

Práticas de Segurança para Administradores de Redes Internet

Checklist

NIC BR Security Office
nbso@nic.br

Versão 1.0.1
17 de julho de 2002

Este *checklist* resume as principais recomendações contidas no documento intitulado “Práticas de Segurança para Administradores de Redes Internet”, um guia com informações para configurar, administrar e operar redes ligadas à Internet de forma mais segura. O documento original pode ser obtido em <http://www.nic.br/docs/seg-adm-redes.html>.

1 Políticas

- elaboração de uma política de segurança, com apoio da administração da organização;
- divulgação da política de segurança entre os usuários da rede;
- elaboração e divulgação de uma política de uso aceitável (AUP).

2 Instalação e Configuração Segura de Sistemas

1. Antes da instalação:

- planejamento dos propósitos e serviços do sistema;
- definição do particionamento do disco;
- provisão de mídias e documentação necessárias à instalação.

2. Durante a instalação:

- escolha de uma senha forte para o administrador;
- instalação do mínimo de pacotes, com o sistema fora da rede;
- documentação da instalação no *logbook*.

3. Após a instalação:

- desativação de serviços instalados e não utilizados;
- instalação de correções de segurança;
- configuração do servidor SMTP, fechando o *relay*;

- configuração do *proxy* Web, ajustando os controles de acesso.

4. Antes de conectar o sistema em rede:

- verificação das portas TCP/UDP abertas, usando um comando como o *netstat*;
- ajuste nas regras de *firewall* apropriadas, para liberar o tráfego para o novo sistema.

Alguns *checklists* mais específicos para determinados sistemas operacionais podem ser encontrados em <http://www.sans.org/SCORE/>.

3 Administração e Operação Segura de Redes e Sistemas

1. Ajuste do relógio:

- instalação e configuração de um servidor local de tempo (por exemplo, NTP);
- sincronização dos relógios dos sistemas da rede com o relógio do servidor local de tempo;
- ajuste do *timezone* dos sistemas.

2. Equipes de administradores:

- criação de listas de discussão para a comunicação entre os administradores de redes e sistemas da organização;
- estabelecimento de procedimentos e/ou instalação de ferramentas para controle de alterações na configuração dos sistemas;
- estabelecimento de procedimentos e/ou instalação de ferramentas que permitam um controle sobre a utilização de contas privilegiadas (*root* e *Administrator*).

3. *Logs*:

- habilitação do *logging* em sistemas e serviços;
- estabelecimento de um procedimento de armazenamento de *logs*;
- instalação e configuração de um *loghost* centralizado;
- estabelecimento de um procedimento de monitoramento de *logs*;
- instalação de ferramentas de monitoramento automatizado de *logs*.

4. DNS reverso:

- configuração do DNS reverso para todas as *hosts* da rede.

5. Informações de contato:

- implementação dos *emails* abuse e security;
- atualização do contato de SOA no DNS;
- atualização dos contatos (especialmente o técnico) no WHOIS.

6. Eliminação de protocolos sem criptografia:

- substituição de Telnet/FTP/rlogin/rsh/rexec por SSH;
- substituição de POP3 e IMAP sem criptografia por soluções de *email* com criptografia (POP3 ou IMAP sobre SSL, Webmail sobre HTTPS).

7. Cuidados com redes reservadas:

- filtragem dos endereços pertencentes a redes reservadas;
- configuração de tabelas de *hosts* e/ou servidores DNS privados quando são utilizados internamente endereços de redes reservadas.

8. Políticas de *backup* e restauração de sistemas:

- definição da periodicidade dos *backups*;
- definição dos dados que devem ser copiados;
- escolha de um local adequado para o armazenamento dos *backups*;
- estabelecimento de um procedimento de verificação de *backups*;
- estabelecimento de um procedimento para a restauração de sistemas a partir do *backup*.

9. Como manter-se informado:

- inscrição nas listas de anúncios de segurança dos fornecedores de *software* e/ou *hardware*;
- inscrição nas listas de administradores e/ou usuários dos produtos usados na sua rede;
- inscrição na lista de alertas de segurança do CERT/CC.

10. Precauções contra engenharia social:

- treinamento de usuários e administradores contra possíveis tentativas de descoberta de informações sobre a rede da organização;
- busca e remoção de documentos que contenham tais informações e que estejam disponíveis nos servidores de rede;
- preservação de informações sensíveis ao solicitar auxílio em fóruns públicos na Internet.

11. Uso eficaz de *firewalls*:

- escolha de um *firewall* que rode em um ambiente com o qual os administradores estejam acostumados;
- instalação de *firewalls* em pontos estratégicos da rede, incluindo, possivelmente, *firewalls* internos;
- uso de uma DMZ para confinamento dos servidores públicos;
- implementação de *ingress* e *egress filtering* no perímetro da rede.