FOCO NO MERCADO DE TRABALHO

# SEGURANÇA DE REDES

Emilio Tissato Nakamura

## PONTOS DE ATAQUE

Ações de tratamento dos riscos podem ser executadas para que incidentes de segurança sejam evitados.

Fonte: Shutterstock.

**Deseja ouvir este material?**

Áudio disponível no material digital.

## SEM MEDO DE ERRAR

Você, como responsável pela segurança da empresa em que trabalha, deve preparar um relatório que complemente a primeira apresentação realizada para a diretoria executiva e que teve sucesso para chamar a atenção para os riscos de forma mais conceitual.

O seu relatório e sua apresentação devem focar o grande projeto em andamento que já chegou a grandes resultados, com os cientistas tendo descoberto um novo composto que será utilizado na indústria agrícola.

O cenário que você deve considerar é a proteção do projeto que está em execução pelas pessoas, que possuem as ideias, e que essas informações vão de forma digital do *notebook* até o servidor da empresa, passando pela rede.

Comece **elencando os pontos** de ataque que envolvem o fluxo da informação, que começa nas pessoas. O que surge delas passa para o *notebook*, que pode estar em diferentes localidades e em transporte. Do *notebook*, as informações vão para o servidor da empresa, passando pela rede. No *notebook* há, além do *hardware*, aplicações e sistema operacional. No servidor da empresa há, além do *hardware*, aplicações, sistema operacional, banco de dados e *middleware*.

Pense nos **controles de segurança**. Entre o *notebook* e o servidor da empresa há, além da rede, controles de segurança como *firewall* e IPS. No *notebook* podem existir controles de segurança como *antimalware* e *firewall*; no servidor, também podem existir controles de segurança como *firewall* de aplicação (WAF).

Considere as **ameaças e as técnicas de ataques** relacionadas com as ameaças. A ameaça de vazamento do projeto pode se tornar realidade (um incidente de segurança) no caso de um *cracker* (agente de ameaça) realizar um ataque do homem do meio durante a conexão entre o *notebook* do funcionário com o servidor da empresa. Há uma série de outras possibilidades de ataques ligadas à ameaça de vazamento do projeto; uma delas é a contaminação do *notebook* do funcionário por um *malware* ou a descoberta da senha do funcionário. Explore as

possibilidades de ataques que resultam em roubo do projeto e relacione os controles de segurança correspondentes. Por exemplo: para o caso do *malware*, o controle de segurança é o *antimalware*.

Avance nas situações de segurança explorando as **ameaças de negação de serviço**, indicando as técnicas de ataque relacionadas, bem como os controles de segurança recomendados.

Pense em ameaças que levam à **perda da integridade do projeto** com alterações de informações e não se esqueça de que há vários pontos de ataques.

Dê uma atenção especial para a autenticação dos usuários, indicando para a diretoria executiva os aspectos relacionados aos fatores de autenticação e os problemas de segurança existentes em cada abordagem.

Ao final da apresentação, a diretoria executiva da empresa estará, ao mesmo tempo, preocupada pelos riscos existentes que podem causar grandes impactos, mas aliviada por ter tido acesso a informações valiosas sobre os riscos. O ponto fundamental é que os riscos representam o futuro, ou seja, são situações que podem ocorrer, tornando-se incidentes de segurança. Com isso, ações de tratamento dos riscos podem ser executadas, de modo a se evitar incidentes de segurança.



AVANÇANDO NA PRÁTICA

## SEGURANÇA EM CAMADAS: CONTROLES DE SEGURANÇA, *FIREWALL* – IDS, IPS, *ANTIMALWARE*, *ENDPOINT* E CORRELAÇÃO DE EVENTOS

Você, enquanto profissional de segurança, deve ter uma visão sobre como controles de segurança podem ser violados. Isso vem do entendimento de como os controles de segurança funcionam e também das técnicas de ataques. Considere que você também é o dono de uma loja virtual de materiais preciosos e está usando um *datacenter* próprio com o objetivo de fazer a proteção do servidor que está hospedado nele.

A partir disso, vá construindo a sua estratégia de segurança para proteger o servidor e **apresente a razão de este controle não ser suficiente, indicando, logo a seguir, outro controle de segurança capaz de criar uma camada adicional de segurança.**

Considere os seguintes controles de segurança: *firewall*, IDS, IPS e correlação de eventos, que trata de forma integrada e correlacionada diferentes logs de vários ativos, tais como o *firewall*, os equipamentos de rede como roteador, servidor de aplicação ou *middleware*, além da aplicação e das autenticações.

Caso queira ir adiante, você pode considerar, ainda, a autenticação duplo fator dos clientes de sua loja e o *firewall* de aplicação.



RESOLUÇÃO

Pense sempre nos pontos de ataque. No caso da loja virtual, você não possui controle sobre os dispositivos de seus clientes ou os *endpoints*; logo, o que resta a você é partir para a arquitetura de rede segura, que começa com a segmentação de rede. O servidor deve estar em uma DMZ para proteger a sua rede interna, que deve estar isolada; a segmentação e o controle de acesso de rede podem ser feitos pelo *firewall*, que bloqueia tentativas de ataques a portas filtradas. Porém, em portas liberadas pelo *firewall*, necessárias para que os clientes cheguem ao servidor, ataques podem ocorrer. O controle adicional sugerido é o IDS, que faz a detecção de ataques. Para que as detecções reflitam ações como o encerramento das conexões dos ataques, um IPS deve ser utilizado. O problema do IPS é que ele atua na rede, e ataques com construções de pacotes de rede, que são mais difíceis de serem detectados, podem ser feitos contra a sua empresa. Nesse caso, a correlação de eventos, que considera logs de ativos como o servidor de aplicação ou *middleware*, além da aplicação e das autenticações, pode ser correlacionada às informações da camada de rede, resultando em detecções mais assertivas.

Você pode, ainda, explorar novas tecnologias de detecção que utilizam técnicas de inteligência artificial e detectam situações como desvios de padrão.

Ver anotações 0