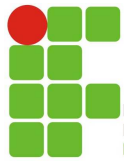
Segurança de Redes

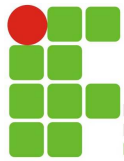
Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 01
Fundamentos de Segurança



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"A arte de perceber de forma clara e real nossas mais íntimas intenções é uma das tarefas do processo evolutivo pelo qual todos estamos passando." (Hammed)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Apresentar o conceito de Segurança da Informação (SI)
- Discutir a importância da SI no contexto das redes de computadores
- Introduzir os pilares da SI: Confidencialidade, Integridade, Disponibilidade (CID).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Segurança da informação é o conjunto de medidas utilizadas para prevenir, detectar e corrigir violações de segurança da informação de diversas ameaças. Este medidas visam tentar garantir a confidencialidade, integridade e disponibilidade dos dados. Além disso, podem estar envolvidos outros atributos, como autenticidade, responsabilidade, não repúdio e confiabilidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

Segurança de computadores e redes é uma batalha de inteligência entre um criminoso que tenta encontrar buracos e o projetista ou administrador que tenta fechá-los. A grande vantagem que o atacante possui é que ele precisa encontrar uma simples brecha, enquanto o projetista tem que encontrar e eliminar todas as possíveis brechas para garantir uma segurança perfeita.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Não existe rede 100% segura. O objetivo não é tornar um sistema absolutamente invulnerável (o que é tecnicamente inviável), mas sim reduzir os riscos ao menor nível possível, dentro de critérios aceitáveis. Existem diversos fatores que impedem uma rede de ser totalmente segura, entre elas: fatores humanos, complexidade dos sistemas, evolução constante das ameaças e desastres naturais ou vulnerabilidades desconhecidas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

ECONOMIA

TECNOLOGIA

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades

Vazamento sem precedentes expôs dados de 50 milhões de usuários e mergulhou empresa em nova crise, pouco tempo depois de comoção sobre disseminação de notícias falsas

BBC NEWS Por BBC

20/03/2018 13h40 · Atualizado há 7 anos

O Facebook sofreu um forte abalo no último sábado com a revelação de que as **informações de mais de 50 milhões de pessoas foram utilizadas sem o consentimento delas pela empresa americana Cambridge Analytica** para fazer propaganda política.

A empresa teria tido acesso ao volume de dados ao lançar um aplicativo de teste psicológico na rede social. Aqueles usuários do Facebook que participaram do teste acabaram por entregar à Cambridge Analytica não apenas suas informações, mas os dados referentes a todos os amigos do perfil.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Edição: ESPAÑA

ASSINE FAÇA LOGIN

EL PAÍS

Internacional

AMÉRICA LATINA · ÁFRICA · EUROPA · ORIENTE MÉDIO · CHINA · EUA

O ciberataque: apertar um botão e desligar o mundo

Reconstrução do ataque que paralisou os sistemas informáticos de mais de 170 países. O próximo pode causar o caos em escala global

JUAN DIEGO QUESADA | ROSA JIMÉNEZ CANO

Madri / São Francisco - 21 MAY 2017 - 13:01 BRT

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

exame.

Ataque de 2013 violou todas as 3 bilhões de contas, diz Yahoo

Número de contas afetadas é o triplo do originalmente relatado pela companhia

Yahoo: todas as contas foram afetadas (Andrew Harrer/Bloomberg/Bloomberg)

AFP
Publicado em 3 de outubro de 2017 às 19h29.
Última atualização em 3 de outubro de 2017 às 19h49.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

A Segurança da Informação baseia-se em três pilares fundamentais:

- Confidencialidade: refere-se à proteção das informações contra acessos não autorizados. Isso envolve garantir que apenas usuários autorizados tenham permissão para visualizar ou acessar informações sensíveis.
- Integridade: diz respeito à proteção das informações contra alterações ou destruição não autorizadas. É importante garantir que as informações permaneçam precisas e íntegras ao longo do tempo.
- Disponibilidade: refere-se à garantia de que as informações estejam disponíveis quando necessário. Isso envolve proteger os sistemas contra falhas e ataques que possam prejudicar o acesso às informações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Além da confidencialidade, integridade e disponibilidade, algumas aplicações no campo da segurança necessitam de características adicionais, são elas:

- Autenticidade: refere-se à garantia de que uma pessoa, processo ou sistema é realmente quem ou o que afirma ser. Em outras palavras, é a confirmação da identidade ou origem de algo. Por exemplo, em sistemas de autenticação de usuário, como o uso de senhas ou biometria.
- Responsabilização ou Não Repúdio: se refere à impossibilidade de negar a autoria ou a realização de uma ação previamente realizada. Em outras palavras, quando alguém realiza uma ação ou transação, não pode posteriormente negar ter feito essa ação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Técnicas de Defesa

Para tentar garantir a segurança da informação, são utilizadas diversas medidas, tais como:

- Firewall;
- Antivírus;
- Criptografia;
- Rede Virtual Privada (VPN);
- Autenticação e Controle de Acesso;
- Assinatura e Certificado Digital;
- Sistema de Detecção de Intruso;
- Segurança Física;
- Políticas de Segurança e Educação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os Desafios

A segurança da informação enfrenta uma série de desafios constantes devido à evolução das tecnologias e das ameaças cibernéticas. Alguns dos principais desafios incluem:

- Aumento de ataques cibernéticos: com o crescimento da conectividade e da quantidade de dados online, os ataques cibernéticos estão se tornando mais frequentes e sofisticados;
- Vulnerabilidades de software e hardware: À medida que novas tecnologias são desenvolvidas, surgem também novas vulnerabilidades que podem ser exploradas por atacantes. Ataques são projetados para explorar uma fraqueza inesperada.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os Desafios

- Ameaças internas: Além das ameaças externas, as organizações também enfrentam desafios relacionados a ameaças internas, como funcionários mal-intencionados ou inadvertidos que podem comprometer a segurança dos sistemas.
- Complexidade dos sistemas de TI: a crescente complexidade dos sistemas de TI torna mais difícil garantir sua segurança. A integração de diferentes tecnologias e a diversidade de dispositivos aumentam os pontos de vulnerabilidade que precisam ser protegidos.
- Privacidade dos dados: Com a quantidade cada vez maior de dados pessoais armazenados online, proteger a privacidade desses dados tornou-se um desafio significativo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os Desafios

- Cumprimento de regulamentações: Com a introdução de regulamentações como a LGPD, as organizações enfrentam o desafio de garantir que estão em conformidade com as leis;
- Falta de conscientização e treinamento: A falta de conscientização sobre as práticas de segurança da informação e a importância de proteger os sistemas pode levar a vulnerabilidades causadas por erros humanos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Profissionais de Segurança de Redes

O profissional que pretende atuar nessa área deve estar ciente de que ela é bastante dinâmica e envolve diversos setores da computação, como programação e desenvolvimento de sistemas, redes de computadores, sistemas operacionais e bancos de dados, entre outras. As Principais carreiras são:

- Analista de Segurança da Informação: responsável por monitorar e proteger os sistemas de informação de uma organização contra ameaças de segurança. Realiza análises de risco, levantamento de vulnerabilidades, implementa medidas de segurança e responde a incidentes de segurança.
- Engenheiro de Segurança da Informação: projeta, implementa e gerencia sistemas de segurança da informação, incluindo firewalls, sistemas de detecção de intrusão, VPNs e criptografia. Desenvolve scripts de automação que ajudarão a gerenciar e rastrear incidentes.

Profissionais de Segurança de Redes

- Auditor de Segurança da Informação: realiza auditorias de segurança em sistemas de informação para garantir conformidade com políticas, padrões e regulamentações de segurança. Eles são responsáveis por investigar vários vazamentos de dados e incidentes de segurança, recuperar e examinar dados armazenados em dispositivos eletrônicos.
- Analista de Forense Digital: investigação de incidentes de segurança cibernética, coletando e analisando evidências digitais para determinar a causa e impacto de um incidente.
- Especialista em Teste de Invasão: realiza testes de penetração em sistemas de informação para identificar vulnerabilidades e garantir a segurança dos sistemas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE