# Introdução a Segurança da Informação – Parte 8

13 de abril de 2015 / maximoz

## Segurança Física

Para proteger suas informações de caírem em mãos erradas, você não somente precisa se preocupar acerca da segurança do software mas também considerar que a segurança física como uma etapa necessária. E se seu servidor com todos os softwares de segurança instalados é roubado de suas instalações? Em tal cenário, todos os seus dados importantes e confidenciais serão perdidos e comprometidos mesmo depois de tomar todas as medidas de segurança de software. Portanto, a segurança física de um sistema é importante assim como a segurança do software.

A segurança física refere-se a proteger ativos físicos ou computadores/hardwares de acesso físico não autorizado. As ameaças podem ser ocasionadas pelos próprios funcionários da empresa. Os documentos importantes ou o hardware da sua empresa pode ser vendidos por ganância por uma fração do custo real do item para empresas rivais ou para outros que possam ser beneficiados com isso.

A segurança física de seus ativos é relativamente fácil de realizar. Os três princípios da segurança física são:

1. **Instalação/Local Seguro:** O primeiro princípio é a segurança do local onde está mantido seu computador/hardware. Você pode reforçar a proteção proibindo a transição de pessoas não autorizadas do local, instalando sistemas de segurança, alarmes de vigilância, sistemas de bloqueio, acrescentando portas extras ao local e limitando o acesso à zonas sensíveis dos negócios. Além disso, você pode definir senhas eletrônicas para cada porta, dobrar sua equipe de segurança ou contratar agentes de segurança para seu escritório.
2. **Detectar o Roubo:** O segundo princípio da segurança física é detectar o roubo em base regular. É importante que você saiba se algo está faltando e que a perda ocorreu. O roubo pode ser detectado usando câmeras de vigilância. Elas também permitem você descobrir quem estava envolvido no roubo. A gravação através dessas câmeras também podem ser usadas como prova no tribunal, como todos sabem.
3. **Recuperar-se do Roubo:** O terceiro princípio da segurança física é fazer planos de recuperação a partir de um roubo e voltar para os seus negócios normais. Por exemplo, se um de seus servidores importantes é destruído ou os detalhes de contas bancárias são roubados, em seguida, quanto tempo você vai demorar para voltar para os seus negócios normais? A recuperação de roubo envolve grande dose de planejamento, pensamento, e testes. Uma boa prática e manter sempre uma cópia de todos os documentos importantes (backup) distante da área de negócios, em algum local seguro.

## Escaneamento de Vulnerabilidades

O escaneamento de vulnerabilidades é um processo de varredura em seu sistema, aplicação ou rede cuja finalidade é encontrar agentes vulneráveis ou pontos fracos. As ferramentas de varredura de vulnerabilidades permitem você descobrir no sistema ou dispositivos na sua rede se estão com a segurança comprometida. Uma vez que você souber as áreas mais fracas, você pode consertá-las. No entanto, se uma varredura de vulnerabilidade é feita na sua rede por uma outra pessoa então essa pessoa pode usá-la contra vocẽ. Portanto, é importante que você use a varredura antes que essa pessoa use contra você primeiro. A varredura de vulnerabilidades pode ser de dois tipos:

1. **Varredura de Vulnerabilidade Ativa:** Esta é uma abordagem ativa que uma organização utiliza para corrigir todos os tipos de violão do sistema através da funcionalidade de monitoramento do núcleo. Ele inclui ferramentas de verificação que exigem atenção constante e vigilância e as áreas de foco específico. Às vezes um produto é configurado para impedir situações particulares. Por exemplo, o uso de unidades USB em uma rede.
2. **Varredura de Vulnerabilidade Passiva:** Esta é uma abordagem passiva em que o pessoal segurança de uma empresa monitora a segurança do sistema. Por exemplo, inclui o monitoramento de sistemas operacionais em uso, a varredura da LAN para o tráfego de entrada e saída, determinando os serviços que estão disponíveis, e determinando as partes do sistema/rede que estão vulneráveis à ameaças de segurança.

Você pode usar ambos tipos de varredura de vulnerabilidade no seu sistema/rede para eliminar os riscos que podem, eventualmente, ser explorados pelos atacantes.

## Engenharia Social

A engenharia social é um tipo de ataque no qual ao invés de interagir diretamente com um software, o atacante tenta explorar o comportamento humano nas pessoas que possam, por acaso, divulgar alguma

informação importante ou confidencial. O atacante ganhar a confiança de pessoas importantes e os manipula desempenhando ações que comprometerem a segurança da rede. Por exemplo, uma pessoa usando engenharia social pode tentar ganhar a confiança de um funcionário que é autorizado a acessar a rede e fazer com que essa pessoa lhe revele alguma informação confidencial como as credenciais (usuário/senha) da empresa.

**Conclusão**

Esse tutorial abordou vários aspectos da segurança da informação. Tal como segurança em software, hardware, políticas de segurança e também foi abordado sobre os processos de segurança, as medidas de segurança e implementações de segurança para proteger dados de uma empresa ou pessoa. Agradeço imensamente quem se deu ao trabalho de ler, espero que tenham aprendido. Lembrando que isso é só uma introdução à essa extraordinária área. Bons estudos!

*Traduzido e adaptado por: Maximoz Sec*
*Artigo original: http://learnthat.com/introduction-to-network-security/*