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

Controle de Acesso Lógico

- Os controles de acesso lógico são um conjunto de medidas e procedimentos, adotados pela organização, ou intrínsecos aos softwares utilizados, para verificar ou identificar pessoas que estão solicitando acesso a recursos computacionais como computadores, notebooks, smartphones, redes de computadores, aplicações, bases de dados, dentre outros hardwares e softwares que possuem um valor grande o suficiente para terem o seu acesso protegido.

Controles de Acesso Lógico

Elementos básicos de controle de Acesso Lógico

- **Dois pontos distintos de controle:**
  - O recurso computacional que desejamos proteger, e
  - O usuário a quem pretendemos conceder os privilégios e acesso aos recursos.
- **Objetivos dos controles:**
  - Apenas usuários autorizados tenham acesso aos recursos.
  - Os usuários devem ter acesso aos recursos necessários a execução de suas tarefas.
  - O acesso a recursos críticos deve ser monitorado e restrito.
  - Os usuários sejam impedidos de executar transações incompatíveis com sua função ou responsabilidades.

Controles de Acesso Lógico

Recursos e informações a serem protegidos

- **Aplicativos**: Programas fonte e objeto. O acesso não autorizado pode alterar as funções e/ou rotinas dos programas.
- **Arquivos de dados**: Bases de dados podem ser alteradas ou deletadas sem a autorização necessária.
- **Utilitários e Sistema Operacional**: O acesso deve ser restrito. Acessos não autorizados podem provocar alterações nos arquivos de configuração ou em arquivos de forma generalizada, podendo ainda permitir a cópia dos mesmos.

Controles de Acesso Lógico

Recursos e informações a serem protegidos

- **Arquivos de Senhas:** A falta de proteção a esses arquivos compromete toda a segurança do seu sistema computacional que seja autenticado através deles. Se as informações neles contidas forem descobertas e decifradas, a vulnerabilidade será total.
- **Arquivos de Log:** *Log*[5] é o registro de atividade gerado por programas e serviços de um computador. Ele pode ficar armazenado em arquivos, na memória do computador ou em bases de dados.

Controles de Acesso Lógico

Recursos e informações a serem protegidos (Arquivos de Log)

- A partir da análise desta informação você pode ser capaz de:
  - Detectar o uso indevido do seu computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema.
  - Detectar um ataque, como de força bruta ou a exploração de alguma vulnerabilidade.
  - Rastrear (auditar) as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema.
  - Detectar problemas de *hardware* ou nos programas e serviços instalados no computador.

Controles de Acesso Lógico

Recursos e informações a serem protegidos (Arquivos de Log)

- Baseado nas informações do arquivo de Log, você pode tomar medidas preventivas para tentar evitar que um problema maior ocorra ou, caso não seja possível, tentar reduzir os danos. Alguns exemplos são:
  - Se o disco rígido do seu computador estiver apresentando mensagens de erro, você pode se antecipar, fazer *backup* dos dados nele contidos e no momento oportuno enviá-lo para manutenção.
  - Se um atacante estiver tentando explorar uma vulnerabilidade em seu computador, você pode verificar se as medidas preventivas já foram aplicadas e tentar evitar que o ataque ocorra;
  - Se não for possível evitar um ataque, os *logs* podem permitir que as ações executadas pelo atacante sejam rastreadas, como arquivos alterados e as informações acessadas.

Controles de Acesso Lógico

Recursos e informações a serem protegidos (Arquivos de Log)

- *Logs* são essenciais para notificação de incidentes, pois permitem que diversas informações importantes sejam detectadas, como por exemplo:
  - A data e o horário em que uma determinada atividade ocorreu.
  - O fuso horário do *log*, o endereço IP de origem da atividade.
  - As portas envolvidas e o protocolo utilizado no ataque (TCP, UDP, ICMP, etc.).
  - Os dados completos que foram enviados para o computador ou rede e o resultado da atividade (se ela ocorreu com sucesso ou não).

Controles de Acesso Lógico

Recursos e informações a serem protegidos (Arquivos de Log)

- Cuidados a serem Tomados:
  - Mantenha o seu computador com o horário correto (o horário em que o log é registrado é usado na correlação de incidentes de segurança e, por este motivo, deve estar sincronizado.
  - Verifique o espaço em disco livre em seu computador (logs podem ocupar bastante espaço em disco, dependendo das configurações feitas.
  - Evite registrar dados desnecessários, pois isto, além de poder ocupar espaço excessivo no disco, também pode degradar o desempenho do computador, comprometer a execução de tarefas básicas e dificultar a localização de informações de interesse.

Controles de Acesso Lógico

Recursos e informações a serem protegidos (Arquivos de Log)

- Cuidados a serem Tomados:
  - Fique atento e desconfie caso perceba que os *logs* do seu computador foram apagados ou que deixaram de ser gerados por um período (muitos atacantes, na tentativa de esconder as ações executadas, desabilitam os serviços de *logs* e apagam os registros relacionados ao ataque ou, até mesmo, os próprios arquivos de *logs*).
  - Restrinja o acesso aos arquivos de logs. Não é necessário que todos os usuários tenham acesso às informações contidas nos logs. Por isto, sempre que possível, permita que apenas o usuário administrador tenha acesso a estes dados.