Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Professor:** Todo núcleo de T.I. (Graduação e Pós) - Wyden Facimp
- **Diretor:** SCS
- **Gerente de Projetos:** Motoca Systems

Redes sociais:

- **Linkedin:** https://www.linkedin.com/in/thalles-canela/
- **YouTube:** https://www.youtube.com/aXR6CyberSecurity
- **Facebook:** https://www.facebook.com/axr6PenTest
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** https://github.com/ThallesCanela
- **Github:** https://github.com/aXR6
- **Twitter:** https://twitter.com/Axr6S

Objetivo da Aula:

- Entender as ameaças e vulnerabilidades à segurança da informação
- Conhecer os tipos de ataques cibernéticos
- Compreender a importância das normas de segurança da informação

Ameaças e Vulnerabilidades à Segurança da Informação

- **Ameaça:** Qualquer coisa que tenha o potencial de causar dano à informação ou aos sistemas que a contêm.
- **Vulnerabilidade:** Uma fraqueza que pode ser explorada para causar dano.

Ameaças e Vulnerabilidades à Segurança da Informação (Expandido)

Definição:

- **Ameaça:** Qualquer fator que tenha o potencial de causar dano à informação ou aos sistemas que a contêm.

- **Exemplo 1:** Um hacker tentando invadir um sistema é uma ameaça.
- **Exemplo 2:** Falta de atualização de software também é uma ameaça, pois deixa o sistema exposto.

Ameaças e Vulnerabilidades à Segurança da Informação (Expandido)
Definição:

- **Vulnerabilidade:** Uma fraqueza em um sistema que pode ser explorada para causar dano.

- **Exemplo 1:** Um sistema operacional desatualizado pode ter falhas de segurança conhecidas.
- **Exemplo 2:** Configurações de rede mal configuradas podem expor o sistema internamente e externamente.

Classificação das Ameaças e Vulnerabilidades

- **Ameaças Físicas:**

- **Exemplos:** Incêndio, inundação, furto de hardware
- **Vulnerabilidades Associadas:** Falta de controle de acesso físico, ausência de sensores de fumaça

Classificação das Ameaças e Vulnerabilidades

- **Ameaças Humanas:**

- **Exemplos:** Engenharia social, erro humano, acesso interno mal-intencionado
- **Vulnerabilidades Associadas:** Treinamento inadequado, falta de verificações de antecedentes em funcionários

Classificação das Ameaças e Vulnerabilidades

- **Ameaças Técnicas:**

- **Exemplos:** Software malicioso, ataques de phishing, ataques DDoS
- **Vulnerabilidades Associadas:** Falhas de configuração, sistemas desatualizados, uso de senhas fracas

Avaliação de Ameaças e Vulnerabilidades

- **Importância da Avaliação:** Identificar e classificar as ameaças e vulnerabilidades ajuda a alocar recursos de maneira eficiente para proteger o sistema.
- **Métodos Comuns:** Penetration testing, análise de risco, auditorias de segurança

Tipos de Ameaças e Vulnerabilidades

- **Ameaças Físicas:** Incêndio, inundação
- **Ameaças Humanas:** Engenharia social, erro humano
- **Ameaças Técnicas:** Software malicioso, falhas de configuração

- **Exemplo de Caso de Uso:**
- Empresa X sofreu uma invasão porque um funcionário clicou em um link malicioso por engano.

Tipos de Ameaças

- **Ameaças Físicas:**

- Incêndio, inundação, terremoto
- **Exemplo de Caso de Uso:** Uma empresa sem um plano de recuperação de desastres pode perder todo o seu data center em caso de incêndio.

Tipos de Ameaças

- **Ameaças Humanas:**

- Engenharia social, erro humano, funcionários descontentes
- **Exemplo de Caso de Uso:** Um funcionário insatisfeito deleta arquivos críticos antes de sair da empresa.

Tipos de Ameaças

- **Ameaças Técnicas:**

- Software malicioso, falhas de configuração, vulnerabilidades de software não corrigidas
- **Exemplo de Caso de Uso:** Um hacker explora uma vulnerabilidade em um aplicativo web mal configurado para roubar informações do banco de dados.

Tipos de Vulnerabilidades

- **Vulnerabilidades de Software:**

- Versões desatualizadas, bugs
- **Exemplo de Caso de Uso:** A empresa A ainda está usando uma versão desatualizada do Windows e se torna vítima de um ataque de ransomware.

Tipos de Vulnerabilidades

- **Vulnerabilidades de Configuração:**

- Senhas fracas, configurações de rede inadequadas
- **Exemplo de Caso de Uso:** O roteador da Empresa B estava configurado com a senha padrão, permitindo que invasores acessassem a rede interna.

Tipos de Vulnerabilidades

- **Vulnerabilidades Humanas:**

- Falta de treinamento, negligência
- **Exemplo de Caso de Uso:** Os funcionários da Empresa C não são treinados em segurança da informação, resultando em vários incidentes de phishing bem-sucedidos.

Ataques Cibernéticos

- **Tipos Comuns de Ataques:**

- Phishing
- Ransomware
- Ataque DDoS

Tipos Comuns de Ataques:

- **Phishing**
  - **O que é:** Tentativa de coletar informações pessoais através de e-mails ou mensagens falsas.
  - **Exemplo:** Você recebe um e-mail se passando pelo seu banco, solicitando que você clique em um link e insira suas credenciais.
  - **Prevenção:** Verifique o e-mail do remetente, não clique em links suspeitos.

Tipos Comuns de Ataques:

- **Ransomware**
  - **O que é:** Um tipo de malware que criptografa os arquivos do usuário e exige um resgate para descriptografá-los.
  - **Exemplo:** O WannaCry paralisou sistemas em todo o mundo em 2017, afetando hospitais, empresas e instituições governamentais.
  - **Prevenção:** Mantenha backups atualizados e proteja-os de acesso não autorizado.

Tipos Comuns de Ataques:

- **Ataque DDoS (Distributed Denial of Service)**
  - **O que é:** Ataque que sobrecarrega um servidor com tráfego falso para torná-lo inacessível.
  - **Exemplo:** Em 2016, o serviço de DNS Dyn foi atacado, afetando sites como Twitter, Netflix e Amazon.
  - **Prevenção:** Utilize medidas como balanceamento de carga e serviços de mitigação de DDoS.

Tipos Comuns de Ataques:

- **Ataque de Força Bruta**
  - **O que é:** Tentativa de invadir um sistema através da repetição exaustiva de combinações de senha.
  - **Exemplo:** Um hacker tenta acessar um banco de dados de cliente usando um script que testa milhares de combinações de senha por minuto.
  - **Prevenção:** Use autenticação de dois fatores e políticas de senha fortes.

Tipos Comuns de Ataques:

- **SQL Injection**
  - **O que é:** Inserir ou "injetar" um código SQL indesejado em um formulário de entrada.
  - **Exemplo:** Um invasor pode injetar código SQL malicioso em um campo de pesquisa em um site para extrair informações do banco de dados.
  - **Prevenção:** Validação rigorosa de entrada e utilização de consultas parametrizadas.

Exemplo de Ataque Cibernético

- Todos os arquivos criptografados
- Resgate solicitado em Bitcoin
- **Solução:** Pagamento ou restauração de backups

- **Caso de Uso:**
- Ataque de Ransomware na Empresa Y

Caso de Uso: Ataque de Ransomware na Empresa Y

- **Cronologia do Ataque:**
- **Dia 1 - Infiltração:**

- Um empregado recebe um e-mail aparentemente legítimo de um fornecedor.
- O e-mail contém um anexo que, quando aberto, libera o ransomware no sistema.

Caso de Uso: Ataque de Ransomware na Empresa Y

- **Cronologia do Ataque:**
- **Dia 2 - Criptografia:**

- O ransomware começa a criptografar arquivos armazenados nos servidores da empresa, tornando-os inacessíveis.

Caso de Uso: Ataque de Ransomware na Empresa Y

- **Cronologia do Ataque:**
- **Dia 3 - Mensagem de Resgate:**

- Uma mensagem de resgate é exibida nas telas, exigindo 5 Bitcoins para desbloquear os arquivos.

Caso de Uso: Ataque de Ransomware na Empresa Y

- **Cronologia do Ataque:**
- **Dia 4 - Decisão Executiva:**

- A liderança da empresa deve decidir entre pagar o resgate ou tentar restaurar os sistemas a partir de backups.

Caso de Uso: Ataque de Ransomware na Empresa Y

- **O Desfecho:**

- **Opção A: Pagamento do resgate**
- Não garante que os arquivos serão descriptografados
- Financia atividades criminosas

- **Opção B: Restaurar a partir de Backups**
- Requer tempo e recursos
- Possível perda de dados mais recentes

Normas de Segurança da Informação

- **Importância:**

- Garantir a integridade, confidencialidade e disponibilidade das informações.

Importância:

- **Integridade:** Certificar-se de que os dados não foram alterados de forma inadequada.
- **Confidencialidade:** Proteger informações contra acesso não autorizado.
- **Disponibilidade:** Garantir que os recursos de informação estejam disponíveis quando necessários.

Exemplos de Normas Comuns:

- **ISO 27001:** Um padrão internacional que especifica os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI).
- **NIST 800-53:** Publicada pelo Instituto Nacional de Padrões e Tecnologia dos EUA, esta norma oferece um conjunto completo de controles de segurança.
- **PCI DSS:** Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento, crucial para organizações que processam pagamentos com cartão de crédito.

Exemplo de Caso de Uso:

- **Hospital A**

- Lida com dados sensíveis de pacientes.
- Implementa a norma HIPAA (Health Insurance Portability and Accountability Act) para proteger informações de saúde.
- Realiza auditorias regulares para garantir conformidade e mitigar riscos.

Como as Normas São Aplicadas:

- **Auditorias:** Examinar processos para garantir que as normas estão sendo seguidas.
- **Controles Técnicos:** Firewalls, sistemas de detecção de invasão, criptografia, etc.
- **Documentação:** Políticas escritas, procedimentos e diretrizes.

Benefícios das Normas:

- **Credibilidade:** Mostra aos stakeholders que a organização leva a segurança a sério.
- **Conformidade Legal:** Ajuda na conformidade com leis e regulamentos.
- **Melhor Gestão de Riscos:** Fornecer uma estrutura para identificar, avaliar e mitigar riscos.

Finalidades e Benefícios das Normas

- Padronização dos Processos
- Mitigação de Riscos
- Conformidade Legal

- **Exemplo de Caso de Uso:**
- Empresa Z segue a norma ISO 27001 e passa por auditorias anuais para garantir conformidade.

Finalidades:

- **Padronização dos Processos:** Cria um conjunto unificado de procedimentos e práticas de segurança.
- **Mitigação de Riscos:** Ajuda a identificar e reduzir os riscos associados às ameaças à informação.
- **Conformidade Legal:** Mantém a organização em conformidade com leis e regulamentações, evitando multas e ações legais.

Benefícios:

- **Melhor Gestão de Ativos:** Normas como a ISO 27001 exigem um inventário detalhado de ativos, permitindo uma melhor gestão e controle.
- **Credibilidade e Confiança:** A conformidade com normas gera confiança entre parceiros e clientes.
- **Eficiência Operacional:** Práticas padronizadas minimizam erros e reduzem o custo de operação.

Exemplo de Caso de Uso: Empresa Z com Norma ISO 27001

- **Situação Antes da Norma:** Empresa Z sofria de frequentes interrupções no serviço devido a falhas de segurança. Eles não estavam em conformidade com as regulamentações locais, colocando-se em risco de multas.

- **Implementação da Norma:** A Empresa Z implementou a ISO 27001 e padronizou seus processos de segurança, criando políticas claras para gerenciamento de ativos, controle de acesso e resposta a incidentes.

Exemplo de Caso de Uso: Empresa Z com Norma ISO 27001

- **Situação Após a Norma:** A Empresa Z viu uma redução de 40% nos incidentes de segurança no primeiro ano e passou a ganhar licitações de contratos que exigiam conformidade com normas de segurança.

- **Benefício Adicional:** Auditorias anuais mantêm a empresa atualizada e permitem a identificação proativa de áreas para melhoria, mantendo um ciclo de aprimoramento contínuo.

Aplicação das Normas

- Análise de Risco
- Políticas de Segurança
- Treinamento de Funcionários
- Monitoramento e Revisão Constantes

1. Análise de Risco

- **Definição:** Identificação e avaliação de riscos associados à segurança da informação.

- **Exemplo de Caso de Uso:**
  - A Empresa A usa software de análise de risco para identificar vulnerabilidades em sua rede. Descobrem que a porta 22 (SSH) está aberta ao público, o que é uma vulnerabilidade.

2. Políticas de Segurança

- **Definição:** Conjunto de diretrizes que orientam como tratar as informações e os sistemas da organização.

- **Exemplo de Caso de Uso:**
  - A Empresa B implementa uma política de "mínimos privilégios", restringindo o acesso a dados sensíveis apenas a funcionários que realmente precisam deles.

3. Treinamento de Funcionários

- **Definição:** Educar funcionários sobre as melhores práticas e políticas de segurança da empresa.

- **Exemplo de Caso de Uso:**
  - Empresa C faz treinamentos mensais anti-phishing, onde ensinam os funcionários a reconhecer emails e links maliciosos.

4. Monitoramento e Revisão Constantes

- **Definição:** O processo contínuo de avaliar a eficácia das medidas de segurança implementadas.

- **Exemplo de Caso de Uso:**
  - A Empresa D usa ferramentas de SIEM (Gerenciamento de Eventos e Informações de Segurança) para monitorar o tráfego de rede em tempo real, detectando e respondendo a ameaças assim que ocorrem.

Conclusão

- A segurança da informação não é apenas uma responsabilidade da equipe de TI, mas uma preocupação organizacional que requer políticas, procedimentos e, acima de tudo, educação e consciência.

Referências Bibliográficas

- "Security in Computing" - Charles P. Pfleeger, Shari Lawrence Pfleeger
- "Cryptography and Network Security" - William Stallings
- "Computer Security: Principles and Practice" - William Stallings, Lawrie Brown

Artigos Científicos

- "The Protection of Information in Computer Systems" - Jerome Saltzer, Michael D. Schroeder
- "A Taxonomy of Computer Program Security Flaws" - Carl E. Landwehr
- "Trends in Cybersecurity Risk and Protective Behaviors" - Various Authors (IEEE Journal)

Periódicos

- Journal of Computer Security
- IEEE Security & Privacy
- Computers & Security

Revistas de Publicação Científica

- ACM Computing Surveys (CSUR)
- Information Systems Security Journal
- Journal of Information Security and Applications

Sites para Publicação Científica

- Google Scholar - scholar.google.com
- arXiv.org - arxiv.org
- IEEE Xplore - ieeexplore.ieee.org
- ScienceDirect - sciencedirect.com