Proteção de Estações de Trabalho e Dispositivos USB no Ambiente Bancário

Conceitos Fundamentais

Proteção de Estações em Agências Bancárias

- **Controle de Acesso Crítico**
  - Bloqueio automático após 3 minutos (padrão bancário)
  - Senha de BIOS com política específica
  - Travas físicas nos terminais de atendimento

Dispositivos USB no Contexto Bancário

- **Classificação por Risco**
  1. Alto Risco: Dispositivos de armazenamento
  2. Médio Risco: Periféricos com memória
  3. Baixo Risco: Periféricos simples

Aplicações Práticas no Dia a Dia Bancário

Cenários Comuns

1. **Terminais de Atendimento**
   - Procedimento para conexão de PIN PAD
   - Protocolo de verificação de dispositivos
   - Checklist diário de segurança
2. **Estações de Trabalho**
   - Rotina de verificação pré-expediente
   - Procedimentos para manutenção
   - Protocolos de fim de expediente

Pontos Críticos (Foco Cesgranrio)

Principais Vulnerabilidades

- **Ameaças Prioritárias**
  - Malware bancário específico
  - Dispositivos USB infectados
  - Vazamento de dados sensíveis

Medidas Preventivas Essenciais

1. **Controles Obrigatórios**
   - Autorização da gerência
   - Registro em sistema
   - Verificação antivírus

Dicas para Prova Cesgranrio

1. **Atenção às Questões Sobre:**
   - Procedimentos de segurança em agências
   - Protocolos de uso de USB em caixas
   - Medidas preventivas no atendimento
2. **Armadilhas Comuns:**
   - Confusão entre políticas gerais e bancárias
   - Ordem incorreta dos procedimentos
   - Negligência de aspectos regulatórios

Exercícios Modelo Cesgranrio

1. (Cesgranrio) Em uma agência bancária, ao conectar um dispositivo USB no terminal de atendimento, o procedimento CORRETO é:
   a) Verificar imediatamente se o dispositivo é reconhecido
   b) Realizar scan antivírus e verificar autorização
   c) Conectar e aguardar instalação automática
   d) Solicitar ao cliente que teste o dispositivo
   e) Desativar o antivírus temporariamente

Estações de Trabalho

Proteção Física

- **Controle de Acesso**
  - Bloqueio automático
  - Senha de BIOS
  - Cadeados e travas
- **Ambiente Seguro**
  - Temperatura adequada
  - Proteção elétrica
  - Limpeza regular

Proteção Lógica

1. **Sistema Operacional**
   - Atualizações automáticas
   - Patches de segurança
   - Firewall ativo
   - Antivírus atualizado
2. **Usuários**
   - Contas limitadas
   - Senhas fortes
   - Política de bloqueio
   - Logs de acesso

Dispositivos USB

Tipos de Dispositivos

1. **Armazenamento**
   - Pen drives
   - HDs externos
   - Cartões de memória
2. **Periféricos**
   - Teclados
   - Mouses
   - Webcams
   - Impressoras

Riscos de Segurança

Ameaças Comuns

- **Malware**
  - Autorun
  - Infecção automática
  - Propagação entre dispositivos
- **Dados**
  - Vazamento
  - Roubo
  - Perda

Vulnerabilidades

- Dispositivos infectados
- Autoexecução
- Firmware malicioso
- BadUSB

Medidas de Proteção

Políticas de Uso

1. **Controle de Acesso**
   - Autorização prévia
   - Registro de uso
   - Bloqueio de portas
2. **Procedimentos**
   - Scan antes do uso
   - Formatação segura
   - Backup antes de conectar

Configurações de Segurança

- **Sistema**
  - Desativar autorun
  - Bloquear execução automática
  - Atualizar drivers
- **Antivírus**
  - Scan automático
  - Quarentena
  - Bloqueio preventivo

Hardening

Configurações Básicas

1. **Sistema Operacional**
   - Remover serviços desnecessários
   - Configurar firewall
   - Atualizar regularmente
2. **Aplicativos**
   - Manter atualizados
   - Remover não utilizados
   - Configurar segurança

Políticas de Segurança

- **Senhas**
  - Complexidade mínima
  - Troca periódica
  - Histórico
- **Acesso**
  - Tempo limite de sessão
  - Bloqueio após tentativas
  - Registro de eventos

Dicas Práticas

1. **Uso Seguro de USB**
   - Sempre escaneie antes de usar
   - Use somente dispositivos confiáveis
   - Mantenha backup dos dados
   - Ejete corretamente
2. **Proteção da Estação**
   - Mantenha updates em dia
   - Use proteção de tela
   - Faça backup regular
   - Monitore atividades

Pontos para Memorizar

1. Importância do controle de dispositivos USB
2. Riscos do autorun
3. Necessidade de scan regular
4. Política de uso de dispositivos
5. Hardening do sistema

Exercícios Práticos

1. Configure bloqueio de portas USB
2. Desative autorun
3. Configure scan automático
4. Implemente política de senhas
5. Realize hardening básico