# Introdução à Segurança da Informação

# Mecanismos de Controle Parte I

Prof. Dr. Daniel Caetano

2021 - 1

# Compreendendo o problema

- **Situação:** Em 2018 foi divulgado por malfeitores:

"Estamos de posse dos dados dos correntistas do Banco Inter. Caso não seja pago o resgate, divulgaremos todos os dados na Internet!"

**Se fosse da equipe de segurança, qual seria sua primeira atitude?**

# Compreendendo o problema

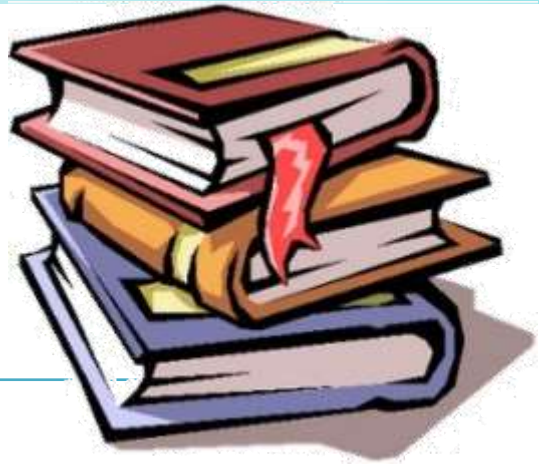
- **Situação:** Ao longo dos anos, diversas empresas como Vivo, Facebook, Sony, Yahoo... Foram vítimas reais de ataques cibernéticos e vazamentos.

**Que tipo de controle as empresas devem adotar para se proteger?**

# Objetivos

- Conceituar segurança lógica e física
- Compreender o que é identificação e autenticação
- Conhecer os procedimentos relacionados aos registros de acesso (logs)

# Material de Estudo

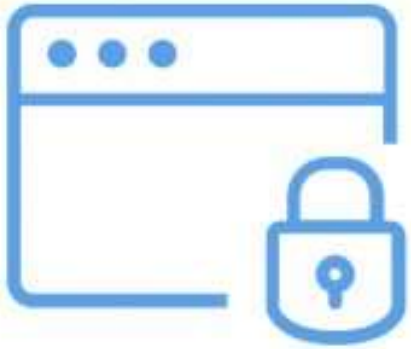


| Material | Acesso ao Material |
|---|---|
| Notas de Aula e Apresentação | http://www.caetano.eng.br/ (Segurança da Informação – Aula 5) |
| Biblioteca Virtual | Fundamentos de Segurança da Informação: com base na ISO 27001 e 27002, dos caps. 9 e 11 |
| Material Didático | Gestão de Segurança da Informação, Caps 1 e 5 |
| Leitura Adicional | http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (TCU - Cap. 2) |

# Aspectos Físicos, Lógicos e Administrativos da Segurança

# Componentes da Segurança

- Segurança, na prática: 3 aspectos
  - Físicos
  - Lógicos
  - Administrativos



# Aspectos Lógicos x Físicos

- Dado em Si x Meio Portante
  - Texto em uma folha de papel
  - Bytes em um SSD.

- Integridade
  - Lógica: conteúdo e autoria preservados
    - Em geral associada à equipe de TI
  - Física: integridade do meio portante
    - Em geral associada à segurança patrimonial
      - Mas está associada a TI também!

# Aspectos Lógicos x Físicos

**Não existe segurança lógica**

**sem segurança física**

# Elemento da Segurança

- Elementos Físicos
  - Barreiras e proteções

- Elementos Lógicos
  - Identificação/Autenticação
  - Registro em Logs
  - Controle de Permissões de Acesso

- Elementos Administrativos
  - Procedimentos

# Segurança Física

- Papel chave na Segurança da informação
  - **Nada** é seguro se houver acesso físico
  - Há muitos anos... (FBI)
    - 72% dos ataques originam-se em funcionários
    - 20% por autorizados pela empresa
    - 8% por agentes externos (pessoas sem permissões)
  - Hoje (Kaspersky/Redteam)
    - 50%+ ainda são originados em funcionários
    - 71% dos vazamentos acidentais
    - 68% dos vazamentos por ignorar a política
    - 61% dos casos de vazamento maliciosos

# Segurança Física

- Segurança totalmente física
  - Portas corta-fogo, diques, sprinklers...
  - Portão com cadeado, porta com chave
    - Autenticação física!
- Segurança mista (física + lógica)
  - Barreiras físicas com controle eletrônico
  - Identificação/autenticação falhou: barrar invasor
    - Portas, muros, grades
  - Invasor entrou: detectá-lo / identificá-lo
    - Sensores, câmeras, alarmes

# Segurança Lógica

- Controle de Acesso a Sistemas
  - Registros de acesso e operações
- Controle de Acesso Físico Automatizado
  - Software de acesso e apoio à auditoria
  - Características desejáveis
    - Impedir ataques forçados e acessos múltiplos
    - Registro de acessos detalhado
    - Autenticação robusta (smartcard + senha)
    - Controle centralizado de acesso e atualizações
    - Monitoração e relatórios de incidentes
    - Proteção de equipamentos e sistema backup.

# Segurança Lógica x Física

- Retomando
  - Segurança Física sem Lógica: Ok (Cadeado)
  - Segurança Lógica sem Física: Não Ok (Muro?)
    - Pular muro
- Investimentos em segurança Física
  - Grades, muros e portas
  - Guardas, crachás, sistemas de portas duplas
- Só isso basta?

**É preciso haver regras!**

# Aspectos Administrativos

- Processos
  - Política de Segurança da Informação
- No âmbito físico
  - Acesso a edifício / Datacenter
    - A pé x de carro
    - Morador x visitante x prestador
    - Entregas?
- No âmbito lógico
  - Quem e como pode acessar cada recurso?
  - Impressora da empresa: aberta para a Internet?
  - ...

## Formalizando:

# Aspectos Lógicos do Controle de Acesso

# Controle de Acesso

- Segurança pressupõe controle de acesso
  - Físico: portões, muros etc.
  - Lógico: login, registros etc.
- Envolve
  - Recurso: o que será protegido
  - Usuário: quem pode acessá-lo / modificá-lo
- Regra de ouro...

**Tudo é proibido a menos que expressamente permitido**

# Controle de Acesso

- Dois pontos fundamentais de interesse
  - **Proteger ativos (informações!) e transações** de usuários não autorizados
  - **Monitoramento do acesso** a recursos críticos para a empresa.
- Permitir a responsabilização dos usuários
- Permitir a auditoria
  - Identificar a falha e como ela foi explorada.

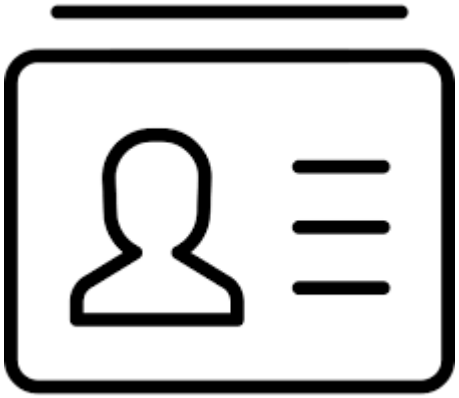
# Controle de Acesso: Procedimento

- **Logon/Login**: dois processos básicos
  - Identificação**:** qual é o usuário e suas permissões
  - Autenticação**:** comprovar a identidade

- Identificação: por meio de informação única
  - Número de identificação, nome de usuário...
- Autenticação: informação ou item de posse exclusiva do usuário
  - Senha, medição biométrica, chave criptográfica...

# Controle de Acesso: Procedimento

- **Logon/Login**: dois processos básicos
  - Identificação**:** qual é o usuário e suas permissões
  - Autenticação**:** comprovar a identidade
- Resumindo
  - **Identificacão** + **Algo que usuário sabe ou tem**



**Mais detalhes na próxima aula!**

# Burlando o Controle de Acesso

https://youtu.be/pZcF4oZbB14

# Burlando o Controle de Acesso

https://youtu.be/pZcF4oZbB14

**O que fazer quando ele falha?**

# Registros de Acesso e Operação: Logs

# Registros de Acesso e Operação

- O que são?
  - Na segurança física/patrimonial...
    - São as imagens das câmeras
  - Quem fez o quê
    - Complementados com registros de identificação

# Registros de Acesso e Operação

- E na segurança lógica?
  - Registros cronológicos e detalhados de:
    - O que foi feito
    - Quem fez
    - Onde/De onde fez (se for o caso).
  - Possibilitam a reconstrução e revisão...
  - ...de uma operação, procedimento ou evento...
  - ...do início ao fim.

Foram encontrados **10320** registros.

Primeira | Anterior | **1** 2 3 4 5 6 ... | Próxima | Última

| Data | Identificador | Usuário | Tipo | IP | Requisição |
|---|---|---|---|---|---|
| 12/05/2010 às 09:49 | aix sistemas | | Outros | 192.168.0.9 | /webgizead/index.php?option=com_aixadministracao&view=logacesso |
| 12/05/2010 às 09:46 | aix sistemas | | Outros | 192.168.0.9 | /webgizead/index.php?option=com_aixadministracao&view=papelpessoa |
| 12/05/2010 às 09:46 | aix sistemas | | Outros | 192.168.0.9 | /webgizead/index.php?option=com_aixadministracao&view=papelpessoa |
| 12/05/2010 às 09:44 | aix sistemas | | Outros | 192.168.0.9 | /webgizead/index.php?option=com_aixadministracao&view=papelpessoa |
| 12/05/2010 às 09:44 | aix sistemas | | Outros | 192.168.0.9 | /webgizead/index.php?option=com_aixadministracao&view=papelpessoa |

# Registro de Acesso e Operação

- Finalidade
  - Auditoria
- Também conhecidos como
  - Logs ou Logging
- Demanda ações da administração do sistema
  - Cadastro / Comunicação de Senhas
    - Cada usuário é único no sistema (incluindo adms)
  - Gerenciamento de permissões
  - Gerenciamento dos próprios logs
  - Auditorias Frequentes.

# Exemplos de Logs

- Log de acesso

```
20/01/2008 - 22:17:55 - IP: 200.178.95.16 - ddamasio logged in.
20/01/2008 - 22:19:30 - IP: 200.192.67.112 - jsoldi logged in.
20/01/2008 - 22:54:17 - IP: 200.178.95.16 - ddamasio logged out.
20/01/2008 - 22:55:32 - IP: 200.192.67.112 - jsoldi logged out.
20/01/2008 - 23:20:13 - IP: 163.102.100.17 - cabrahm logged in.
21/01/2008 - 00:10:11 - IP: 163.102.100.17 - cabrahm logged out.
```

- Log de operações

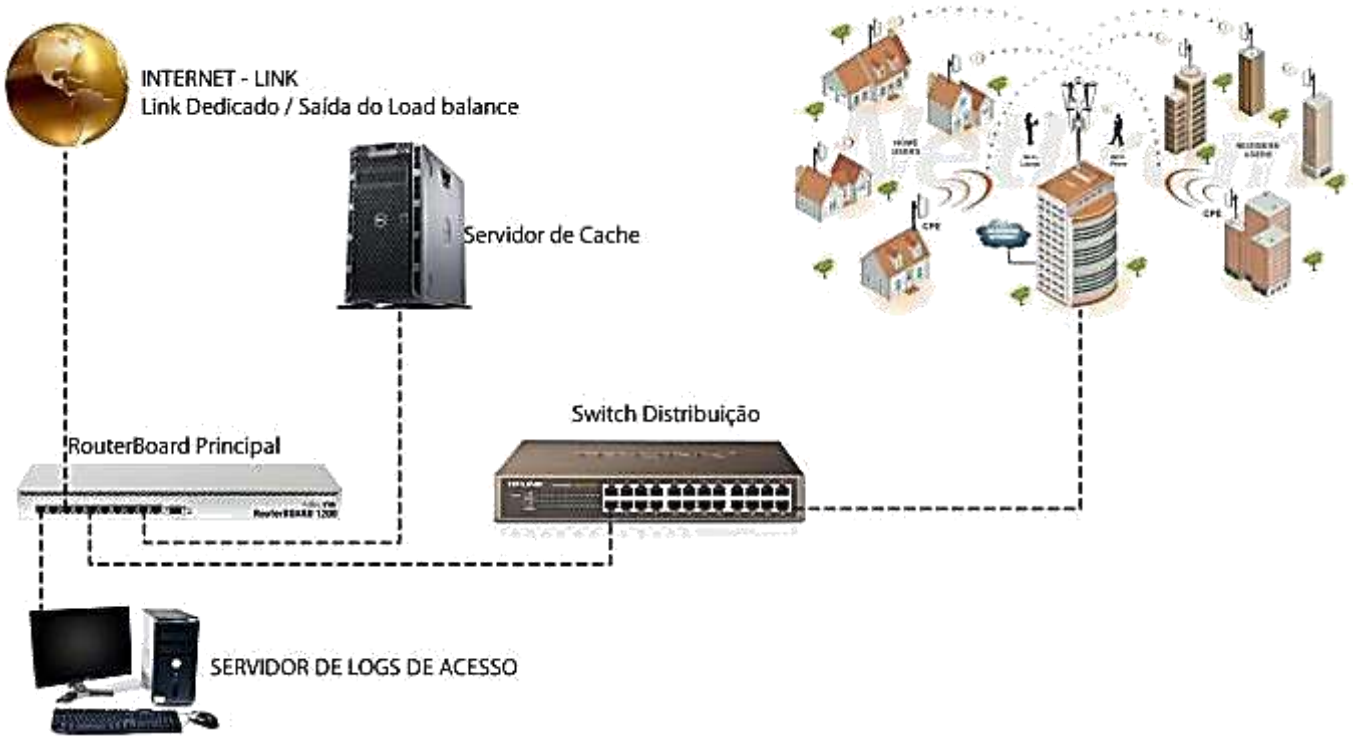
```
20/01/2008 - 23:25:33 - IP: 163.102.100.17 - copied \\COMP3\shared\test.c to c:\work.
20/01/2008 - 23:27:33 - IP: 163.102.100.17 - opened file c:\work\test.c.
21/01/2008 - 00:08:25 - IP: 163.102.100.17 - saved and closed file c:\work\test.c.
```

# Sincronia de Relógios

- A sincronia de relógios é fundamental
- Por quê?
  - Correlacionar logs em máquinas diferentes!
  - Sistemas de Single Sign-On não funcionam sem.
- Como manter a sincronia?
  - Linux: ntpdate –s pool.ntp.br
  - Windows: Configuração > Hora e Idioma
    - “Definir Horário automaticamente” como ligado

# Armazenamento dos Logs/Vídeos

- Onde armazenar os logs e vídeos?
  - Em geral, existe um armazenamento local
  - Pode ser externo (rede) ou misto



# Armazenamento Local de Vídeo

- Vantagens
  - Configuração mais simples
  - Baixo consumo de recursos
  - Funciona mesmo que a rede dê problemas.
- Desvantagens
  - Dano no equipamento pode impedir avaliação
    - Invasor terá acesso ao equipamento!

# Armazenamento Remoto de Vídeo

- “Central de Vídeo”
- Vantagens
  - Administração centralizada
    - Facilita a gestão de espaço em disco
  - Proteção maior: invasor dificilmente terá acesso
    - Limitar significativamente o poder de alterar/apagar.
- Desvantagens
  - Configuração mais complexa
  - Maior consumo de recursos
  - Se a rede cair (ou for cortada)...

# Armazenamento Local de Logs

- Vantagens
  - Configuração mais simples
  - Baixo consumo de recursos
  - Funciona mesmo que a rede dê problemas.
- Desvantagens
  - Administração descentralizada
  - Proteção depende do sistema de arquivos e S.O.
    - Pode ser alterado/apagado, se permissões autorizarem
  - Se disco lotar por alguma outra razão...
    - O registro nos logs ficará comprometido.

# Armazenamento Externo de Logs

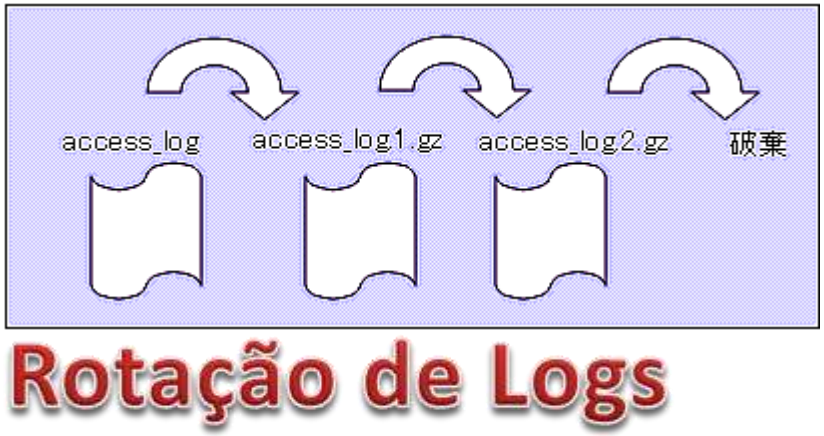
- “Servidor de Log”
- Vantagens
  - Administração centralizada
    - Facilita a gestão de espaço em disco para log
  - Proteção maior: limitar acesso ao servidor de log
    - Limitar significativamente o poder de alterar/apagar.
- Desvantagens
  - Configuração mais complexa
  - Maior consumo de recursos
  - Se a rede cair, pode deixar de realizar registros.

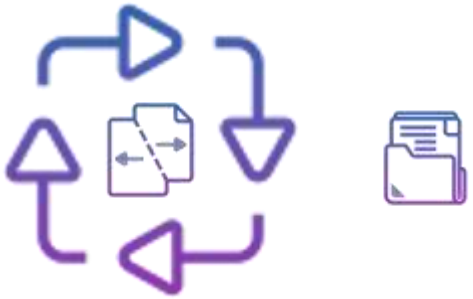
# Armazenamento Misto

- Duplo registro: local e via rede
- Vantagens
  - Maior segurança geral
    - Dificilmente o invasor conseguirá apagar todas as suas pistas
  - Se rede falhar ou disco local lotar, haverá registros
    - Se os dois ao mesmo tempo... Aí não! ☺.
- Desvantagens
  - Administração complexa (espalhada + servidor)
  - Configuração bastante mais complexa
  - Consumo de recursos significativamente maior
  - Maior complexidade na auditoria (logs diferentes).

# Rotação de Logs e Vídeos

- Até quando preciso guardar os logs e vídeos?
  - Critérios legais
  - Critérios de negócio
  - Espaço.
- Liberar espaço...
  - De tempos em tempos, começar um novo
  - Comprimir arquivos mais antigos
  - Apagar os que já “venceram”...
    - ...E/ou foram auditados



# Auditoria de Logs e Vídeos

- Reconstruir eventos
  - “Seguir as migalhas de pão”
- Monitoramento...
  - Proativo x Reativo
- Auditoria frequente
  - Tanto quanto o sistema for crítico
  - Qualquer evento estranho deve ser investigado.

# ATIVIDADE

# Atividade

- Vamos fazer um brainstorm...

**Que mecanismos de controle de acesso você consegue imaginar?**

# ENCERRAMENTO

# Resumo e Próximos Passos

- Segurança lógica x física
  - Envolvimento da TI
- Mecanismo de controle de acesso
- Sistema de registro de acesso
  - Sincronização de relógios e rotação de logs
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

---

- Controle de Acesso
  - Mecanismos de identificação e autenticação

# PERGUNTAS?