Aula 3

Segurança em Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

Meios para Prover a Segurança

Agenda

- Gerenciamento de identidade e acesso
- Infraestrutura da segurança
- Tratamento de incidentes
- Segurança de redes
- Segurança no SDLC

Contextualizando

- Conhecer os riscos e as vulnerabilidades
- Planejar a abordagem

- Meios adequados para:
  - identidade e acesso
  - infraestrutura
  - redes
  - SDLC

Gerenciamento de Identidade e Acesso

- Controle de identidade
- Controle de acesso
- Autorização
- Autenticidade
- Verificação
- Acesso remoto

- Gestão de identidade e acesso é um processo crítico. Simulação, roubo ou alteração de identidade é fácil no mundo digital. Isso requer, além de ID e senha:

- controles biométricos
- certificados digitais
- assinatura eletrônica
- hardware (smart cards, tokens) etc.

- O processo de identificação é geralmente decorrente da verificação de características relativas ao indivíduo ou elemento, algo que este:

- sabe (ID, senha)
- possui (token, smart card)
- é (biometria estática)
- faz (biometria dinâmica)

Infraestrutura de Segurança

- Defesa dos computadores: antivírus, antispam, antimalware etc.
- Proxy
- Firewall
- IDS

- A defesa do computador, tablet ou smartphone pretende evitar a ação de malwares, reduzindo a vulnerabilidade, identificando e inibindo ações indesejadas de:

- vírus
- spams
- keylogging/ audiologging e videologging
- phising etc.

- O controle do perímetro da rede interna é favorecido pelo uso do proxy, que além de prover o NAT (*Network Address Translation*), possibilita também:

- a identificação
- a autenticação
- seleção de tráfego e de endereços
- log de acessos

- O controle do fluxo de informações das redes, com base na política de segurança da informação, também a segregação de ambientes de redes, usa firewalls como:

- filtros de pacotes
- Statefull Inspection
- Application Proxy Gateway

- O monitoramento do tráfego das redes para identificar falhas ou ataques é feito pelo IDS (*Intrusion Detection System*), operando nos modos:

- Knowledge-based
- Behavior-based
- Data Mining

- Se possível em conjunto/integrado a firewalls e proxies

Incidentes de Segurança

- Faltas, erros e falhas
- Ameaças, ataques e malwares
- Vulnerabilidades
- Tratamento de incidentes

- Qualquer anomalia nos sistemas de informação que cause problema ou impeça seu uso resulta em um incidente de segurança
- Isso pode ser causado por:

- hardware
- sistema operacional
- redes
- programas de aplicação ou software

- Para garantir a confiabilidade dos sistemas são necessários meios para atenuar (mitigar) os riscos. Estes meios são agrupados em função de seu propósito, que pode ser:

- prevenção de falhas
- tolerância a falhas
- remoção de falhas

- A segurança da informação sofre ameaças em todo o ciclo de vida da informação. A origem pode ser não intencional ou intencional – os ataques ou uso de malwares:

- vírus/worms
- trojans
- rootkits
- botnets
- spywares
- exploits etc.

- Uma vulnerabilidade é uma falha ou deficiência interna que possibilita a um agente externo – malicioso – atingir o sistema para tirar proveito

- Vulnerabilidades são frequentemente decorrentes de falhas no processo de desenvolvimento, configuração, instalação ou mudanças

Segurança de Redes

- Identificação
- Autorização
- Processos de comunicação
- Aplicação da Política de Segurança
- Criptografia
- Computação móvel

- A segurança da rede inicia-se com o processo de identificação e autenticação do usuário. Após isso, os serviços do NOS (*Networking Operational System*) irá (...)

(...) prover os acessos de acordo com a Política de Segurança e usando recursos como:

- Kerberos, Radius
- VPN
- SSL, SSH, HTTPS etc.

- Com o uso intensivo de dados móveis – computação móvel, cloud, IOT – novos modelos e serviços de segurança têm surgido para enfrentar os desafios:

- acesso físico
- redes, dispositivos e aplicações não confiáveis
- interação com outras plataformas
- novos serviços etc.

Segurança no Desenvolvimento

- Segurança em todo o SDLC
- ISO/IEC 15.408
- Desenvolvimento Dirigido pela Segurança – SDD

- A segurança no processo de desenvolvimento contempla todo o ciclo, incluindo o projeto, os ambientes, as ferramentas e os processos

- Grande parte dos problemas de segurança nos sistemas origina-se de negligências relativas ao teste de software

- A ISO/IEC 15.408 é um padrão de processo de desenvolvimento de software seguro, e abrange os três principais aspectos do SDLC, a saber:

- segurança do software
- segurança do ambiente
- garantia de segurança

- O modelo SDD propõe a abordagem precoce dos problemas de segurança como medida de garantia da confiabilidade, aliada a:

- análise de riscos
- atuação integrada das equipes
- casos de uso impróprio
- máquinas de ataque

Síntese

- Meios para prover a segurança da informação e dos sistemas
- Gestão de identidades e de acesso

- Infraestrutura de segurança
- Tratamento de incidentes
- Segurança de redes
- Segurança no desenvolvimento de software

Referências de Apoio

- ABNT. Segurança da Informação: coletânea eletrônica. Rio de Janeiro: ABNT, 2014.
- AVIZIENIS, A.; LAPRIE, J. C.; RANDELL, B.; Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing vol. 1, n. 1, 2004.
- GALVÃO, Michele da Costa. 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.; 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 Rocha. Segurança e Auditoria em Sistemas de Informação. Rio de Janeiro: Editora Ciência Moderna, 2008.
- MARTINS, José Carlos Cordeiro. 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. Um 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. Setembro. 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.**