Segurança Lógica e Física de Redes

PRINCIPAIS TIPOS DE ATAQUES A REDES E COMO EVITÁ-LOS

Prof. Felipe Oliveira
fdoprof@gmail.com

Agenda

- Segurança de acesso
- Senhas
  - Fragilidades e como corrigí-las
- Controle de acesso físico
- Controles biométricos
- Controles de acesso lógico
- Detecção de Intrusão
- Histórico de acessos e auditoria
- Protocolos de Autenticação

Agenda

- **Segurança de acesso**
- Senhas
  - Fragilidades e como corrigí-las
- Controle de acesso físico
- Controles biométricos
- Controles de acesso lógico
- Detecção de Intrusão
- Histórico de acessos e auditoria
- Protocolos de Autenticação

Segurança de Acesso

- A Segurança de Acesso é hoje:
  - *tanto para acessos físicos a instalações*
  - *quanto para acessos lógicos a plataformas computacionais ou equipamentos de rede,*

Uma das maiores preocupações das Empresas no que se relaciona a:

- *perda de receita, seja por fraudes, operações indevidas e até mesmo roubos.*

Segurança de Acesso

- O ***CONTROLE DE ACESSO***, na Segurança da Informação, é composto dos processos de autenticação, autorização e auditoria (*accounting*).
- Neste contexto o controle de acesso pode ser entendido como:
  - A habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo).

Segurança de Acesso

- A ***autenticação*** identifica quem acessa o sistema.
- A ***autorização*** determina o que um usuário autenticado pode fazer.
- A ***auditoria*** diz o que o usuário fez.

Segurança de Acesso

- Para resolver – ou minimizar ao máximo a ocorrência de falhas nessa área – o profissional da área de segurança deve:
  - Procurar uma solução de Acesso e Segurança que ofereça alta tecnologia em sistemas aliada a equipamentos de última geração.
  - Uma solução que integre todas as rotinas de acesso e segurança de uma empresa, preferencialmente numa única aplicação.
  - Que seja compatível com qualquer projeto de gerenciamento de segurança e,
  - Proporcione proteção pessoal e patrimonial eficiente a todos os segmentos.

Segurança de Acesso

- Em resumo, o profissional da área de segurança deve:
  - Buscar a solução que:

Proporcione ao usuário a proteção do patrimônio da empresa, além de agilizar a tomada de decisão e a centralização do controle dos riscos.

Agenda

- Segurança de acesso
- **Senhas**
  - Fragilidades e como corrigí-las
- Controle de acesso físico
- Controles biométricos
- Controles de acesso lógico
- Detecção de Intrusão
- Histórico de acessos e auditoria
- Protocolos de Autenticação

Senhas de Acesso

- A senha (password) para acesso , faz parte dos mecanismos de autenticação.
- Existem três grupos básicos de mecanismos de autenticação, que se utilizam de:
- ***Aquilo que você é*** (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho).
- ***Aquilo que apenas você possui*** (como seu cartão de senhas bancárias e um *token* gerador de senhas) e,
- ***Aquilo que apenas você sabe*** (como perguntas de segurança e suas senhas).

Senhas de Acesso

- Uma senha, ou *password*, serve para autenticar uma conta.
- É usada no processo de verificação da sua identidade.
- assegura que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão.
- É um dos principais mecanismos de autenticação utilizados devido, principalmente, a simplicidade que possui.

Agenda

- Segurança de acesso
- Senhas
  - **Fragilidades e como corrigí-las**
- Controle de acesso físico
- Controles biométricos
- Controles de acesso lógico
- Detecção de Intrusão
- Histórico de acessos e auditoria
- Protocolos de Autenticação

Senhas de Acesso

Algumas das formas como podem ser descobertas

- ***Ao ser usada em computadores infectados.***

  Muitos códigos maliciosos, ao infectar um computador, armazenam as teclas digitadas (inclusive senhas), espionam o teclado pela *webcam* (caso você possua uma e ela e ela esteja apontada para o teclado) e gravam a posição da tela onde o *mouse* foi clicado.

- ***Ao ser usada em sites falsos.***

  Ao digitar a sua senha em um *site* falso, achando que está no *site* verdadeiro, um atacante pode armazená-la e, posteriormente, usá-la para acessar o *site* verdadeiro e realizar operações em seu nome.

Senhas de Acesso

Algumas das formas como podem ser descobertas

- ***Por meio de tentativas de adivinhação.***

  Isso pode ser ralizado através de um ataque de força bruta, ***Brute Force.***

- ***Ao ser capturada enquanto trafega na rede, sem estar criptografada.***

  Através da interceptação do tráfego ***(Sniffing)***.

Senhas de Acesso

Algumas das formas como podem ser descobertas

- ***SNIFFING***

  É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de ***sniffers.***

  Esta técnica pode ser utilizada de forma:

  Legítima: por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados (Por Exemplo, Wireshark).

  Maliciosa: por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Senhas de Acesso

Como ter uma senha segura:

- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada.
- Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la.
- Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

Senhas de Acesso

Elaboração de boas senhas

Alguns elementos que você **não deve** usar na elaboração de suas senhas são:

- **Qualquer tipo de dado pessoal:** evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você).
- **Sequências de teclado:** evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas.
- **Palavras que façam parte de listas:** evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

Senhas de Acesso

Alguns elementos que você **deve** usar na elaboração de suas senhas são:

- **Números aleatórios:**

  Quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem **exclusivamente** caracteres numéricos.

- **Grande quantidade de caracteres:**

  Quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente.

- **Diferentes tipos de caracteres:**

  Quanto mais "*bagunçada*" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

  Utilizar um gerenciador de senhas pode ajudar (Por exemplo, Keepass)