Segurança Cibernética

Revisão Geral!

Prof. Dr. Daniel Caetano

2021 - 2

PRÉ AV1

SEMANA 1

Importância da Informação

- O mundo mudou muito nas últimas décadas
  - Documentos e processos são digitais: nuvem
  - Todos os dispositivos “sempre online”!

- Tudo, hoje, exige informações
  - São essenciais para os negócios!
  - Informações são ativos!

Princípios Fundamentais

- Quais são?
  - Confidencialidade
  - Integridade
  - Disponibilidade
- Magnitude de Impactos
  - **Baixa**: Efeito adverso limitado nas operações, ativos ou indivíduos
  - **Moderada**: Efeito adverso sério nas operações , ativos ou indivíduos
  - **Alta**: Efeito adverso catastrófico nas operações, ativos ou indivíduos

Hackers x Crackers

- Público: Hackers = Crackers
- Hackers
  - Ação: **SEM quebra da legalidade**

- **Atuação Legal: Hackers Éticos**
  - Identificação e correção de falhas
  - Análise de código
  - Teste de Invasão (*pentesting*)
    - Metaexploits

PRÉ AV1

SEMANA 2

O que precisa ser protegido?

- Dados gerais que são parte da operação
- Dados estratégicos
- Dados associados às leis gerais
  - Lei Geral de Proteção de Dados
  - Marco Civil da Internet...

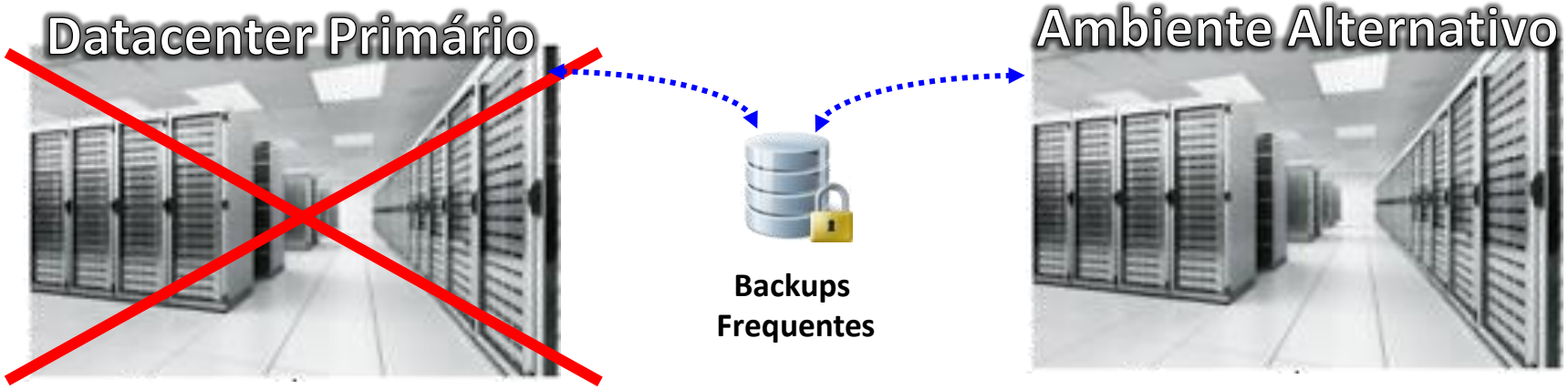
- Dados associados às leis específicas
  - Tributária, sanitária...
- Foco: evitar exposição e perda de dados
  - Adicional: evitar uso abusivo dos dados

Situações indesejáveis

- Revelação não autorizada
  - Quebra de confidencialidade
  - Exposição, interceptação, inferência, intrusão;
- Fraude
  - Quebra de integridade de dados ou sistema
  - Personificação, falsificação, retratação/repúdio;
- Disrupção
  - Quebra da disponibilidade ou integridade (D/S)
  - Incapacitação, corrupção, obstrução;
- Usurpação
  - Quebra da integridade do sistema
  - Apropriação indevida, utilização indevida.

Ambientes Alternativos e Backups

- Ajuda se existir um ambiente “espelho”
  - Ambientes de operação alternativos
- Três tipos
  - Cold Site
  - Warm Site
  - Hot Site

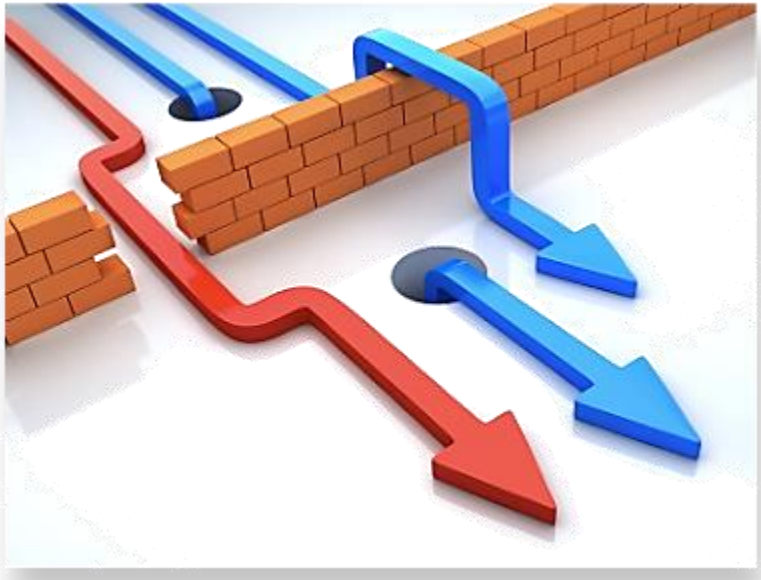


PRÉ AV1

SEMANA 3

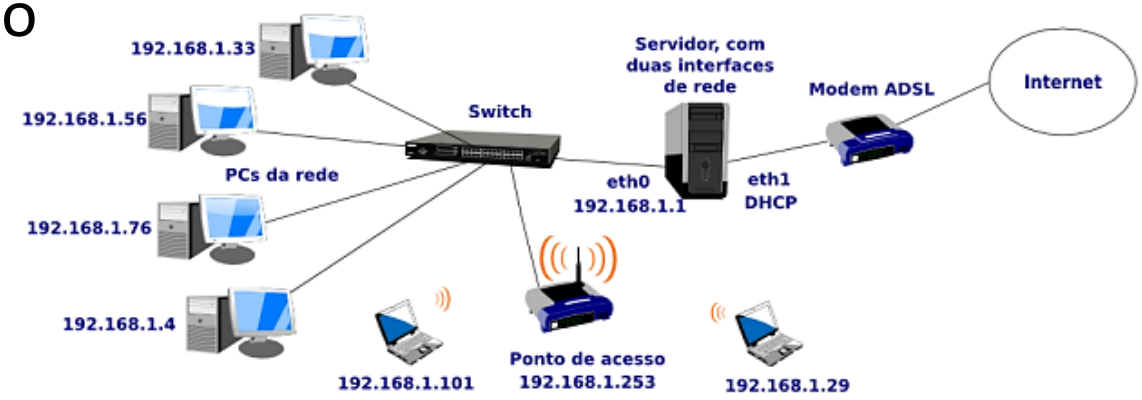
Vulnerabilidades

- Onde estão?
- Múltiplas fontes
  - Pessoas
    - Engenharia Social
  - Softwares
    - Falhas de design
    - Falhas de implementação
    - Problemas de configuração
  - Equipamentos e Infraestrutura
    - Falhas de hardware/software/configuração
    - Problemas de capacidade



Quais são os equipamentos?

- Operações x Datacenter
  - Equipamentos básicos x proteção
- Equipamentos Básicos
  - Infraestrutura de rede
    - Roteadores: encaminham dados entre múltiplas redes
    - Switches: distribuem dados dentro de uma rede
    - Access points: comunicação de dados sem fio
    - Cabeamento: transportam dados por meio físico.
  - Armazenamento
    - *Storages*
  - Processamento
    - Servidores.

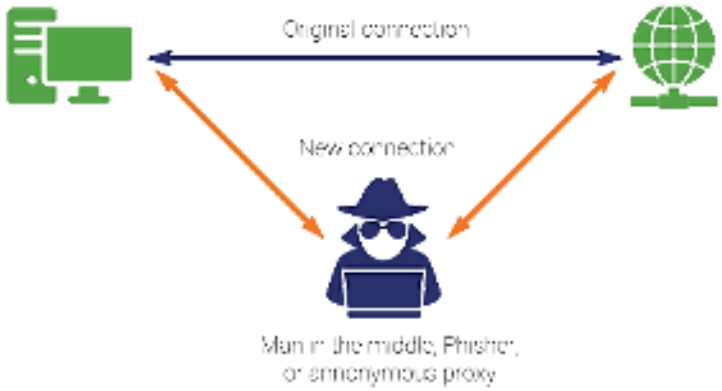


Preparação de um ataque

- Ataques são planejados
- Inicio dos ataques:
  - Coleta de dados
- Como fazer isso?
  - Técnicas de reconhecimento
    - Engenharia social, mergulho no lixo, rastreio...
  - Uso de software/hardware específico
    - Farejadores, por exemplo

Vulnerabilidades do TCP/IP

- Sem criptografia ou autenticação por padrão
- Falsificação de IP
- Sequestro de conexão
- Ataque ICMP (DoS)
- Ataque TCP SYN (DoS)
- Ataque RIP

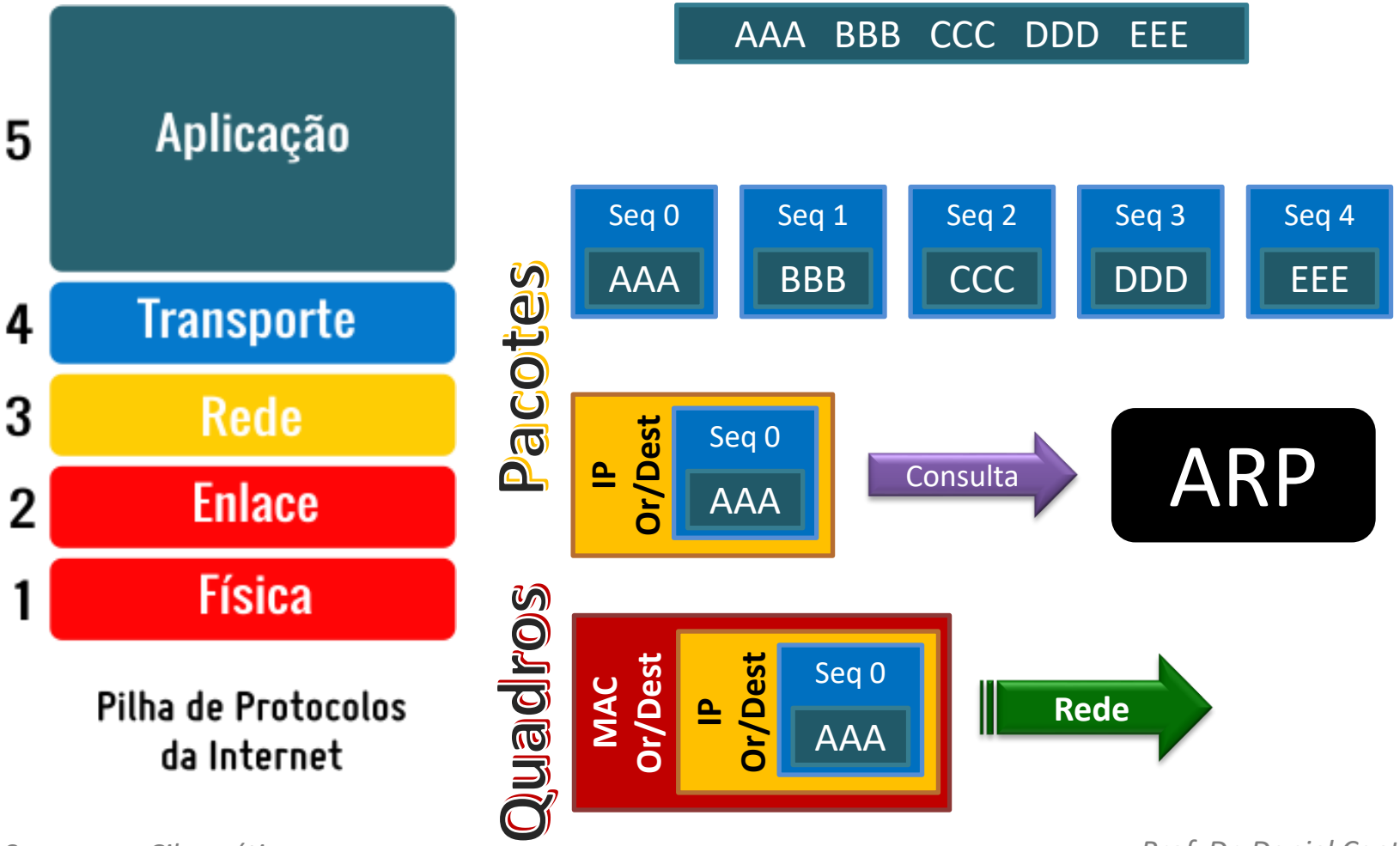


PRÉ AV1

SEMANA 4

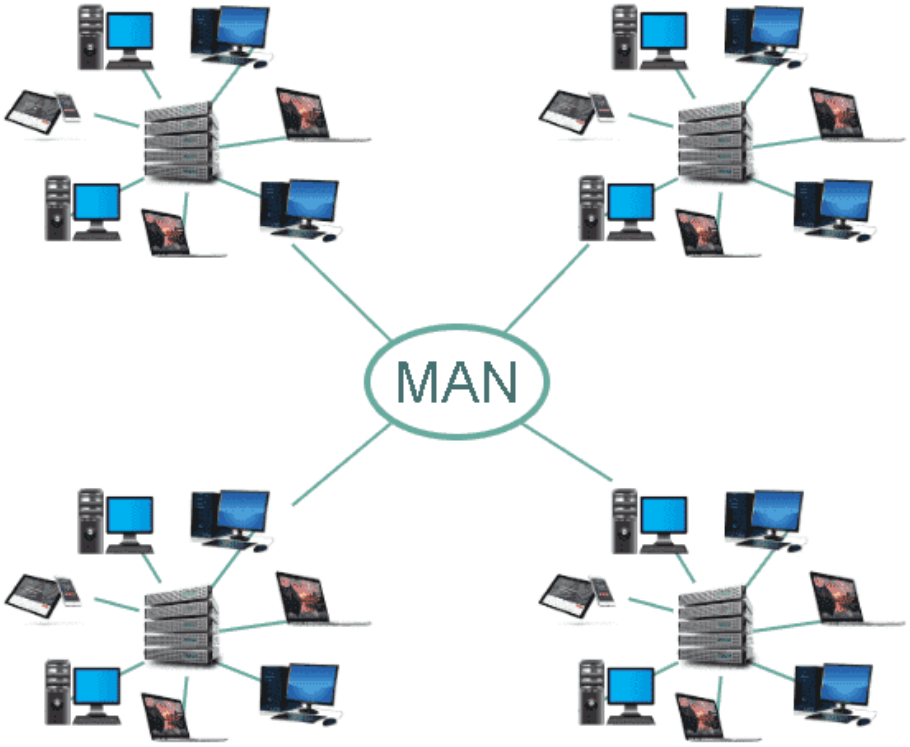
Preparação dos Dados

- Dados → Pacotes → Quadros



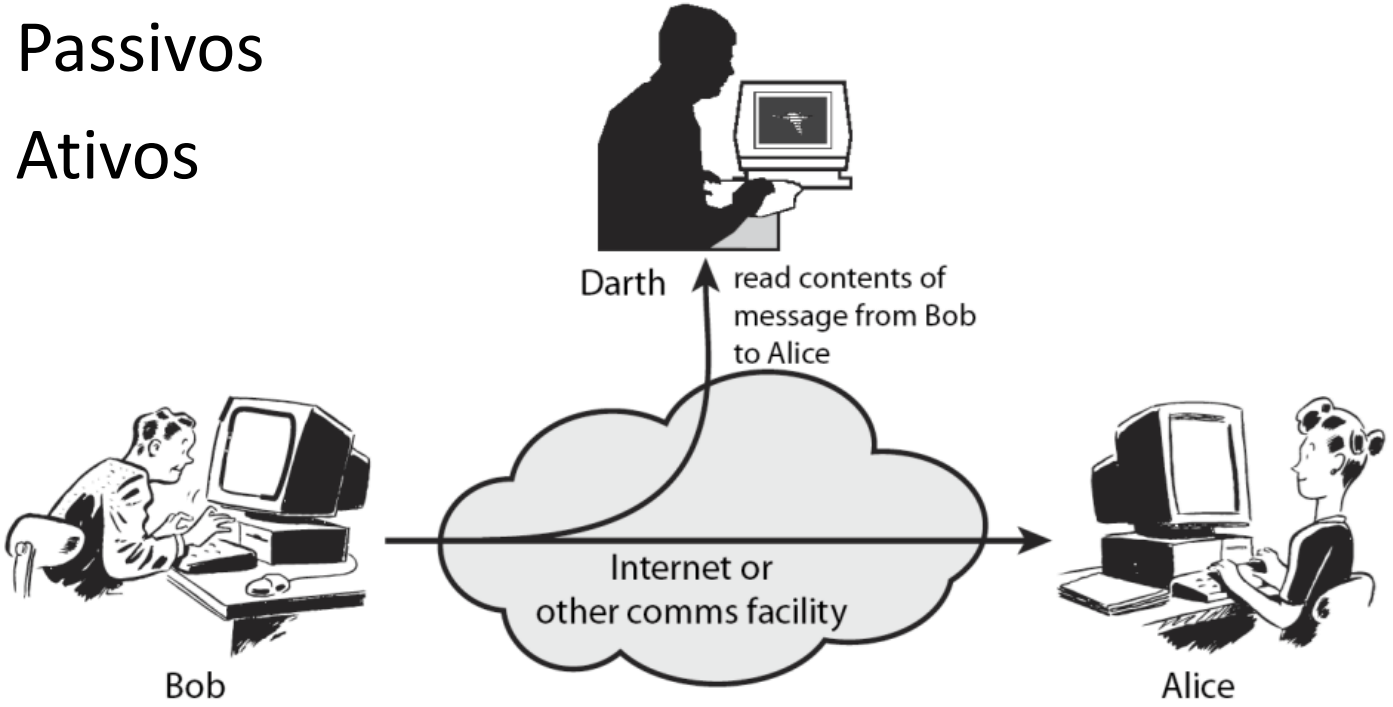
Encaminhamento dos Dados

- Destino na Rede Local x Internet
  - Verifica pela máscara de rede



Sniffers

- O que são?
- Há dois tipos
  - Passivos
  - Ativos

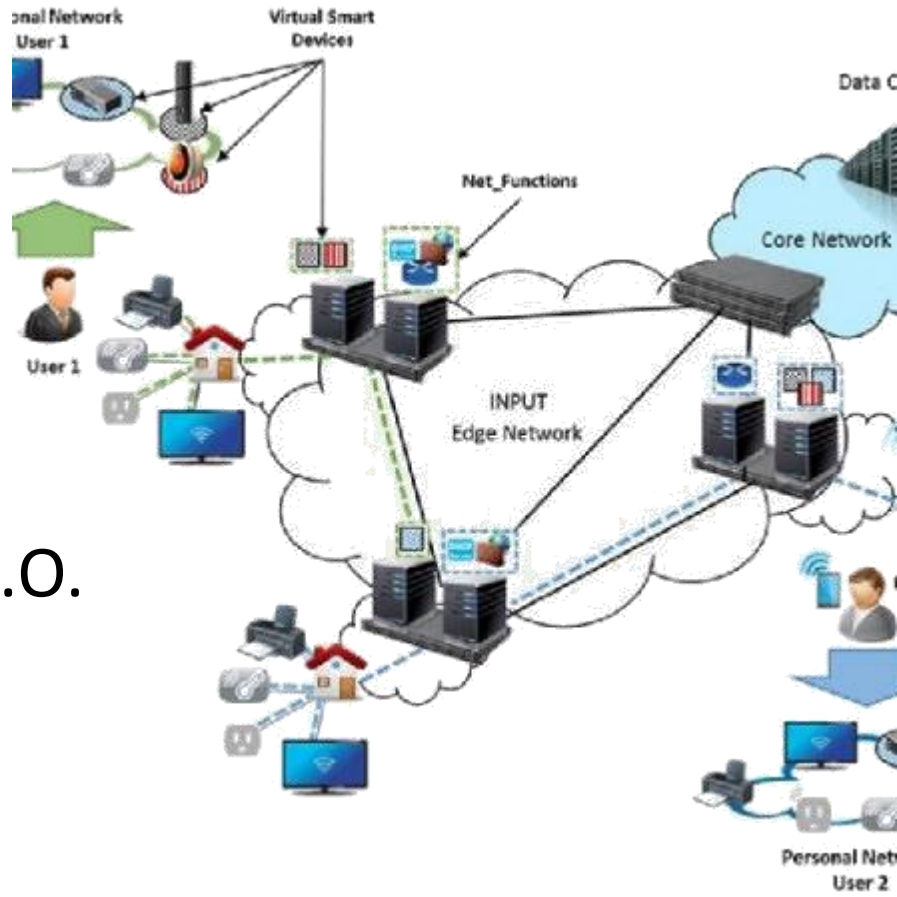


Sniffers

- Eficácia
  - Limitado ao segmento de rede
    - Ideal instalar no gateway
  - Placas de rede em modo promíscuo
    - Todos os dados da rede ficam disponíveis
  - Analisar “offline”
    - Analisar em tempo real pode ser muito confuso!

Mapeamento de Rede

- O que é isso?
- Identificar
  - Caminhos dos dados
  - Portas em uso
  - Serviços em execução
  - Versão de software e S.O.
  - ...



Mapeamento de Rede

- Efetividade
  - Depende das configurações do firewall
    - Pode bloquear muitas consultas
  - Fica na zona cinza da lei
    - Similar a observar dentro da casa de outra pessoa
  - Para testar...
    - Site: scanme.nmap.org

PRÉ AV1

SEMANA 5

Tecnologias para a Web

- Página/Aplicação Web
  - Conteúdo
  - Forma
  - Ações (cliente)
  - Ações (servidor)

- Cada parte...
  - Desenvolvida com tecnologias próprias
- Vulnerabilidades
  - Na interação entre esses elementos!

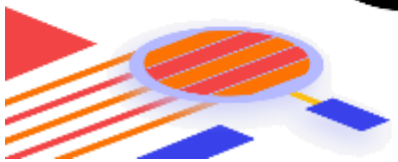
Maiores Riscos a Aplicações Web

- Segundo o OWASP (https://owasp.org/www-project-top-ten/)
  1. Injeção de Código
  2. Quebra de Autenticação
  3. Exposição de dados sensíveis
  4. Entidades externas de XML
  5. Quebra de controle de acesso
  6. Configuração incorreta de segurança
  7. Cross-Site Scripting (XSS)
  8. Desserialização Insergura
  9. Utilização de Componentes Vulneráveis
  10. Logs e monitoramento insuficientes

Ferramentas para Prevenção

- Existem diversas ferramentas
  - Incluindo as mantidas pela OWASP
- São recursos adicionais:
  - Importante é entender os mecanismos
  - E agir preventivamente

- Luta constante e eterna
  - Client Side x Server Side
  - Em ataques, as coisas se misturam



Ferramentas

- Netcat
  - Ncat é instalado no Windows com o Zenmap
  - Nc pode ser instalado no Linux separadamente
- Google Hacking
- Ferramentas de varredura
  - Dirb, DirBuster, DirStalk, Scout...
- Ferramentas de varredura de vulnerabilidade
  - wapiti

Engenharia Social

- Principal técnica de combate...

Informação

Qual Treinamento?

Tipo	Quem
Conscientização	Todos
Conhecimentos básicos de segurança	Todos que lidem com TI
Treinamento	Papeis e responsabilidades funcionais relativas a sistemas de TI
Educação de Segurança	Especialistas/Profissionais de Segurança em TI

	Conscientização	Treinamento	Educação
Atributo	"O quê"	"Como"	"Por quê"
Nível	Informação	Conhecimento	Percepção
Objetivo	Reconhecimento	Habilidade	Entendimento
Método de ensino	**Mídia** — Vídeos — Boletins informativos — Pôsteres etc.	**Instrução prática** — Palestra — Seminário de estudo de caso — Prática	**Instrução teórica** — Seminário de discussão — Leitura sobre o assunto
Tipo de teste	Verdadeiro/falso Múltipla escolha (identifica aprendizado)	Solução de problemas (aplica aprendizado)	Ensaio (interpreta aprendizado)
Impacto	Curto prazo	Prazo intermediário	Longo prazo

PRÉ AV1

SEMANA 6

Redes sem fio

- Equipamentos usuais:
  - *Access Point* (AP, ponto de acesso)
    - Apenas faz a conexão
  - Roteador *Wireless* (Roteador + AP)
    - Faz conexão e inclui recursos de roteamento
    - Em geral provém DHCP
  - “Estações” WiFi

Tipos de ataques comuns

- Usando adaptadores em “modo monitor”
  - Similar ao modo “promíscuo”
  - Ataques usuais:
    - Força Bruta no WPS (modo PIN)
    - Monitoramento de tráfego / Crack Offline
    - Monitoramento de conteúdo (rede aberta)
    - DoS por desconexão.
- Usando APs portáteis (ou Tethering)
  - Redes Abertas WiFi Falsas
  - Evil Twin (Gêmeo do mal – variante!).

Como proteger a rede?

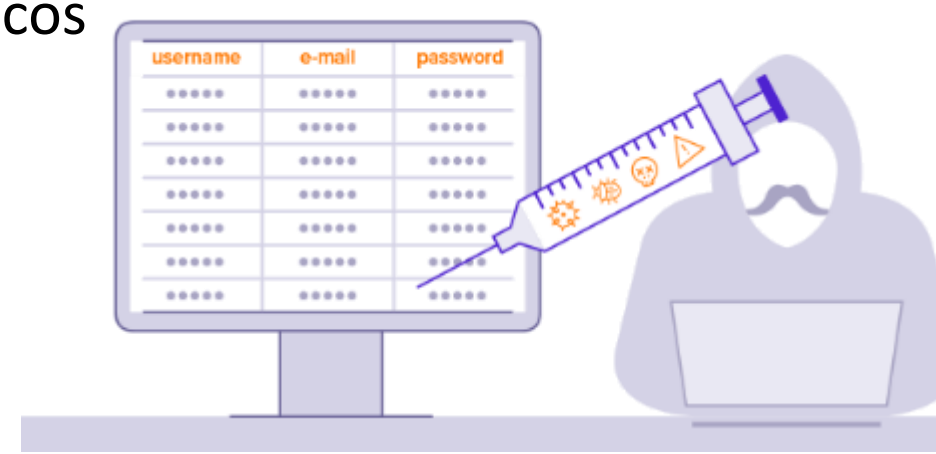
- Redes Abertas e Criptografadas
  - IPs / Esconder o SSID / Filtrar MAC / Desligar WPS
- Criptografia
  - WEP – Wired Equivalent Privacy
  - WPA – WiFi Protected Access
  - WPA2 – Evolução:
    - Personal: PSK – Pre-Shared Key
    - Enterprise: Servidor de autenticação
    - Criptografia: TKIP/AES
  - WPA3 – Ainda não amplamente disponível

Pós AV1

SEMANA 7

Injeção de Código

- O que é?
  - Alguém executar códigos em sua aplicação
- Dois tipos mais importantes
  - SQL Injection
    - Quebra de Autenticação
    - Exposição de Dados
    - Apagar Tabelas e Bancos
  - Code Injection
    - Include x Eval

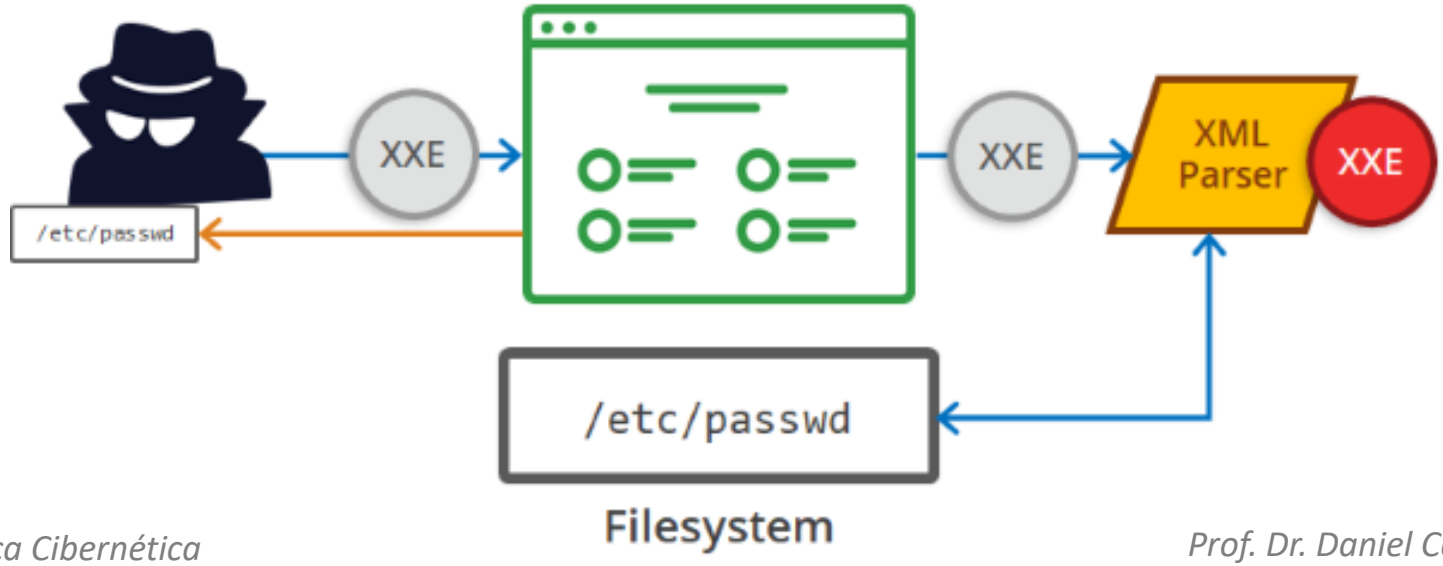


Injeção de Código

- Como evitar?
  - Configurar adequadamente os programas
    - Limitar a inclusão aos diretórios permitidos;
    - Limitar as permissões do banco de dados;
  - Tratar a entrada de dados
    - Garantir que são válidos, e se não forem, valor padrão
    - SQL: comando “prepare”
      - https://www.devmedia.com.br/evitando-sql-injection-em-aplicacoes-php/27804
    - Evitar comandos do tipo eval($variavel);

Entidades Ext. de XML (XEE)

- O que é?
  - Ferramentas que decodificam XML que processam entidades externas... Mal configuradas.
- Como evitar?
  - Usar ferramentas atualizadas e bem configuradas

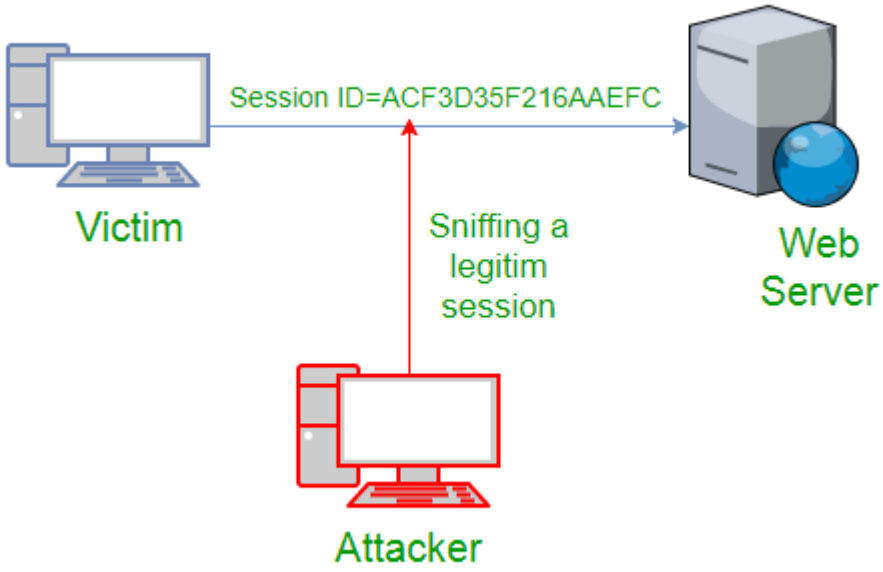


Pós AV1

SEMANA 8

Sequestro e Quebra de Sessão

- O que é?
  - Alguém “roubar” a sessão de outro usuário
  - Alguém forjar sessões válidas.

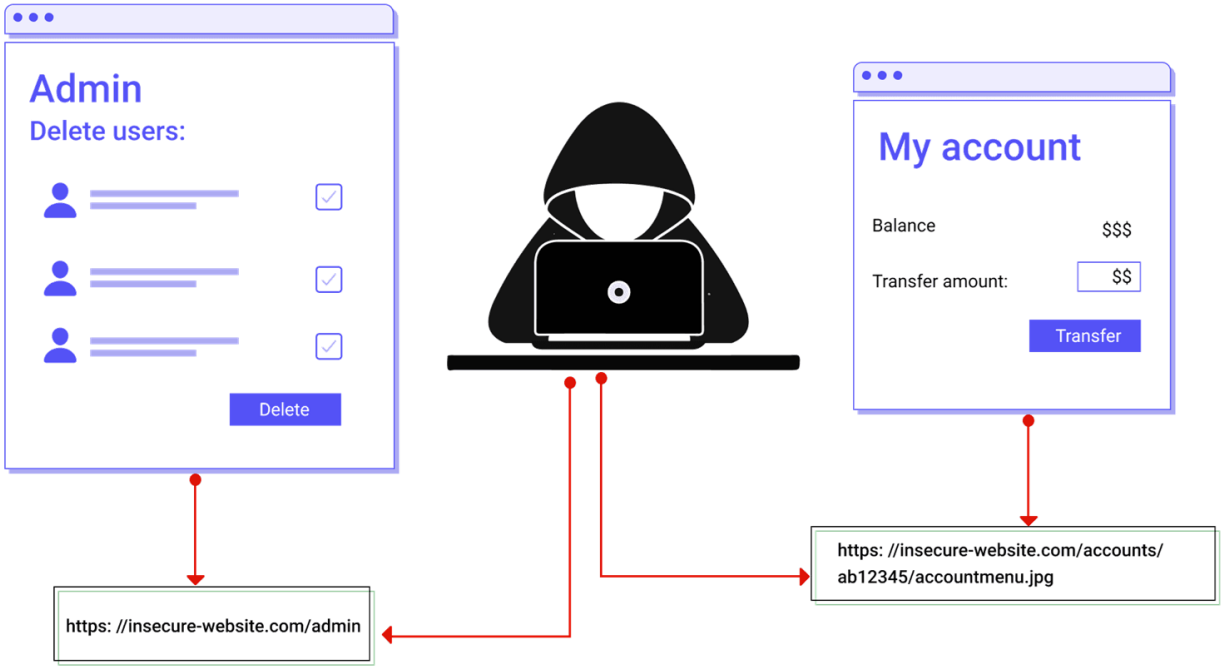


Sequestro e Quebra de Sessão

- Como evitar?
  - Tratar adequadamente a sessão
    - Codificar dados
    - Usar cookies.
  - Manter a sessão em banco de dados
    - Sessão se torna um ID, dados estão no banco
    - Associar ID da sessão ao IP do computador
    - Associar um *timeout* à sessão.
  - Colocar o identificador da sessão como httponly
  - Usar linguagem que controle a sessão.

Quebra de Controle de Acesso

- O que é?
  - Usuário acessar página que não deveria
  - Em geral: falta de verificação de permissões.

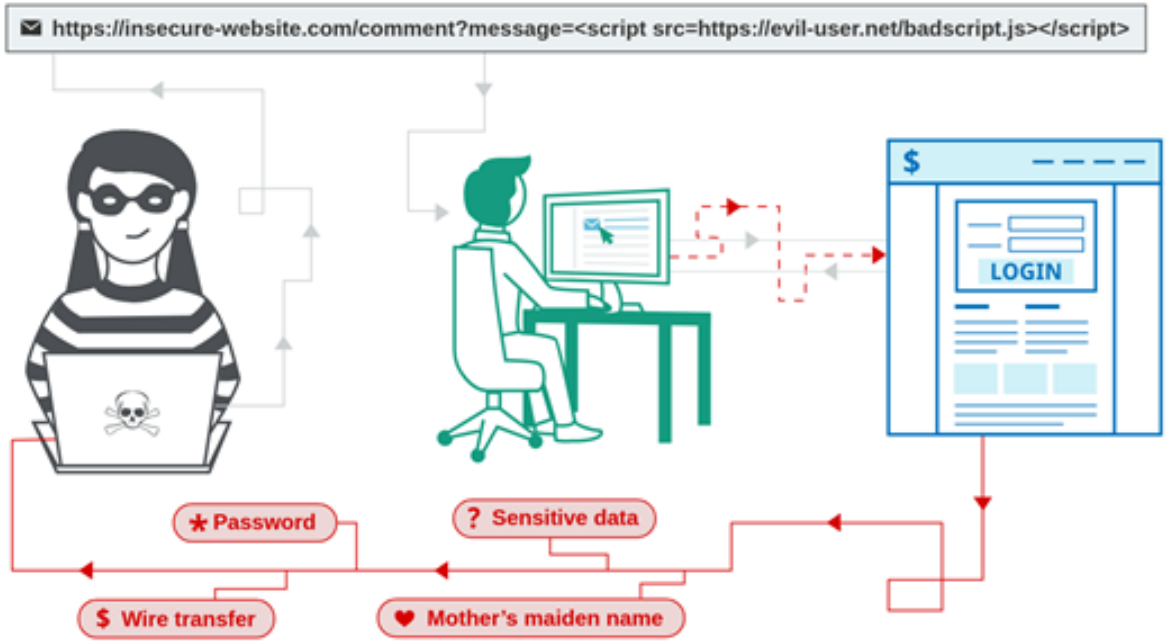


Quebra de Controle de Acesso

- Como evitar?
  - Verificar permissões em toda página “protegida”
    - Não se limitar ao menu!
  - Verificar permissões na execução de ações
    - Front e Backend
  - Manter permissões em BD, se possível
    - Facilitar a manutenção e revogação.

Cross-Site Scripting (XSS)

- O que é?
  - Um tipo de injeção de código...
  - Quando o código é executado do lado do cliente
    - Em geral... JavaScript.

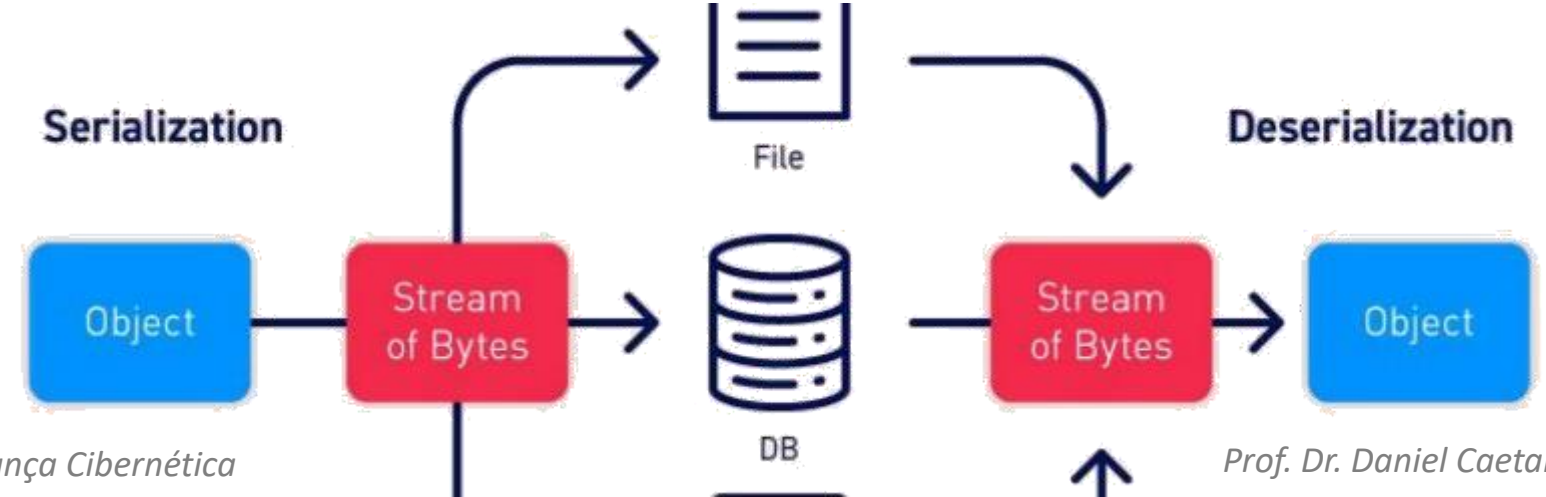


Cross-Site Scripting (XSS)

- Como evitar?
  - Configurar web server para não aceitar
    - No httpd.conf
    - Header always set X-XSS-Protection "1; mode=block"
  - Configurar navegador para não aceitar
    - No cabeçalho
    - Content-Security-Policy: script-src 'self’
  - Trate corretamente as entradas de usuário
  - Nunca apresentar/usar diretamente dados digitados pelo usuário
    - Ser o mais restrito possível

Desserialização Insegura

- O que é?
  - Serializar: objeto (dados+código) → String
  - Desserializar: String → objeto (dados+código)
  - Objetivo: armazenar ou transferir objeto pela rede
  - Ataque: alterar o “texto” transmitido...
    - Enviando um código malicioso no lugar.

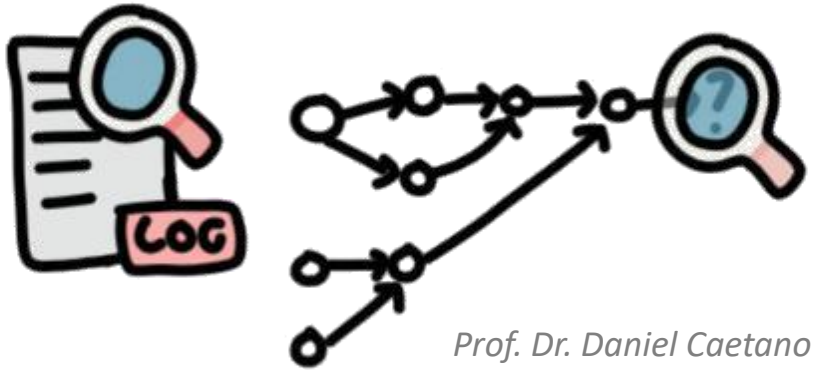


Desserialização Insegura

- Como evitar?
  - Assinar digitalmente os dados
    - Rejeitando dados cuja assinatura não seja válida
  - Quando não for possível assinar?
    - Servidor intermediário para checar os dados
  - Monitorar processos de desserialização
    - Alerta caso algum usuário ocasione muitas.

Monitoramento Insuficiente

- O que é?
  - Registro incompleto de operações...
  - Ou acompanhamento insuficiente dos registros...
  - Ou relógios dessincronizados (ambiente de rede)
- Consequências?
  - Impossibilidade de rastrear ocorrências...
    - E de apurar os responsáveis



Monitoramento Insuficiente

- Como evitar problemas?
  - Período agendado para monitoramento passivo
    - Frequente!
  - Rastrear operações normais
    - Para verificar rastreabilidade
  - Proteger os arquivos de log
    - Evitar que sejam apagados
  - Simular ataques e tentar rastreá-los
  - Usar sistemas de monitoramento ativo

Pós AV1

SEMANA 9

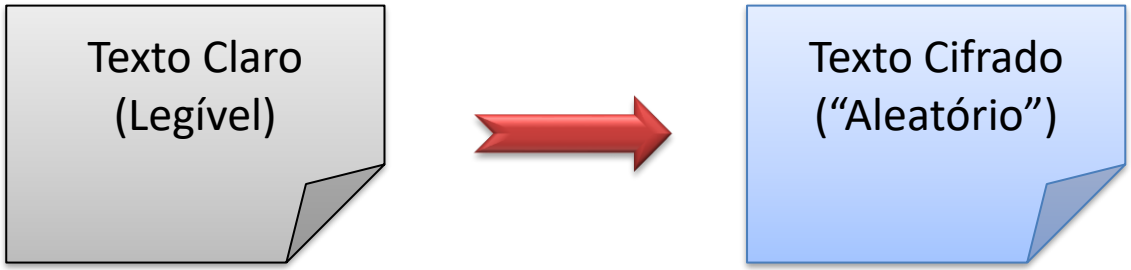
Mecanismos de Segurança

- Os mecanismos mais clássicos são:
  - Criptografia dos dados
  - Assinatura digital dos dados

- Focam em garantir
  - Sigilo: só quem pode acessar, acessará
  - Integridade: conferir se dado permanece “original”
  - Autenticação: de usuário, remetente, destinatário
  - Atualidade: a mensagem é nova, não um reenvio.

Criptografia

- Codificação dos dados
- Processo que transforma



- Algoritmo de criptografia
  - Cifragem: tornar o texto claro em cifrado
    - “Criptografar” ou “Encriptar”
  - Decifragem: tornar o texto cifrado em claro
    - “Decriptografar” ou “Decriptar”

Uso da Criptografia

- Assim, dados criptografados...
  - Armazenados ou transmitidos
  - Só serão legíveis por quem tiver a chave

Estarão mais seguros!

Assinaturas Digitais

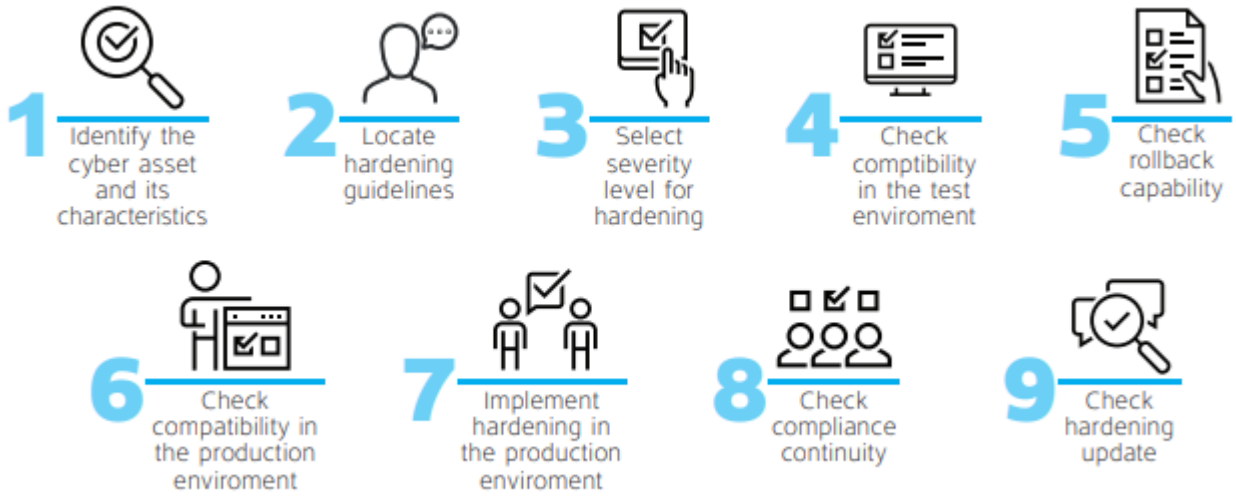
- Objetivo: garantir integridade e não-repúdio
- Requisitos
  - Receptor: verificar identidade do autor
  - Autor: não repudiar o conteúdo
  - Receptor/Intermediário: não alterar/forjar conteúdo.
- Meio comum:
  - Criptografia Assimétrica
  - Hash Criptográfico

Hardening

- O que é?
  - “Blindagem”.
- Como se faz?
  - Configurar adequadamente o SO
  - Configurar adequadamente os serviços
  - Configurar adequadamente os programas.
- Propósito:
  - Diminuir riscos de invasão ou sucesso em ataques.

Hardening

- Procedimento para Atenuação de Riscos:
  - Mapear ameaças
  - Desativar serviços desnecessários
  - Retirar privilégios desnecessários
  - Atuar com atividades preventivas e corretivas.



Questões de IoT

- Maioria dos dispositivos: dados por WiFi
  - Segurança mais delicada
- Permitem controle/monitoramento
  - Da casa ou da empresa
- Podem possuir falhas que permitam...
  - Instalação de malwares, sniffers, etc.

Questões de IoT - Soluções

- Proteção das redes da casa
  - Firewall, criptografia, tudo que for possível
- Controle pela rede
  - Não rotear dados de equipamentos IoT <-> WAN

Pós AV1

SEMANA 10

Plano de Continuidade de Negócios

- Objetivo geral: minimizar impactos
  - Manter a integridade e disponibilidade dos dados
    - Continuar operando em caso de desastre
    - Recuperação ordenada no menor tempo possível.

- Metas
  - Segurança das pessoas
  - Minimizar perdas e danos imediatos
  - Rápida restauração das atividades
  - Rápida reativação dos processos críticos
  - Conscientização e treinamento.

Elaborando o PCN

- Insumos
  - Análise de Risco
  - Identificação de Mecanismos de Prevenção
  - Estratégias de Recuperação.
- Plano de Contingência/Disaster Recovery Plan
  - Informação de Suporte
  - Notificação/Ativação
  - Recuperação
  - Reconstituição
  - Anexos.

Partes do PCN

- Informação de Suporte
  - O quê, quando, quem
- Notificação/Ativação
  - Primeiros socorros
  - Quem, em que ordem
  - Avaliação de danos
  - ANPD
- Recuperação
  - Procedimentos, ordem, testes

Partes do PCN

- Reconstituição
  - Testes
  - Integração de dados
  - Desmobilização
- Anexos
  - Responsáveis
  - Checklists
  - Documentos técnicos

Além do PCN

- Tomar todas as medidas!
  - Proatividade na segurança!
  - Forense computacional
- Atenção ao SLA dos serviços de manutenção
  - Service Level Agreement
- Contratação de seguros
  - Seguro Cibernético.

Avaliação da Disciplina

Avaliação

https://docs.google.com/forms/d/e/1FAIpQLSc00x72elj5sul0IblBSKQv3Wt185GhwzTB1bAhBmgO0lwdvQ/viewform

PERGUNTAS?