Guia de resolução de problemas da Cisco

Tirar o maior partido das TI – dez dicas essenciais sobre segurança para a sua empresa

Se tem uma empresa, tem de se preocupar com a sua segurança. A segurança das suas informações, das suas instalações e dos dados dos seus clientes deverá ser essencial para si, mesmo que esta não faça parte do objectivo principal da sua empresa. A dificuldade reside no facto de ter muitas informações à sua disposição e de nem todas serem muito úteis. O não especialista deve tomar constantemente decisões, como por exemplo: Disseram-me que preciso de uma firewall, mas actualmente o Windows já tem uma integrada. Preciso de outra?

Neste guia, o nosso objectivo é analisar consigo diversos temas dos quais deve estar a par. Vamos também começar a fornecer-lhe informações de que provavelmente irá precisar. Iremos também revelar alguns dos problemas de gestão, e não apenas técnicos, com os quais as pessoas que se preocupam com a protecção das suas empresas se deparam.

Dez dicas essenciais

1. Antivírus:

Um pacote antivírus é algo excelente, mas nem todos fazem o suficiente. Como provavelmente já deve saber, um pacote antivírus funciona utilizando uma base de dados de informações sobre o que constitui uma ameaça num determinado momento (por isso, é essencial manter a subscrição actualizada).

No entanto, isto significa que, se o seu pacote antivírus não "conhecer" um determinado vírus, não pode proteger o utilizador. É por este motivo que a Cisco® defende não apenas um sistema antivírus, como também um Sistema de Prevenção de Intrusões. A diferença é dupla: em primeiro lugar, um Sistema de Prevenção de Intrusões detecta qualquer anomalia num pacote completo de informações; em segundo lugar, monitoriza também comportamentos fora do normal de parcelas de software do seu computador. Por isso, por outras palavras, não só procura vírus que conhece, como também, se uma parte de um código começar algo que provavelmente não devia – como eliminar outros ficheiros, inspeccionar a sua base de dados de clientes, etc. –, o pára. Os especialistas em segurança designam esta acção como ataque de dia zero - um ataque que explora uma vulnerabilidade ou um vazio num programa ou sistema, antes de este ser conhecido pelo fabricante. Ao procurar comportamentos fora do normal e não códigos já conhecidos, podemos travar estes ataques.

Há diferentes níveis de Sistemas de Prevenção de Intrusões – os baseados no anfitrião e os baseados na rede. Um Sistema de Prevenção de Intrusões baseado na rede está instalado num ponto de entrada da sua rede. Um Sistema de Prevenção de Intrusões baseado no anfitrião está instalado no seu portátil e não na sua rede – por isso, mesmo quando estiver ligado a outra rede durante trabalhos externos, continua protegido.

2. Firewall:

Uma firewall é muito mais do que apenas marcar uma caixa onde diz "Tenho uma firewall". Algumas estão integradas no sistema operativo e outras em máquinas separadas na rede.

Um ponto muito mais importante é aquilo que a firewall vai procurar. Muitas procuram aquilo que percepcionam como um ataque à rede, o que é uma parte essencial daquilo que necessita enquanto utilizador. Na Cisco, também oferecemos protecção ao nível das aplicações, pelo que, se uma parcela de código parecer fazer um determinado programa comportar-se de forma bizarra, será detectada. É fundamental ter uma firewall que, na verdade, não esteja no seu computador, mas sim noutro computador, num router ou noutro dispositivo que actue como porta de ligação para a sua rede. Se esta se tratar da única porta de ligação através da qual o tráfego deve passar para entrar no seu sistema informático, faz todo o sentido conferir-lhe algum tipo de segurança. A Cisco possui diversos níveis de segurança entre as suas ofertas.

3. Colaboradores:

Antes de nos concentrarmos na tecnologia, vale a pena considerar até que ponto os riscos para uma empresa são de natureza não técnica. Seguem-se algumas áreas nas quais muitas pessoas já perderam ou comprometeram os seus dados:

- Apesar de ter instituído uma política rigorosa sobre quem pode visualizar o quê no arquivo electrónico, essa política não é aplicada às impressões físicas, que são esquecidas em comboios, lobbies de hotel, etc.
- Não conseguir convencer as pessoas da necessidade de desligar os seus monitores quando abandonam a secretária. Neste caso, os visitantes podem e irão ler informações confidenciais nos monitores (neste ponto, é de notar que as protecções de ecrã utilizam electricidade desnecessária e que os dias em que protegiam o ecrã de alguma coisa já passaram há muito).
- Perdoem se voltamos ao mesmo tema, mas isto continua a suceder – o nome do cão/parceiro/rua não é uma palavra-passe segura, tal como o não é utilizar "palavra-passe".
- Normalmente, não ter uma política definida sobre o que é preciso fazer para tornar uma rede segura, quem precisa de o fazer e as sanções para os infractores. Trate as pessoas como adultos inteligentes e ficará espantado com a forma rápida com que irão querer cooperar.
- Inclua nessa política que as pessoas não poderão fazer downloads de software sempre que o desejarem. Muitos desses softwares são inofensivos, mas é necessário que controle as licenças e se proteja contra o risco de malware.

4. Dispositivos:

Os dispositivos que entram e saem de um edifício: se trabalhasse para o Ministério da Defesa, segundo consta, teria de entregar o telemóvel ou o leitor de música à entrada, só o reavendo à saída. Isto não é feito porque se pensa que as pessoas não vão realizar o seu trabalho a tempo, mas porque os telefones, câmaras e dispositivos semelhantes podem conter dados. Um iPhone 3G (escolhido apenas por se tratar de um bestseller) tem, em alguns casos, 16 gigabytes de espaço. Estes dispositivos podem ser ligados a uma porta USB de um computador e as pessoas podem sair do trabalho com a lista de clientes da empresa transferida para o suporte que levam no bolso. De igual modo, podem introduzir um vírus no seu sistema.

Poderá não enveredar por uma decisão draconiana de proibir todas as formas de dispositivos pessoais de transporte de dados no seu local de trabalho, mas pode tomar precauções:

- Os computadores podem ser configurados para não aceitarem dispositivos USB;
- Um software de monitorização inteligente deste tipo, pré-carregado com todos os produtos Cisco, detecta actividades fora do normal na sua rede e comunica-lhe a situação.
- Se tiver utilizadores que iniciem sessão na sua rede, é imperativo que os seus equipamentos (se estiverem a utilizar os seus próprios computadores portáteis) sejam verificados pelo antivírus, para que estejam seguros como se fossem seus. Mais uma vez, os equipamentos da Cisco verificam estes computadores quando iniciam sessão, procurando não só os vírus conhecidos, como também actividades fora do normal.

5. Proteger os dados de colaboradores locais e remotos:

Como é evidente, não vale a pena proteger a sua rede internamente, se começar a ter fugas quando estiver fora do escritório. Isto significa muita coisa. Primeiro, assegurar que qualquer ligação da sua rede à Internet é efectuada através de uma Rede Privada Virtual adequada, que disponha de todas as funções de segurança habituais. Segundo, certificar-se de que todas as ferramentas não técnicas da actividade dos seus colaboradores estão sujeitas à mesma segurança que teriam se estivessem no escritório. Deste modo, se não estão autorizados a imprimir documentos, a transferir itens para dispositivos de armazenamento USB, etc. quando estão no escritório, não devem pensar que podem fazê-lo em casa.

Muitas destas situações podem ser conseguidas através da instalação de uma rede de comutação inteligente no escritório, protegendo a respectiva porta de ligação com o conjunto adequado de produtos Cisco.

6. Redes sem fios:

Uma subsecção do ponto acerca da protecção dos dados de colaboradores locais e remotos é a análise das configurações das redes sem fios, tanto interna como externamente, quando estiverem sob o seu controlo. Não confie numa rede apenas porque esta é identificada como "segura" por um computador portátil ou um smartphone. Esta indicação pode apenas significar que tem segurança WEP, que é um tipo de protecção já bastante ultrapassado e qualquer pirata informático experiente pode ultrapassá-la.

No escritório, todos os equipamentos de rede da Cisco possuem segurança integrada de série que pode ser configurada pelos nossos parceiros especializados. Fora do escritório, os seus colaboradores podem utilizar os seus próprios equipamentos sem fios. É razoável insistir para que estejam protegidos pelos seguintes elementos:

- Se tiverem configuração WEP, precisam de ser actualizados para WPA.
- As palavras-passe predefinidas fornecidas com o equipamento devem ser alteradas.
- O computador e o router da rede devem ter um identificador denominado SSID, que pode ser encontrado no menu de configuração do router. Altere o identificador e pare a transmissão do SSID, para que outras pessoas não consigam ver o seu computador se estiverem à procura de redes para atacar.
- Desligue a ligação automática a redes WiFi, para que o utilizador apenas estabeleça ligação com redes em que confie.
- Atribua um endereço IP estático aos seus dispositivos. A alternativa é que a sua rede atribua esses endereços aleatoriamente, o que provoca problemas quando desligar um determinado dispositivo.
- O seu router deverá ter uma firewall – certifique-se de que esta está ligada, pois muitos são instalados com as firewalls desligadas por predefinição.
- Desligue a rede, se esta não for utilizada durante um período de tempo prolongado.

7. Pirataria informática – quais as probabilidades?

Até agora, debruçámo-nos sobre como evitar ser atacado e sobre como evitar intrusões indesejadas na sua rede informática. Mas quais são as probabilidades de alguém tentar entrar no seu sistema? Muitos clientes da Cisco são pequenas empresas e têm a certeza de que ninguém estará interessado em atacá-las.

Nos dias em que apenas havia piratas informáticos humanos, isto provavelmente seria mais verdadeiro do que agora. O problema é que muitos dos ataques e intrusões actuais são automatizados. Pense no pirata informático como um líder de muitos ladrões que têm de invadir casas desprotegidas para confirmar se têm alguma coisa que valha a pena roubar. Neste cenário, as casas são os computadores e estas parecem idênticas, pelo que a única forma de comprovar se vale a pena uma visita é entrar primeiro e dar uma espreitadela.

Isto é feito por "bots" automatizados na Internet, que efectuam uma acção denominada "verificação da porta" – basicamente, eles chegam à "porta" da sua rede e a primeira coisa que fazem é ver se está trancada. É claramente do seu interesse certificar-se de que está.

(E não se esqueça de verificar também as suas portas reais. A Cisco dispõe de câmaras que podem ser ligadas à Internet para que possa ver o que se passa no seu escritório, onde quer que esteja. Algumas são activadas por movimento, por isso, será alertado sempre que alguém estiver num local não autorizado).

8. Negócios online:

Se a maioria ou todos os seus negócios se processarem online, é evidente que precisa de tomar medidas para proteger tanto as suas informações de stocks, se forem confidenciais, como os dados dos seus clientes. Todas as medidas que mencionámos até agora vão contribuir para essa protecção, mas há mais algumas – mais uma vez, são medidas tanto ao nível da gestão como técnicas e incluem não fazer coisas como aquelas que se sabe que o Governo fez, que foi deixar CDs não encriptados ao alcance de qualquer pessoa e que mais tarde foram descobertos em autocarros, por exemplo! (Não se esqueça de encriptar os CDs – assim, ninguém pode ler os dados, mesmo se descobrirem a palavra-passe).

9. Valerá então a pena?

Muitas pequenas empresas, especialmente em tempos de crise financeira, terão a preocupação que cada investimento em tecnologia tenha retorno. Isto é um pouco complicado em termos de despesas com segurança, pois isto é intangível. É provável que já tenha pago por fechaduras para sua casa, sem nunca se preocupar em calcular ao fim de quanto tempo o investimento foi amortizado; sabe apenas o quanto poderia perder quando há problemas.

Contudo, é fácil ter a percepção de algum retorno do investimento em segurança. Se tiver uma empresa de comércio electrónico e não conseguir fazer crer aos seus clientes que os seus dados ficam seguros, por exemplo, pode optar por não fazer nada e aguardar que a sua empresa vá à falência. Se tiver convidados nas suas instalações e estes estabelecerem ligações à sua rede, acabando por ficar com um novo vírus informático devido à sua configuração de segurança da rede, prepare-se para os deixar de ter como clientes. E os exemplos continuam.

É importante realçar, porém, que pouco do equipamento básico custa assim tanto dinheiro. Um pequeno escritório com meia-dúzia de colaboradores pode comprar um bom router sem fios, com firewall e protecção total por cerca de 175€ e ainda receber troco.

10. Contratar serviços de segurança externos:

Se ainda assim achar o processo intimidante, vale a pena contratar um serviço externo para tratar da segurança de toda a sua infra-estrutura. A Cisco tem muitos parceiros especializados em tornar as pequenas empresas mais seguras do que eram e, sendo especialistas, dispõem já de economias de escala e de conhecimentos, pelo que não precisará de despender tempo a adquiri-los. Retirar todos os dados das suas instalações e ter uma empresa qualificada e de confiança a tomar conta deles, constitui um nível extra de segurança, que muitas pequenas empresas recebem de braços abertos.

Tal como referimos no início, se estiver envolvido em qualquer tipo de negócio, está também envolvido no negócio da segurança, quer queira ou não. Felizmente, os elementos iniciais para proteger a sua rede não custam fortunas e tem à sua disposição muitos conhecimentos para a configurar.

Boa sorte!