1. Gestão da segurança de rede

As redes formam a espinha dorsal da maioria, senão de todos os sistemas de informação, e proteger essas redes ajuda a proteger a informação. A gestão da segurança de rede ajuda a manter os maus elementos longe dos ativos importantes.

É importante notar que, embora a proteção das redes seja uma parte importante da segurança da informação, não é suficiente tratar apenas da segurança de rede ao lidar com segurança da informação, não é suficiente tratar apenas da segurança de rede ao lidar com segurança da informação. Quando informações confidenciais estão envolvidas, é importante lembrar que a maioria dos equipamentos conectados à rede, tais como impressoras, é equipada com um disco rígido. Esses discos armazenam todas as informações que devem ser processadas. Por meio de aplicações especiais, é muitas vezes possível obter acesso a esse disco rígido e copiar todos os dados nele existentes. Além disso, um "engenheiro de manutenção" pode retirar tal disco rígido do prédio muitas vezes sem ser notado

1.1 Controles de rede

Devem ser estabelecidos procedimentos e responsabilidades para a gestão de equipamentos de rede. Quando sistemas dentro de uma única empresa estão conectados uns aos outros, procedimentos devem ser desenvolvidos e implementados com antecedência, a fim de proteger a informação contra riscos de segurança evitáveis.

Embora as aplicações possam ser efetivamente protegidas individualmente, vulnerabilidades podem surgir inesperadamente quando elas são interligadas. Quando as informações são mantidas seguras na aplicação de contabilidade, mas o sistema de administração contém uma vulnerabilidade, os dados compartilhados com essa aplicação também estão em risco. Vulnerabilidades também podem surgir nas conexões dos sistemas de comunicação da empresa, tais como chamadas telefônicas ou audioconferências, conversas telefônicas confidenciais ou armazenamento digital de faxes. Portanto, é importante saber quais sistemas estão conectados à rede e tomar medidas para que apenas os sistemas autenticados possam ter acesso à rede. Outra medida básica é limitar ao mínimo o acesso de sistemas à rede e realizar verificações regulares sobre quais sistemas estão conectados e por quê.

Ao lidar com conexões a outras redes, os riscos associados devem ser levados em conta. Se estiver lidando com informações confidenciais ao se conectar a uma rede sem fio e/ou pública, pode ser necessário tomar medidas adicionais para proteger a confidencialidade e a integridade dos dados que estão sendo transferidos. Ao lidar com requisitos de alta disponibilidade, a escolha do tipo de rede pode ser importante. Por exemplo, em ambientes com grande interferência elétrica, pode haver um elevado risco das redes sem fio não serem capazes de transmitir informações.

Para reagir às mudanças na segurança de rede, é importante conhecer o que está ocorrendo nas redes. Portanto, dependendo dos requisitos de segurança, devem ser projetados e implementados registros apropriados e monitoramentos de rede e de serviços de rede. O

objetivo do registro e do monitoramento deve estar focado na detecção de violações de segurança, mas também pode servir para examinar a causa de um incidente

Em redes interconectadas, é cada vez mais comum que as redes e os serviços de rede sejam mantidos e gerenciados por diferentes unidades organizacionais, ou mesmo gerenciados por diferentes organizações, como no caso da terceirização ou dos provedores de rede, como um serviço de telecomunicações. Isso requer uma coordenação estreita entre essas diferentes redes e serviços de rede, para poder determinar quais requisitos de segurança são necessários e quais medidas melhor se adequam a esses requisitos.

1.2 Segurança dos serviços de rede

Há uma variedade de formas pelas quais o acesso às redes pode ser controlado, dependendo em parte do tipo de rede. Por exemplo, pontos de acesso sem fio usam padrões de controle de acesso como WPA2. Para evitar que usuários não autorizados acessem uma rede, é importante verificar se credenciais como frases-senha para acesso a uma rede sem fio, não são facilmente adivinháveis ou estão definidas com valores padrão.

Há muitas outras tecnologias de segurança que podem ser usadas para proteger serviços de rede, tais como o uso de certificados digitais ou outros métodos de autenticação de usuário, firewalls, sistemas de detecção de intrusão e o uso de criptografia para as informações em trânsito.

1.3 VPNs (Virtual Private Network)

Uma VPN faz uso de uma rede já existente, normalmente a Internet, a fim de permitir a troca de informações entre redes geograficamente separadas como se estivessem na própria rede da empresa. Os dados são efetivamente protegidos enquanto são enviados. Muitos protocolos técnicos foram desenvolvidos para assegurar a disponibilidade desse serviço e atualmente, o protocolo mais conhecido e amplamente usado é o IPSec.

1.4 Segregação de redes

Um desafio significativo em segurança da informação é que as redes compartilhadas podem se estender para além dos limites da organização.

1.5 Intranet

Uma Intranet é uma rede privada dentro de uma organização. Para o usuário, a Internet é uma versão privada da Internet. O objetivo principal da Intranet é o compartilhamento digital de informações dentro de uma organização. Ela também pode ser usada para teleconferências e para facilitar e estimular a colaboração digital em grupos. Através de uma rede pública, como a Internet, é possível para uma organização ligar as partes da Intranet que são separadas. Métodos especiais de criptografia, juntamente com outras medidas adicionais de segurança, garantem a confiabilidade dessa transferência. Quando uma organização torna parte de sua Intranet acessível para clientes, parceiros, fornecedores ou outras partes de fora da organização, essa parte da rede é chamada de Extranet.

1.6 Extranet

Uma Extranet é um tipo de rede de computadores dentro de uma organização. A Extranet está ligada à Internet. O objetivo da Extranet é tornar a informação da empresa disponível, de forma segura, para clientes, parceiros e fornecedores fora da organização. Uma Extranet requer o uso de medidas de proteção e privacidade

2.Transferência de informações

A fim de evitar que informações cheguem a partes para as quais não são destinadas, é importante estabelecer acordos internos e externos relativos ao intercâmbio de informações. O objetivo do intercâmbio de informações e o que as partes acordaram devem ser documentadas. O acordo deve especificar a frequência com que as informações devem ser compartilhadas e de que forma. É importante evitar a troca de informações entre pessoas de diferentes empresas. Sem perspectivas claramente documentadas, um empregado ou contratado pode compartilhar informações confidenciais com uma pessoa errada sem perceber o efeito prejudicial que isso pode ter sobre a posição competitiva de sua própria empresa.

2.1 Mensagens eletrônicas

Mensagens eletrônicas apresentam riscos que não estão presentes no caso da comunicação em papel. É por isso que informações trocadas digitalmente devem ser protegidas de forma adequada. É particularmente importante estar ciente de que quando as informações são enviadas por e-mail, elas podem ser lidas por qualquer pessoa que deseje fazê-lo. Além disso, cópias do e-mail podem ser armazenadas em servidores espalhados por todo o mundo. A Internet, afinal de contas, não escolhe o caminho mais curto, mas o caminho mais rápido. Se as informações forem altamente confidenciais, é melhor não às enviar por e-mail. Se não houver outra maneira, então você deve assegurar a proteção da mensagem através do uso de criptografia.

2.2 Contratos de confidencialidade ou de não divulgação

Informações sensíveis devem ser devidamente identificadas e adequadamente protegidas, mas as pessoas de dentro da empresa e os parceiros externos precisam de acesso a informações sensíveis, ou podem obter acesso a tais informações. Tome como exemplo um administrador de banco de dados que pode ter acesso a informações sensíveis devido à natureza de seu trabalho. Ou que a empresa concordou que o novo sistema de TI deve ser localizado na nuvem, o que potencialmente significa que o fornecedor de serviços em nuvem pode ter acesso a dados sensíveis da empresa.

Para ser capaz de proteger as informações e criar uma estrutura juridicamente exequível, devem existir acordos de confidencialidade ou de não divulgação elaborados e assentados. Nesses acordos, são estabelecidos por escrito o proprietário dos dados, o acesso que é permitido, bem como as ações a serem tomadas no caso de violação da sua confidencialidade. Esses acordos devem ser elaborados com a ajuda de um consultor jurídico.