Introdução à Segurança da Informação

Ameaças e Vulnerabilidades partes II e III

Prof. Dr. Daniel Caetano

2021 - 1

Trabalhos, Datas e Aprovação

Trabalho	Valor	C.H.	Data
Desafios até Aula 05	0,5 em Prova	2h	Segunda (Web)
Desafios após Aula 05	0,5 em Prova	2h	Segunda (Web)
Atividade Avaliativa – Aula 02	1,0 na AV1		13/04
Atividade Avaliativa – Aula 05	2,0 na AV1		27/04
Avaliação P1	**7,0 na AV1**	**2h**	**04/05 (Aula)**
Avaliação P2	**10,0 na AV2**	**2h**	**15/06 (Aula)**
Avaliação P3	**10,0 na AV3**	**2h**	**29/06 (Aula)**
Avaliação Digital (AVD)	**10,0 na AVD**		**07~18/06**
Avaliação Digital Substitutiva (AVDS)	**10,0 na AVD**		**24~30/06**

Os desafios serão sempre postados aqui:
https://padlet.com/djcaetano/seguranca

Compreendendo o problema

- **Situação:** empresas de 74 países foram alvos de ataques e seus dados sequestrados. Serão devolvidos mediante pagamento.

O que você faria?

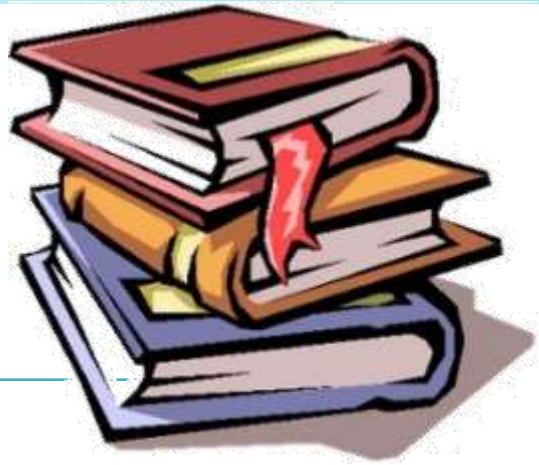
Maior Ação de Hackers da História

https://youtu.be/9MfTLSuZBAI

Objetivos

- Conhecer as principais ameaças
- Entender o mecanismo de atuação das ameaças
- Compreender o conceito de vulnerabilidades
- Conhecer os mecanismos básicos de prevenção em segurança da informação

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 3)
Biblioteca Virtual	Fundamentos de Segurança da Informação: com base na ISO 27001 e 27002, do item 12.4 a 12.5
Material Didático	Gestão de Segurança da Informação, Caps 3 e 5
Leitura Adicional	Pra quem não leu ainda: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf (Cartilha do CERT – Cap. 4) http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf (Cartilha do TCU)

CONTEXTO

Ameaças à Informação: Contexto

- Segurança da Informação...
  - É uma preocupação antiga!

Ameaças à Informação: Contexto

- O mundo mudou muito nas últimas décadas
  - Documentos são digitais
  - Processos são digitais
  - Uso da “nuvem”
  - Dispositivos “sempre online”
  - Todos os dispositivos sempre online...!

Maior Exposição!

Ameaças à Informação: Contexto

- Os “armários”, hoje em dia, são digitais!

Ameaças à Informação: Contexto

- Política de Segurança da Informação (PSI)
  - Regulatória x Informativa x Consultiva
  - Procedimentos e obrigações
    - Quem pode/deve o quê
  - Imprescindível!

Ameaças à Informação: Contexto

- Fontes para uma PSI (ABNT)
  - Princípios, objetivos e necessidades da organização
  - Legislação vigente (Marco Civil e LGPD, p. exemplo)
  - Avaliação de riscos
    - Identificar ameaças e vulnerabilidades

Ameaças à Segurança das Informações

Ameaças à Segurança

- Potencial de violação à segurança
  - Circunstância, ação ou evento
    - → quebra da segurança

Ameaças à Segurança

- Ameaça Organizacional
  - Situações externas
  - Tempo presente ou futuro
  - Podem afetar a empresa negativamente.

Eliminar, minimizar ou evitar

Ameaças à Segurança Organizacional

- Referem-se à perda de:
  - Integridade
    - Informação exposta ao manuseio não autorizado
  - Confidencialidade
    - Informação exposta à visualização não autorizada
  - Disponibilidade
    - Informação deixa de estar acessível no momento necessário às atividades do negócio

Ameaças à Rede ou Sistemas

- As informações e processos digitais...
  - Dependem do uso de redes e sistemas
- Ameaças podem focar nesses elementos

Aparte: Hackers x Crackers

- Hackers
  - Muito conhecimento em TIC
  - Conhecimento avançado de programação
  - Conhecimentos de eletrônica, psicologia etc...
  - Ação: dentro da legalidade(?)
  - Motivação: avanço tecnol.(?), causa(?)...

- Crackers
  - Conhecimento como o dos hackers
  - Ação: quebra da legalidade
  - Motivação: notoriedade, vingança, ganhos...

Aparte: Hackers x Crackers

- Na terminologia hackers
  - Chapéu Branco (White Hat)
  - Chapéu Preto (Black Hat)
  - Chapéu Cinza (Gray Hat)
    - Fins do White Hat
    - Meios do Black Hat

PRINCIPAIS TIPOS DE AMEAÇAS

Principais Tipos de Ameaças

- Pessoas mal intencionadas!
  - E seus ataques...

- Golpes diversos (mais na aula que vem)
- Softwares do tipo "*malware*"
  - **Mal**icious Soft**ware**
  - Software que se infiltra na máquina de forma ilícita
    - Causa danos, alterações ou roubo de informações

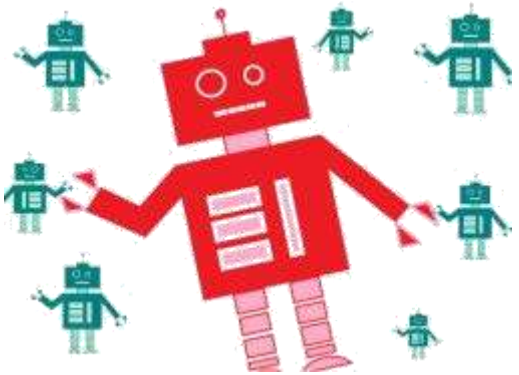
Principais Tipos de Ameaças

- Softwares do tipo "*malware*"
  - Como se infiltram?

- Diversos mecanismos:
  - Vulnerabilidades de programas existentes
  - Execução de arquivos infectados
  - Auto-execução de mídias infectadas
  - Acesso a páginas web com navegadores vulneráveis
  - Ação direta de atacantes.

Principais Tipos de Ameaças

- Principais tipos de *malware*
  - Vírus
  - *Worms*
  - *Trojans*
  - *Bots* e *Botnets*
  - *Spywares*
  - *Rootkits*



Malwares - Vírus

- Programas que alteram softwares instalados
- Propagação: execução de arquivos infectados
  - Mídias Removíveis (Disquetes, pen drives...)
  - Comunicação (E-mails, mensagens...)
  - Repositórios
- Tipos
  - Vírus em executável (mais comum em e-mails)
  - Vírus de script (em geral vem por e-mail também)
  - Vírus de macro (em geral em documentos)
  - Vírus de smartphone (mensagens MM ou por BT).

Malwares - Worms

- Programas que alteram softwares instalados
- Propagação: automática
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores
- Processo
  - Identifica os computadores alvos
  - Envia cópias
  - Ativação (automática ou por ação do usuário)
  - Volta ao primeiro passo...

Malwares - Trojan

- Programa “legítimo”, inclui “surpresas”
  - Cartões virtuais, jogos, cracks
- Propagação: ação do usuário
- Tipos de *Trojans*
  - *Downloader/Scareware*: baixa/exec. códigos maliciosos
  - Dropper: executa códigos maliciosos embutidos.
- Ações comuns dos *Trojans*
  - *Proxy/Backdor*: age como *proxy* ou abre *backdoor*
  - *Destructor*: apaga coisas, formata discos...
  - *Ransonware*: criptografa os dados dos usuários
  - *Clicker*: redireciona a navegação do usuário.
  - *Bots, Spyware e Rootkits*...

Malwares - Bots

- Programas que permitem controle da máquina
  - Por meio da rede!
  - Computador vira um “zumbi”
  - Pode-se comandar vários: Botnet

- Propagação
  - *Worms* ou *trojans*
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores... Quando ativos!

Malwares - Spyware

- Programas que permitem monitorar a máquina
  - Envia informação de interesse para terceiros
- Propagação
  - *Worms* ou *trojans*
- Tipos comuns
  - Keylogger: captura as teclas pressionadas
  - Screenlogger: captura a tela da aplicação
  - Banker: obter dados bancários
  - Adware: mostrar propagandas

Malwares - Rootkits

- Programas que alteram o sistema operacional
  - Abrindo diversas brechas de segurança
- Propagação
  - *Worms* ou *trojans*

- Características
  - Comprometem severamente a máquina
    - Permitem que o invasor assuma o papel de “root”
  - Muito difíceis de detectar
  - Muito difíceis de remover

Mentimeter

VULNERABILIDADES

Vulnerabilidades

- O que são?
  - Pontos fracos existentes nos ativos

  - Quando explorados, afetam
    - Integridade, disponibilidade e confidencialidade.

Vulnerabilidades

- Não seriam um problema se...
  - Não houvesse ameaças que as explorem
  - Mas as ameaças existem!

  - E com a evolução...
    - As vulnerabilidades tendem a aumentar

Pontos fracos devem ser eliminados!

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.

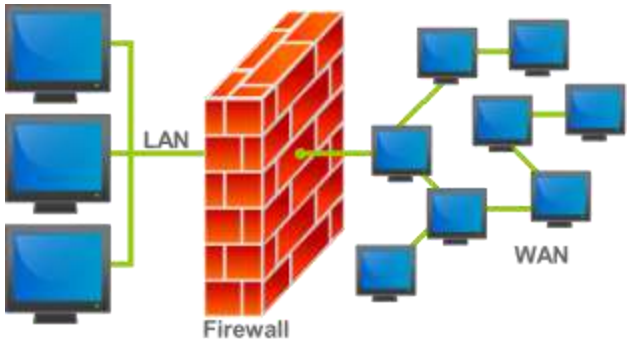
Proteção Básica - Antivírus

- O que tem de importante?
  - Use.
  - Use sempre.
  - Ative a proteção em tempo real
  - Ative a proteção contra *scam*/*phishing*
  - 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.

Próxima Aula!

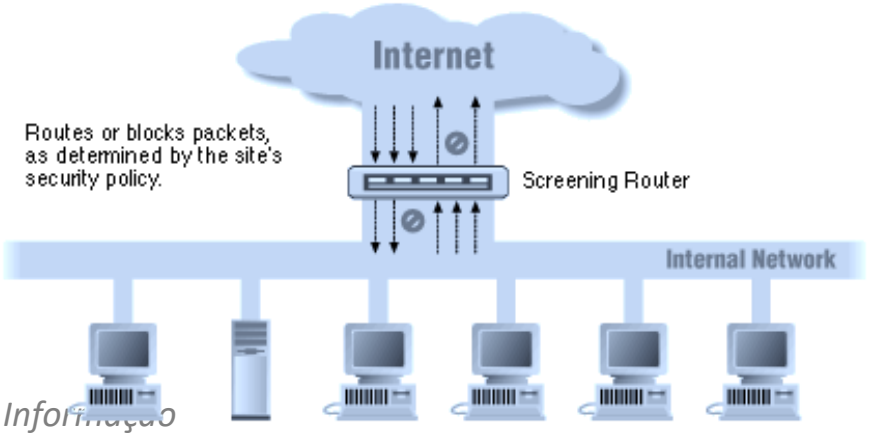
Proteção Básica - Firewall

- 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



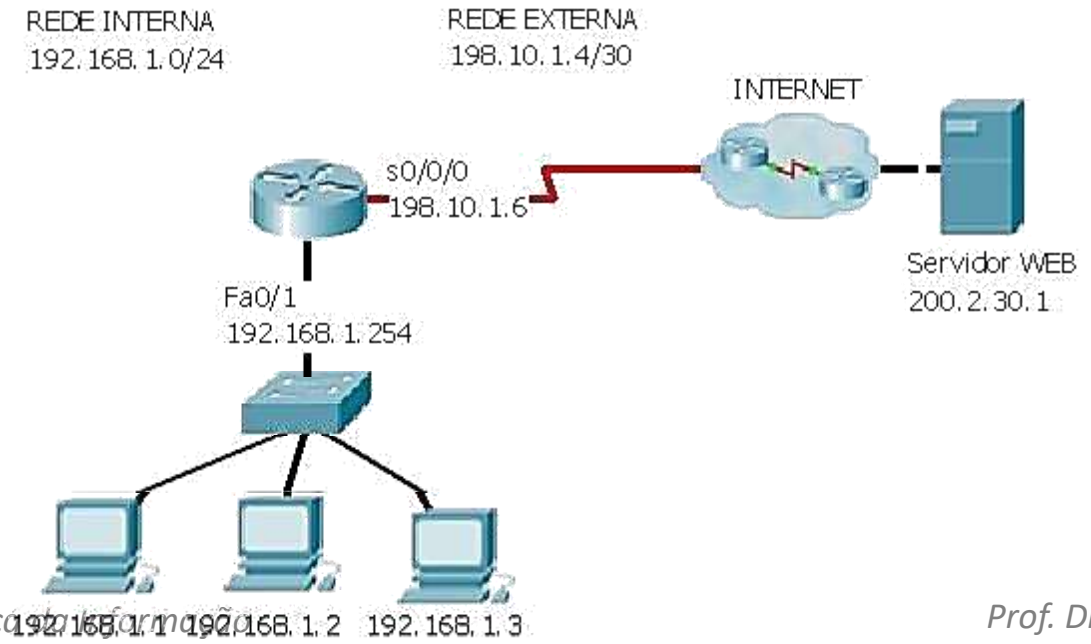
Proteção Básica - Rede

- 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.

Mentimeter

ATIVIDADE

Atividade

- Grupos – 15 minutos
  - Conforme canais do Teams
- Procurem na internet casos reais em que houve ataque de *malware* em uma empresa.
- Discuta com seu grupo e selecione UM dos casos.
- Quando chegar a vez do grupo, explique a ocorrência, o tipo de *malware* e qual seria a forma de evitar que o problema ocorresse.

ENCERRAMENTO

Resumo e Próximos Passos

- Principais tipos de Ameaças
  - E suas características
- O que são as vulnerabilidades
- Mecanismos de prevenção básicos
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Técnicas de Ataques Cibernéticos
  - Vulnerabilidades, ataques e ferramentas

PERGUNTAS?