Redes de computadores

As necessidades de redes informáticas de um escritório ou instalação são muito específicas dos orçamentos, da dimensão, da capacidade, e das necessidades operacionais globais da agência. As agências devem investigar a contratação de pessoal especializado em TI e redes para apoiar a criação de redes de escritórios e subescritórios.

Configuração de escritório/instalações

Na maioria dos locais no terreno, haverá uma mistura de vários equipamentos de rede de escritório. Tais podem incluir:

Ligação a ISP externo – A ligação a um Fornecedor de Serviços Internet externo (ISP) pode vir sob a forma de Internet por satélite, linha telefónica, ou qualquer outra forma de ligação dedicada a uma rede comprovada pelo ISP.

Modem – Os modems recebem sinais provenientes de ISP e traduzem-nos em sinais utilizáveis por redes domésticas ou de escritório. Os modems também contêm informação específica do utilizador que é utilizada para identificar, localizar e monitorizar o tráfego para fins de segurança e faturação. Sem um modem, qualquer equipamento de rede baseado em casa ou no escritório seria incapaz de falar efetivamente com redes externas.

Router – Um Router é um dispositivo que divide e gere o tráfego da Internet, permitindo que múltiplos dispositivos informáticos tenham os seus próprios endereços IP e MAC únicos, e comuniquem com a Internet e uns com os outros ao mesmo tempo através de uma rede. Os routers têm uma variedade de configurações e funções. Alguns podem monitorizar e controlar o tráfego na rede local, e outros têm capacidade wi-fi. O tipo de router utilizado dependerá das necessidades operacionais.

Firewall – Uma firewall é qualquer dispositivo que monitoriza e filtra especificamente o conteúdo da Internet proveniente de redes externas. As firewalls são úteis para prevenir software malicioso, intrusão casual não autorizada em redes, ou mesmo bloquear conteúdos não permitidos pela política de TI de organizações individuais. Em redes simplificadas, as firewalls são frequentemente fundidas com modems ou routers, mas as redes avançadas podem ter firewalls autónomas que têm diferentes protocolos para diferentes utilizadores do serviço.

Comutador – Um comutador (ou switch) de rede é uma espécie de forma avançada de route: controla e distribui a Internet entre múltiplos dispositivos em rede. Contudo, os comutadores são capazes de monitorização e controlo detalhados até ao nível do dispositivo individual. Os comutadores são também utilizados para filtrar, bloquear e proteger redes internas, de forma semelhante a firewalls que protegem de ameaças externas.

Servidor – Os servidores são definidos como computadores totalmente dedicados ao armazenamento e partilha de ficheiros dentro de uma rede. Os servidores podem ser tão simples como computadores normais, ou tão complexos como grandes dispositivos informáticos especializados que têm requisitos especiais de instalação. Nos últimos anos, muitas agências começaram a utilizar servidores remotos, que hospedam e gerem ficheiros e dados a partir de locais fora dos escritórios, por vezes num país diferente. Servidores remotos são soluções perfeitamente aceitáveis; no entanto, se os utilizadores do servidor tiverem uma ligação inconsistente à Internet, um servidor localizado pode ser preferível.

1 ISP externo

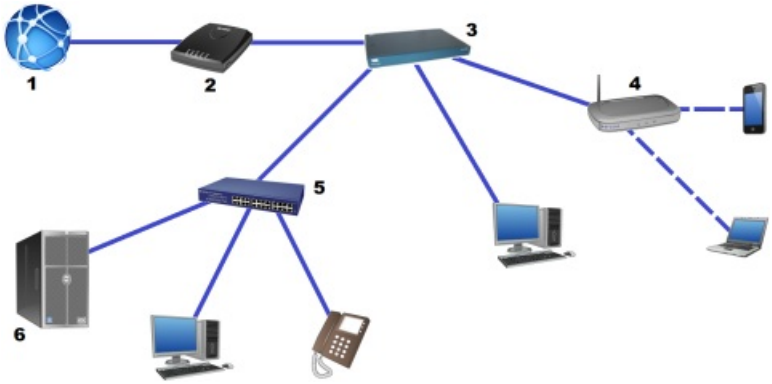
2 Modem

3 Router/Firewall

4 Router Wi-Fi

5 Comutador de rede

6 Servidor



Segurança operacional

Os requisitos de segurança operacional de cada uma das redes locais devem seguir regras básicas.

Controlo de acesso – Apenas pessoas autorizadas devem ter acesso a redes e dispositivos informáticos. Todos os computadores devem ser protegidos por palavra-passe, e os routers wifi devem também requerer credenciais de início de sessão. Algumas redes permitem o acesso temporário de convidados, contudo as necessidades de configurações especiais variam consoante o ambiente operacional.

Software malicioso – Todos os dispositivos informáticos em redes devem ter alguma forma de software antivírus, e os sistemas operativos devem estar sempre atualizados. As agências devem considerar a instalação de firewalls e/ou interruptores com definições geridas para reduzir também as tentativas de intrusão ou a transmissão de software malicioso.

Política de TI – As agências devem desenvolver e partilhar políticas internas de TI para todos os funcionários e utilizadores da rede. As políticas de TI devem incluir regras e regulamentos para o que é considerado comportamento aceitável, quais são as regras para a utilização de diferentes tipos de hardware, e estabelecer diretrizes para o incumprimento.