Introdução à Segurança da Informação

Boas Práticas da Segurança da Informação – Parte I

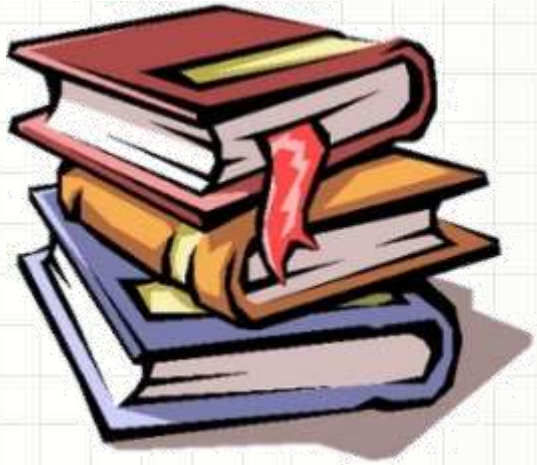
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Recordar os mecanismos básicos de segurança da informação
- Conhecer os conhecimentos básicos a serem transmitidos para os usuários nos treinamentos
- Compreender a lógica das políticas de senhas

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 7)
Material Didático	Gestão de Segurança da Informação, Cap 5.
Leitura Adicional	http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (Cartilha do TCU)

Mecanismos Básicos de Proteção

Proteção Básica

- Qual é o mínimo que devo fazer?
  - Antivírus
  - Firewall
  - Configuração Segura da Rede
  - Configuração Segura de Software
  - Rotinas de segurança

Proteção Básica

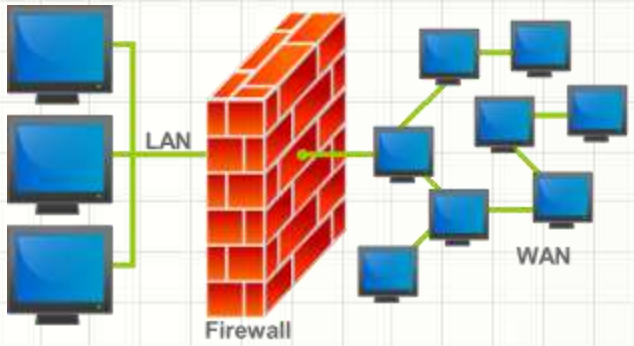
- Sempre que possível...
  - Soluções gerenciadas remotamente
    - Limite o acesso às máquinas de gestão de segurança.

Proteção Básica - Antivírus

- O que tem de importante?
  - Use.
  - Use sempre.
  - Ative a proteção em tempo real
  - Ative a proteção contra scam
  - Agende checagens semanais
    - No fim de semana, se máquinas ficam ligadas
    - Segunda no início do expediente, se ficam desligadas.
  - Agente atualizações diárias
    - Do antivírus
    - Das definições de ameaças.

Proteção Básica - Firewall

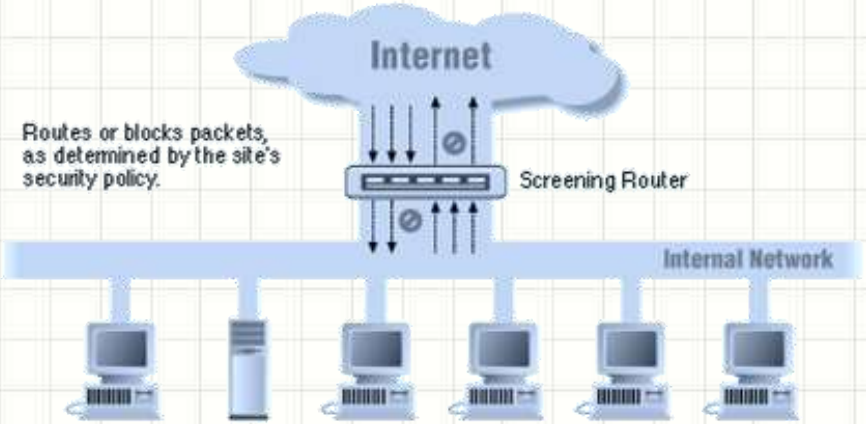
- O que tem de importante?
  - Use.
  - Use sempre.



  - Feche absolutamente todas as entradas novas
    - Abra apenas aquelas absolutamente necessárias.
  - As portas que precisem ficar abertas...
    - Se possível, abra apenas para os IPs necessários
      - Pelas interfaces necessárias
    - Se possível, use alternativas (como SSH... 22 para xx)
    - Monitore-as (SSHGuard, por exemplo).
  - Conexões negadas: use DROP ao invés de REJECT

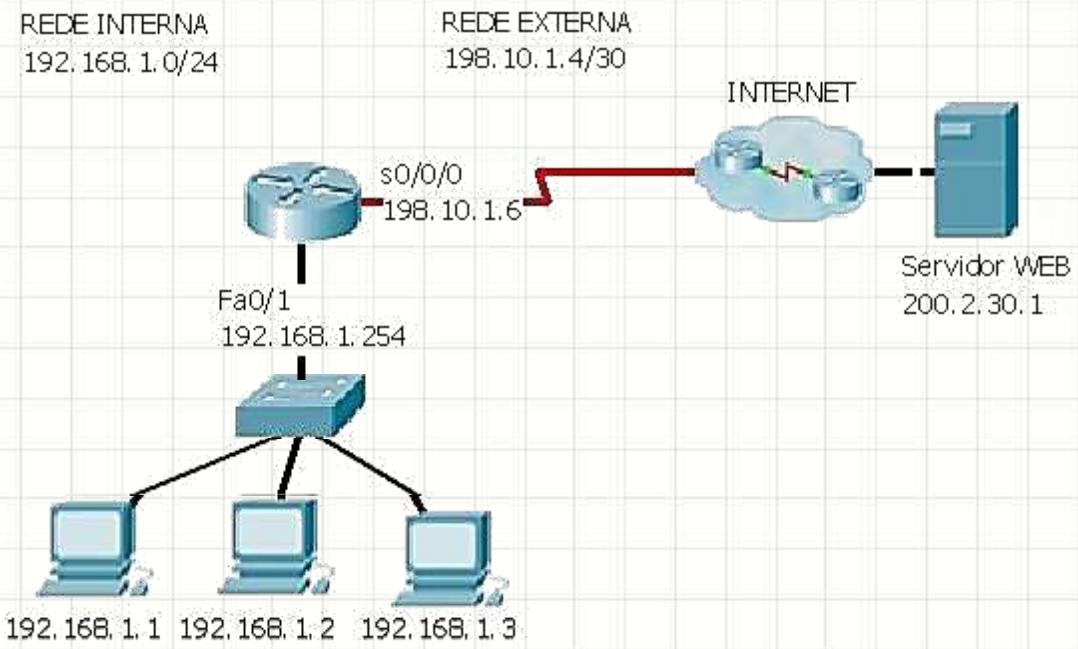
Proteção Básica - Rede

- Preciso fazer algo?
  - Configure o roteador adequadamente
    - IPv4 e IPv6
    - Use VLANs (LANs virtuais) adequadamente.
  - Roteador: há recursos de filtragem?
    - Use!
    - Compartilhamento de Arquivos e Impressoras?.



Proteção Básica - Rede

- Preciso fazer algo?
  - Se usar IPv4...
    - Dê preferência para alocar IPs locais para as máquinas
    - Disponibilize publicamente apenas portas necessárias.
  - Se usuários precisarem de acesso remoto: VPN



Proteção Básica - Software

- Preciso fazer algo?
  - Nunca permita que usuário instale software
    - Se necessário, deve solicitar... E software será avaliado.
  - Sempre mantenha a versão mais atualizada
    - Em especial de softwares que abrem portas na rede.

Proteção Básica - Software

- Preciso fazer algo?
  - Sempre verifique e configure muito bem
    - A maior parte das “falhas” são configurações ruins.
  - Se possível, use um servidor proxy web (squid etc.)
    - Bloqueie o acesso a sites indesejados
    - Alternativa: liberar apenas os sites “úteis”: cuidado!.

Proteção Básica - Rotinas

- O que é “rotina de segurança”?
  - Verificação e rotação de logs
    - Sistema, falhas de login, aplicações....
  - Verifique tráfego, CPU, espaço livre etc.
    - Se possível, use um monitor (Zabbix, Nagios...).
  - Cuidar da política de senhas
  - Verificar a execução dos backups
    - Se possível, verificar a restauração dos mesmos.

Treinamento aos Usuários

Treinamento

- É importante?
  - Evitar “desconhecimento”
  - Com relação à lei, desconhecer não é desculpa.

Treinamento

- Alguns elementos que não podem faltar:
  - Regras para os Recursos Disponibilizados
    - O que pode ou não ser feito com os mesmos!
    - Atividades ilegais são de responsabilidade dos autores!.
  - Sistemas de Monitoramento
    - Funcionários precisam estar cientes!
    - E-mail, sites visitados, ligações feitas e recebidas....

Treinamento

- Alguns elementos que não podem faltar:
  - Inspeção de Conteúdos
    - Empresa pode inspecionar qualquer dado
  - Instalação de Software
    - Que não podem instalar sem autorização formal e expressa da empresa

Treinamento

- Alguns elementos que não podem faltar:
  - Regras de Firewall/Proxy
    - Quais são as regras e que elas não podem ser alteradas
  - Divulgação de informações
    - Quais são as regras, classificações, penalidades...

Treinamento

- Alguns elementos que não podem faltar:
  - Uso recreativo da Internet
    - Se for possível, apenas no almoço ou fora de expediente
    - Apenas para atividades legais.
  - Preservação dos dados de acesso
    - Cuidados com as senhas...

Políticas de Senhas

Senhas: Quebrando-as

- Existem 2 formas básicas de se obter senhas
  - Engenharia Social **Com jeitinho**
    - Conseguir que a pessoa a forneça
    - Encontrar a mesma registrada em local não seguro
    - Senhas óbvias (informações facilmente encontradas).
  - Força Bruta **Na marra**
    - Testar usuários/senhas até encontrá-los
    - Palavras comuns
    - Senhas simples (usando apenas letras, por exemplo).
- Vejamos regras e orientações para dificultar...

Senhas: Regras

- As seguintes regras devem ser seguidas
  - Manter a confidencialidade das senhas
  - Nunca compartilhar senhas
  - Evitar registrar as senhas em papel
    - Se precisar registrar, use um software adequado
    - Ex.: KeePass, mSecure, LastPass, DashLane....

LastPass •••|

Senhas: Regras

- As seguintes regras devem ser seguidas
  - Selecionar senhas de boa qualidade
    - Muito curtas: ruim
    - Muito longas: ruim
    - De 6 a 8 caracteres.
  - Alterar quando houver indício de anormalidade
  - Alterar as senhas em intervalos regulares
    - Usuários com acesso privilegiado: intervalos menores.

Senhas: Regras

- Informe sempre aos usuários
  - Evitar reutilizar senhas já usadas no passado
  - Obrigar mudar senhas temporárias no 1º acesso
  - Não incluir senhas em processos automáticos
    - Macros, navegador etc.
    - Repositórios de código!.
  - Evitar usar a mesma senha para vários sistemas
    - Se usar do tipo Single Sign-On, use uma complexa
    - Ex.: Google, Facebook etc..

Senhas: Orientações

- Algumas orientações podem ser passadas
  - E muitas delas podem virar regras também!
- Evitar senhas facilmente identificáveis
  - Nome do usuário ou user id (mesmo embaralhado)
  - Nomes (familiares, amigos, lugares etc).
  - Nome do sistema operacional ou da máquina
  - Números de telefone ou documentos
  - Datas.

Senhas: Orientações

- Evitar senhas facilmente identificáveis (cont.)
  - Placas, marcas de carro, etc..
  - Palavras que constam em dicionários
  - Letras ou números repetidos
  - Letras seguidas do teclado
    - ASDF, QWERTY, 123456...
  - Objetos ou locais visíveis da mesa do usuário
    - Livro na estante, loja vista pela janela...
  - Qualquer senha com menos de 6 caracteres.

Senhas: Orientações

- Dificultar “adivinhação” e “força bruta”
- Boas práticas em senhas
  - Fácil de memorizar por você, mas não por outros
  - Usar, simultaneamente:
    - Números
    - Caracteres especiais.
    - Letras maiúsculas e minúsculas
  - Senhas que possam ser digitadas rapidamente
  - Seguir todas as regras anteriores

Senhas: Distribuição

- Deve ser feita com cuidado e com orientação
  - O usuário precisa saber a importância da senha!.
- Solicitar que usuário assine declaração
  - Tomando ciência da confidencialidade da senha.
- Garantir senha temporária segura
  - E forçar usuário a mudá-la no primeiro acesso
  - Fornecer senha temporária em mãos, se possível
  - Se fornecer link para cadastro de senha...
    - Limitar o tempo para isso (1 hora, por exemplo)
    - Ter certeza que e-mail é do usuário e não foi invadido.

Senhas: Medidas Adicionais

- Uso de sistemas que dificultem quebra
- No cadastro da senha
  - Indicar o nível de segurança da senha
  - Impedir o cadastro de senhas “fracas”
  - Expirar as senhas de tempos em tempos
    - Ex.: 42, 45, 90... dias
  - Evitar reuso de uma das últimas senhas
    - Ex.: 5, 12, 24...
  - Guardar as senhas na forma de hashs.

Senhas: Medidas Adicionais

- Uso de sistemas que dificultem quebra
- Na tela de *login*
  - Bloqueio após erros
    - 3 ou 5 erros (mínimo 30 minutos)
  - SSHGuard
  - Captchas

  - Nunca informar que “usuário não existe” ou “senha incorreta”, isoladamente, em caso de erro de *login*

Senhas: Alternativas

- Há alternativas ao uso de senhas
  - Uso de *Tokens* (cartões de senha ou dispositivos)
  - Certificados Digitais (*smartcard*)
  - Uso de biometria
  - Ativação de dispositivos.



- Em geral, em sistemas de alta segurança...
  - Usa-se esses métodos alternativos...
  - ...**E** uma senha + verificação 2 passos

Senhas: Administração de Usuários

- Desativar usuários inativos
  - Demitidos, transferidos etc.
  - Em férias?.
- Todo funcionário inativado...
  - Deve ser inativado em todos os sistemas
- Não apague os dados do usuário
  - Apenas desative-os
  - Não forneça acesso livre a esses dados.

QUESTÕES

Quiz

Uma senha deve ser moderadamente longa e incluir diferentes tipos de caracteres para...

https://kahoot.it/

Conclusões

Resumo e Próximos Passos

- Principais medidas básicas de segurança
- Treinamento básico de usuários
  - Aspectos de segurança
- Política de Senhas
  - Regras, orientações e procedimentos

- + Boas práticas em segurança da informação
  - Controle de Acesso
  - Gestão de Logs
  - Políticas de Backup

PERGUNTAS?