Semana 28 - Aula 1

Tópico Principal da Aula: Segurança em Aplicações em Nuvem

Subtítulo/Tema Específico: Introdução, Desafios e Melhores Práticas em Segurança na Nuvem

Código da aula: [SIS]ANO1C2B4S28A1

Objetivos da Aula:

- Compreender os principais desafios de segurança inerentes às aplicações desenvolvidas e implantadas em ambientes de nuvem.
- Conhecer as melhores práticas de segurança que devem ser adotadas para mitigar riscos e proteger dados e sistemas em Cloud Computing.
- Aplicar técnicas de gestão de dados e parametrização para soluções seguras em nuvem.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 06 - Os principais desafios de segurança

- **Definição:** A migração de sistemas para a nuvem introduz novos desafios de segurança que exigem uma mudança na mentalidade tradicional de proteção perimetral. Os principais desafios giram em torno da **gestão de identidade e acesso**, **proteção dos dados**, e a **governança** em um ambiente distribuído e dinâmico.
- **Aprofundamento/Complemento (se necessário):** O modelo de **Responsabilidade Compartilhada** (Shared Responsibility Model) é central. Nele, o provedor de nuvem (AWS, Azure, Google Cloud, Oracle Cloud) garante a segurança *da* nuvem (infraestrutura física, hardware, software de computação, armazenamento, redes), mas o cliente é responsável pela segurança *na* nuvem (dados, aplicações, configurações de segurança, gerenciamento de acesso).
- **Exemplo Prático:** Uma empresa que usa IaaS (Infraestrutura como Serviço) é responsável por aplicar patches e atualizações no sistema operacional da máquina virtual. Se um hacker explora uma vulnerabilidade não corrigida, o erro de segurança é do cliente, não do provedor.
    - **Link de Vídeo:**
        - Segurança em Ambientes de Nuvem: Desafios e Soluções
        - Segurança em Ambientes de Nuvem

Referência do Slide: Slides 09 a 13 - As melhores práticas de segurança

- **Definição:** As melhores práticas são um conjunto de medidas proativas e reativas essenciais para mitigar ameaças cibernéticas e garantir a confiança do usuário no ambiente de nuvem. Elas incluem estratégias técnicas e de governança.
- **Aprofundamento/Complemento (se necessário):** A **Autenticação Multifator (MFA)** é destacada como um método eficaz que exige duas ou mais formas de verificação (ex: senha e código temporário) para acessar recursos, elevando significativamente a segurança da identidade. Outras práticas cruciais são a **Criptografia** dos dados em repouso e em trânsito, o **Monitoramento Contínuo** de atividades e a **Educação** da equipe.
- **Exemplo Prático:** Implementar MFA para todos os acessos administrativos (root users) à console do provedor de nuvem. Além disso, usar serviços de **Gerenciamento de Chaves** (Key Management Service - KMS) para criptografar automaticamente todos os dados sensíveis armazenados em bancos de dados na nuvem.

Semana 01 - Aula 2

Tópico Principal da Aula: Segurança em Aplicações em Nuvem

Subtítulo/Tema Específico: Riscos na Migração para a Nuvem e Mitigação (Foco em Phishing)

Código da aula: [SIS]ANO1C2B4S28A2

Objetivos da Aula:

- Compreender os riscos de segurança mais comuns associados ao processo de migração de aplicações e dados para a nuvem.
- Identificar a ameaça de Phishing e Engenharia Social como um risco crítico para credenciais de nuvem.
- Aprender as medidas práticas e políticas que podem ser implementadas para mitigar o risco de contas comprometidas por ataques de Phishing.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 08 a 10 - Riscos de Contas Comprometidas (Phishing) e Impactos

- **Definição:** A migração de cargas de trabalho para a nuvem, embora benéfica, expõe as empresas a novos vetores de ataque. Um dos riscos mais significativos é o comprometimento de contas, frequentemente causado por ataques de **Phishing**. Phishing é uma técnica de engenharia social onde o atacante se disfarça de entidade confiável para induzir a vítima a fornecer informações sensíveis, como credenciais de acesso à nuvem.

- **Aprofundamento/Complemento (se necessário):** O impacto de uma conta de nuvem comprometida é severo e abrange **perda de dados**, **interrupção de negócios**, **danos à reputação** e **custos financeiros** decorrentes de vazamento, multas ou uso indevido de recursos (ex: mineração de criptomoedas em instâncias comprometidas). A conta de um administrador de nuvem, se comprometida, pode levar a um desastre completo.
- **Exemplo Prático:** Um funcionário de TI recebe um e-mail urgente, aparentemente da equipe de segurança interna (e-mail forjado), solicitando a "revalidação" de suas credenciais de console. Ele clica no link, insere seu nome de usuário e senha em uma página falsa, e as credenciais são roubadas, permitindo que o atacante acesse os serviços da nuvem.
    - **Link de Vídeo:**
        - Phishing e Engenharia Social: Proteja-se dos Crimes Digitais (CT015)
        - Migração segura para a nuvem

Referência do Slide: Slide 11 - Medidas de Mitigação

- **Definição:** Para mitigar o risco de Phishing e credenciais comprometidas, é essencial implementar uma defesa em camadas. As principais medidas incluem: **Educação e conscientização** dos funcionários sobre como identificar ataques, **fortalecimento das credenciais** (uso de senhas complexas e MFA), **monitoramento e detecção** de atividades anômalas, e a elaboração de um plano de **resposta a incidentes**.
- **Aprofundamento/Complemento (se necessário):** O fortalecimento das credenciais deve ir além do MFA, incluindo políticas de rotação de chaves de acesso (API Keys) e o princípio do **menor privilégio** (Least Privilege), garantindo que os usuários tenham apenas as permissões estritamente necessárias para suas funções.
- **Exemplo Prático:** Realizar simulações de ataques de Phishing na empresa para medir e melhorar a conscientização dos funcionários. Se um funcionário cair na simulação, ele é imediatamente encaminhado para um treinamento de reciclagem.

Semana 01 - Aula 3

Tópico Principal da Aula: Segurança em Aplicações em Nuvem

Subtítulo/Tema Específico: Segurança de Rede: Apresentação e Funcionalidades do Firewall Cisco ASA

Código da aula: [SIS]ANO1C2B4S28A3

Objetivos da Aula:

- Entender o papel do Firewall de Rede como um componente de segurança fundamental em ambientes locais e de nuvem.
- Conhecer o Cisco ASA (Adaptive Security Appliance) e suas funcionalidades avançadas de proteção de rede.

- Identificar como recursos como Stateful Firewall, VPN e IPS contribuem para a defesa de aplicações em nuvem e infraestruturas híbridas.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 06 a 08 - Firewall de Rede e Cisco ASA

- **Definição:** O **Firewall** atua como uma barreira de segurança, controlando o tráfego de entrada e saída em uma rede privada, com base em regras de segurança configuráveis. Ele é essencial para proteger a rede contra acessos não autorizados e ataques. O **Cisco ASA** (Adaptive Security Appliance) é um appliance de segurança projetado para oferecer proteção contra ameaças, controlando rigorosamente o tráfego de rede.
- **Aprofundamento/Complemento (se necessário):** O ASA não é apenas um firewall tradicional, mas uma solução de segurança unificada que incorpora várias funcionalidades avançadas, sendo ideal para infraestruturas complexas, incluindo aquelas que interligam data centers locais com a nuvem (ambientes híbridos) via VPN.
- **Exemplo Prático:** Uma empresa utiliza um Cisco ASA em seu data center local. Ao migrar parte dos seus serviços para a nuvem, ela configura uma **VPN Site-to-Site** no ASA para criar um túnel seguro de comunicação entre a rede local e a VPC (Virtual Private Cloud) na nuvem, garantindo que o tráfego entre os ambientes seja criptografado e inspecionado.
    - **Link de Vídeo:**
        - Cisco ASA Basics | #2 ASA Firewall Overview
        - Cisco Adaptive Security Appliance ASA Firewall

Referência do Slide: Slides 09 e 10 - Funcionalidades e Recursos do Cisco ASA

- **Definição:** As funcionalidades do Cisco ASA englobam diversos mecanismos de segurança, sendo o **Stateful Firewall** um destaque, que monitora o estado das conexões ativas para tomar decisões de segurança mais precisas. Outras funções cruciais são: **VPN** (para acesso remoto seguro ou conexões site-to-site), **Inspeção de Protocolo**, **Controle de Acesso**, **Filtragem de Pacotes** e **Prevenção Contra Intrusões (IPS)**.
- **Aprofundamento/Complemento (se necessário):** Um **Stateful Firewall** é mais inteligente que um firewall sem estado, pois ele se lembra das conexões que foram iniciadas internamente. Isso significa que, se um pacote de resposta legítimo vier de fora, o firewall o permitirá sem a necessidade de uma regra de entrada explícita, ao contrário de um firewall de filtragem de pacotes simples.
- **Exemplo Prático:** Um usuário interno acessa um site externo. O Stateful Firewall cria uma entrada temporária na sua tabela de estado, permitindo que a resposta do

site retorne sem ser bloqueada. No entanto, se um usuário externo tentar iniciar uma conexão com o usuário interno (sem uma solicitação anterior), o pacote é descartado, pois não há um estado de conexão correspondente.