

Segurança da Informação

Atualmente, analisamos o conceito de segurança da informação como um conjunto de ações e políticas, visando proteger o tráfego de informações que circulam em nossa rede (tráfego de entrada e saída), e devido ao risco de ações voluntárias ou involuntárias dos usuários.

Vamos dividir nosso estudo em quatro partes:

- 1 – Tráfego de saída de forma involuntária
- 2 – Tráfego de entrada de forma involuntária
- 3 – Tráfego de saída de forma voluntária
- 4 – Tráfego de entrada de forma voluntária

1 – Tráfego de saída de forma involuntária

Consideramos como tráfego de saída de forma involuntária toda informação que sai de nossa rede sem que o usuário se dê conta do que está acontecendo. Este fato acontece devido à falta de conhecimento dos usuários na utilização dos recursos disponibilizados na rede. Alguns exemplos de como isso pode acontecer:

- Cavalos de tróia instalados nas estações de trabalho que enviam informações para terceiros;
- Visita a sites de *phishing* (sites falsos desenvolvidos com o intuito de roubar dados dos usuários);
- Engenharia social, onde o usuário pode passar informações por telefone através de um contato forjado por alguma empresa relacionada a prestação de serviços (ex: empresas de telecom, crédito, etc).

Como solução para esses problemas temos as seguintes ações a executar:

- Manter o sistema operacional das estações atualizados com os *patches* (remendos) de segurança lançados pelo fabricante;
- Usar navegadores seguros com políticas *anti-phishing* sempre atualizadas;
- Utilizar ferramentas *anti-phishing* sempre atualizadas;
- Utilizar ferramentas de detecção em tempo real e de remoção de cavalos de tróia sempre atualizadas;
- Utilizar anti-vírus sempre atualizados;
- Utilizar anti-vírus corporativos com gestão e administração centralizadas;
- Orientar/informar os usuários/funcionários das técnicas recentes de engenharia social e *phishing* utilizadas para roubo de informações;
- Utilização de servidor de *proxy* que filtre o acesso a sites de *phishing*.

2 – Tráfego de entrada de forma involuntária

Todo tráfego de entrada independente de ação dos usuários e do administrador da rede, é sempre considerado como uma invasão da rede. Hoje existem três formas de se invadir uma rede:

- a – Via Internet;
- b – Através de dispositivos móveis conectados a rede pelos usuários;
- c – Invasão física, seja através de um equipamento plugado na rede ou conectado na rede via rede *wireless* (conexão sem fio).

A invasão via Internet deve ser controlada em dois pontos: o *gateway* (porta de entrada da rede) e nas estações.

A segurança no *gateway* é realizada com a configuração de um servidor de *firewall* na porta de entrada da internet, que será responsável por bloquear o acesso interno de pacotes de dados através de serviços inexistentes em nossa rede.

Os serviços em nossa rede que precisam transmitir informação para o mundo exterior devem garantir sua própria segurança com atualizações constantes e utilização de softwares seguros nas aplicações que rodam em nossa rede.

Exemplos de aplicações são servidores de páginas *web*, servidores de email, servidores de banco de dados para aplicações externas, etc.

As estações de trabalho podem servir como fonte de invasão devido a cavalos de tróia, serviços de acesso remoto e outros softwares maliciosos que podem ser instalados via internet ou através de dispositivos móveis como pen drives, tocadores de mp3, disquetes, CDs & DVDs, que podem estar infectados e automaticamente contaminar a estação de trabalho ao serem plugados ou acionados.

As invasões físicas são feitas ao se conectar computadores móveis (notebooks) no cabeamento físico ou através de conexões sem fio. Nos dois casos os servidores da rede devem estar configurados para negarem conexão na rede de equipamentos desconhecidos.

Como solução para estes problemas, temos as seguintes ações a executar:

- Todas as ações do item 1;
- Configuração apropriada do servidor de *firewall*;
- Controle das aplicações que podem ser executadas com o nível do usuário na estação de trabalho;
- Controle de acesso a rede por domínio e *login* centralizado;
- Não utilizar distribuição de endereços de rede automaticamente ou fazê-lo por controle de *hardware*;
- Manter aplicações de acesso externo sempre atualizadas e selecionar aplicações seguras;
- Bloquear o acesso a dispositivos móveis nas estações (tocadores de mp3, *pen drives*, etc).

3 - Tráfego de saída de forma voluntária

O usuário pode deliberadamente tentar extrair informações da rede e transmiti-las para terceiros ou levar consigo para benefício próprio.

Existem dois tipos de informações que um usuário pode ter acesso em nossa rede:

a informação que precisa acessar para fazer seu trabalho e a informação que ele não necessita para seu trabalho mas que está disponível. Temos que encarar a segurança dessas informações de maneira diferenciada.

A informação que o usuário não precisa ter acesso, não deve ser disponibilizada a ele. Por mais óbvio que isso pareça, essa não é a realidade normalmente encontrada nas redes corporativas. Temos três focos de atuação para barrar o acesso a essas informações: internet, servidores de arquivos e softwares de gestão.

O acesso a informações indevidas na internet é barrado através de um servidor de *proxy*. O acesso a arquivos é barrado através de um servidor de arquivos com políticas de segurança eficazes e bem definidas. A informação obtida no banco de dados através de um sistema de gestão corporativa deve ser barrada através de políticas do próprio sistema de gestão.

À informação que o usuário tem acesso, devemos barrar o envio via internet ou a retirada da informação através de dispositivos móveis. Se o usuário tem acesso a Internet, não temos como coibir o envio de informação, mas podemos inibir através de sistemas de auditoria, como auditoria de sites acessados (servidor de *proxy*), auditoria de emails recebidos e enviados, e auditoria de conversas em comunicadores instantâneos se os mesmos forem liberados para utilização.

Os dispositivos móveis podem ser barrados através da desconfiguração física das conexões USB da estação de trabalho ou através do controle lógico por uma política de segurança imposta por um servidor de domínio.

Apesar dos controles exemplificados acima, ainda existem três maneiras da informação sair da empresa: impressa, por telefone/fax ou por memorização do usuário, mas para essas três formas não há muito que possamos fazer, a não ser: gravação das ligações, controle rigoroso da utilização do fax, controle da utilização de impressoras e assim por diante.

4 - Tráfego de entrada de forma voluntária

Esse tipo de ataque pode ser liberado pelo controlador do *firewall*, o administrador da rede ou um usuário que instale um software de acesso remoto em sua estação de trabalho através da internet ou de um dispositivo móvel. Partindo-se do princípio que o administrador da rede seja de confiança, a hipótese de um usuário conseguir instalar um software de acesso remoto em sua estação de trabalho é eliminada por nossas ações dos itens 1 e 2.

Autor: Engº Fernando Segalla, diretor de tecnologia do Grupo CI (01/02/2008)