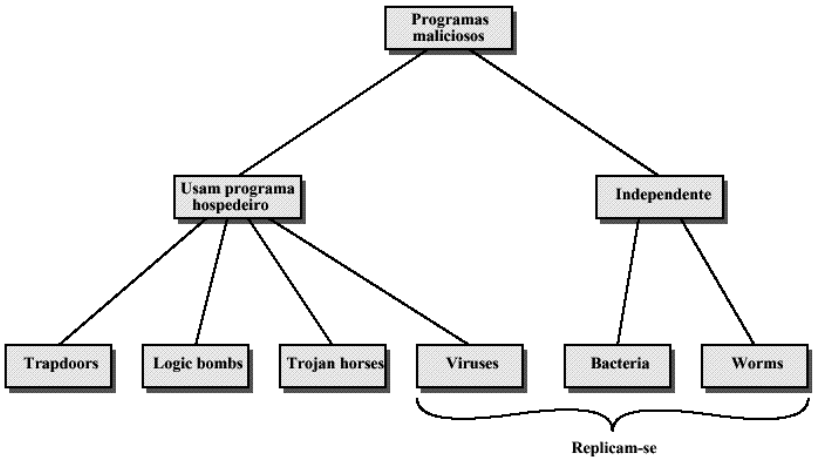
Programas Maliciosos



Vírus de Computador

- Vírus de computador
  - Código intruso que se anexa a outro programa
  - Ações básicas: propagação e atividade
- A solução ideal para vírus é prevenção
- O problema é que essa meta é muito difícil de ser alcançada - infecções sempre ocorrem
- A solução para sistemas infectados é:
  - Detecção: localizar a infecção e o alvo infectado
  - Identificação: identificar o vírus que infectou
  - Remoção: remover o vírus e restaurar o sistema

Entidades Infectadas

- Setor de boot (Boot sector em disquetes ou o Master Boot Record em HDs)
- Programas executáveis (.EXE, .COM)
- Bibliotecas (.DLL, .OVL, .OVR, etc.)
- Arquivos de dados de programas que tem recursos de linguagem de macro (Word, Excel, Access, etc.)
- Arquivos compactados (.ZIP, .ARJ, etc.)

Gerações de Antivírus

- Primeira: scanner de seqüência de bytes
  - busca por seqüências de bytes específicas
  - verificação do tamanho de arquivos
- Segunda: scanners heurísticos
  - busca de padrões genéricos de vírus
  - verificação de integridade de arquivo (CRC, hash)
- Terceira: monitoração de comportamento
  - programa residente que analisa o comportamento dos programas que são executados
  - identificam determinadas ações são suspeitas (gravação em arquivo executável)
- Quarta: proteção combinada
  - pacotes que combinam todas as técnicas disponíveis

Localização do Antivírus

- Uso permanente de antivírus é essencial
- Antivírus podem estar instalados em cada computador e no servidor gateway de email
- É recomendado que seja instalado em ambos
- Antivírus no gateway intercepta os emails que chegam e verifica cada arquivo anexado
- Alguns simplesmente removem arquivos anexo
- É comum que o gateway seja o Firewall

Atualização do Antivírus

- Novos vírus surgem todo dia
- E-mail, conexões permanentes e computação móvel contribuem para rápida proliferação
- É importante que o antivírus seja mantido atualizado para que possa identificar os novos vírus
- Os vírus recentes são mais perigosos:
  - em geral são tecnologicamente superiores
  - pelo fato de serem recentes, passam despercebidos por antivírus desatualizados

Controle de Senhas

- Educação do usuário
  - Orientações sobre importância de senhas seguras e diretivas para boa definição/escolha de senhas
- Senhas geradas por computador
  - Senhas aleatórias geradas são seguras, mas em geral são difíceis de serem memorizadas
- Verificação reativa
  - Execução periódica de sistema interno de quebra de senhas para descobrir senhas fáceis
- Verificação proativa
  - Validação de regras no momento da escolha

Backups

- Motivos para a prática regular de backups
  - Erros de usuário: exclusão ou alteração indevida de arquivos ou conteúdo
  - Erros administrativos: remoção indevida de uma conta ativa, configuração errada danosa, etc.
  - Falha de hardware que danifiquem HDs ou dados armazenados
  - Falha de software que corrompem dados
  - Roubo ou vandalismo eletrônico
  - Disastres naturais
  - Arquivamento e controle de versões

Tipos de Backup

- Backup Dia-Zero
  - Cópia completa do sistema original e limpo
  - Facilita re-instalação rápida
- Backup Completo
  - Cópia de todos os arquivos armazenados, feita periodicamente
- Backup incremental
  - Cópia de todos os itens modificados desde certo evento ou data (ex: desde último backup completo)

Diretivas de Backup

- Rodízios de múltiplas fitas (mídias) de backup
  - Evita desgaste contínuo
  - Permite manter várias versões
- Combinar ciclos de backups completos e incrementais e períodos de armazenamento: turno, dia, semana, mês, ano etc.
- Armazenar mídia em local adequado, seguro
  - Cofre térmico: proteção contra roubo, intempéries
  - Segunda cópia de segurança em local externo
- Testar integridade das cópias periodicamente

Política de Segurança

- Propósitos da política de segurança
  - Descreve o que está sendo protegido e porquê
  - Define prioridades sobre o que precisa ser protegido em primeiro lugar
  - Pode estabelecer acordo explícito com as várias partes da empresa em relação ao valor segurança
  - Fornece ao setor de segurança motivos concretos para dizer “não” quando necessário
  - Motiva o setor de segurança no desempenho efetivo de seu papel

Política de Segurança

- Armadilhas e dificuldades
  - Prioridade
    - As prioridades operacionais da empresa podem conflitar com políticas de segurança que impliquem atraso
  - Política interna
    - Políticas ou fatores internos gerais da empresa podem afetar ou prejudicar decisões ou prática de segurança
  - Propriedade e poder
    - Podem existir brigas ou desentendimentos entre grupos pela propriedade e controle da política de segurança
  - Legibilidade e compreensão
    - Uma boa política deve ser também bem redigida; para tanto, deve ser escrita correta, precisa, clara e objetiva

Preparativos para Segurança

- Análise de risco
  - Levantamento (identificação e quantificação) de objetivos e valores
  - Identificar vulnerabilidades e ameaças prováveis
  - Identificar contra-medidas (respostas)
  - Desenvolver análise de custo-benefício, com definição de prioridades
  - Planejar políticas e procedimentos de segurança

Preparativos para Segurança

- Formação de equipes de segurança
  - Perfil do pessoal: integridade, confiabilidade, capacitação, iniciativa, malícia, disponibilidade
  - Equipes
    - Equipe de resposta a ataques
    - Equipe de investigação, análise e pesquisa
    - Equipe de observação (monitoramento e testes)
  - Administração e coordenação
  - Treinamento técnico e geral de funcionários

Procedimentos de Segurança

- Segurança de pessoal (RH)
  - Contratação: concordância com a política de segurança e acordos de não-divulgação (sigilo)
  - Demissão: desativação de acesso imediata, alteração de procedimentos se ligado à segurança
  - Permissões de acesso sempre atualizadas
  - Questões administrativas: regras e infrações
- Segurança física
  - Instalações físicas adequadas e protegidas
  - Equipamentos, no-breaks, backups
  - Controle e registro de acesso: locais, horários etc.

Procedimentos de Segurança

- Monitoração da rede
  - Registros, sensores e alarmes permanentes
  - Detecção de falhas, intrusos e ataques
- Auditoria da rede
  - Revisão, testes e análises periódicas
- Plano de resposta a ataques
  - Procedimentos, preparativos e ferramentas para ação imediata
  - Controle de danos e recuperação de desastres
  - Registro e investigação