**Segurança da Rede**

O conceito de segurança dentro do ambiente de rede inclui todos os aspectos de sistemas operacionais, pacotes de software, hardware e configurações de rede, além de qualquer conectividade de compartilhamento de rede.

Este não é o único escopo da segurança. Como profissional, você verá que, no mundo de hoje, a segurança física também está ligada à segurança de TI. As câmeras de segurança precisam de endereço IP e espaço para armazenara s gravações, planos de recuperação de desastre agora precisam abranger a entidade de negócios inteira, e não apenas o departamento de TI, e o acesso físico a áreas não autorizadas pode ser desastroso para uma empresa.

Princípios de Segurança

O mundo moderno dos computadores é uma mistura complexa de diferentes componentes com a finalidade de tornar recursos disponíveis para os que precisam deles. Infelizmente, durante a última década, o acesso à s redes por usuários não autorizados cresceu numa velocidade que supera qualquer coisa que poderíamos ter imaginado. Reagimos rapidamente, desenvolvendo e implantando hardware e software para atender às demandas dos consumidores profissionais e domésticos, mas deixamos de testar e proteger corretamente essas tecnologias. Isso coloca nossas redes em risco, não apenas pelo hacker profissional, mas também os funcionários curiosos ou descontentes.

A segurança não é apenas uma diretiva ou um plano, mas uma atitude mental. Você precisa treinar corretamente e incentivar os funcionários para que fiquem atentos à segurança. Lembre-se de que sua rede é tão forte quanto seu elo mais fraco, que normalmente é um ser humano, um conceito que discutiremos melhor na seção "Engenharia social", mais adiante neste capítulo. Você também terá que ficar atualizado com as ameaças e reparos disponíveis para garantir que servidores e estações de trabalho sejam protegidos corretamente. Aprender a implementar a criptografia sobre dados confidenciais fará parte do seu trabalho.

A recuperação de desastre e planos de resposta à ocorrência precisam ser testados e atualizados regularmente. Tudo isso começa com um planejamento apropriado.

Ameaças

Um Profissional de TI tem a responsabilidade de garantir que a rede esteja segura e protegida contra-ataques --- uma grande tarefa. Uma ameaça é qualquer coisa que coloque em perigo a segurança da rede. As ameaças vêm em todas as formas e tamanhos. A avaliação das ameaças precisa começar quando se configura o servidor. A maioria dos servidores vem com uma grande variedade de serviços e protocolos, muitos deles ativados como padrão. Isso os deixa abertos a acesso não autorizado ou ameaças, especialmente se você não estiver ciente de que esses serviços estão rodando. Outra área de preocupação com relação a ameaças é o uso de um servidor Web público. Aplicações mal escritas deixam os computadores abertos a estouros de buffer. (Discutiremos sobre estouros de buffer mais adiante nesta seção.) O software malicioso (malware), ou vírus, impõe uma ameaça aos servidores de correio e podem se espalhar com extrema velocidade. Os humanos impõem provavelmente a maior ameaça a uma rede, pois seu comportamento não pode ser facilmente controlado.

Como você pode ver, as ameaças são uma parte da vida diária de um administrador de rede. Como você não pode tornar um ambiente completamente à prova de ameaças, é preciso estar constantemente atento para garantir que sua rede esteja o mais segura possível. O primeiro passo para a segurança completa é estabelecer uma politica de segurança.

Aspectos da Política de Segurança

Para garantir que as ameaças sejam gerenciadas e mantidas corretamente, é importante estabelecer políticas de segurança claras e detalhadas que são incentivadas pela gerência de uma organização e praticadas por seus usuários. As políticas que não possuem suporte da gerência podem ser impraticáveis, e aquelas que os usuários não têm conhecimento são ineficazes. Os detalhes do planejamento da política de segurança são muito extensos, e depois que a política estiver pronta, ela precisa ser testada e atualizada regularmente.

Desde o ataque de 11 de setembro de 2001 nos EUA, mais empresas estão levando a segurança a sério e tomando medidas para implementar um plano eficaz. Parte do problema com a obtenção de fundos e preparação de políticas de segurança é que o retorno do investimento pode ser difícil de se calcular, e esse tipo de despesa não gera receita. Às vezes, é difícil para uma empresa ser proativa em vez de reativa tratando-se de segurança. Muitas empresas utilizam a técnica de enfrentar o problema quando ocorrer alguma situação.

Os usuários precisam estar cientes das políticas de segurança e expectativas para minimizar os pontos fracos em potencial na segurança.