Aula 1 – Introdução à Segurança da Informação

Nesta aula iremos explorar um cenário de ataque cibernético em uma empresa de e-commerce, destacando a importância da Segurança da Informação para proteger dados e operações. Nosso objetivo é entender as causas, impactos e como prevenir futuros incidentes.

Caso Exemplo – Ataque Cibernético

A empresa **TechShop**, que atua no comércio eletrônico de produtos eletrônicos, recentemente sofreu um ataque cibernético grave. Durante o incidente, dados pessoais e financeiros de clientes foram expostos, o sistema de pagamentos ficou fora do ar por várias horas, e as operações do site foram interrompidas, causando prejuízos financeiros e perda de confiança dos consumidores.
A diretoria da TechShop está preocupada e solicitou uma equipe de analistas para investigar o ocorrido.

Seu grupo foi contratado para:

- Identificar as possíveis causas do ataque, incluindo vulnerabilidades e falhas de segurança.
- Apontar quais tipos de ameaças podem ter sido exploradas pelos invasores.
- Avaliar se as políticas de segurança adotadas pela empresa eram suficientes.
- Sugerir medidas iniciais para mitigar riscos futuros e proteger os dados, sistemas e comunicações da empresa.

Considerando esse cenário:

- Quais elementos da segurança da informação devem ser analisados?
- Que tecnologias e práticas poderiam ajudar a evitar esse tipo de incidente?
- Como a criptografia e os firewalls podem contribuir para a defesa da empresa?

Levantamento de Hipóteses e Áreas Chave

Para enfrentar o desafio proposto, precisamos levantar hipóteses sobre as possíveis ameaças e vulnerabilidades envolvidas no ataque. Além disso, vamos identificar as políticas de segurança que poderiam ter evitado o problema.

1 Ameaças e Vulnerabilidades

Quais falhas permitiram a exposição de dados e a interrupção do serviço?

2 Políticas de Segurança

Que diretrizes e controles faltaram para proteger a empresa?

3 Foco na Segurança

Aplicações, bases de dados, comunicações e dispositivos móveis.

4 Tecnologias Essenciais

O papel crucial da criptografia e dos firewalls na defesa cibernética.

Conceitos Fundamentais da Segurança da Informação

A Segurança da Informação é a disciplina focada em proteger os ativos de informação contra acessos não autorizados, uso, divulgação, interrupção, modificação ou destruição.

Confidencialidade

Garantir que a informação só seja acessível por quem tem autorização. Pense em mensagens criptografadas ou documentos protegidos por senha.

Integridade

Assegurar que a informação seja precisa, completa e não alterada sem permissão. Isso é fundamental para dados financeiros ou registros médicos.

Disponibilidade

Manter o acesso à informação e aos sistemas sempre que necessário. Interrupções podem causar grandes prejuízos, como no caso do e-commerce.

Ameaças e Vulnerabilidades Comuns

Ataques cibernéticos são complexos e envolvem uma combinação de ameaças e vulnerabilidades.

Ameaças

- Malware: vírus, ransomware
- Phishing: e-mails enganosos
- Engenharia Social: manipulação humana
- Ataques de Força Bruta: tentativa e erro de senhas

Vulnerabilidades

- Software Desatualizado
- Senhas Fracas
- Falhas de Configuração
- Falta de Conscientização dos Usuários

O ataque ao e-commerce provavelmente explorou uma combinação dessas falhas.

Políticas de Segurança da Informação

As Políticas de Segurança da Informação (PSI) são o alicerce para proteger os ativos de uma organização. Elas definem as regras, procedimentos e responsabilidades que todos devem seguir.

Por que são Essenciais?

Estabelecem um framework claro, garantindo a conformidade legal, reduzindo riscos e protegendo a reputação da empresa.

Responsabilidades

Definem papéis e deveres para cada membro da equipe, desde a alta gerência até o usuário final, na manutenção da segurança.

Boas Práticas

Incentivam o uso de senhas fortes, a atualização de sistemas e a identificação de e-mails suspeitos, fortalecendo a cultura de segurança.

Protegendo Aplicações, Bancos de Dados e Comunicações

A segurança digital vai além dos conceitos básicos, exigindo atenção em cada camada da infraestrutura de TI.

- Aplicações: Falhas em códigos podem ser portas de entrada. Validação de entradas e atualizações são cruciais.
- Bancos de Dados: Onde os dados valiosos residem. Proteção contra injeção SQL e controle de acesso rigoroso são mandatórios.
- Comunicações: O tráfego de dados precisa ser seguro. Protocolos criptografados (HTTPS, SSL/TLS) e monitoramento de rede são indispensáveis.

A chave é o monitoramento contínuo e a atualização constante de todos os sistemas.

Segurança em Dispositivos Móveis

Com a crescente ubiquidade de smartphones e tablets, a segurança em dispositivos móveis tornou-se um ponto crítico para qualquer organização. Estes dispositivos são alvos atraentes para ataques devido à sua portabilidade e à quantidade de dados sensíveis que armazenam.

1

Riscos Específicos

Perda ou roubo, malware móvel, redes Wi-Fi públicas inseguras e aplicativos maliciosos são as principais ameaças.

2

Boas Práticas

Uso de senhas fortes/biometria, VPN em redes públicas, atualização de software, e cautela com apps de fontes desconhecidas.

Fundamentos da Criptografia

A criptografia é a arte de codificar informações para proteger sua confidencialidade e integridade, tornando-as ilegíveis para pessoas não autorizadas.

1 Conceito Básico

Transformação de dados claros em dados cifrados, e vice-versa, usando algoritmos e chaves.

2 Objetivos

Garantir confidencialidade, integridade, autenticidade e não repúdio.

3 Criptografia Simétrica

Uma única chave para cifrar e decifrar (ex: AES). Rápida, mas a gestão da chave é um desafio.

4 Criptografia Assimétrica

Duas chaves (pública e privada) (ex: RSA). Usada para assinaturas digitais e troca segura de chaves simétricas.

É a espinha dorsal da segurança online, presente em tudo, de transações bancárias a comunicações pessoais.

Firewalls: A Barreira de Proteção

Os firewalls são como guardiões da rede, atuando como uma barreira entre uma rede interna confiável e redes externas não confiáveis, como a internet.

O que são?

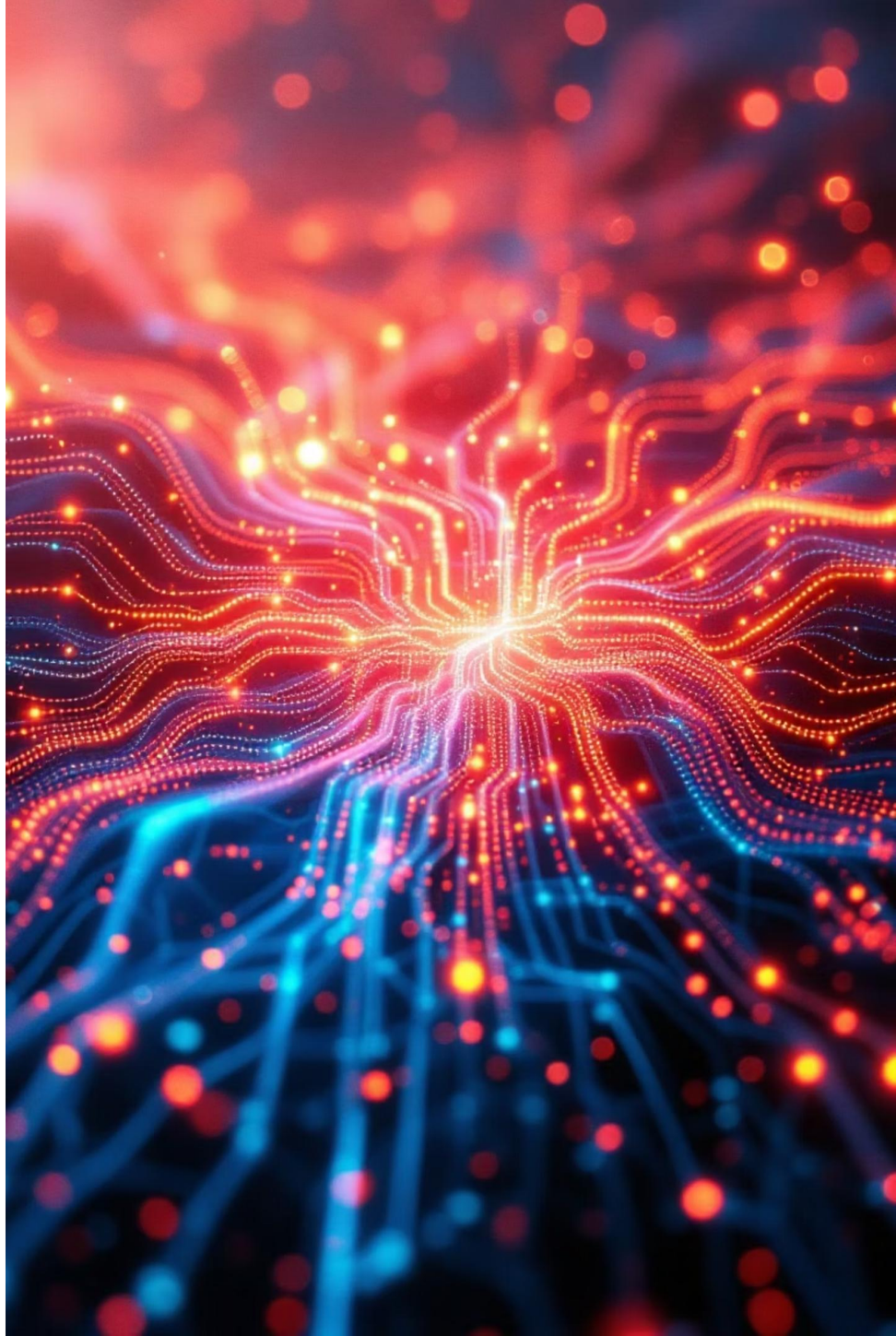
Sistemas de segurança de rede que monitoram e controlam o tráfego de rede de entrada e saída com base em regras de segurança predeterminadas.

Funções Principais

Filtrar tráfego, bloquear acessos não autorizados, registrar eventos de segurança e proteger contra ataques externos.

Importância na Rede

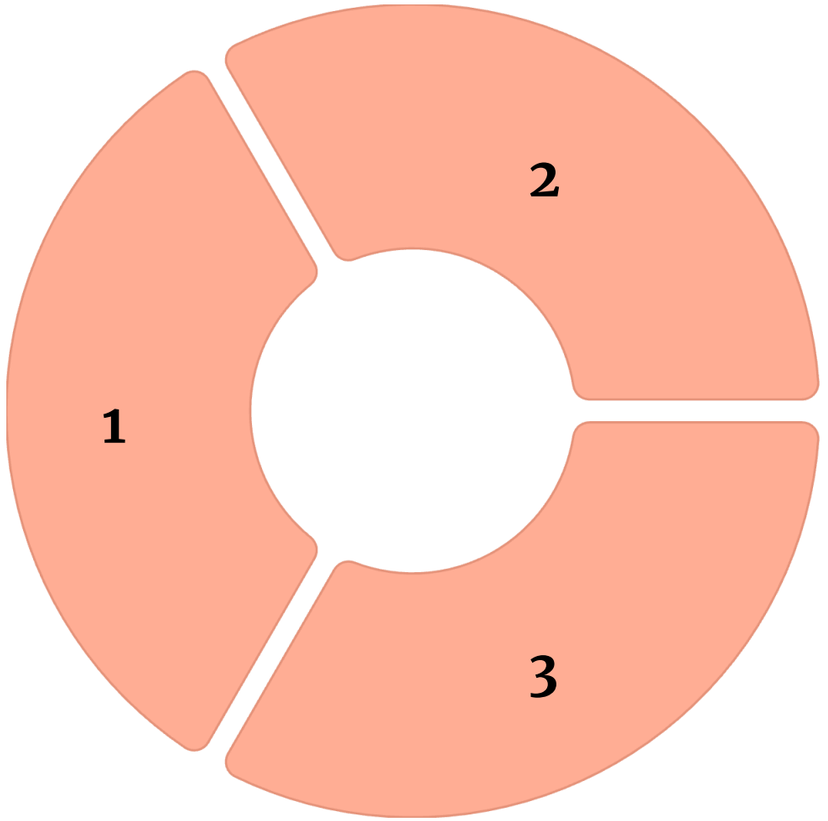
Essenciais para criar uma primeira linha de defesa, isolando a rede interna de ameaças externas e garantindo a confidencialidade e integridade dos dados.



Reflexão Final: Chaves para a Segurança

Ameaça vs. Vulnerabilidade

A ameaça é um evento que pode causar dano (ex: malware). A vulnerabilidade é uma fraqueza que a ameaça pode explorar (ex: software desatualizado). Uma não existe sem a outra.



Por que a Criptografia é Fundamental?

É a base para garantir a confidencialidade e integridade dos dados, protegendo informações sensíveis de acessos e modificações não autorizadas em qualquer contexto digital.

Políticas de Segurança Eficazes

São cruciais para orientar o comportamento dos usuários, minimizar riscos internos e estabelecer diretrizes claras para a proteção de ativos da informação.

A segurança da informação é um processo contínuo de adaptação e defesa.