ser mais longos que curtos e consistir de frases de passagem que combinem letras minúsculas e maiúsculas, dígitos e outros caracteres.
Uma vez escolhida, a proteção destes *tokens* secretos é muito importante. Alguns são usados como identificadores numéricos para dispositivos de hardware (como cartões de *token*) e estes não devem ser escritos abaixo ou colocados em mesmo local do dispositivo com os quais são associados. Outros, como uma chave do PGP, devem ser protegidos de acesso não autorizado.
Uma última palavra neste assunto. Quando da utilização de produtos de criptografia, como PGP, tome cuidado em determinar o comprimento apropriado da chave e assegurar que seus usuários estejam treinados para fazer igualmente. Como avanços de tecnologia, o comprimento seguro mínimo de chave continua crescendo. Tenha certeza de que seu *site* mantenha o mais recente conhecimento na tecnologia de forma que você possa assegurar que qualquer criptografia em uso esteja provendo a proteção que você acredita que ele realmente esteja.

4.1.4 Garantia da Senha

Enquanto a necessidade de eliminar o uso de senhas padrão reutilizáveis não pode ser exagerada, é reconhecido que algumas organizações ainda podem estar usando-as. É recomendado que estas organizações mudem para o uso de uma melhor tecnologia. Enquanto isso, nós temos o seguinte conselho para ajudar com a seleção e manutenção de senhas tradicionais. Mas lembre-se, nenhuma destas medidas provê proteção contra revelação devido a programas de visualização de pacotes.
(1) A importância de senhas robustas - Em muitos (se não a maioria) casos de penetração de sistema, o intruso precisa ganhar acesso à uma conta no sistema. Uma maneira em que esta meta é tipicamente alcançada é adivinhando a senha de um usuário legítimo. Isto é freqüentemente realizado através da execução de programa automático de quebra de senhas, o qual utiliza um dicionário muito grande contra o arquivo de senhas do sistema. O único modo de resguardar-se contra a descoberta de senhas desta maneira é pela seleção cuidadosa de senhas que não podem ser facilmente adivinhado (i.e., combinações de números, letras e caráter de pontuação). Senhas também devem ser tão compridas quanto suportado pelo sistema e toleradas pelo usuário.
(2) Troca de senhas padrão - Muitos sistemas operacionais e programas de aplicação são instalados com contas e senhas padrão. Estas devem ser mudadas imediatamente para algo que não possa ser adivinhado ou quebrado.

(3) Restringindo acesso ao arquivo de senhas - em particular, um *site* deseja proteger a porção de senha codificada do arquivo para que os pretendentes a intrusos não os tenham disponíveis para a quebra. Uma técnica efetiva é usar senhas de sombra onde o campo de senha do arquivo padrão contém uma senha boba ou falsa. O arquivo contendo as senhas legítimas é protegido em outro lugar do sistema.
(4) Envelhecimento de senhas - Quando e como expirar senhas ainda é um assunto de controvérsia entre a comunidade de segurança. Geralmente é aceito que uma senha não deve ser mantida uma vez que uma conta não se encontra mais em uso, mas é ardentemente debatido se um usuário deve ser forçado a mudar uma senha boa na que esta em uso ativo. Os argumentos para a troca de senhas relaciona-se à prevenção do uso continuo de contas penetradas. Entretanto, a oposição reivindica que mudanças de senha freqüentes conduza usuários a escreverem suas senhas em áreas visíveis (como cola-las em um terminal) ou selecionarem senhas muito simples as quais sejam fáceis de adivinhar. Também deve ser declarado que um intruso provavelmente usará uma senha capturada ou adivinhada mais cedo do que tarde. Neste caso o envelhecimento da senha provê pequena ou nenhuma proteção.
Enquanto não há resposta definitiva a este dilema, uma política de senhas deve dirigir a questão diretamente e prover diretrizes para com que freqüência um usuário deve mudar a senha. Certamente, uma mudança anual em sua senha não é difícil para a maioria dos usuários, normalmente, e você deve considerar esta requisição. É recomendado que senhas sejam mudadas pelo menos sempre que uma conta privilegiada seja compromissada, exista uma mudança pessoal crítica (especialmente se for um administrador!) ou quando uma conta seja compromissada. Ainda, se a senha de uma conta privilegiada é compromissada, todas as senhas no sistema devem ser alteradas.
(5) Bloqueio de contas e senhas - Alguns *sites* acham útil desabilitar contas depois de um número pré-definido de não sucedidas tentativas de autenticação. Se seu *site* decidir empregar este mecanismo, é recomendado que o mecanismo não avise a sim mesmo. Depois de
desabilitar, até mesmo se a senha correta for apresentada, a mensagem exibida deve permanecer como a de uma tentativa não sucedida de *login.* A implementação deste mecanismo requererá que usuários legítimos contatem seus administradores de sistema para pedir que sua conta seja reativada.
(6) Uma palavra sobre o *finger daemon* - O *finger daemon* exibe, como padrão, informação considerável do sistema e do usuário. Pôr exemplo, ele pode exibir uma lista de todos os usuários que atualmente usam um sistema ou todo o conteúdos do arquivo *.plan* de um usuário específico. Esta informação pode ser usada pôr possíveis intrusos para identificar *usernames* e adivinhar suas senhas. É recomendado que *sites* considerem modificar o *finger* para restringir a informação exibida.

4.2 Confiança

Haverá recursos de informação que seu *site* desejará proteger da revelação à entidades não autorizadas. Sistemas operacionais possuem freqüentemente mecanismos de proteção de arquivo embutidos que permitem um administrador controlar quem no sistema pode acessar ou "enchergar" o conteúdo de um determinado arquivo. Um modo mais forte de prover confiança é através de criptografia. Criptografia é realizada misturando dados de forma que venha a ser muito difícil e consuma tempo demasiado para que qualquer um que não um receptor ou proprietário autorizado possa obter o texto claro. Os receptores e autorizados e proprietários da informação possuirão as chaves de decriptação correspondentes as quais lhes permitem ordenar facilmente o texto para uma forma legível (texto claro). Nós recomendamos que *sites* usem criptografia para prover confiança e proteger informação valiosa.
O uso de criptografia é controlado às vezes pôr regulamentos governamentais e de *sites*, portanto nós encorajamos que os administradores tornem-se informados de leis ou políticas que regulem seu uso antes de empregá-la. Está fora do escopo deste documento discutir os vários algoritmos e programas disponíveis para este propósito, mas nós acautelamos contra o uso casual do programa *crypt* do UNIX pôr ter sido achado facilmente quebrável. Nós também encorajamos todos a levarem tempo para entender a força da criptografia em qualquer algoritmo/produto dado antes de usá-lo. A maioria dos produtos famosos é bem-documentada na literatura, devendo ser esta uma tarefa bastante fácil.

4.3 Integridade

Como um administrador, você desejará ter certeza que informações (pôr exemplo, arquivos de sistema operacional, dados de companhia, etc.) não tenham sido alteradas de uma maneira não autorizada. Isto significa que você desejará prover alguma garantia sobre a integridade da informação em seus sistemas. Um modo de prover isto é realizar um *checksum* do arquivo inalterado, armazenar o *checksum* de maneira *offline* e periodicamente (ou quando desejado) conferir para ter certeza que o checksum do arquivo *online* não tenha sido alterado (que indicaria a alteração dos dados).
Alguns sistemas operacionais vêm com programas de *checksum*, como o programa *sum* do UNIX. Entretanto, estes podem não prover a proteção da que você precisa de fato. Arquivos podem ser modificados arquivos de tal forma que o resultado do programa *sum* do UNIX seja conservado! Assim, nós sugerimos a utilização de um forte programa de criptografia, como o programa de condensão de mensagem MD5 [ref.], para produzir os *checksums* que você usará para garantir a integridade.
Há outras aplicações onde a integridade precisará ser assegurada, como quando da transmissão de um *email* entre duas entidades. Existem produtos disponíveis os quais podem prover esta capacidade. Uma vez que você identificar esta capacidade como sendo necessária, você pode identificar tecnologias que proverão isto.

4.4 Autorização

Autorização se refere ao processo de conceder privilégios para processos e, fundamentalmente, usuários. Isto difere daquela autenticação que é o processo de identificação de um usuário. Uma vez identificados (seguramente), os privilégios, direitos, propriedade e ações permissíveis do usuário são determinados através da autorização.
Listar explicitamente as atividades autorizadas de cada usuário (e processo de usuário) com respeito a todos os recursos (objetos) é impossível em um sistema razoável. Em um sistema real certas técnicas são usadas para simplificar o processo de conceder e verificar autorizações.
Uma abordagem, popularizada em sistemas de UNIX, é associar a cada objeto três classes de usuário: proprietário, grupo e mundo. O proprietário é o criador do objeto ou o usuário associado como proprietário pelo super usuário. As permissões de proprietário (leitura, escrita e execução) aplicam-se somente para o proprietário. Um grupo é uma coleção de usuários que compartilham direitos de acesso sobre um objeto. As permissões de grupo (leitura, escrita e execução) aplicam-se a todos os usuários no grupo (exceto o proprietário). O mundo refere-se a todos outros com acesso ao sistema. As permissões de mundo (leitura, escrita e execução) aplicam-se a todos os usuários (menos o proprietário e membros do grupo).
Outra abordagem é associar a um objeto uma lista que explicitamente contém a identidade de todos usuários permitidos (ou grupos). Esta é uma Lista de Controle de Acesso (ACL). A vantagem de ACLs é que elas são
facilmente mantidas (uma lista central pôr objeto) e é muito fácil verificar visualmente quem tem acesso ao que. As desvantagens são os recursos extras exigidos armazenar tais listas, como também o vasto número de listas requeridas para sistemas grandes.

4.5 Auditoria

Esta seção cobre os procedimentos para coletar os dados gerados pela atividade de rede, que podem ser úteis para analisar a segurança de uma rede e responder a incidentes de segurança.

4.5.1 O que coletar

Dados de auditoria deveriam incluir qualquer tentativa de obter um nível de segurança diferente pôr qualquer pessoa, processo, ou outra entidade da rede. Isto inclui "login" e "logout", acesso de super-usuário (ou o equivalente não-UNIX), geração de tíquete (para Kerberos, pôr exemplo) e qualquer outra mudança de acesso ou estado. É especialmente importante notar o acesso "anonymous" ou "guest" a servidores públicos.

Os dados reais a coletar irão diferir para locais diferentes e para mudanças de diferentes tipos de acesso dentro de um local. Em geral, as informações que você quer coletar incluem: código do usuário e nome do host para login e logout; direitos de acessos prévios e novos; e um "timestamp". É claro, há muito mais informações que poderiam ser coletadas, dependendo do que o sistema torna disponível e quanto espaço está disponível para armazenar aquelas informações.

Uma nota muito importante: não colete senhas. Isto cria uma brecha potencialmente enorme na segurança se os registros de auditoria forem inadequadamente acessados. Também não colete senhas incorretas, já que elas diferem das senhas válidas somente pôr um caracter ou transposição.

4.5.2 Processo de Coleta

O processo de coleta deveria ser ordenado pelo host ou recurso sendo acessado. Dependendo da importância dos dados e a necessidade de tê-los localmente em instâncias nas quais os serviços estão sendo negados, os dados poderiam ser guardados localmente ao recurso até que sejam necessários ou serem transmitidos para armazenamento após cada evento.

Há basicamente 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 (pôr exemplo um CD-ROM ou uma unidade de fita especialmente configurada), ou num dispositivo somente de escrita (pôr exemplo uma impressora). Cada método tem suas vantagens e desvantagens.

O registro em um sistema de arquivos é o que consome recursos menos intensamente dentre os três métodos. Ele permite acesso instantâneo aos registros para análise, o que pode ser importante se um ataque está em curso. Entretanto, é também o método menos confiável. Se o host que efetua o registro foi comprometido, o sistema de arquivos é usualmente a primeira coisa onde ir; um intruso poderia facilmente acobertar rastear uma intrusão.

Coletar dados de auditoria em um dispositivo de escrita única é ligeiramente mais trabalhoso de configurar que um simples arquivo, mas ele tem a significante vantagem da segurança significativamente aumentada porque um intruso não poderia alterar os dados indicadores de que uma invasão aconteceu. A desvantagem deste método é a necessidade de manter um fornecimento de meio de armazenamento e o custo desse meio. Também, os dados podem não estar instantaneamente disponíveis.

Registro em impressora é útil em sistemas onde registros ("logs") permanentes e imediatos são necessários. Um sistema de tempo real é um exemplo disto, onde o ponto exato de falha ou ataque deve ser registrado. Uma impressora laser, ou outro dispositivo que buferiza dados (pôr exemplo um servidor de impressão) podem sofrer de dados perdidos se os buffers contém os dados necessários num instante crítico. A desvantagem de, literalmente, trilhas de papel é a necessidade de vasculhar os registros a mão.

Há também a questão de tornar seguro o caminho entre o dispositivo que gera o registro e o que realmente armazena o registro (pôr exemplo um servidor de arquivos, uma unidade de fita/CD-ROM, uma impressora). Se o caminho está comprometido, o registro pode ser parado ou adulterado ou ambos. Em um mundo ideal, o dispositivo de registro estaria diretamente ligado pôr um simples e único cabo ponto-a-ponto. Como isto é usualmente impraticável, o caminho deveria passar pôr um número mínimo de redes e roteadores. Mesmo que os registros possam ser bloqueados, adulteração pode ser evitada com somas de verificação criptográficas (provavelmente não é necessário criptografar os registros porque e‡es não deveriam conter informações sensitivas em primeiro lugar.

4.5.3 Carga da Coleta

Coletar dados de auditoria pode resultar em um rápido acúmulo de octetos, logo a disponibilidade de armazenamento para estas informações devem ser consideradas desde cedo. Existem poucas maneiras de reduzir o espaço de armazenamento exigido. Primeiro, os dados podem ser compactados, usando um de muitos métodos. Ou, o espaço exigido pode ser minimizado guardando dados pôr um período mais curto de tempo com somente os sumários de dados sendo guardados em arquivos de longo prazo. Um grande inconveniente deste último método envolve a resposta a incidentes. Freqüentemente, um incidente já vem ocorrendo pôr algum período de tempo, quando um local o percebe e começa a investigar. Neste momento é muito útil ter disponíveis registros de auditoria detalhados. Se estes são apenas sumários, pode não haver detalhes suficientes para tratar plenamente o incidente.

4.5.4 Manipulando e Preservando os Dados de Auditoria

Os dados de auditoria deveriam estar entre aqueles mais protegidos no local e nos backups. Se um intruso ganhasse 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. Pôr esta razão, é recomendável buscar a orientação da equipe jurídica ao decidir como os dados de auditoria devem ser tratados. Isto deveria acontecer antes que um incidente ocorra.

Se um plano de manipulação de dados não for adequadamente definido antes de um incidente, isso pode significar que não há como recorrer do resultado de um evento, e isso pode criar responsabilidades resultantes do tratamento impróprio dos dados.

4.5.5 Considerações Legais

Devido ao conteúdo dos dados de auditoria, há um número de questões que surgem que poderiam precisar da atenção da sua equipe jurídica. Se você coleta e salva dados de auditoria, você precisa estar preparado para as conseqüências resultantes tanto da sua existência como do seu conteúdo.

Uma área diz respeito a privacidade dos indivíduos. Em certas instâncias, os dados de auditoria podem conter informações pessoais. A investigação nos dados, ainda que para uma verificação de rotina da segurança do sistema, poderia representar uma invasão de privacidade.

Uma segunda área de preocupação envolve o conhecimento de comportamento intrusivo proveniente de seu local. Se uma organização mantém dados de auditoria, será ela responsável pôr examiná-los para investigar incidentes ? Se um host em uma organização é usado como uma base de lançamento para um ataque contra outra organização, pode a segunda organização usar os dados de auditoria da primeira organização para provar negligência pôr parte da primeira ?

Pretende-se que os exemplos acima sejam compreensivos, mas eles deveriam motivar sua organização a considerar as questões legais envolvidas com dados de auditoria.

4.6 Acesso

4.6.1 Acesso Físico

Restrinja o acesso físico aos hosts, permitindo acesso somente a aquelas pessoas que devem usá-los. Hosts incluem terminais confiáveis (ou seja, terminais que permitem uso não autenticado tais como consoles do sistema, terminais de operadores e terminais dedicados a tarefas especiais), e microcomputadores e estações de trabalho individuais, especialmente aqueles conectados a sua rede. Certifique-se de que as áreas de trabalho das pessoas se ajusta bem às restrições de acesso; caso contrário elas encontrarão maneiras de evitar sua segurança física (pôr exemplo portas fechadas abrindo).

Mantenha cópias originais e backup de programas e dados seguras. Além de mantê-los em boas condições para fins de backup, eles devem ser protegidos contra furtos. É importante manter backups em uma localização separada dos originais, não somente em consideração a danos, mas também para proteger contra furtos.
Hosts portáteis são um risco particular. Certifique-se que eles não causarão problemas se um computador portátil de seu pessoal for roubado. Considere o desenvolvimento de políticas para as espécies de dados que deveriam ser permitidas residirem em discos de computadores portáteis bem como a maneira pela qual os dados deveriam ser protegidos (pôr exemplo criptografia) quando estivessem em computadores portáteis.
Outras áreas onde o acesso físico deveria ser restringido são os gabinetes de fiação e elementos importantes de rede como servidores de arquivos, hosts servidores de nomes e roteadores.

4.6.2 Conexões de Rede "Walk-Up"

Pôr conexões de rede "walk-up", nos referimos a pontos de conexão localizados a fim de proporcionar uma maneira conveniente para usuários conectarem um host portátil a sua rede.
Considere que você precise fornecer este serviço, tendo em mente que isto permite a qualquer usuário conectar um host não autorizado a sua rede. Isto aumenta o risco de ataques usando técnicas tais como corrupção ("spoofing") de endereços IP, espionagem ("sniffing") de pacotes, etc. A gerência da instalação e os usuários devem estimar os riscos envolvidos. Se você decide fornecer conexões "walk-up", planeje o serviço cuidadosamente e defina precisamente onde você irá fornecê-lo a fim de que você possa assegurar a segurança de acesso físico necessária.
Um host "walk-up" deveria ser autenticado antes que seja permitido ao usuário do mesmo acessar recursos na sua rede. Como uma alternativa, pode ser possível controlar o acesso físico. Pôr exemplo, se o serviço destina-se a estudantes, você poderia fornecer tomadas de conexão "walk-up" somente nos laboratórios de estudantes.
Se você está fornecendo acesso "walk-up" para visitantes se conectarem de volta a suas redes de origem (pôr exemplo para ler mail, etc) em sua facilidade, considere o uso de uma sub-rede separada que não tem nenhuma conectividade com a rede interna.
Fique de olho em qualquer área que contem acesso não monitorado à rede, tais como escritórios vazios. Pode ser sensato desconectar tais áreas no gabinete de cabeamento, e considerar o uso de hubs seguros e monitoramento de tentativas de conexão de hosts não autorizados.

4.6.3 Outras Tecnologias de Rede

Tecnologias consideradas aqui incluem X.25, RDSI, SMDS, DDS e Frame Relay. Todas são fornecidas através de enlaces físicos que passam pôr centrais telefônicas, fornecendo o potencial para que estes sejam desviados. Os "crackers" estão certamente interessados em comutações telefônicas bem como em redes de dados !
Com tecnologias comutadas, use circuitos virtuais permanentes (PVCs) ou grupos de usuários fechados sempre que possível. Tecnologias que fornecem autenticação e/ou criptografia (tais como IPv6) estão evoluindo rapidamente; considere usá-las nos enlaces onde a segurança é importante.

4.6.4 Modems

4.6.4.1 Linhas de Modem devem ser Gerenciadas

Ainda que elas forneçam acesso conveniente a um local para todos seus usuários, elas podem também fornecer um desvio efetivo dos firewalls do local. Pôr esta razão é essencial manter um controle apropriado dos modems.
Não permite aos usuários instalar uma linha de modem sem uma autorização apropriada. Isto inclui as instalações temporárias (pôr exemplo, pendurar um modem em um aparelho de fax ou uma linha telefônica durante a noite.

Tenha um registro de todas as suas linhas de modem e mantenha-o atualizado. Conduza verificações regulares (idealmente automatizadas) dos modems não autorizados no "site".

4.6.4.2 Usuários de Discagem devem ser Autenticados

A verificação do código de usuário e da senha deveria ser completada antes que o usuário possa ter acesso a qualquer coisa na sua rede. Considerações normais sobre segurança de senhas são particularmente importantes (veja a seção 4.1.1).
Lembre que linhas telefônicas podem ser escutadas clandestinamente, e que é muito fácil interceptar mensagens em telefones celulares. Os modems modernos de alta velocidade usam técnicas de modulação mais sofisticadas que tornam-nos mais difíceis de monitorar, mas é prudente assumir que "hackers" sabem como escutar escondidos suas linhas. Pôr esta razão, você deveria usar senhas "one-time" sempre que possível.
É de grande utilidade ter um único ponto de entrada para acessos discados (pôr exemplo um único grande "pool" de modems) para que todos usuários sejam autenticados da mesma forma. Os usuários irão eventualmente digitar incorretamente uma senha. Estabeleça um intervalo curto - digamos de dois segundos - após o primeiro e o segundo "login" falho, e force uma desconexão após o terceiro. Isto irá frear ataques de senha automatizados. Não diga ao usuário se foi o seu código, a senha, ou ambos que estavam errados.

4.6.4.3 Capacidade de Chamada Reversa

Alguns servidores "dial-in" oferecem facilidades de chamada reversa (ou seja, o usuário disca e é autenticado, então o sistema desconecta a chamada e chama de volta no número especificado). A chamada reversa é útil porque se alguém estava para adivinhar um código e senha de usuário, é desconectado e o sistema chama de volta o usuário real cuja senha foi quebrada; chamadas aleatórias de um servidor são suspeitas, quando muito. Isto significa que os usuários podem se logar somente de um único local (para onde o servidor está configurado para discar de volta), e é claro podem existir despesas associadas com a localização da chamada reversa.
Este recurso deveria ser usado com cuidado; ele pode ser facilmente desviado. No mínimo, certifique-se que a chamada de retorno nunca é feita a partir do mesmo modem que recebeu a chamada de entrada. Em geral, ainda que a chamada reversa possa aumentar a segurança de modems, você não deveria depender exclusivamente dela.

4.6.4.4 Todos os Logins deveriam ser Registrados no Log

Todos os logins bem-sucedidos ou não deveriam ser registrados no log. Entretanto, não guarde senhas corretas no log. Ao invés registre-as como uma simples tentativa de login bem-sucedida. Já a maioria das senhas são digitas incorretamente pôr usuários autorizados. Elas variam somente pôr um único caracter da senha real. Além disso se você não puder manter tal log seguro, não as registre em hipótese alguma.
Se a identificação da linha chamadora está disponível, tome vantagem disso para registrar o número chamador para cada tentativa de login. Seja sensível as questões de privacidade atingidas pela identificação da linha chamadora. Também esteja ciente que a identificação da linha chamadora não deve ser considerada confiável (já que intrusos têm sabido como arrombar comutações telefônicas e "rotear" números de telefone ou fazer outras mudanças); use os dados para fins informativos somente, não para autenticação.

4.6.4.5 Escolha seu "Banner" de Abertura Cuidadosamente

Muitos locais usam um "default" do sistema contido em um arquivo de mensagem do dia para seu "banner" de abertura. Infelizmente, isto freqüentemente inclui o tipo de hardware e sistema operacional do host. Isto pode fornecer informações valiosas para um possível intruso. Ao invés, cada local deveria criar seu próprio "banner" de login especifico, tomando cuidado para somente incluir as informações necessárias.

Exiba um "banner" curto, mas não ofereça um nome "convidativo" (pôr exemplo "Universidade XYZ", "Sistema de Registro de Estudantes"). Ao invés, forneça o nome de seu local, uma advertência curta de que as sessões podem ser monitoradas, e um "prompt" de código de usuário e senha. Verifique possíveis questões legais relacionadas ao texto que você põe no "banner".
Para aplicações de alta segurança considere o uso de uma senha "cega" (isto é, não dê nenhuma resposta a uma chamada que chega até que o usuário tenha digitado uma senha). Isto efetivamente simula um modem morto.

4.6.4.6 Autenticação "Dial-Out"

Usuários "dial-out" deveriam ser também autenticados, particularmente porque seu local terá de pagar pelas despesas telefônicas.
Jamais permita discagem de saída a partir de uma chamada de entrada não autenticada, e considere se você irá permití-la a partir de uma autenticada. O objetivo aqui é evitar que chamadores usem seu "pool" de modems como parte de uma cadeia de "logins". Isto pode ser difícil de detectar, em especial se um "hacker" estabelece um caminho através de muitos hosts em seu local.
No mínimo não permita que os mesmos modems e linhas telefônicas sejam usadas para discagem de entrada e de saída. Isto pode ser facilmente implementado se você operar "pools" de modems separados para discagem de entrada e discagem de saída.

4.6.4.7 Torne sua Programação de Modems a "Prova de Bala" tanto quanto o Possível

Certifique-se de que os modems não podem ser reprogramados enquanto estiverem em serviço. No mínimo, certifique-se que três sinais de mais ("+++") não colocarão seus modems de discagem de entrada em modo de comando !
Programe seus modems para "resetarem" sua configuração padrão no início de cada chamada. Esta precaução protegerá você contra a reprogramação acidental de seus modems. "Resetando-os" tanto no início como no final de cada chamada irá assegurar um nível regularmente alto de confidencialidade que um novo chamador não herdará da sessão do chamador prévio.
Verifique se seus modems encerram chamadas limpamente. Quando um usuário se desloga de um servidor de acesso, verifique se o servidor desliga a linha telefônica adequadamente. É igualmente importante que o servidor force "logouts" sempre que as sessões estiverem ativas e o usuário desliga inesperadamente.

4.7 Protegendo Backups

O procedimento de criar backups é uma parte clássica de operar um sistema de computação. Dentro do contexto deste documento, backups são tratados como parte do plano global de segurança de um local. Há muitos aspectos de backups que são importantes neste contexto:

1. Certifique-se de que seu local está criando backups
2. Certifique-se de que seu local está usando armazenamento em separado para os backups. A localização deveria ser cuidadosamente selecionada tanto para a sua segurança como para a sua disponibilidade.
3. Considere criptografar seus backups para proporcionar proteção adicional das informações uma vez que estão guardadas em separado. Entretanto, esteja ciente de que você precisará de um bom esquema de gerência de chaves para que você possa recuperar os dados em qualquer ponto no futuro. Também, certifique-se de que você terá acesso aos programas de decodificação necessários no futuro quando você precisar efetuar a decodificação.
4. Não assuma sempre que seus backups estão bons. Tem havido muitos exemplos de incidentes de segurança de computador que ocorreram pôr longos períodos de tempo antes de serem notados. Em tais casos, backups dos sistemas afetados estão também corrompidos.

5. Periodicamente verifique a correção e a complexão de seus backups.

5. Tratamento de Incidentes de Segurança

Este capítulo do documento será um guia a ser usado antes, durante, e depois de um incidente de segurança de computador que aconteça em host, rede, site, ou ambiente de multi-site. A filosofia de operação no caso de uma brecha de segurança de computador é reagir conforme um plano. Isto é verdade 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 enfadado. Cada um dos possíveis tipos de eventos, como esses listados, deveriam ser previstos com antecedência pôr planos de contingência adequados.
Segurança de computador tradicional, enquanto bastante importante no plano global de segurança do site, normalmente presta pouca atenção em como agir de fato uma vez que um ataque ocorra. O resultado é que quando um ataque está ocorrendo, são tomadas muitas decisões com pressa e podem estar prejudicando a identificação da fonte do incidente, a coleta de evidências para serem usadas em esforços de prossecução, preparar para a recuperação do sistema, e protegendo os dados valiosos contidos no sistema.
Um dos mais importantes, mas freqüentemente ignorados, benefícios paro tratamento eficiente do incidente é a economia. Quando ambos pessoal técnico e administrativo respondem a um incidente, isto requer recursos consideráveis. Se treinados para lidar com incidentes eficazmente, menos tempo de pessoal é requerido quando um acontece.
Devido à Internet a maioria dos incidentes não estão restritos a um único local. Vulnerabilidade de sistemas operacionais aplicam-se (em alguns casos) para vários milhões de sistemas, e muitas vulnerabilidades são exploradas dentro da própria rede. Então, é vital que todos os sites com partes envolvidas sejam informados o mais cedo possível.
Outro benefício é relacionado a relações públicas. Notícias sobre incidentes de segurança de computadores tendem a danificar a imagem de uma organização entre os clientes atuais ou potenciais. O tratamento eficiente de incidentes minimiza a exposição negativa.
Um benefício final de tratamento incidente eficiente é relacionado a assuntos legais. É possível que num futuro próximo organizações possam ser consideradas responsáveis porque um de seus nodos foi usado para lançar um ataque à rede. Em uma situação semelhante, podem ser processadas as pessoas que desenvolvem remendos ou workarounds, caso estes sejam ineficazes, resultando em comprometimento dos sistemas, ou se danificam os mesmos. Sabendo sobre vulnerabilidades do sistema operacional e padrões de ataques, e tomando medidas apropriadas para se opor a estas ameaças potenciais, é crítico para evitar possíveis problemas legais.
As seções neste capítulo provêem um esboço e ponto de partida para criar a política de seu site para tratar incidentes de segurança. As seções são:
1. preparando e planejando (quais são as metas e objetivos no tratamento de um incidente).
2. notificação (quem deveria ser contactado no caso de um incidente).
* Os gerentes locais e pessoal
* Agências investigativas e executoras da lei
* Grupos que tratam de incidentes de segurança de computador
* Locais afetados e envolvidos
* Comunicações internas
* Relações públicas e imprensa
3. identificando um incidente (é um incidente e o quanto é sério).
4. tratamento (o que deveria ser feito quando um incidente acontece).
* 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)
* Seqüência (que ação deveriam ser tomadas depois do incidente)
5. conseqüências (quais as implicações de incidentes passados).
6. resposta administrativa para incidentes.
O resto deste capítulo detalhará os assuntos envolvidos em cada dos tópicos importantes listados acima, e provê alguma direção sobre o que deveria ser incluído em uma política do site para tratar incidentes.

5.1 Preparando e Planejando o Tratamento de Incidentes

Parte do tratamento de um incidente é estar preparado para responder a um incidente antes dele acontecer em primeiro lugar. Isto inclui estabelecer um nível satisfatório de proteções como o explicado nos capítulos anteriores. Fazer isto ajudaria seu site a prevenir incidentes como também limitar dano potencial resultante de incidentes. Proteção também inclui preparar diretrizes de tratamento de incidentes como parte de um plano de contingência para sua organização ou site. Ter planos escritos elimina muito da ambigüidade que acontece durante um incidente, e conduzirá a um conjunto mais apropriado e completo de respostas. É vitalmente importante testar o plano proposto antes de um incidente acontecer através de "dry runs". Um grupo poderia considerar a contratação de um grupo-tigre até mesmo para agir em paralelo com o "dry runs" (Nota: um grupo-tigre é um grupo de especialistas que tentam penetrar a segurança de um sistema.)

1. Aprender a responder eficazmente a um incidente é importante pôr um número de razões:
2. proteger os recursos que poderiam ser comprometidos
3. proteger os recursos que poderiam ser utilizados mais eficientemente se um incidente não requeresse seus serviços
4. seguir os regulamentos (do governo ou outros)
5. prevenir o uso de seus sistemas em ataques contra outros sistemas (que poderia implicar em obrigações legais)
6. minimizar o potencial para exposição negativa

Como em qualquer conjunto de procedimentos previamente planejados, deve ser dada a atenção a um conjunto de objetivos para tratar incidentes. Estas metas terão prioridades diferentes dependendo do site. Um conjunto específico de objetivos pode ser identificado:

1. descobrir como aconteceu.
2. descobrir como evitar exploração adicional da mesma vulnerabilidade.
3. evitar a expansão e incidentes adicionais.
4. avaliar o impacto e dano do incidente.
5. recuperar-se do incidente.
6. atualizar políticas e procedimentos conforme necessário.
7. descobrir quem fez isto (se apropriado e possível).

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 ser tomadas durante um incidente com bastante antecendência 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.(Esteja atento aos regulamentos de seu site ou do governo)

Prioridade 3--proteja 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.

Prioridade 4--previna dano para sistemas (pôr 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. Os sites terão que avaliar a melhor opção entre desligar e desconectar, manter o sistema funcionando. Pode haver acordos de serviços em lugares que podem requerer a manutenção dos sistemas no ar mesmo com a possibilidade de danos adicionais. Porém, o dano e escopo de um incidente podem ser tão extensos que aqueles acordos de serviço podem ter que ser ignorados.

Uma implicação importante para definir prioridades é que uma vez que a vida humana e considerações de segurança nacionais foram previstas, é geralmente mais importante salvar dados que software e hardware. Embora é indesejável ter qualquer dano ou perda durante um incidente, sistemas podem ser substituídos. Porém, a perda ou comprometimento de dados (especialmente classificados ou proprietários) normalmente não é de forma alguma um resultado aceitável.

Outra preocupação importante é o efeito em outros, além dos sistemas e redes onde o incidente acontece. Dentro dos limites impostos pôr regulamentos governamentais é sempre importante informar as partes afetadas o mais cedo possível. Devido às implicações legais deste tópico, ele deveria ser incluído nos procedimentos planejados para evitar demoras adicionais e incertezas para os administradores.

Qualquer plano para responder a incidentes de segurança deveria ser guiado pôr políticas locais e regulamentos. Sites privados e do governo que lidem com material classificado tem regras específicas que eles devem seguir.

As políticas escolhidas pôr seu site sobre como reagir a incidentes irá moldar sua resposta Pôr exemplo, pode fazer pouco sentido criar mecanismos para monitorar e rastrear intrusos se o seu site não planeja entrar em ação contra os intrusos caso eles sejam pegos. Outras organizações podem ter políticas que afetam seus planos. Companhias de telefone freqüentemente liberam informações sobre rastreamento de telefones apenas para agências responsáveis pela execução da lei.

Tratar incidentes pode ser tedioso e requerer qualquer número de tarefas rotineiras que poderiam ser tratadas pelo pessoal de apoio. Para liberar o pessoal técnico, é útil identificar pessoal de apoio que ajudará com tarefas como: fotocopiar, passar fax, etc.

5.2 Notificação e Pontos de Contato

É importante estabelecer contatos com várias pessoas antes de um incidente real acontecer. Muitas vezes, incidentes não são emergências reais. Na realidade, com freqüência você poderá tratar as atividades internamente. Porém, também haverá muitas vezes quando outros fora de seu departamento imediato precisarão ser incluídos no tratamento de incidentes. Estes contatos adicionais incluem os gerentes locais e os administradores de sistemas, contatos administrativos para outros sites na Internet, e várias

organizações investigativas. Conhecendo estes contatos antes dos incidentes acontecerem ajudará a fazer seu processo de tratamento de incidentes mais eficiente.
Para cada tipo de contato de comunicação, Pontos de Contato (POC) específicos deveriam ser definido. Estes podem ser de natureza técnica ou administrativa e podem incluir agências legais ou investigativas como também os provedores de serviço e vendedores. Ao estabelecer estes contatos, é importante decidir quanta informação será compartilhada com cada classe de contato. É especialmente importante definir, com antecedência, que informação será compartilhada com os usuários de um site, com o público (inclusive a imprensa), e com outros sites.
Determinar estes assuntos é especialmente importantes para a pessoa local responsável pôr tratar o incidente, já que essa pessoa é responsável pela notificação dos outros. Uma lista de contatos em cada uma destas categorias representam uma economia de tempo importante para esta pessoa durante um incidente. Pode ser bastante difícil achar uma pessoa apropriada durante um incidente quando muitos eventos urgentes estão acontecendo. É fortemente recomendado que os números de telefone pertinentes (também endereços de correio eletrônicos e números de fax) sejam incluídos na política de segurança do site. Os nomes e informações de contato de todos os indivíduos que estarão envolvidos diretamente no tratamento de um incidente devem ser colocados no topo desta lista.

5.2.1 Gerentes locais e Pessoal

Quando um incidente está ocorrendo, uma questão importante é decidir quem está encarregado de coordenar a atividade dos diversos jogadores. Um dos maiores enganos que pode ser cometido é ter várias pessoas cada qual trabalhando independentemente, mas não trabalhando junto. Isto só aumenta a confusão do evento e provavelmente conduzirá a esforço desperdiçado ou ineficaz.
O único POC pode ou não ser a pessoa responsável pôr tratar o incidente. Há dois papéis distintos a serem preenchidos quando se está decidindo quem será POC e quem será a pessoa encarregada do incidente. A pessoa encarregada do incidente tomará decisões sobre a interpretação da política aplicada ao evento. Em contraste, o POC deve coordenar os esforços de todas as partes envolvidas no tratamento do evento.
O POC deve ser uma pessoa com perícia técnica para coordenar com sucesso os esforços dos gerentes de sistemas e usuários envolvidos na monitoração e reação ao ataque. Cuidado deveria ser tomado ao identificar quem será esta pessoa. Não deveria ser necessariamente a mesma pessoa que tem responsabilidade administrativa pelos sistemas comprometidos uma vez que freqüentemente tais administradores tem conhecimento suficiente apenas para o uso dos computadores no dia-a-dia, faltando-lhes conhecimento técnico mais profundo.
Outra função importante do POC é manter contato com as autoridades legais competentes e outras agências externas para assegurar que o envolvimento multi-agência. O nível de envolvimento será determinado através de decisões de administração bem como pôr restrições legais.
Um único POC também deveria ser a única pessoa encarregada de coletar evidências, desde que como regra geral, quanto mais pessoas tocam uma peça potencial de evidência, o maior a possibilidade de que esta seja inadmissível no tribunal. Para assegurar que as evidências serão aceitáveis para a comunidade legal, a coleta de evidências deve ser feita seguindo-se procedimentos predefinidos, de acordo com leis locais e regulamentos legais.
Um das tarefas mais críticas para o POC é a coordenação de todos os processos pertinentes. Responsabilidades podem ser distribuídas sobre o site inteiro, envolvendo múltiplos departamentos ou grupos independentes. Isto irá requerer um esforço bem coordenado para alcançar sucesso global. A situação fica ainda mais complexa se múltiplos sites estão envolvidos. Quando isto acontece, raramente um único POC num site poderá coordenar o tratamento do incidente inteiro adequadamente. Ao invés disso, deveriam ser envolvidos grupos apropriados de resposta a incidentes.
O processo de tratamento de incidentes deveria prover alguns mecanismos de ampliação. Para definir tal mecanismo, os sites precisarão criar um esquema de classificação interno para incidentes. Associado a cada nível de incidente estarão o POC e procedimentos apropriados. Conforme um incidente aumenta, pode haver uma mudança do POC que precisará ser comunicada a todos os outros envolvidos no tratamento do incidente. Quando uma mudança no POC acontece, o POC antigo deve fazer um resumo para o POC novo sobre toda a informação background.

Finalmente, usuários têm que saber informar incidentes suspeitos. Os sites devem estabelecer procedimentos de informe que irão funcionar durante e fora de horas de trabalho normais. "Help desks" freqüentemente são usadas para receber estes relatórios durante horas de trabalho normais, enquanto beepers e telefones podem ser usados fora de hora.

5.2.2 Agências de Investigação e de Execução da Lei

No caso de um incidente que tem conseqüências legais, é importante estabelecer contato com agências investigativas (pôr exemplo, o FBI e Serviço Secreto nos E.U.A.) o mais cedo possível. As autoridades locais, escritórios de segurança locais, e departamento policial do campus também deveriam ser informados conforme apropriado. Esta seção descreve muitos dos assuntos que serão confrontados, mas é reconhecido que cada organização terá suas próprias leis e regulamentos locais e do governo que terão impacto sobre como eles interagem com a execução da lei e agências investigativas. O ponto mais importante é que cada site precisa trabalhar estes assuntos.

Uma razão primária pôr determinar estes pontos de contato com antecedência, antes de um incidente é que uma vez que um ataque maior está em progresso, há pouco tempo para chamar estas agências para determinar exatamente quem é o ponto de contato correto. Outra razão é que é importante cooperar com estas agências de maneira a nutrir uma boa relação de trabalho, e a estar de acordo com os procedimentos de trabalho destas agências. Conhecer os procedimentos de funcionamento com antecedência, e as expectativas de seu ponto de contato é um grande passo nesta direção. Pôr exemplo, é importante juntar evidências que serão admissíveis em qualquer procedimento legal subseqüente, e isto requer conhecimento anterior de como juntar tal evidência. Uma razão final para estabelecer contatos o mais cedo possível é que é impossível conhecer que agência em particular assumirá a jurisdição em um dado incidente. Fazer contatos e achar os canais apropriados cedo farão a resposta a um incidente transcorrer consideravelmente mais suavemente.

Se sua organização ou site tem um conselho legal, você precisa notificar esta entidade logo em seguida que você perceber que um incidente está ocorrendo. No mínimo, seu conselho legal precisa estar envolvido para proteger os interesses legais e financeiros de seu site ou organização. Existem muitos assuntos legais e práticos, alguns deles sendo:

(1) Se seu site ou organização está disposta a arriscar publicidade ou exposição negativa para cooperar com esforços de prossecução legais.

(2) Obrigação "downstream"-se você deixa um sistema comprometido como está para poder ser monitorado e outro computador é danificado porque o ataque se originou de seu sistema, seu site ou organização pode ser responsável pôr danos incorridos.

(3) Distribuição de informação--se seu site ou organização distribui informações sobre um ataque no qual outro site ou organização pode ser envolvida ou a vulnerabilidade dm um produto isso pode afetar a habilidade de comercializar aquele produto, seu site ou organização pode ser novamente responsabilizado pôr qualquer dano (incluindo dano de reputação).

(4) Obrigações devido a monitoração--seu site ou organização pode ser processada se usuários em seu site ou em outro lugar descobrem que seu site está monitorando atividades das contas sem informar os usuários.

Infelizmente, não há ainda nenhum precedente claro nas obrigações ou responsabilidades de organizações envolvidas em um incidente de segurança ou quem poderia ser envolvido no apoio a um esforço investigativo. Investigadores encorajarão freqüentemente organizações para ajudar a rastrear e monitorar intrusos. Realmente, a maioria dos investigadores não pode procurar intrusões de computador sem apoio extenso das organizações envolvidas. Porém, investigadores não podem prover proteção contra reivindicações de obrigação, e estes tipos de esforços podem se arrastar pôr meses e tomar muito esforço.

Pôr outro lado, o conselho legal de uma organização pode aconselhar precaução extrema e sugerir que atividades de rastreamento sejam detidas e um intruso mantido fora do sistema. Isto, em si mesmo, pode não prover proteção de responsabilidades, e pode impedir os investigadores de identificar o perpetrador.

O equilíbrio entre apoiar atividade investigativa e limitar obrigação é enganador. Você precisará considerar as sugestões de seu conselho legal e o dano que o intruso está causando (se algum) ao tomar sua decisão sobre o que fazer durante qualquer incidente em particular.
Seu conselho legal também deveria ser envolvido em qualquer decisão para contactar agências investigativas quando um incidente acontece em seu site. A decisão para coordenar esforços com agências investigativas é de seu site ou organização. Envolver seu conselho legal também nutrirá a coordenação multi-nível entre seu site e a agência investigativa envolvida, o que resulta em uma divisão eficiente de trabalho. Outro resultado é que é provável que você obtenha direcionamento que o ajudará a evitar futuros enganos legais.
Finalmente, sua conselho legal deveria avaliar o procedimentos escritos de seu site para responder a incidentes. É essencial obter uma aprovação de uma perspectiva legal antes que você de fato leve a cabo estes procedimentos.
É vital, quando lidando com agências investigativas, verificar que a pessoa que chama pedindo informação é uma representante legítima da agência em questão. Infelizmente, muitas pessoas bem intencionadas têm vazado detalhes sensíveis sobre incidentes sem perceber, permitido pessoas sem autorização nos sistemas, etc., porque um visitante disfarçou-se como representante de uma agência governamental. (Nota: esta palavra de precaução na verdade se aplica a todos os contatos externos.)
Uma consideração semelhante envolve usar meios seguros de comunicação. Porque muitos atacantes de rede podem desviar correio eletrônico facilmente, evite usar correio eletrônico para comunicar-se com outras agências (como bem com outros lidando com o incidente em questão). Linhas telefônicas inseguras (os telefones normalmente usados no mundo empresarial) também são alvos freqüentes para escutas pôr intrusos de rede, logo tenha cuidado!
Não há um conjunto estabelecido de regras para responder a um incidente quando o governo local é envolvido. Normalmente (nos E.U.A.), exceto através de ordem legal, nenhuma agência pode o forçá-lo a monitorar, desconectar da rede, evitar contato de telefone com os atacantes suspeitos, etc. Cada organização terá um conjunto de leis e regulamentos locais e nacionais aos quais devem ser aderidos quando do tratamento de incidentes. É recomendado que cada site esteja familiarizado com essas leis e regulamentos, e identifique e conheça os contatos para agências com jurisdição com antecedência do tratamento de um incidente.

5.2.3 Grupos de Tratamento de Incidentes de Segurança de Computadores

Há atualmente vários Grupos de Resposta a Incidentes de Segurança (CSIRTs) como o CERT Coordination Center, o DFN-CERT alemão, e outros ao redor do globo. Esses grupos existem para muitas agências governamentais importantes e corporações grandes. Se um desses grupos está disponível, notificá-lo deveria ser de consideração primária durante as fases iniciais de um incidente. Estes times são responsáveis pôr coordenar incidentes de segurança de computador numa série de sites e entidades maiores. Até mesmo acreditando-se que o incidente está contido dentro de um único site, é possível que a informação disponível pôr um grupo de resposta possa ajudar a solucionar o incidente completamente.
Se é determinado que a brecha aconteceu devido a uma falha no hardware do sistema ou software, o vendedor (ou provedor) e um Grupos de Tratamento de Incidentes de Segurança de Computadores deve ser notificado tão logo possível. Isto é especialmente importante porque muitos outros sistemas são vulneráveis, e este vendedor e grupos de resposta podem ajudar a disseminar ajuda para outros locais afetados.
Ao montar uma política de site para tratamento de incidente, pode ser desejável criar um subgrupo, semelhante aos que já existem, que será responsável pôr tratar de incidentes de segurança para o site (ou organização). Se tal grupo é criado, é essencial que linhas de comunicação sejam abertas entre este grupo e outros. Uma vez que um incidente ocorre, é difícil abrir um diálogo confiante entres grupos, se não havia nenhum antes.

5.2.4 Sites Afetados e Envolvidos

Se um incidente tem um impacto em outros sites, informá-los é uma boa prática. Pode ser óbvio desde o princípio que o incidente não é limitado para o site local, ou isso pode só emergir depois de análise adicional.
Cada site pode escolher contatar outros sites diretamente ou passar a informação para um grupo de resposta a incidentes apropriado. É freqüentemente difícil de achar o POC responsável pôr sites distantes e o grupo de resposta poderá facilitar esse contato fazendo uso de já canais estabelecidos.
As questões legais e de obrigação que surgem de um incidente de segurança diferirá de site para site. É importante definir uma política para o compartilhando e logging de informação sobre outros sites antes que um incidente aconteça.
Informação sobre pessoas específicas é especialmente sensível, e pode estar sujeito a leis de privacidade. Para evitar problemas nesta área, deveria ser apagada informação irrelevante e uma declaração de como tratar a informação restante deveria ser incluída. Uma declaração clara de como esta informação será usada é essencial. Ninguém que informa um site sobre um incidente de segurança quer ler sobre isto na imprensa pública. Grupos de resposta a incidentes são valiosos neste sentido. Quando eles passam informações para POCs responsáveis, eles podem proteger o anonimato da fonte original. Mas, esteja atento que, em muitos casos, a análise de logs e informações em outros sites vai revelar endereços de seu site .
Os problemas discutidos acima não deveriam ser considerados razões para não envolver outros sites. De fato, as experiências de grupos existentes revelam que a maioria dos sites informados sobre problemas de segurança nem mesmo haviam notado que seu site havia sido comprometido. Sem serem informados a tempo, outros sites estão freqüentemente impossibilitados entrar em ação contra intrusos.

5.2.5 Comunicações internas

É crucial durante um incidente grande, comunicar porque certas ações estão sendo tomadas, e como se espera que os usuários (ou departamentos) se comportem. Em particular, deveria ser deixado muito claro para os usuários o que lhes é permitido dizer (e não dizer) para o mundo externo (incluindo outros departamentos). Pôr exemplo, não seria bom para uma organização se os usuários respondessem aos clientes com algo como, " Eu lamento, os sistemas estão fora do ar, nós tivemos um intruso e nós estamos tentando esclarecer as coisas". Seria muito melhor se ensinassem que eles respondessem com uma declaração preparada como, " Lamento, nossos sistemas não estão disponíveis, eles estão sendo em manutenção para melhor servi-lo no futuro".
Comunicações com os clientes e sócios contratuais devem ser dirigidos de modo sensato, mas também sensível. Uma pessoa pode se preparar para os assuntos principais preparando um cheklist. Quando um incidente acontece, a lista pode ser usada com a adição de uma frase ou duas sobre as circunstâncias específicas do incidente.
Departamentos de relações públicos podem ser muito úteis durante incidentes. Eles deveriam ser envolvidos em todo o planejamento e podem prover respostas bem construídas para uso quando contato de fora dos departamentos e organizações são necessários.

5.2.6 Relações públicas - "Press Releases"

Houve um tremendo crescimento na cobertura de mídia dedicada a incidentes de segurança de computador nos Estados Unidos. Tal cobertura de imprensa está fadada a se estender a outros países, como a Internet continua crescendo e se expandindo internacionalmente. Leitores de países onde tal atenção da mídia ainda não aconteceu, podem aprender com as experiências dos E.U.A. e deveriam ser avisados e preparado.

Um dos assuntos mais importantes a considerar é quando, quem, e quanto liberar ao público em geral pela imprensa. Há muitos assuntos para considerar quando decidindo este ponto em particular. Primeiro e antes de mais nada, se um escritório de relações públicas existe para o site é importante usar este escritório como ligação para a imprensa. O escritório de relações públicas é treinado no tipo e formulação de informação a serem liberadas, e ajudará a assegurar que a imagem do site é protegida durante e depois do incidente (se possível). Um escritório de relações públicas tem a vantagem de que você pode se comunicar francamente com eles, e provê um pára-choque entre a atenção de imprensa constante e a necessidade do POC para manter controle sobre o incidente.
Se um escritório de relações públicas não está disponível, a informação, lançado à imprensa deve ser considerada cuidadosamente. Se a informação é sensível, pode ser vantajoso só prover mínima informação para a imprensa. É bastante possível que qualquer informação provida à imprensa será vista depressa pelo perpetrador do incidente. Também note que enganar a imprensa pode sair pela culatra freqüentemente e pode causar mais dano que liberar informações delicadas.
Enquanto é difícil de determinar com antecedência que nível de detalhe prover à imprensa, algumas diretrizes para serem lembradas são:

(1) mantenha o nível de detalhes técnicos baixo. Informação detalhada sobre o incidente pode prover bastante informação para outros lançarem ataques semelhantes em outros sites, ou até mesmo danificar habilidade do site para processar a parte culpada uma vez que o evento terminou.
(2) Mantenha a especulação fora de declarações de imprensa. Especulação sobre quem está causando o incidente ou os motivos, está muito sujeita a erros e pode causar uma visão inflamada do incidente.
(3) Trabalhe com profissionais da lei para assegurar que a evidência é protegida. Se prossecução for envolvida, assegurar que a evidência coletada não é divulgada à imprensa.
(4) Tente não ser forçado a uma entrevista de imprensa antes de você estar preparado. A imprensa popular é famosa pela "entrevista das 2 das manhã", onde a esperança é pegar o entrevistado desprevenido e obter informação não disponível em outras circunstâncias.
(5) Não permita que a atenção de imprensa diminua o tratamento do evento. Sempre se lembre que o fechamento com sucesso de um incidente é de importância fundamental.

5.3 Identificando um Incidente

5.3.1 É Real ?

Esta fase envolve determinar se um problema realmente existe. Naturalmente muitos, se não a maioria, dos sinais associados freqüentemente com infeção de vírus, intrusões de sistema, usuários maliciosos, etc., simplesmente são anomalias tal como falhas de hardware ou comportamento de suspeito de sistema/usuário. Para ajudar a identificar se realmente há um incidente, é normalmente útil obter e usar qualquer software de detecção que possa estar disponível. Informação de auditoria também é extremamente útil, especialmente para determinar se há um ataque a rede. É extremamente importante obter um retrato instantâneo do sistema assim que se suspeite que algo está errado. Muitos incidentes levam uma cadeia dinâmica de eventos a acontecer, e um retrato instantâneo do sistema inicial pode ser a mais valiosa ferramenta para identificar o problema e qualquer fonte de ataque. Finalmente, é importante começar um livro de log. Gravar eventos de sistemas , conversas de telefone, timestamps, etc., pode conduzir a uma identificação mais rápida e sistemática do problema, e é a base para fases subseqüentes de tratamento de incidente.
Há certas indicações ou " sintomas " de um incidente que merecem atenção especial:

(1) *Crashes* de sistemas.
(2) Novas contas de usuário (a conta RUMPLESTILTSKIN foi criada inesperadamente), ou atividade alta em uma conta previamente pouco usada.
(3) arquivos novos (normalmente com nomes de arquivo estranhos, como data.xx ou k ou .xx).

(4) discrepância de contabilidade (em um sistema de UNIX pode você notar a diminuição de um arquivo de contabilidade chamado /usr/admin/lastlog, algo que o deveria muito desconfiado de que pode haver um intruso).
(5) mudanças em tamanho ou data de arquivo (um usuário deveria desconfiar se .arquivos EXE em um computador MS-DOS tenha inexplicavelmente aumentado mais de 1800 bytes).
(6) Tentativas de escrever em system (um gerente de sistema nota que um usuário privilegiado em um sistema de VMS está tentando alterar RIGHTSLIST.DAT).
(7) modificação de dados ou apagamento (arquivos começam a desaparecer).
(8) negação de serviço (gerente de sistema e todos os outros usuários são impedidos de entrar num sistema de UNIX, agora em modo de usuário único).
(9) desempenho de sistema inexplicavelmente, baixo
(10) anomalias (GOTCHA " é exibido no monitor ou há freqüentes e inexplicáveis "beeps ").
(11) sondas suspeitas (há numerosas tentativas de login sem sucesso de outro nodo).
(12) Browsing suspeito (alguém se torna um usuário root em um sistema UNIX e acessa arquivos arquivo após arquivo em contas de muitos usuário.)
(13) inabilidade de um usuário para se logar devido a modificações em sua conta.

De forma alguma esta lista é completa; nós listamos apenas um certo número de indicadores comuns. É melhor colaborar com outro pessoal técnico e de segurança de computador para tomar uma decisão como um grupo sobre se um incidente está acontecendo.

5.3.2 Tipos e Escopo de Incidentes

Junto com a identificação do incidente, está a avaliação do âmbito e impacto do problema. É importante identificar os limites do incidente corretamente para lidar efetivamente com ele e priorizar respostas.
Para identificar o escopo e impacto um conjunto de critérios deveria ser definido, o qual é apropriado para o site e para o tipo de conexões disponíveis. Alguns dos pontos incluem:

(1) é este um incidente multi-site?
(2) muitos computadores em seu site oram afetados pôr este incidente?
(3) há informação delicada envolvida?
(4) qual é o ponto de entrada do incidente (rede, linha telefônica , terminal local, etc.)?
(5) a imprensa está envolvida?
(6) qual é o dano potencial do incidente?
(7) qual é o tempo calculado para encerrar o incidente?
(8) que recursos poderiam ser exigidos para tratar o incidente?
(9) há autoridades legais envolvidas?

5.3.3 Avaliando Dano e Extensão

A análise do dano e extensão do incidente pode consumir muito tempo, mas deveria 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 deveriam ser considerado suspeitos. Software de sistema é o alvo mais provável. Preparação é chave para poder descobrir todas as mudanças num sistema possivelmente afetado. Isto inclui fazer checksum de todas os meios do vendedor usando um algoritmo que é resistente a falsificações. (Veja seções 4.3)
Assumindo que meios de distribuição originais do vendedor estão disponíveis, uma análise de todos os arquivos de sistemas deveria começar, e qualquer irregularidade deveria ser notada e deveria referida a todas as partes envolvidas no tratamento do incidente. Pode ser muito difícil, em alguns casos, decidir que meios de backup estão mostrando um estado de sistema correto. Considere, pôr exemplo que o incidente pode ter continuado pôr meses ou anos antes de descoberta, e o suspeito pode ser um empregado do site,

ou que tenha conhecimento íntimo ou acesso aos sistemas. Em todos os casos, a preparação antes do incidente determinará se a recuperação é possível.
Se o sistema suporta logs centralizados (a maioria o faz), volte para os logs e procure anormalidades. Se contabilidade de processo e tempo de conexão estiver habilitada, procure padrões de uso do sistema. Numa menor extensão, o uso do disco pode jogar luz no incidente. Contabilidade pode prover muita informação útil em uma análise de um incidente e prossecução subseqüente. Sua habilidade para verificar todos os aspectos de um incidente específico depende fortemente do sucesso desta análise.

5.4 Tratando um Incidente

São necessários certos passos durante o tratamento de um incidente. Em todas as atividades de segurança relacionadas, o mais importante ponto à ser feito é que todos os sites deveriam ter políticas no local.
Sem políticas e metas definidas, as atividades empreendidas permanecerão sem enfoque. As metas deveriam ser definidas com antecedência pela administração e com deliberação legal.
Um dos objetivos mais fundamentais é restabelecer controle dos sistemas afetados e limitar o impacto e dano. No pior caso, fechando o sistema, ou desconectando o sistema da rede, possa ser a única solução prática.
Como as atividades envolvidas são complexas, tente adquirir tanta ajuda quanto necessário. Enquanto tenta resolver o problema sozinho, danos reais podem acontecer devido a demoras ou a informações perdidas. A maioria administradores levam a descoberta de um intruso como um desafio pessoal.
Procedendo deste modo, outros objetivos como esboçou em suas políticas locais sempre podem não ser consideradas. Tentar pegar os intrusos pode ser uma prioridade muito baixa, se comparada a integridade do sistema, pôr exemplo. Monitorar a atividade de um hacker é útil, mas pode não sido considerado preço o risco para permitir o acesso continuado.

5.4.1 Tipos de Notificação e Troca de Informação

Quando você confirmou que um incidente está acontecendo, o pessoal apropriado deve ser notificado. Como esta notificação é passada é muito importante para manutenção do evento sob controle ambos pontos de vista, o técnico e o emocional. As circunstâncias devem ser descritas em tantos detalhes quanto possível para facilitar o pronto reconhecimento e entender o problema. Muito cuidado quando determinar para quais grupos técnicos a informação será enviada durante a notificação. Pôr exemplo, é útil passar este tipo de informação para um grupo de tratamento de incidentes pois eles podem lhe ajudar com sugestões úteis para erradicar as vulnerabilidades envolvidas em um incidente. Pôr outro lado, pondo o conhecimento crítico no domínio público (pôr exemplo, pôr newsgroups de USENET ou remetendo para listas) pode pôr um número grande de sistemas potencialmente a risco de intrusão. É nulo assumir que todos os administradores que lêem um newsgroup particular têm acesso ao código fonte do sistema operacional, ou podem entender o bastante para fazer os passos adequados.
Em primeiro lugar, qualquer notificação para local ou pessoal de fora do site deve ser explícito. Isto requer que qualquer declaração (seja isto uma mensagem de correio eletrônico, telefonema, fac-símile, beeper, ou semaphone) provendo informação sobre o incidente seja clara, concisa, e completamente qualificada. Quando você está notificando outros que o ajudarão a tratar um evento, uma "tela de fumaça" só dividirá o esforço e criará confusão. Se uma divisão de trabalho é sugerida, é útil prover informações para cada participante sobre o que está sendo realizado em outros esforços. Isto não só reduzirá duplicação de esforços, mas permite que as pessoas que trabalham em partes do problema possam saber onde obter informações pertinentes a parte deles no incidente.
Outra consideração importante quando comunicar sobre o incidente é ser efetivo. Tentar esconder aspectos do incidente provendo falsa ou incompleta informação não só podem evitar uma solução com sucesso para o incidente, mas pode até mesmo piorar a situação.

A escolha do idioma usado 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.
Outra consideração é que nem todas as pessoas falam o mesmo idioma.
Devido a este fato, podem surgir enganos e demora, especialmente se é um incidente multinacional. Em outras preocupações internacionais inclua a diferença nas implicações legais de um incidente de segurança e diferenças culturais. Porém, diferenças culturais não só existem entre países. Elas igualmente existem dentro de países, entre diferente grupos sociais ou de usuários. Pôr exemplo, administrador de um sistema universitário é muito relaxado sobre tentativas para conectar o sistema pôr telnet, mas é provável que o administrador de um sistema militar considere a mesma ação como um possível ataque.
Outro assunto associado com a escolha de idioma é a notificação de pessoas não técnicas ou de fora do site. É importante descrever o incidente com precisão sem gerar alarme impróprio ou confusão. Enquanto é mais difícil de descrever o incidente a uma conjunto de pessoas não-técnicas, é freqüentemente mais importante. Uma descrição não-técnica pode ser requerida pela administração de níveis superiores, a imprensa, ou instituições responsáveis pela execução de lei. A importância destas comunicações não pode ser menosprezada e pode fazer a diferença entre a solução do incidente corretamente ou eleva-lo a algum nível mais alto de dano.
Se um grupo de resposta a incidentes é envolvido, poderia ser necessário preencher um modelo para a troca de informação. Embora isto possa parecer ser um fardo adicional e possa somar uma certa demora, isto, ajuda o grupo para agir neste mínimo conjunto de informação. O grupo de resposta poderá responder a aspectos do incidente do qual o administrador local é desavisado. Se a informação é dada para uma pessoa de fora então, esta pessoa deveria ter um mínimo de informação contando o seguinte:

1. timezone de logs,... em GMT ou hora local
2. informação sobre o sistema remoto, inclusive nomes de host, endereços IP e (talvez) IDs de usuários
3. todas as entradas de log relevantes para o local distante
4. tipo de incidente (o que aconteceu, pôr que se você deveria se preocupar)

Se informações locais (i.e., IDs de usuários locais) são incluídas nas entradas de logs, será anteriormente necessário a **sanitize** as entradas para evitar assuntos de isolamento. Em geral, toda a informação que poderia ajudar um local distante solucionando um incidente deveria ser distribuídas, a menos que políticas locais proíbem isto.

5.4.2 Protegendo as Evidências e Logs de Atividade

Quando você responde a um incidente, documente todos os detalhes relacionados ao incidente. Isto proverá valiosa informação para você e outros como você tentando desvendar o curso dos eventos. Documentando todos os detalhes economizarão em última instância, seu tempo. Se você não documenta todos os telefonemas importantes, pôr exemplo, é provável que você esqueça uma porção significante de informação você obtém o que requer que você contacte a fonte de informação novamente. Ao mesmo tempo, detalhes armazenados proverão evidências para esforços de prossecução e proverão os movimentos naquela direção. A documentação de um incidente também lhe ajudarão a executar uma taxa final de dano (alguém da administração, como também instituições de execução de lei, poderão querer saber), e proverá a base para mais recentes fases do processo de tratamento de incidentes:
erradicação, recuperação, e seqüência, "lições aprendidas".
Durante as fases iniciais de um incidente, é freqüentemente imprevisível determinar se a prossecução é viável, assim você deveria documentar como se você pois está juntando evidências para um caso de tribunal. Um mínimo, você deverá registrar:

todos os eventos de sistemas (registros de auditoria)
todas as ações que você fez (tempo usado)

todas as conversações externas (inclusive a pessoa com quem você falou, a data e tempo, e o conteúdo da conversação)

O modo mais direto para manter documentação é mantendo um livro de log. Isto lhe permite ter uma centralizada e cronológica fonte de informação quando você precisar disto, em vez do requerer, chame pôr folhas individuais de papel. Muitas destas informações são evidências potenciais em um tribunal de lei. Assim, quando um procedimento legal é uma possibilidade, a pessoa deveria seguir os procedimentos preparados e evitar pôr em perigo o procedimento legal pôr manipulação imprópria de possível evidência. Se apropriado, os passos seguintes podem ser levados.

1. regularmente (pôr exemplo, diariamente) fazer cópias assinadas de seu logbook (como também mídias que você usa para registrar eventos de sistemas) para um administrador de documentos.
2. administrador deveria armazenar estas páginas copiadas em um seguro lugar (pôr exemplo, uma caixa forte).
3. quando você submete informação para armazenamento, você deve receba um recibo datado e assinado pelo administrador do documento.

Fracasso para observar estes procedimentos pode resultar em invalidação de qualquer evidência que você obtém em um tribunal de lei.

5.4.3 Retenção

O propósito de retenção é limitar a extensão de um ataque. Uma parte essencial de retenção é decisão do que fazer (pôr exemplo, determinando desligar um sistema, desconectar da rede, monitorar sistemas ou atividades de rede, set traps, incapacitar funções como transferência de arquivo remotoss, etc.).

Às vezes esta decisão é trivial; desligar o sistema se a informação é secreta, importante, ou proprietária. Tenha em mente que isso remove todo o acesso enquanto um incidente está em progresso, obviamente notifique todos os usuários, inclusive os usuários que alegaram problemas, que os administradores estão atentos ao problema; isto pode ter um efeito danoso uma investigação. Em alguns casos, é prudente remover todo o acesso ou funcionalidade o mais cedo possível, então restabeleça operação normal em fases limitadas. Em outros casos, vale a pena arriscar algum dano para o sistema, se manter o sistema poderiam habilitar você à identificar o intruso.

Esta fase deveria se desenvolver levando a cabo procedimentos predeterminados.

Sua organização ou site devem, pôr exemplo, definir riscos aceitável lidando com um incidente, e deveria prescrever ações específicas e estratégias adequadas. Isto é especialmente importante quando uma decisão rápida é necessária e não é possível contactar todas as partes envolvidas primeiro para discutir a decisão. Na ausência de procedimentos predefinidos, a pessoa no cargo do incidente não terá freqüentemente o poder para tomar decisões de administração difíceis (como perder os resultados de uma experiência cara desligando um sistema). Uma atividade final que deveria acontecer durante esta fase de tratamento do incidente é a notificação de autoridades apropriadas.

5.4.4 Erradicação

Uma vez que o incidente foi contido, é tempo para erradicar a causa. Mas antes de erradicar a causa, deveria ser tomado grande cuidado colecionar todas as informações necessárias sobre os sistemas comprometidos e a causa do incidente como elas serão provavelmente serão perdidas quando o sistema for limpo.

Softwares podem estar disponíveis para ajudar no processo de erradicação, como software de anti-vírus. Se qualquer falso arquivos foram criados, devem ser apagados. No caso de infeções de vírus, é importante limpar e reformatar qualquer mídia que contém arquivos infetados. Finalmente, assegura que todos os backups estão limpos. Muitos sistemas infetados com vírus ficam periodicamente ré-infetados

simplesmente porque as pessoas não erradicam o vírus do backup. Depois de erradicação, deveria ser feito um novo backup.
Removendo todas as vulnerabilidades uma vez um incidente aconteceu é difícil. A chave para remover vulnerabilidades é conhecimento e entendimento da brecha.
Pode ser necessário voltar para as mídia de distribuição originais e ré-customizar o sistema. Para facilitar esta situação de pior caso, um registro do setup do sistema original e de cada mudança de customização deveria ser mantido. No caso de um ataque baseado na rede, é importante instalar remendos para cada vulnerabilidade de sistema operacional que foi explorado.
Como discutido na seção 5.4.2, um log de segurança pode ser muito valioso durante esta fase de remover vulnerabilidade. Os logs que mostram como o incidente foi descoberto e foi contido pode ser usado para ajudar depois a determinar qual a extensão do dano de um determinado incidente. O passos podem ser usados no futuro para ter certeza que o problema não irá ocorrer. Idealmente, a pessoa deveria automatizar e regularmente deveria aplicar o mesmo teste como foi usado para descobrir o incidente de segurança.
Se uma vulnerabilidade particular é isolada como explorada, o próximo passo é achar um mecanismo para proteger seu sistema. A segurança que remete listas e boletins seria um lugar bom para procurar esta informação, e você pode obter conselhos dos grupos de resposta a incidentes.

5.4.5 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 e com um mínimo de inconveniência aos usuário é a melhor prática. Entenda que os procedimentos de recuperação formais para o sistema é extremamente importante e deveria ser específico para o site.

5.4.6 Prosseguimento

Uma vez que você acredita que o sistema foi restabelecido a um " estado seguro ", ainda é possível que buracos, e até mesmo armadilhas, podem estar espreitando o sistema. Uma das fases mais importantes de respostas a incidentes também é freqüentemente omitida, a fase de seguimento. Na fase de seguimento, o sistema deveria ser monitorado com vistas à aspectos que podem ter sido perdidos durante a fase de cleanup. Seria prudente utilizar, como um começo, algumas das ferramentas de gerenciamento.
Lembre-se, estas ferramentas não substituem uma monitoração continuada do sistema e boas práticas de administração de sistemas.
O elemento mais importante da fase de seguimento é executar uma análise de pós morte. Exatamente o que aconteceu, e quanto tempo? Como foi a performance do pessoal envolvido com o incidente? Que tipo de informação foi necessária rapidamente para o pessoal, e como eles adquirir aquela informação o mais cedo possível? O que faria o pessoal diferentemente da próxima vez?
Após um incidente, é prudente escrever um relatório que descreve a sucessão exata de eventos: o método de descoberta, procedimento de correção, procedimento de monitoração, e um resumo da lição aprendida.
Isto ajudará na compreensão clara do problema. Criando uma cronologia formal de eventos (inclusive time stamps) também é importante pôr razões legais.
Um relatório de seguimento é valioso pôr muitas razões. Provê uma referências a serem usadas no caso de outros incidentes semelhantes. Também é importante para que, tão depressa quanto possível obtenha-se uma estimativa da quantia monetária dos danos que o incidente causou. Esta estimativa deve incluir custos associados com qualquer perda de software e arquivos(especialmente o valor de dados proprietário que podem ter sido descoberto), dano de hardware, e força de trabalho usada para restabelecer arquivos alterados, reconfigure sistemas afetados, e assim sucessivamente. Esta estimativa pode se tornar a base

para atividade de prossecução subseqüente. O relatório também pode ajudar justifique o esforço de segurança dos computadores de uma organização para administração.

5.5 Resultado de um Incidente

Após um incidente, deveriam acontecer várias ações. Estas ações podem ser resumidas nas seguintes:

1. um inventário deveria ser feito dos recursos dos sistemas,(i.e., um exame cuidadoso deveria determinar como o sistema foi afetado pelo incidente).
2. as lições aprendidas como resultado do incidente deveria ser incluído em plano de segurança revisado para impedir o incidente de re-acontecer.
3. uma análise de risco nova deveria ser desenvolvida levando em conta o incidente.
4. uma investigação e prossecução dos indivíduos que causaram o incidente deveria começar, se é julgado desejável.

Se um incidente está baseado em política pobre, e a menos que a política seja mudada, você então é sentenciado repetir o passado. Uma vez que um site se recuperou de um incidente deveriam ser revisadas a política do site e os procedimentos para cercar mudanças para prevenir incidentes semelhantes. Até mesmo sem um incidente, seria prudente revisar políticas e procedimentos com uma base regular. Revisões são imperativas devido aos ambientes de computação variáveis de hoje.

O propósito inteiro deste processo de pós morte é melhorar toda a segurança para proteger o site contra ataques futuros. Como resultado de um incidente, um site ou organização ganhar conhecimento prático da experiência. Uma meta concreta do pós morte é desenvolver novos métodos de proactive. Outra faceta importante do resultado pode ser a educação do usuário final e administrador para prevenir a nova ocorrência do problema de segurança.

5.6 Responsabilidades

5.6.1 Não cruzando a Linha

Uma coisa é proteger a sua própria rede, mas outra é assumir que deve proteger outras redes. Durante o tratamento de um incidente, certas vulnerabilidade dos próprios sistemas e os sistemas de outros ficam aparentes. É bastante fácil e pode ser tentador rastrear os intrusos para localizá-los. Tenha em mente que em certo momento é possível cruzar a linha e, com a melhor das intenções, comportar-se não melhor do que o intruso.

A melhor regra a seguir é não usar facilidades de sistemas remotos que não sejam públicas. Isto claramente exclui qualquer entrada em um sistema (usando um shell ou login remoto) que não seja explicitamente permitido. Isto pode ser muito tentador depois que uma brecha de segurança é descoberta; um administrador de sistema pode ter os meios para, averiguar que danos podem ter sido feitos ao site remoto. Não faça! Ao invés, tente buscar o contato apropriado para o site afetado.

5.6.2 Política de boa vizinhança na Internet

Durante um incidente de segurança há duas escolhas que a pessoa pode fazer. Primeiro, um site pode escolher observar o intruso na expectativa de pega0lo; ou, o site pode limpar o sistema depois do incidente e manter o intruso fora dos sistemas. Esta é uma decisão que deve ser tomada com muito cuidado, pois poderá haver conseqüências legais se você optar pôr deixar seu site aberto sabendo que um intruso está usando-o como um ponto de lançamento para atacar outros sites. Sendo um "bom vizinho" na Internet você deveria tentar alertar outros sites que podem ter sidos impactados pelo intruso. Estes locais afetados podem ser detectados após uma revisão completa de seus arquivos de log.

5.6.2 Resposta administrativa para Incidentes

Quando um incidente de segurança envolve um usuário, a política de segurança do site deveria descrever que ação será tomada. A transgressão deve ser levada a sério, mas é muito importante estar seguro sobre o papel do usuário. O usuário era ingênuo? Poderia haver um engano atribuindo a quebra de segurança ao usuário? Aplicar alguma penalidade administrativa assume que o usuário intencionalmente causou o incidente e isto pode não ser apropriado para um usuário que simplesmente cometeu um engano. Pode ser apropriado prever sanções adequadas a cada situação em sua política (pôr exemplo, educação ou repreensão a um usuário) além para medidas mais duras para atos intencionais de intrusão e abuso do sistema.

6. Atividades em andamento

Neste momento, seu site esperançosamente desenvolveu uma política completa de segurança bem como os procedimentos para assistir na configuração e gerenciamento da sua tecnologia no suporte destas políticas. Como seria bom se você pudesse sentar e relaxar neste momento já que você concluiu com o trabalho de segurança. Infelizmente isto não é possível. Os seus sistemas e redes não são um ambiente estático, então você terá que rever suas políticas e procedimentos nos seus fundamentos. Há um número de passos que você pode seguir para ajuda-lo a manter as mudanças sob controle de forma a poder tomar as ações correspondentes. A seguir é apresentado um conjunto inicial de passos ao qual você pode adicionar outros de forma a ajustá-lo ao seu site.

(1) Assine as publicações que são editadas pôr vários times de resposta a incidentes de segurança, como os Centros de Coordenação CERT, e atualize os seus sistemas contra as ameaças que se aplicam à tecnologia do seu site.

(2) Mantenha-se atualizado sobre os patches produzidos pêlos vendedores do seu equipamento e obtenha e instale os que se aplicam ao seu sistema.

(3) Mantenha sob vigilância as configurações do seu sistema para identificar qualquer mudança que possa ter ocorrido e investigar anomalias.

(4) Revise todas as políticas de segurança e procedimentos anualmente (no mínimo).

(5) Leia os mailing lists relevantes e USENET newsgroups para manter-se atualizado das últimas informações compartilhadas pêlos colegas de classe.

(6) Verifique regularmente pôr políticas e procedimentos complacentes. Esta auditoria deve ser feita preferencialmente pôr alguém que não tenha participado da definição ou implementação destas políticas ou procedimentos.