GESTÃO DE SEGURANÇA DA INFORMAÇÃO

VULNERABILIDADE DE SEGURANÇA

Olá!

Nesta aula você irá compreender o que é vulnerabilidade no contexto da segurança da Informação.

1. Os conceitos básicos
2. Os principais tipos de vulnerabilidades.
3. As principais ferramentas para análise de vulnerabilidade de segurança.

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvos de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essas possibilidades aparecem, a quebra de segurança é consumada.

As vulnerabilidades estão presentes no dia-a-dia das empresas e se apresentam nas mais diversas áreas de uma organização.

Se partimos do princípio de que não existem ambientes totalmente seguros, podemos afirmar que todos os ambientes empresariais são vulneráveis e muitas vezes encontramos também vulnerabilidades nas medidas implementadas pela empresa.

Mas, o que é vulnerabilidade?

VULNERABILIDADE é a fragilidade presente ou associada a ativos que manipulam ou processam informações que, ao ser explorada por ameaças (uma ameaça é um possível perigo que pode explorar uma vulnerabilidade), permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios de segurança da informação, ou seja, a :

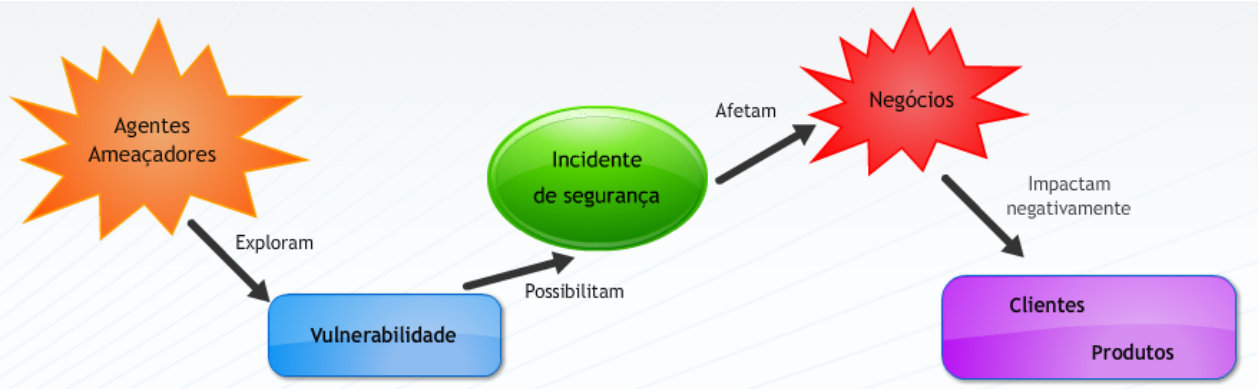
Fique ligado

Identificar as vulnerabilidades que podem contribuir para as ocorrências de incidentes de segurança é um aspecto importante na identificação de medidas adequadas de segurança. As vulnerabilidades são as principais causas das ocorrências de incidentes de segurança.

Você sabia?

Que as vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou uma condição favorável que são as ameaças.

Podemos concluir então que...



Exemplos de vulnerabilidades ....

Não existe uma única causa para surgimento de vulnerabilidades. A negligência por parte dos administradores de rede e a falta de conhecimento técnico são exemplos típicos de vulnerabilidade, porém diferentes tipos de vulnerabilidade podem estar presente em diversos ambientes computacionais. As vulnerabilidades podem ser..

Físicas

Vulnerabilidades Físicas

Os pontos fracos de ordem física são aqueles presentes nos ambientes em que estão sendo armazenadas ou gerenciadas as informações. Ao serem explorados por ameaças, afetam diretamente os princípios básicos da segurança da informação, principalmente a disponibilidade.

São exemplos de vulnerabilidades físicas:

-Instalações prediais fora do padrão;

-Salas de CPD mal planejadas;

-Falta de extintores e detectores de fumaça;

-Risco de explosões, vazamentos ou incêndios.

Naturais

Vulnerabilidades Naturais

Os pontos fracos naturais são aqueles relacionados às condições da natureza que podem colocar em risco as informações. A probabilidade de estar expostos às ameaças naturais é fundamental na escolha e na preparação de um ambiente. Devem ser tomados cuidados especiais com o local, de acordo com o tipo de ameaça natural que possa ocorrer em uma determinada região geográfica.

São exemplos de vulnerabilidades naturais:

-incêndios;

-enchentes;

-terremotos;

-tempestades;

-falta de energia;

-acúmulo de poeira;

-aumento de umidade e de temperatura.

Hardware

Vulnerabilidade de Hardware

Os pontos fracos de Hardware são os possíveis defeitos de fabricação ou configuração dos equipamentos das empresas que podem permitir o ataque ou a alteração dos mesmos.

São exemplos de vulnerabilidades de hardware:

-A ausência de atualizações de acordo com as orientações dos fabricantes dos programas utilizados;

-A conservação inadequada dos equipamentos;

-Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização);

-Erros durante a instalação.

Software

Vulnerabilidades de Software

Podem ser classificadas como vulnerabilidade de aplicativo ou de sistema operacional. Neste caso os pontos fracos de software ocorrem quando aplicativos/sistema operacional permitem que ocorram acessos indevidos aos sistemas de computador, inclusive sem o conhecimento de um usuário ou administrador de rede.

São exemplos de vulnerabilidades de software:

-A configuração e a instalação indevidas dos programas de computador/sistemas operacionais, podem levar ao

-uso abusivo dos recursos por parte de usuários mal-intencionados;

-Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias

Vulnerabilidades de Mídias

Os pontos fracos de mídias são as formas de utilização inadequadas dos dispositivos de armazenamento das informações, que podem deixar seu conteúdo vulnerável a uma série de fatores que poderão afetar a integridade, a disponibilidade e a confidencialidade das informações.

São exemplos de vulnerabilidades de mídias:

-Uso incorreto das mídias de armazenamento (pen-drive, CDROM, DVDROM, HD);

-Discos, fitas, relatórios e impressos podem ser extraviados;

-Local de armazenamento em locais insalubres ou com alto nível de umidade, magnetismo ou estática, mofo;

-Defeito de Fabricação;

Comunicação

Vulnerabilidade de Comunicação

Os pontos fracos de comunicação abrange todo o tráfego de informações, onde quer que transitem, seja por cabo, satélite, fibra óptica ou ondas de rádio. Abrange qualquer falha na comunicação que faça com que uma

informação fique indisponível para os seus usuários, ou, pelo contrário, fique disponível para quem não possua direitos de acesso ou ainda que as informações sejam alteradas em seu estado original, afetando sua integridade.

São exemplos de vulnerabilidade de comunicação:

-Acesso não autorizado;

-Perda de comunicação;

-A ausência de sistemas de criptografia nas comunicações ;

-A má escolha dos sistemas de comunicação para envio de mensagens de alta prioridade da empresa;

Humanas

Vulnerabilidades Humanas

Os pontos fracos humanos relaciona-se aos danos que as pessoas podem causar às informações e ao ambiente tecnológico que lhes oferece suporte, podendo ser intencional ou não e interna ou externa. Um importante exemplo de vulnerabilidade humana interna é o desconhecimento das medidas de segurança adequadas que são adotadas pela organização.

São exemplos de vulnerabilidades humanas:

-Falta de treinamento; -Compartilhamento de informações confidenciais,;

-Não execução de rotinas de segurança;

-Erros ou omissões nos procedimentos operacionais da organização;

-Ameaça de bomba,

-Sabotagens;

-Vandalismo, roubo ou destruição da propriedade ou dos dados.

Análise vulnerabilidades

A verificação das vulnerabilidades é essencial para garantir a segurança do sistema e da rede. A análise de vulnerabilidades tem por objetivo verificar a existência de falhas de segurança no ambiente de TI das empresas. Esta análise é uma ferramenta importante para a implementação de controles de segurança eficientes sobre os ativos de informação das empresas. É realizada através de um levantamento detalhado do ambiente computacional da empresa, verificando se o ambiente atual fornece condições de segurança compatíveis com a importância estratégica dos serviços que a empresa fornece ou desempenha. Esta análise compreende todos os ativos da informação da empresa que abrange:

Tecnologias: software e hardware usados em servidores, estações de trabalho e outros equipamentos pertinentes, como sistemas de telefonia, rádio e gravadores;

Ambientes: é o espaço físico onde acontecem os processos, onde as pessoas trabalham e onde estão instalados os componentes de tecnologia. Este item é responsável pela análise de áreas físicas.

Processos: análise do fluxo de informação, da geração da informação e de seu consumo. Analisa também como a informação é compartilha entre os setores da organização;

Pessoas: As pessoas são ativos da informação e executam processos, logo, precisam ser analisadas.

A análise de vulnerabilidade permite que os profissionais de segurança e TI da empresa possam ter maior conhecimento do ambiente de TI e seus problemas; assim como a possibilidade de tratamento das vulnerabilidades, com base nas informações geradas.

Os testes de vulnerabilidade consistem na determinação de que falhas de segurança podem ser aplicadas à máquina ou rede alvo. O objetivo do teste é a identificação nas máquinas da rede alvo de:

As portas do protocolo TCP/IP que encontram-se desprotegida (abertas);

Os sistemas operacionais utilizados;

Patches e service packs (se for o caso) aplicados e os aplicativos instalados.

Existem também diferentes tipos de vulnerabilidades que podem ser encontradas:

Bugs específicos dos sistemas operacionais/ aplicativos;

Fraqueza nas implementações de segurança dos sistemas operacionais/aplicativos;

Falhas nos softwares dos equipamentos de comunicações;

Fraquezas nas implementações de segurança dos equipamentos de comunicação;

Fraqueza de segurança/falhas nos scripts que executam nos servidores web;

Falhas nas implementações de segurança nos compartilhamentos de rede entre os sistemas e pastas de arquivos.

Ferramentas para análise de Vulnerabilidades de segurança

Existem vários softwares para detectar vulnerabilidades e a cada dia com o avanço das tecnologias surgem novas versões e novos produtos. Clique aqui e veja alguns exemplos? http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/doc02_aula03_GSI.pdf

Além da análise de vulnerabilidade também é muito importante que o profissional de TI periodicamente realize uma pesquisa de vulnerabilidade sobre os produtos ou aplicações utilizados em sua organização.

O que é pesquisa de vulnerabilidade?

Significa descobrir as falhas e deficiências em um produto ou aplicação que podem comprometer a segurança. Quando um atacante encontra uma vulnerabilidade em um produto ou aplicação, ele tenta explorá-la.

Porque é importante realizar uma pesquisa de vulnerabilidade?

Por que auxilia os profissionais de segurança a:

Identificar e corrigir vulnerabilidades de rede;

Proteger a rede de ser atacada por invasores;

Obter informações que auxiliam a prevenir os problemas de segurança;

Obter informações sobre vírus;

Conhecer as fragilidades de redes de computadores;

Conhecer os alertas de segurança antes de um ataque de rede;

Conhecer como recuperar uma rede após um ataque.

Em 2010 uma importante empresa do ramo de segurança publicou em relatório com as 10 empresas cujos produtos apresentaram uma maior quantidade de problemas de vulnerabilidades.

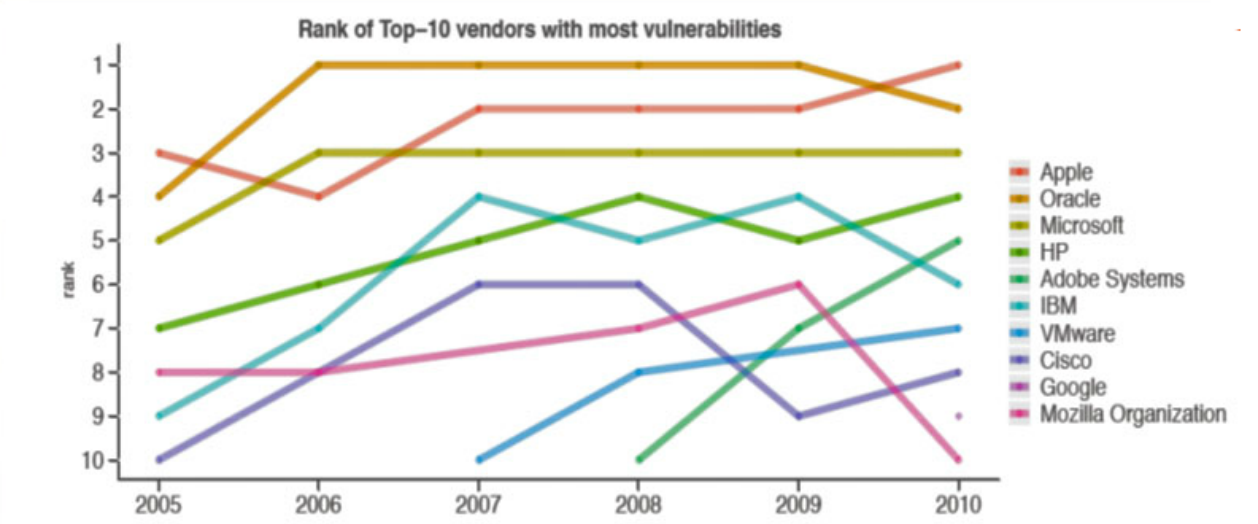


Figure 2 Ranking of the Top-10 vendors with most vulnerabilities per year. Oracle includes also vulnerabilities from Sun Microsystems and BEA logic.

Você sabia?

Você sabe o que é um exploit?

Um exploit, em segurança da informação, é um programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional como o próprio sistema operacional ou serviços de interação de protocolos (ex: servidores Web). São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas. Fonte: http://pt.wikipedia.org/wiki/Exploit

O que vem na próxima aula

Na próxima aula, aprenderemos o seguinte tema: Ameaça aos sistemas de informação

•Assunto 1: Introdução às ameaças de segurança.

•Assunto 2: Principais tipos de ameaças.

•Assunto 3: Ameaças ativas x passivas.

CONCLUSÃO

Nesta aula, você:

- Compreendeu o conceito básico sobre vulnerabilidade.
- Conheceu os principais tipos de vulnerabilidades.
- Conheceu as principais ferramentas para análise de vulnerabilidade...