Segurança em Sistemas de Informação

Aula 04

Prof. Luis Gonzaga de Paulo

CONVERSA INICIAL

Olá, seja bem-vindo(a) à Aula 4 de Segurança em Sistemas de Informação. Nosso objetivo, neste encontro, é conhecer a abrangência das respostas aos desafios de segurança da informação e de sistemas no ambiente computacional das organizações. Para tanto, vamos precisar avaliar e entender o funcionamento das soluções de segurança da informação e de sistemas para os sistemas computacionais, os sistemas operacionais, os bancos de dados, a segurança na internet e para o comercio eletrônico.

No ambiente organizacional, é necessário conhecer os riscos, as vulnerabilidades e as necessidades do negócio que implicam em requisitos para a segurança da informação e dos sistemas. Conhecer as particularidades de cada segmento e área de TIC, e buscar soluções adequadas a estas particularidades e ao negócio, é uma missão que requer determinação e preparo. Devido à sua abrangência e à demanda de conhecimento de diversas áreas da atividade humana, a segurança da informação e dos sistemas requer preparo especial e multidisciplinar, além da colaboração e trabalho de equipe para cobrir ao máximo a ampla extensão de requisitos e componentes envolvidos.

Saiba Mais

Assista Pesquisa Global de Segurança da Informação 2014 – PwC

https://www.youtube.com/watch?v=rpeVu_hYAQ8

CONTEXTUALIZANDO

No dia a dia das organizações são requeridas ações e respostas à segurança da informação assertivas e efetivas por parte dos diversos elementos de suporte à informação. Em ambientes computacionais complexos e interdependentes, itens como os sistemas operacionais, os bancos de dados, o uso da internet e o

suporte à mobilidade e ao comercio eletrônico requerem cuidados específicos e diferenciados, exigindo conhecimento, planejamento e atuação constante.

Nesta aula, abordaremos os aspectos mais pragmáticos da segurança da informação, as necessidades especificas dos diversos componentes dos ambientes computacionais e as respostas à estas necessidades. Antes, releia o conteúdo da Unidade 2 e estude a Unidade 3 do livro **Fundamentos em Segurança da Informação**. Para tanto, acesse a Biblioteca Virtual, pelo UNICO, e pesquise pela obra:

Tema 1 - Sistemas computacionais

Um sistema computacional é um conjunto ou ambiente com dispositivos com capacidade para produzir, armazenar e transportar dados, geralmente em formato digital. Este sistema ou ambiente computacional compõe-se de hardware, software, processos e também as informações, seus usuários, a documentação e a infraestrutura de energia e comunicação necessárias a seu perfeito funcionamento. Pode ser fixo, móvel ou embarcado, e também genérico ou especialista.

Portanto, por mais simples que possa parecer, um sistema computacional envolve uma considerável complexidade, e cada um de seus componentes requer medidas de segurança distintas, que vão desde o controle de acesso físico até o uso de mecanismos de proteção sofisticados, como criptografia, certificação digital, identificação biométrica e outros, passando por fontes de energia de reserva – os no breaks ou geradores, segurança de armazenagem – os backups, redundância de comunicação e serviços de alta disponibilidade. Em determinados casos, é necessário até mesmo prover instalações ou ambientes completos em redundância, como nos data centers e sites backup.

Cada sistema computacional possui suas particularidades, quer seja em função de suas capacidades – processamento, memória, interfaces, autonomia – quer seja em função de sua constituição física ou mobilidade, e também da programação a qual é capaz de corresponder. E estas particularidades determinam e requerem proteção adequada. Dispositivos de computação móvel como os smartphones e os tablets, de uso pessoal, requerem tipos de proteção diferentes dos controladores lógicos programáveis de uma fábrica, tanto quanto notebooks e desktops requerem proteção diferenciada dos mainframes e caixas eletrônicos de um banco.

De todo modo, é possível classificar e separar os tipos de proteção necessária aos componentes do sistema computacional em grupos com características distintas, a saber:

- Acesso e ambiente físico para os quais existem os controles de identificação, acesso e transporte, proteção contra intempéries (frio, calor, umidade, luz, radiação, etc.) e fenômenos naturais (chuva, inundação, vibrações, raios, impactos, pressão, etc.)

- Fornecimento de energia, composto dos controles de qualidade (filtros de transientes e surtos ou picos de tensão), interrupção de fornecimento (nobreaks e geradores)

- Comunicação, com os controles de acesso, criptografia, autenticação, redundância, capacidade de tráfego, etc.

- Armazenamento, com os controles de acesso, capacidade, cotas de uso, compactação, redundância, cópias de segurança (backups), recuperação de dados, remoção e descarte

- Hardware, que implica em controle de temperatura, de capacidade, redundância e tolerância a falhas, manutenção preventiva e corretiva, vida útil

- Software, com os controles de registro e licenciamento, atualização e alteração (permitida ou não permitida), proteção no desenvolvimento, cópia e descarte, entre outros

Todos estes aspectos abordados implicam em questões da segurança da informação e de sistemas, com impactos na confidencialidade, integridade e disponibilidade, requerendo uma avaliação dos riscos e vulnerabilidades e o planejamento da proteção adequada a cada um, bem como o monitoramento, a atualização e a revisão constante em função dos resultados obtidos.

Tema 2 - Sistema Operacional

A segurança da informação entendida em um aspecto amplo, no qual impõe-se como condição a proteção de todos os recursos computacionais voltados para o provimento de serviços e, portanto, de informação, passa necessariamente pela segurança do sistema operacional, um dos principais componentes de praticamente todo sistema computacional. Este tópico apresenta características dos principais sistemas operacionais ora em uso, e a relação destes com os aspectos de segurança da informação.

Leitura recomendada

Segurança em Sistemas Operacionais

https://portalsis.wordpress.com/2011/06/15/seguranca-em-sistemas-operacionais/

Windows

Por ser o mais utilizado em servidores de rede, desktops, notebooks e netbooks, o sistema operacional Windows, da Microsoft, também é o mais visado em ataques e que apresenta historicamente a maior quantidade de vulnerabilidades. Embora, em sua estrutura, o Windows incorpore técnicas básicas e eficazes de autenticação, controle de acesso e auditoria, estas funcionalidades foram sendo inseridas e aprimoradas com o suceder das versões e atualizações – os patches – e deixando um histórico negativo de vulnerabilidades e incidentes de segurança que depõem contra este SO.

A iniciativa Microsoft TWC (TrustWorthy Computing), iniciada em 2002, com o objetivo de elevar a segurança, a privacidade e a confiabilidade no Windows e em seus demais produtos tem buscado, desde então, tenta reverter esse quadro.

UNIX/LINUX

O sistema operacional Unix e as suas derivações, como as diversas distribuições do Linux, por terem sido originalmente projetados para serem compartilhados – multitarefa e multiusuário – além de implementarem as técnicas de autenticação, controle de acesso e auditoria, também incorporam mecanismos de segurança mais elaborados, principalmente devido ao fato de terem sido exaustivamente utilizados em ambientes acadêmicos e de pesquisa, e terem seu uso primário voltado para o compartilhamento de recursos em servidores, o que por si só requer um grau de confiabilidade mais elevado.

Mainframes

Outros sistemas operacionais voltados para o processamento centralizado, com os produtos da IBM VSE, VM, MVS, OS/390 e z/OS têm características de projeto que reforçam a segurança da informação, uma vez que, além de proprietários e voltados para hardware específico, foram projetados e desenvolvidos para uso em computadores de grande porte – mainframes – e voltados para operações recorrentes onde a continuidade, a exigência de grande capacidade de processamento, o alto volume de operações e de dados e a elevada segurança e estabilidade são requisitos indispensáveis.

Os sistemas operacionais mobile

Os sistemas operacionais para ambientes de computação móvel são especialmente importantes para a segurança da informação nestes ambientes, uma vez que são profundamente adaptados aos recursos computacionais e à infraestrutura de serviços e funcionalidades específicas do ambiente e dos equipamentos. A seguir são apresentadas as características principais de alguns dos sistemas operacionais para ambientes de computação móvel (mobile) utilizados pelos maiores fabricantes destes equipamentos.

a) Google Android

Da mesma forma que o Microsoft Windows em computadores desktop e servidores de rede, o Google Android sofre as consequências de liderar o número de usuários no que diz respeito a ambientes de computação móvel – à exceção dos dispositivos com software embarcado. Entretanto, por ser baseado no núcleo do Linux e ser um SO de código aberto e arquitetura voltada a serviços, a evolução do Android tem apresentado significativas melhorias no que tange à segurança da informação, e as respostas às falhas e ameaças são mais eficazes e mais rápidas.

Devido à sua proeminência, o Android é objeto dos mais variados estudos e, no entanto, algumas questões cruciais ainda permanecem em aberto, como a autenticação do usuário, as permissões requeridas pelas aplicações e o tratamento de informações entre aplicações multitarefas.

b) Apple iOS

O sistema operacional iOS, em parte, devido ao fato de ser proprietário e voltado apenas para os equipamentos produzidos pela Apple, apresenta maior robustez e não é tanto explorado quanto o Android. Porém vem crescendo o surgimento de malwares para esse ambiente, bem como as iniciativas da própria Apple para fazer frente a essas questões. Um exemplo desse esforço é a arquitetura do iOS, que provê APIs de segurança na camada Core Services e a evolução dos security services na versão iOS 7.

c) Microsoft Windows Phone

O Windows Phone, sistema operacional da Microsoft para computação móvel, é o sucessor do Windows CE e do Windows Mobile e faz parte da unificação promovida pela Microsoft quanto à arquitetura e a apresentação dos seus sistemas operacionais. A necessidade de controle das aplicações desenvolvidas por terceiros é uma iniciativa que tem por objetivo a segurança da informação, uma vez que exige a homologação das aplicações antes da distribuição pela Microsoft.

Por outro lado, a integração total com os produtos do pacote Office – Office 365 – e serviços Microsoft na nuvem também reforçam o domínio da Microsoft e objetivam prover segurança através da segregação.

d) Nokia Symbian

Desenvolvido orginalmente pela Symbian Ltd. e posteriormente incorporado pelo consórcio entre as fabricantes Nokia, Sony Ericsson e a operadora NTT DoCoMo, o sistema operacional Symbian é atualmente suportado pela

Accenture, e voltado para os equipamentos da Nokia e da Sony-Ericsson. Sua arquitetura específica dificultou a existência de ataques no princípio de seu uso, porém o fato de ser de código parcialmente aberto – algumas interfaces são proprietárias – e de ter sido o primeiro SO para sistemas de computação móvel com interface gráfica logo chamou a atenção, tendo sido vítima do primeiro ataque por um worm – o Cabir – ocorrido em 2004.

Tema 3 - Banco de dados

Em uma definição simplificada, um banco de dados é um conjunto organizado de dados com características comuns, que tem por objetivo possibilitar o armazenamento, a recuperação e a modificação da maneira mais rápida possível e, obviamente, preservar estes dados de maneira confiável e segura. Para que a segurança da informação seja obtida, um sistema gerenciador de banco de dados – SGBD – e seus mecanismos e componentes devem prover a segurança por meio de controle de acesso e permissões, registro de atividades e histórico de modificações – o log – e a preservação por meio de cópias de segurança – os backups e redundância.

Parece algo simples e trivial, mas não é. Com o advento das redes e a comunicação entre os computadores e dispositivos de computação, o volume de dados produzido, acessado e armazenado pelas pessoas e organizações atinge números astronômicos, com um crescimento exponencial. Além disso, os bancos de dados passaram a responder pelo armazenamento de outros tipos de dados que não somente textos e números, mas também multimídia – voz, imagens e filmes, cujo volume de dados é de extrema grandeza.

Para fazer frente a esta demanda, surgiram inicialmente os data centers – motivados pela crescente necessidade de processamento e armazenagem e favorecidos pela comunicação provida pela internet. Na sequência veio a nuvem – o cloud computing – uma promessa de capacidade inesgotável de

processamento e armazenagem. Juntamente com esta evolução outros serviços vinculados aos bancos de dados, como o Data Warehouse – DW, o Business Inteligence – BI e o Big Data passaram a fazer parte do cotidiano das pessoas e das organizações.

Embora muitas destas evoluções incorporem mecanismos e soluções de segurança da informação e dos sistemas que a sustenta, o fato é que também representam novos riscos, que são acrescentados àqueles aos quais a organização e as pessoas já estão expostas e que demandam novas abordagens para prover a segurança necessária.

Leitura recomendada

Cloud computing e a segurança

http://computerworld.com.br/cloud-computing-e-seguranca-como-coisas-funcionam-30-mil-pes

Tema 4 - Segurança na Internet

Leitura recomendada

Segurança na Web: Uma janela de oportunidades

https://www.owasp.org/images/1/16/Seguranca_na_web_-_uma_janela_de_oportunidades.pdf

A internet é, indubitavelmente, no advento da era da informação, o item de maior importância, podendo até mesmo ser considerada como a alavanca para o processo de globalização. Porém a internet também é uma “terra sem lei”, onde a liberdade criativa e de informação dá margem para a ação de criminosos e irresponsáveis de toda ordem.

E é imprescindível que sejam adotadas medidas de proteção que permitam o uso de acordo com o necessário sem, entretanto, expor ao risco as pessoas e as organizações que dela fazem uso.

Vídeos recomendados

Internet revelada: https://www.youtube.com/watch?v=NUPjk-wtWhQ

Navegar é preciso: https://www.youtube.com/watch?v=YjsuyXgxgtg

Invasores: https://www.youtube.com/watch?v=DyirFu77F9Y

Spam: https://www.youtube.com/watch?v=6pBoJhryp0Q

A defesa: https://www.youtube.com/watch?v=L1goq_YEwSQ

Tanto para os indivíduos como para as organizações, os perigos são inúmeros: invasões, depredação, roubo de informações e identidades, spam, invasão de privacidade, pedofilia e pornografia, calúnia, injúria e difamação. Enfim, um universo de ilegalidades e imoralidades pode apoderar-se dos recursos computacionais pelo simples fato de conectar-se à internet e dela fazer uso. Felizmente, existem mecanismos e soluções que reforçam a segurança da informação e dos sistemas que são utilizados, como já vimos no estudo de proxies, firewalls e antivírus, além de VPNs, certificação digital e assinatura eletrônica, criptografia e outros.

É fato que a segurança da informação e dos sistemas que fazem uso da internet está ligada à segurança das redes – locais e de longa distância. Os diversos serviços colocados à disposição, entre eles o correio eletrônico – o e-mail, as redes sociais, os serviços de mensagem instantânea e os serviços de comércio eletrônico dependem da infraestrutura de rede e de recursos como:

- **IP Security ou IPSec**, conjunto de protocolos desenvolvido pelo IETF – Internet Engineering Task Force, que visa oferecer segurança para pacotes de dados na rede, provendo confidencialidade e autenticação no protocolo padrão da internet, o IP;

- **Secure Sockets Layer e Transport Layer Security, ou SSL/TLS**, protocolos que oferecem segurança ponto a ponto para aplicações que necessitam segurança na camada de transporte de dados do protocolo padrão da internet, o TCP;

- **Pretty Good Privacy ou PGP**, um dos protocolos utilizados para a autenticação e privacidade das informações na camada de aplicações quando não há o estabelecimento de sessões de troca de informações, como é o caso dos e-mails;

- **Virtual Privative Network ou VPN**, uma rede virtual ou uma rede criptografada dentro da internet, que oferece comunicação segura ponto a ponto por meio da internet;

- **Firewalls**, são computadores ou roteadores interpostos entre a rede local e a internet – ou a rede interna da organização e a rede externa – para filtrar a comunicação e aplicar as regras da política de segurança da organização, visando proteger e controlar o acesso a sistemas e informações.

Mas não se pode resumir a segurança da informação em ambiente de internet à mecanismos e soluções de defesa: é necessário que sejam adotadas iniciativas proativas, como a educação e o treinamento, o uso responsável e consciente dos recursos e a correta aplicação da política de segurança da informação.

Tema 5 - Comércio eletrônico

O modo como as pessoas e as organizações fazem seus negócios estão constantemente mudando e evoluindo, chegando no presente aos negócios feitos por meio da comunicação eletrônica e dos computadores, conhecido como e-commerce. O comércio eletrônico ou suas operações não estão restritas à internet, pois existem outras soluções, como o uso de bancos e cartões, compras e negociações feitas por terminais e dispositivos específicos. Com o avanço das comunicações e da tecnologia, foram sendo aperfeiçoadas as formas deste tipo de comércio e diferenciando-se em vista dos agentes e da finalidade, criando os seguintes modelos:

- **B2C** – Business to Consumer, que é o tradicional comércio pela internet, no qual clientes adquirem seus produtos diretamente de fabricantes, distribuidores e revendedores.

- Existe também o processo de negociação entre indivíduos, o **C2C** – Customer to Customer, por meio dos sites de compra, venda e troca.

- Já as organizações, realizam operações entre si por meio do **B2B** – Business to Business, como as operações financeiras, de logística e suprimentos, por exemplo.

Importante

Outro exemplo é o oferecido pelos serviços de Governo Eletrônico, que possibilita o relacionamento dos cidadãos e das organizações com o Governo. Também se enquadram neste modelo os serviços de banco eletrônico, o internet banking ou e-Banking.

Neste ambiente, a privacidade, a identidade, a autenticidade e o não repúdio são aspectos de suma importância, além de confidencialidade, integridade e disponibilidade da informação. Com o crescimento do volume de negócios e a adesão cada vez maior de pessoas e organizações, o crime organizado tem cada

vez mais se tornado presente neste ambiente, e o ferramental de proteção mencionado anteriormente, por si só, já não basta, pois o comportamento humano é fator essencial para que as defesas e a proteção sejam efetivas.

Outro aspecto de suma importância é a segurança do sistema, que deve compreender defesas e proteção contra as diversas formas de ataque e vulnerabilidades conhecidas. Para tanto é recomendável que as equipes de desenvolvimento de software trabalhem em conjunto com os especialistas em rede e segurança, recebendo as informações sobre riscos e vulnerabilidades e tratando os requisitos de segurança no software em tempo de construção.

Leitura recomendada

OWASP Top Ten Project (Português)

https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf

TROCANDO IDEIAS

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

- Quais são os problemas de segurança da informação mais conhecidos ou divulgados pela mídia?
- Qual é o impacto destes problemas na opinião pública e nos negócios?

NA PRÁTICA

Para avaliar e aplicar seus conhecimentos, busque na mídia notícias recentes sobre problemas de segurança, avalie e discuta com seus colegas:

1. Quais foram as vulnerabilidades e os riscos que levaram à ocorrência?

2. Proponha soluções para os problemas identificados.
3. Leia nas Referências – especialmente nos livros indicados da Biblioteca Virtual – os temas relativos ao assunto, para embasar sua proposta.
4. Discuta com seus colegas no Fórum “Segurança na Prática”, no AVA UNIVIRTUS, e compare com os estudos dos demais.
5. Em caso de dúvidas ou dificuldades, faça uso do canal de Tutoria do AVA UNIVIRTUS.

SÍNTESE

Nesta aula foram abordados os temas relativos à aplicação prática da Segurança da Informação e de Sistemas nas organizações, fazendo uso dos recursos e soluções técnicas disponíveis para os diversos componentes dos sistemas computacionais, incluindo o sistema operacional, a rede, o banco de dados, a internet e os serviços de comércio eletrônico.

Referências

STALLINGS, W. **Criptografia e segurança de redes**. 6 ed. São Paulo: Pearson Education, 2014.

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

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

TANENBAUM, A. S.; WETHERAL, D. **Redes de Computadores**, 5 ed. São Paulo: Pearson Education, 2013.

TANENBAUM, A. S. **Sistemas Operacionais Modernos**. 3 ed. São Paulo: Pearson Education, 2009.