Segurança em Sistemas de Informação

Aula 03

Prof. Luis Gonzaga de Paulo

CONVERSA INICIAL

Olá, seja bem-vindo(a) à Aula 3 de Segurança em Sistemas de Informação. Nosso objetivo, neste encontro, é apresentar a aplicação de métodos, técnicas e ferramentas que visam prover a segurança da informação e dos sistemas. Para tanto, vamos precisar conhecer, avaliar e aplicar os mecanismos e as ferramentas de gerenciamento de identidade e acesso, a infraestrutura da segurança, o tratamento de incidentes, a segurança das redes de computadores e no desenvolvimento de software.

A necessidade de prover a segurança da informação e dos sistemas é indissociável do conjunto de responsabilidades de todos os profissionais envolvidos com a tecnologia da informação nas organizações. A segurança da informação e dos sistemas não admite iniciativas isoladas ou parciais, bem como requer meios conhecidos e adequados ao grau de proteção desejado pela organização. O principal ator deste complexo cenário é o indivíduo, em qualquer papel que desempenhe dentro da organização. Entretanto existe um vasto ferramental que viabiliza e complementa qualquer ação no sentido de prover a segurança. O objeto de estudo desta aula é o conhecimento destes meios e o ambiente no qual são empregados, bem como o resultado esperado de seu uso correto.

Saiba Mais

Navegar é preciso: http://www.antispam.br/videos/#a1

Os invasores: http://www.antispam.br/videos/#a2

Spam: http://www.antispam.br/videos/#a3

A defesa: http://www.antispam.br/videos/#a4

CONTEXTUALIZANDO

Para prover a segurança da informação e dos sistemas em uma organização é necessário conhecer os riscos e as vulnerabilidades, planejar a maneira de enfrentá-los e, então, prover os meios para tornar efetiva a segurança da informação e dos sistemas. No complexo ambiente computacional das organizações, acrescido da vasta conectividade posta à disposição, é de primordial importância conhecer tais meios e adequá-los à necessidade da organização e de seus negócios.

Antes de partirmos para os conteúdos desta aula, que tal pesquisar um pouco? Estude o capítulo 1 e também os capítulos 15 até 20 do livro **Criptografia e Segurança de Redes – Princípios e Práticas**, da bibliografia básica da disciplina.

Também é importante que, a partir de agora, você pesquise o tema “Ferramentas de Segurança da Informação” na internet, leia os artigos e textos disponibilizados em “Materiais complementares” das aulas no UNIVIRTUS e assista os vídeos recomendados. Exponha suas conclusões, opiniões e dúvidas nos fóruns da disciplina no AVA, compartilhando e discutindo os assuntos com seus colegas.

Tema 1 - Gerenciamento de Identidade e Acesso

O controle de identidade é imprescindível para a segurança da informação e dos sistemas, e requer um tratamento especial. Diferentemente do ambiente natural, no mundo digital, a simulação de perfis ou identidades é algo relativamente simples, exigindo muito dos dispositivos e das técnicas de controle, pois são estes controles que garantirão a autorização e a autenticidade das operações, além do não repúdio. Além desta garantia, tais controles de também têm que resistir ao roubo de identidades, evitando que agentes ou usuários mal-intencionados possam simular ou passar-se por alguém devidamente autorizado, e assim realizar operações fraudulentas.

Os controles de acesso geralmente operam em conjunto com os controles de verificação para estabelecer a devida autorização e garantir a autenticidade das operações. A maioria dos sistemas baseia-se no conjunto identificação (ID) e senha (PASSWORD), porém para muitas operações críticas e o uso de informações sensíveis estes controles não são suficientes. Controles biométricos, certificados digitais e assinaturas eletrônicas complementam esses controles, e cada vez mais é necessário o uso de técnicas e mecanismos que garantam a identidade dos agentes, mas que, ao mesmo tempo, permitam a independência do ambiente, a flexibilidade e a interatividade com diversas tecnologias e funcionalidades, além de um desempenho elevado em um mundo extremamente veloz e cada vez mais conectado.

O processo de identidade e autorização é parte importante da proteção, especialmente no que diz respeito à autenticação do usuário remoto – aquele que pleiteia o acesso à rede, aos recursos computacionais e à informação, estando fora do perímetro de segurança da organização. O processo de identificação precisa ser completado com a verificação, com base em algo que o indivíduo:

- **sabe** – sua identidade (PIN: Personal Identification Number) e as senhas
- **possui** – um token, chave criptográfica ou física, ou um smart card
- **é** – biometria estática, como a digital ou a íris
- **faz** – a biometria dinâmica, como o padrão de voz, caligrafia e taxa de digitação

Tema 2 - Infraestrutura de Segurança da Informação e de Sistemas

A infraestrutura de segurança da informação está diretamente ligada à infraestrutura que suporta a informação em si, quer sejam os computadores e os componentes das redes de computadores, e determinadas funções destes dispositivos acabam mesclando-se. Entretanto, alguns dispositivos desta infraestrutura têm funções claramente definidas, como os proxies, os firewalls e os detectores de intrusão.

Antivírus e outros softwares de defesa dos computadores

Os softwares de defesa são aqueles responsáveis por buscar evitar a ação de malwares em computadores ou dispositivos computacionais como smartphones ou tablets. Sua função é monitorar o uso dos recursos para identificar e inibir ações indesejadas ou danosas à informação e aos sistemas, combatendo as ameaças e reduzindo a vulnerabilidade destes ambientes. Muitas vezes, tais softwares incluem um conjunto de funcionalidades como personal firewall, combate ao spam, ao keylogging e ao pishing, entre outras diversas funcionalidades.

Proxy

São conjuntos, dispositivos ou appliances (software mais hardware) – também chamados de servidor proxy – que funcionam como intermediários entre usuários de uma rede interna e outra externa – normalmente a internet – executando operações de autenticação e identificação, filtragem de informações, log de acessos e tradução de endereços internos para externos, função conhecida como NAT (Network Address Translation).

O proxy atua na camada 7 (Aplicação do modelo OSI). Sua principal função, de tradução de endereços, é uma medida de segurança que impede a identificação de endereços da rede interna aos elementos da rede externa. Esta função pode ser executada de várias formas, entre as quais:

- **Configuração estática** – endereço interno X endereço externo
- **Ocultação de endereços** – endereço externo único X endereços internos diversos
- **Tradução das portas** – porta externa X porta interna, host ou serviço

Firewall

São conjuntos, dispositivos ou appliances (software ou hardware mais software) que controlam o fluxo de informações entre a rede de computadores interna da organização – geralmente considerada como um ambiente conhecido e seguro – e a rede externa, geralmente considerada como um ambiente desconhecido e inseguro. Os proxies e os firewalls também servem de apoio à implementação da política de segurança da informação, permitido a aplicação de regras dessa política ao tráfego de informação pela rede da empresa e para fora dela. O funcionamento de um firewall é semelhante ao de um roteador. Os tipos de firewalls mais empregados podem ser classificados em:

- **Filtros de pacotes** – que são os mais simples, atuam na camada 3 do modelo OSI (rede) e analisa e filtra os endereços IP

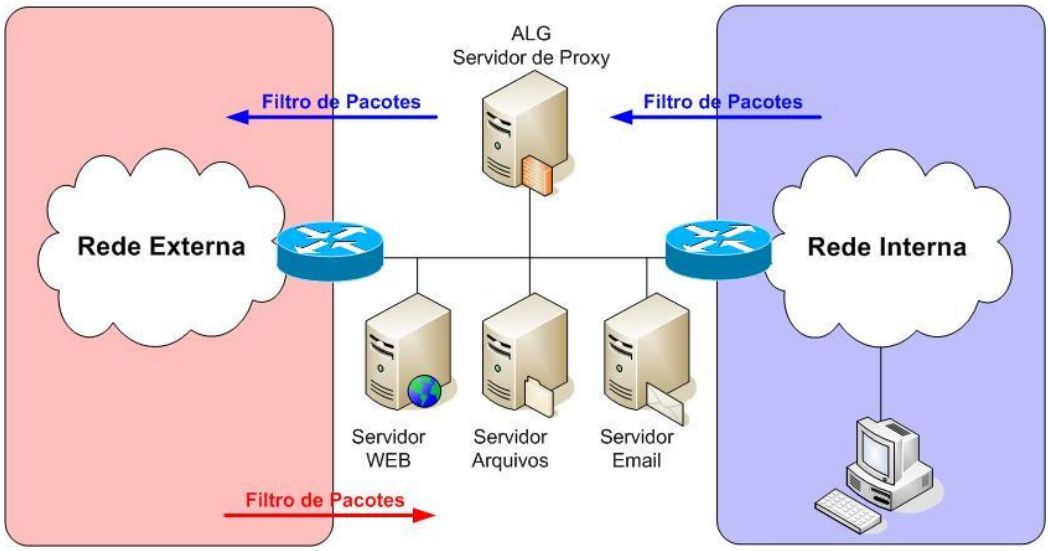
- **Stateful Inspection** – que analisa os pacotes até a camada 4 do modelo OSI, e também controla as conexões

- **Application Proxy Gateway** – que exige a autenticação, atua na camada 7 do modelo OSI, e analisa as solicitações da aplicação

Por meio do uso dos firewalls é possível criar e administrar ambientes distintos nas redes de dados da organização, tais como:

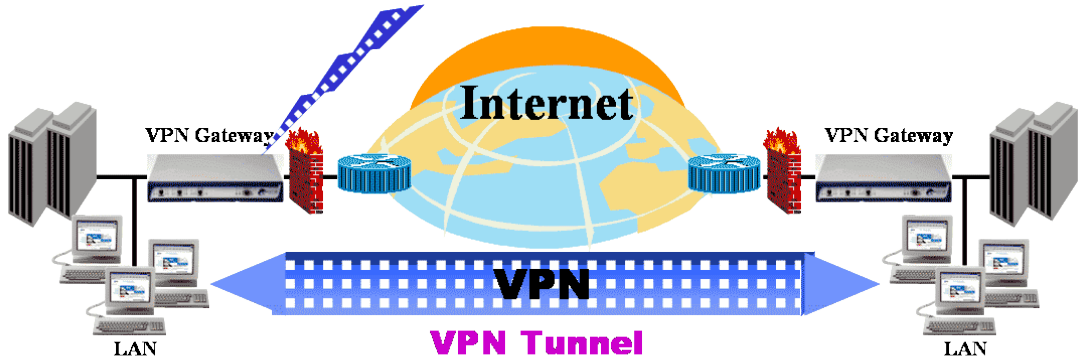
- **DMZ (Demilitarized Zone)** – um ambiente que segrega os recursos de rede e as informações, permitindo o compartilhamento seguro destes recursos
- **VPN (Virtual Private Network)** – usuários remotos e extranets

A figura a seguir apresenta uma visão de uma DMZ, com um firewall do tipo filtro de pacotes:

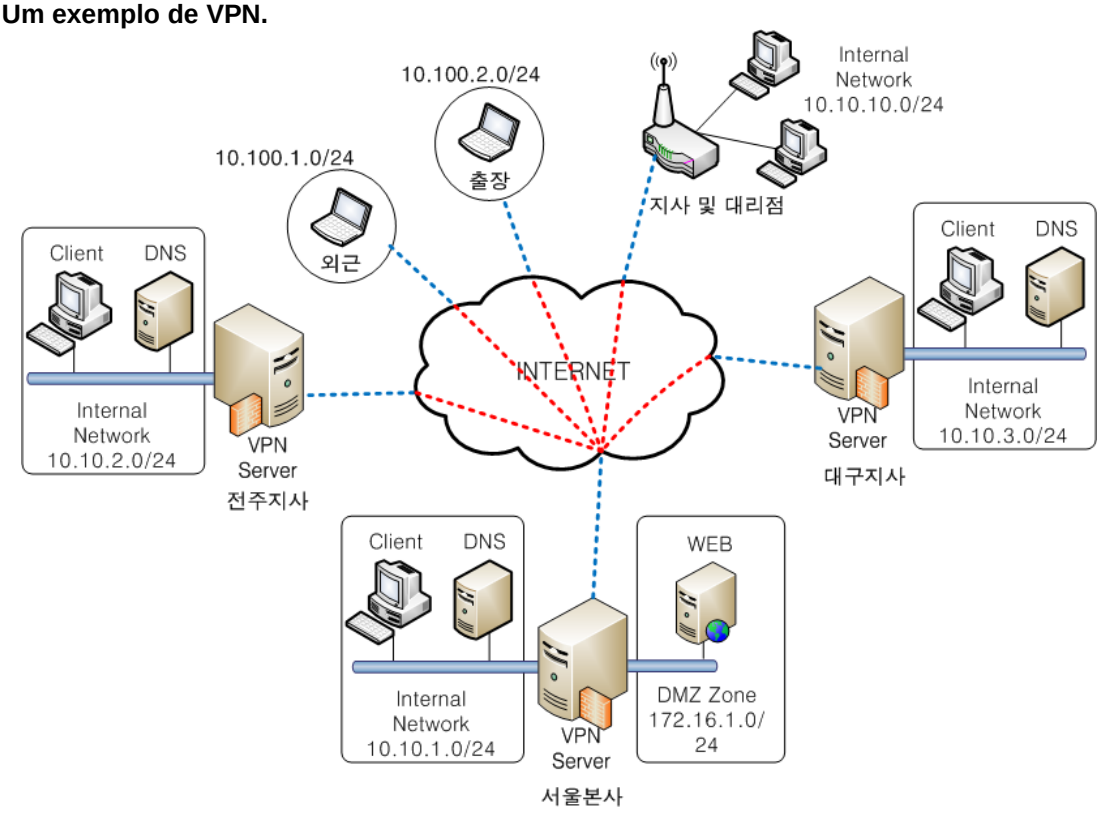


As **regras do firewall** determinam o modo como será analisado e filtrado o tráfego de dados que passa por ele. Devido a esta atividade, o firewall é um gargalo, isto é, um ponto de estrangulamento do tráfego de rede, que gera impacto no desempenho e na velocidade do tráfego de rede. As figuras a seguir apresentam os detalhes de uma Virtual Privative Network, que possibilita o uso da internet para estender o alcance da rede interna da organização.

A estrutura e os elementos da VPN.



Um exemplo de VPN.

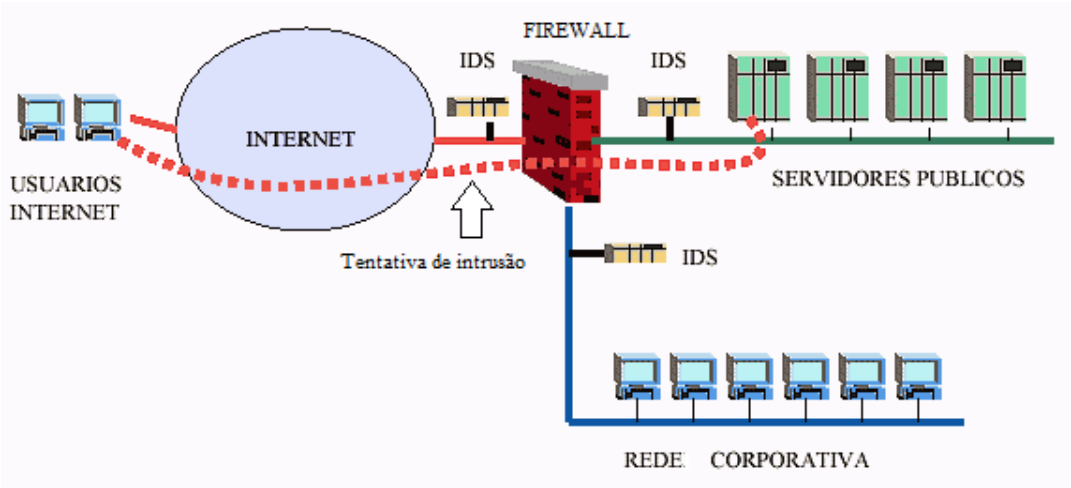


IDS – Intrusion Detection System

Os sistemas de detecção de intrusão ou IDS (Intrusion Detection System) são dispositivos que analisam o uso e o tráfego de informações nas redes, buscando identificar desvios de comportamento ou anomalias que possam sinalizar falhas ou tentativas de fraudes. Estes dispositivos não atuam diretamente na proteção, porém, em conjunto com proxies e firewalls, podem aumentar a efetividade desses, além de prover informações para os administradores de rede e de segurança e possibilitarem a adequação de regras e da política de segurança da informação das organizações.

O IDS é uma ferramenta para detectar, notificar e prevenir acessos não autorizados, tentativas ou ataques à rede de dados da organização. Ele funciona como um sniffer, capturando e analisando informações da rede e buscando identificar evidências de uma tentativa ou ataque em andamento. O IDS pode (e deveria) atuar de forma integrada com o firewall, interagindo e ajustando as regras deste firewall de forma dinâmica, à medida que são identificadas as anormalidades.

Posicionamento do IDS na rede.



Um IDS pode ser do tipo host ou HIDS (Host IDS) ou do tipo rede, NIDS (Network IDS). Um IDS de rede é um analisador de protocolos e pode classificado nos seguintes tipos:

- **Knowledge-based** – usa uma base de dados de ataques conhecidos para identificar as tentativas de intrusão e os ataques. À medida que vai assinalando novos incidentes, vai expandindo a base de dados com as "assinaturas" dos ataques

- **Behavior-based** – aprende o padrão de comunicação de dados da rede e analisa desvios no padrão de tráfego para procurar divergências que possam representar um ataque ou tentativa de intrusão

- **Data Mining** – busca por padrões conhecidos, associações, mudanças e anomalias em um conjunto de dados ou eventos

Um IDS deve ter a capacidade de prover informações como:

- A quantidade de tentativas de ataque identificadas
- Os tipos de tentativas e ataques que foram identificados ou utilizados
- As origens destas tentativas ou ataques

Entre os diversos tipos de IDS existentes podem ser mencionados:

- **Snort** – disponível em <www.snort.org>, é um IDS de software livre, de fácil manuseio e configuração, alta confiabilidade, e de uso muito comum

- **NMAP** – disponível em <http://nmap.org>, é um conjunto de ferramentas que inclui um IDS confiável e de alto desempenho, também do modelo de software livre. É bastante robusto para os testes de firewall e identificação de assinaturas das tentativas e dos ataques, os fingerprints

- **TWWWSCAN**, um IDS e scanner de vulnerabilidades para o ambiente Windows, disponível em <https://packetstormsecurity.com>, identifica vulnerabilidades de código, fingerprints de host e endereços IP dos ataques

Os principais problemas de um IDS, além da necessidade de alta capacidade de processamento do volume do tráfego de rede, são:

- **Falsos positivos** – são processos que geram um alerta ou disparam um tratamento de exceção sem, entretanto, tratar-se de um efetivo ataque ou tentativa de intrusão

- **Falsos negativos** – pelo contrário, são ataques ou tentativas de intrusão que, por sua sofisticada elaboração ou exploração de vulnerabilidade desconhecida, passam desapercebidos pelo sistema de detecção

Tema 3 - Incidentes de Segurança da Informação

A informação é um bem, um ativo, de valor muitas vezes intangível, mas geralmente de grande valor. Na era da informação na qual vivemos, o volume de informação que produzimos, manipulamos e armazenamos é muito elevado, dada a facilidade de fazê-lo através dos meios eletrônicos. Embora a informação possa manifestar-se em diversos meios – impressa ou eletrônica, analógica ou digital, ente outros, é no modelo digital e eletrônico que tem seu expoente em termos de volume, flexibilidade e facilidade de uso e acesso. Nesse contexto, essa mesma informação está continuamente exposta a riscos de segurança, os quais atentam contra as suas características básicas:

- Confidencialidade
- Integridade
- Disponibilidade da informação

Tais riscos implicam na possibilidade da perda de valor da informação, devido a um evento provocado por uma ameaça, que pode trazer danos a estas características. Uma vez concretizado o risco, este evento ou ocorrência é então denominado incidente de segurança da informação.

Importante

Incidentes são eventos ocasionados ou provocados por incompetência, imprudência, mau uso ou uso de má fé que, explorando a existência de falhas, situações não previstas ou fraquezas de um software, ou em decorrência delas – as vulnerabilidades, causam o uso indevido do sistema ou das informações tratadas pelo mesmo.

Os incidentes de segurança da informação mais conhecidos estão associados ao acesso, à modificação ou divulgação da informação sem o consentimento dos seus proprietários ou gestores, além da violação de regras e políticas das organizações. Entretanto, os erros e as falhas dos sistemas computacionais de qualquer porte, a indisponibilidade ou a má qualidade de serviços cuja finalidade é prover a informação – como uma conexão à internet ou até mesmo uma chamada telefônica – também podem configurar um incidente de segurança da informação.

Sob um ponto de vista abrangente, os incidentes de segurança da informação incluem, além de tentativas e ações nitidamente fraudulentas ou criminosas, o baixo desempenho, as falhas e os erros dos sistemas computacionais em geral, pois tais eventos tornam indisponível ou invalidam a informação necessária à uma atividade ou tarefa.

Atenção

A qualidade dos processos ou serviços cuja finalidade é prover a informação, também pode afetar as características da segurança da informação e expor as informações a riscos ou depreciação de seu valor, tornando-a até mesmo inútil.

Faltas, erros e falhas

Quando se considera um ambiente computacional, o uso da informação depende de um conjunto de componentes e funcionalidades que interagem entre si, com o usuário, com o próprio ambiente computacional no qual estes operam – hardware, sistema operacional, redes e programas de aplicação ou software – e, portanto, é dependente do comportamento e do correto funcionamento de todo este complexo sistema. Qualquer anomalia no funcionamento ou comportamento de um ou mais desses elementos pode causar problemas, transformando-se em um incidente de segurança da informação.

- **Anomalia de origem intencional**: causada por um agente malicioso
- **Anomalia de origem acidental**: causada por falhas físicas, de projeto ou decorrente do uso inadequado

Importante

Um software ou sistema computacional deve prover um serviço ao usuário através de suas interfaces – sendo a parte perceptível ao usuário decorrente da interface externa do sistema, e o restante decorrente de suas interfaces internas. Esses serviços são ameaçados por falhas, erros e faltas.

Segundo Avizienis (2004), um serviço provido pelo software ou sistema pode falhar por não atender a especificação funcional ou porque essa especificação não reflete corretamente a necessidade do usuário, levando o serviço de seu estado correto para um estado incorreto – ou indisponibilidade – para o qual deverá ser providenciada uma recuperação.

Esse desvio ou mudança de estado – de correto para incorreto – é denominado erro, e a causa do erro é uma falta. Ou seja, um erro é uma parte dos estados do sistema que pode levar a uma falha no serviço prestado por esse sistema, isto é, uma falha ativa. Entretanto, alguns erros podem não ocasionar uma falha de imediato ou na sequência das operações de determinada funcionalidade, redundando em uma falta dormente ou inativa.

As falhas também podem resultar em uma degradação do serviço prestado, com redução do desempenho, inexatidão ou entrega parcial dos serviços, ou seja, em uma falha parcial que não comprometa todo o sistema, fazendo-o operar de forma mais demorada, em regime parcial, limitado ou de emergência. Considerando a ameaça representada por tais desvios, é necessário empregar todos os meios possíveis para mitigar/atenuar os riscos que elas representam, buscando a confiabilidade do sistema. Os meios para atingir a confiabilidade necessária aos sistemas podem ser agrupados em:

- Prevenção de falhas, isto é, as formas de prevenir as ocorrências ou a introdução de falhas
- Tolerância a falhas, ou seja, evitar a falha dos serviços mesmo na ocorrência de falhas no sistema
- Remoção de falhas, o que significa reduzir o número e a gravidade das falhas

Importante

A garantia da confiabilidade é a manutenção da previsibilidade do comportamento do software ou do sistema como um todo, de modo que, dadas as condições estabelecidas no projeto, os resultados esperados sejam apresentados.

Ameaças, ataques e malwares

As ameaças estão presentes em todo o ciclo de vida da informação, desde sua geração até o descarte. Em se tratando de sistemas computacionais que suportam a informação, as ameaças permeiam todo o ciclo de vida dos sistemas, desde a concepção e o projeto de desenvolvimento do software até o momento de desativação do mesmo.

Parte dessas ameaças, como já visto, podem ser decorrentes de faltas, erros e falhas de causa não humana e/ou não intencional, mas existem ameaças causadas intencionalmente e por agentes humanos – os ataques – comandados por indivíduos mal-intencionados e com propósitos ruins, os quais, explorando fraquezas, falhas de projeto ou falta de proteção adequada, interferem no funcionamento dos sistemas e provocam danos às informações ou serviços providos por estes.

Boa parte destes ataques fazem uso dos softwares maliciosos – os malwares (do Inglês *malicious software*) – para conseguir seus objetivos. Este tipo de software recebe diversas denominações em função de suas características e propósitos, como as estabelecidas por Lapolla (2013), a saber:

- **Vírus** – uma sequência de código cuja finalidade é reproduzir-se em áreas importantes dos dispositivos de armazenamento (unidades de disco, pendrives, memory cards, etc.) ou anexando-se a programas e arquivos

- **Worms (vermes)** – programas que se propagam através de cópias de si próprios para os dispositivos de armazenamento através das redes, sem, a princípio, contaminar programas e arquivos

- **Trojans, (cavalos de Tróia)** – uma forma de software com alguma funcionalidade específica e interessante, como, por exemplo, a recuperação de senha de programas ou arquivos protegidos, a conversão de formatos de arquivos de dados ou a geração de números de licença para software licenciado, e que traz em seu código funcionalidades maliciosas, com o intuito de explorar as vulnerabilidades

- **Rootkits** – códigos maliciosos que normalmente infectam o sistema operacional, com o intuito de ocultar operações que demonstram a contaminação, por vírus ou cavalos de Tróia, por exemplo; desabilitar ou superar uma contramedida ou defesa, como antivírus ou firewalls; e

-

permitir que um usuário mal-intencionado tenha acesso ou mesmo controle o dispositivo infectado

- **Botnets (de Robot Network)** – agentes de software autônomos e automáticos, cuja finalidade é colocar os dispositivos contaminados a serviço de um controlador, formando, assim, uma rede de zumbis prontos para executar tarefas como o envio de spam ou ataques de DoS

- **Spywares** – programas que recolhem informações fornecidas pelo usuário e sobre o uso que este faz do seu equipamento e as transmite a uma entidade externa, geralmente na internet. Estas informações são usadas posteriormente para burlar sistemas de autenticação e verificação de identidade ou como base para trabalhos de engenharia social, com o intuito de possibilitar operações fraudulentas baseadas em falsidade ideológica

- **Exploits** – programas ou trechos de código que buscam explorar vulnerabilidades ou falhas de ambientes computacionais, geralmente dos sistemas operacionais, recentemente descobertas para conseguir acesso privilegiado aos sistemas

- **RiskTools ou Riskware** – programas ou funcionalidades de programas, cujo intuito é avaliar vulnerabilidades do ambiente computacional para, então, comunicá-las à sua fonte, possibilitando assim a exploração dessas vulnerabilidades de forma mais efetiva. Seu modo de atuação se assemelha aos Trojans, com a diferença que trazem, geralmente, um apelo à elevação da segurança do ambiente, promovendo falsas notificações de ameaças ou falhas como reforço para a sua instalação

- **Adwares** – programas ou funcionalidades de programas, normalmente shareware, que apresentam anúncios de versões mais completas ou outros produtos do fabricante e, muitas vezes, obtêm informações sobre o usuário e o ambiente computacional, e as enviam, sem o consentimento

ou conhecimento do mesmo, para uma base de dados remota, com o intuito de avaliar o perfil e o possível interesse do usuário

Importante

De uma maneira em geral o termo vírus de computador é usado pela mídia e pelo público como sinônimo de malware, representando qualquer software, programa ou agente que interfere no funcionamento de um software com o propósito de modificar seu funcionamento e obter algum proveito desta modificação.

Vulnerabilidades

As falhas decorrentes da interação – ou as operacionais – ocorrem durante o uso do sistema e em função da interação deste com o ambiente e com os usuários; de problemas na configuração ou da mudança de parâmetros operacionais; da instalação; da manutenção ou atualização do sistema. Geralmente, essas falhas ocorrem devido a uma vulnerabilidade, isto é, uma falha interna que possibilita a um agente externo, geralmente malicioso, atingir o sistema.

As vulnerabilidades podem ser de desenvolvimento ou operacionais. Elas podem ser maliciosas ou não, tal como podem ser os agentes que as exploram. Nesse aspecto, existem semelhanças interessantes e óbvias entre uma tentativa de intrusão e uma falha externa física que explora (*exploits*) uma vulnerabilidade – que também pode ser resultado de uma falha de desenvolvimento deliberado, por questões de redução de custo ou por questão de usabilidade, resultando em uma proteção limitada ou mesmo na ausência total de proteção.

Importante

As falhas físicas estão mais diretamente relacionadas a aspectos ambientais que interferem no hardware, tais como interferência eletromagnética, ruídos e

problemas da alimentação elétrica ou de temperatura de operação e, de certo modo, podem ser também consideradas como vulnerabilidades.

Mobilidade, flexibilidade, capacidade de personalização, conectividade, convergência de tecnologias e capacidades reduzidas de armazenamento, bem como processamento de informações, são algumas características de dispositivos e ambientes computacionais que favorecem as vulnerabilidades.

Reflita: dispositivos de computação móvel, como smartphones e tablets, são mais vulneráveis devido às suas características?

Tema 4 - Segurança de Redes

A aplicação de meios para prover a segurança da informação e dos sistemas tem ênfase especial nos processos de comunicação que faz uso das redes de computador. Ao percorrer os dispositivos e canais de comunicação que compõem a rede, a informação torna-se ainda mais vulnerável, necessitando de proteção adicional que, entretanto, tenha o mínimo de impacto na velocidade e na qualidade da comunicação.

A segurança na rede começa com o processo de identificação e autorização, que provê o controle de acesso à rede. Neste processo, é necessário que o requisitante de acesso (AR) seja submetido a um serviço de aplicação de políticas de segurança, que determina o tipo de acesso a ser concedido. Uma vez estabelecido o conjunto de regras a ser aplicado ao acesso, um outro serviço irá prover acesso e controle aos recursos requisitados e devidamente concedidos. Dentre os recursos usados neste processo estão o Kerberos e o Radius.

O **Kerberos** é um protocolo de rede criado pelo MIT para a comunicação individual segura e devidamente identificada, que utiliza criptografia simétrica. O **Radius** (Remote Authentication Dial In User Service) é um protocolo de rede destinado a centralizar os serviços de autenticação, autorização e contabilização de acessos, para controlar os computadores que se conectarão e usarão um determinado serviço de rede.

O meio de comunicação exige que a informação seja protegida durante o processo de transporte, o que é feito também com uso da criptografia. Como em VPN (Virtual Privative Network), o tráfego protegido por SSL, SSH e HTTPS, e o uso de certificados digitais. O SSL é um conjunto de serviços de comunicação criptográfica, que opera sobre redes TCP, de forma especial para a comunicação na web, em conjunto com navegadores e servidores web. O SSH é um protocolo de segurança simples e ágil, que permite a conexão e o logon remoto seguro. O HTTPS é uma combinação do HTTP com o SSL, utilizado para a navegação segura na internet, que inclui a autenticação e a identificação do requisitante, e a criptografia do tráfego.

Outro aspecto das redes que requer atenção especial – e, por isso, inclui um considerável arsenal de medidas de proteção – é a comunicação sem fio, as redes WiFi ou redes Wireless. Entre as medidas possíveis estão a ocultação do sinal e a criptografia da conexão e da transmissão em níveis e processos diferentes.

Com o crescente número de usuários de serviços de dados móveis, é necessário também prover a segurança neste modelo de rede, com especial cuidado aos seguintes aspectos, dentre diversas outras e crescentes funcionalidades que representam riscos à organização, que levam à adoção de políticas de controle restritivas ou até mesmo à proibição do uso de tais dispositivos:

- Não há controle de acesso físico
- Os dispositivos não são naturalmente confiáveis

- As redes de acesso não são totalmente confiáveis
- As aplicações não estão submetidas a um controle mais rigoroso e efetivo
- Há grande interação com outras plataformas (telefonia, vídeo, mensagens...)
- Os usuários podem servir-se de informações e conteúdos não confiáveis
- Uso de serviços de rastreamento e localização (GPS)

Tema 5 - Segurança no Desenvolvimento de Software

Uma abordagem bastante efetiva no sentido de prover a segurança da informação é a que adota os mecanismos de segurança desde o início do processo de desenvolvimento do software. O quão mais cedo neste processo se pensar em riscos, ameaças e formas de proteger a informação, mais efetivas e abrangentes tornam-se as medidas, além de aumentarem as opções quanto a estratégias e mecanismos de segurança a serem adotados, bem como métodos, técnicas e ferramentas auxiliares e disponíveis para o processo de desenvolvimento e redução do custo para a implementação da segurança.

A segurança no processo de desenvolvimento deve contemplar o projeto do software, o ambiente de desenvolvimento em si e a garantia da segurança quando da operação do software. Uma boa parte desta segurança é estabelecida pelos procedimentos de testes de software, os quais são frequentemente negligenciados em função de custos e prazos reduzidos, já que as etapas de testes compõem o final do processo de desenvolvimento e, geralmente, são usadas como “áreas de escape”, para compensar os atrasos dos projetos. A consequência disso é que faltas, erros e vulnerabilidades são identificadas tardiamente, quando sua correção ou eliminação torna-se muito dispendiosa ou inviável, normalmente quando o software já se encontra em operação.

Importante

A norma ISO/IEC 15.408 é um padrão internacional para o desenvolvimento de software seguro, contemplando os três aspectos citados: a segurança do software, a segurança do ambiente de desenvolvimento e a garantia de segurança do software desenvolvido.

Um modelo de desenvolvimento que tem como foco a segurança da informação e dos sistemas é o proposto por Paulo (2015): o Desenvolvimento Dirigido pela Segurança – SDD. Este modelo é baseado na proposta do BSIMM (Build Security In Maturity Model), de Verdon e McGraw (2004), e McGraw (2005), acrescentando e adequando atividades e técnicas para aprimorar a segurança da informação no SDLC (Software Development Life Cycle). O SDD leva em consideração a possibilidade de uso concomitante com qualquer modelo de desenvolvimento utilizado, o uso de ferramental simples e compatível com diversos ambientes computacionais e o mínimo impacto possível no custo, no esforço e no prazo de desenvolvimento do software.

As principais características do SDD são:

- A abordagem precoce da segurança da informação no SDLC, iniciando já no processo de levantamento de requisitos e até mesmo antes, considerando-se a necessidade de uma base de conhecimentos de ameaças e vulnerabilidades que antecede ao projeto do software

- A atuação integrada entre a equipe de desenvolvimento de software e a equipe de segurança da informação em todas as etapas do SDLC

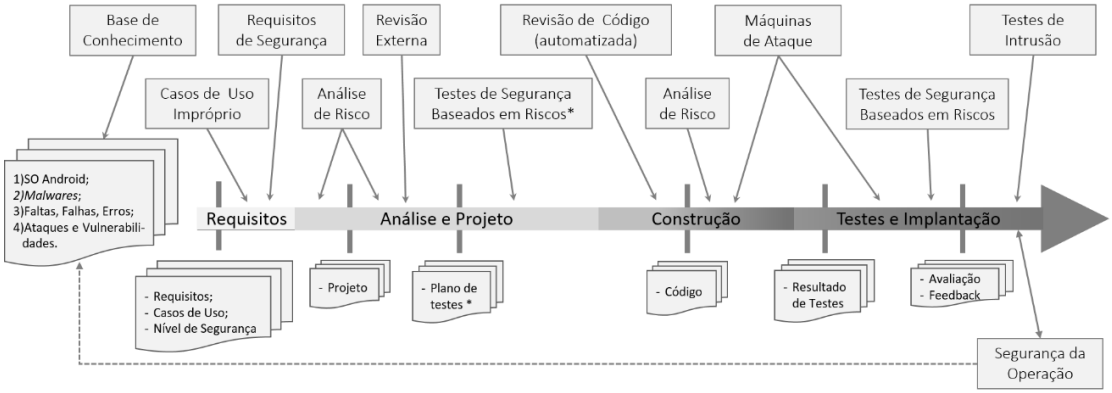
- O foco na segurança da informação no âmbito do software de aplicação e em seu uso

- A utilização dos casos de uso impróprio para fins de análise de risco, planejamento e especificação de testes

- A especificação e a construção de máquinas de ataque para a execução dos testes de segurança da informação

- A aplicação da análise de riscos em todas as etapas do SDLC, e mais especificamente nas etapas de projeto, construção e validação do software

O SDD enfrenta os principais riscos decorrentes do uso e do processo de desenvolvimento do software. Para fazer frente a esta e outras questões, a proposta do modelo SDD prioriza a segurança da informação em todo o ciclo de vida do software, desde as primeiras atividades que objetivam a caracterização da necessidade e do produto, até a sua manutenção durante o uso, como mostrado na figura a seguir:



Um importante aspecto do SDD é a sua aderência aos principais modelos adotados no SDLC, tendo como pontos de atenção a complexidade dos softwares e a avaliação do nível de segurança requerido pelo usuário. Ou seja, parte-se da premissa de que seja possível utilizar o modelo SDD no desenvolvimento de qualquer tipo de software por meio de quaisquer modelos de SDLC adotado.

TROCANDO IDEIAS

Acesse o fórum “Segurança da Informação e de Sistemas na Prática” no UNIVIRTUS e discuta com seus colegas de turma, tendo como premissa os seguintes questionamentos:

- Qual é a importância da infraestrutura na segurança da informação e dos sistemas?
- Qual é a relação de frameworks de governança, como o ITIL e o COBIT, por exemplo, no tratamento de incidentes de segurança da informação e dos sistemas?
- Qual é o impacto dos incidentes de segurança da informação nas redes e no processo de desenvolvimento?

NA PRÁTICA

- Para avaliar e aplicar seus conhecimentos, avalie nos ambientes onde você utiliza os recursos de TI (casa, transporte, trabalho, polo, comércio, lazer, etc.) quais meios de segurança da informação e de sistemas são utilizados.
- Faça um levantamento e anote os pontos que considerar importantes
- Discuta com seus colegas no fórum “Segurança da Informação e de Sistemas na Prática” e compare os levantamentos realizados por seus colegas de turma
- Proponha melhorias ou mudanças nos pontos considerados. Mas, antes, leia nas referências bibliográficas – especialmente nos livros indicados da Biblioteca Virtual – os temas relativos ao assunto, para validar e basear a sua proposta

- Apresente suas conclusões e avalie a de seus colegas no fórum “Segurança da Informação e de Sistemas na Prática” da disciplina, no ambiente virtual de aprendizagem UNIVIRTUS

- Em caso de dúvidas ou dificuldades, faça uso do canal de Tutoria do UNIVIRTUS.

SÍNTESE

Nesta aula foram abordados os temas relativos à aplicação de meios para prover a Segurança da Informação e de Sistemas nas organizações. Foram apresentados os desafios e os mecanismos de enfrentamento dos problemas, dos quais a organização e os profissionais de TI podem lançar mão para prover a segurança da informação e dos sistemas no nível requerido.

Referências

ABNT. **Segurança da Informação** – Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.

AVIZIENIS, A., *et al*. **Basic Concepts and Taxonomy of Dependable and Secure Computing**. IEEE Transactions on Dependable and Secure Computing. Vol. 1, n. 1, 2004.

GALVÃO, Michele da C. **Fundamentos em Segurança da Informação**. São Paulo: Pearson Education, 2015.

GOODRICH, Michael T. **Introdução à Segurança de Computadores**. Porto Alegre: Bookman. 2012.

LAPOLLA, M., MARTINELLI, F. e SGANDURRA, D. **A Survey on Security for Mobile Devices**. IEEE Communications Surveys & Tutorials Vol. 15, n. 1, First Quarter of 2013:446-471.

LYRA, Maurício R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MARTINS, José C. C. **Gestão de Projetos de Segurança da Informação**. São Paulo: Brasport, 2003.

McGRAW, G. **Bridging the gap between software development and information security**. IEEE Security & Privacy, September/October of 2005:75-79.

PAULO, L. G. U**m modelo complementar para aprimorar a segurança da informação no SDLC para dispositivos móveis**: SDD - security driven development. Dissertação de mestrado. UTFPR/PPGCA:2015, Curitiba/PR.

RESS, Weber. **Começando em Segurança**. MSDN - Microsoft Developer Network. 2011. Disponível em: <http://msdn.microsoft.com/pt-br/library/ff716605>. Acesso em: 16 set. 2013.

VERDON, D.; McGRAW, G. **Risk Analysis in Software Design**. IEEE Security & Privacy, May/June of 2004:32-37.