Segurança

03/13/11

Objectivos

- Reconhecer os perigos inerentes à utilização de um sistema operativo.
- Aplicar com sucesso técnicas de protecção.
- Encontrar o correcto compromisso entre segurança e facilidade de utilização.

Problemas de Segurança

- Malware
- Utilizadores
- Ameaças Externas

Ameaças Externas e Utilizadores

- Incêndios
- Inundações
- Terramotos

- Falta de formação
- Formação errada
- Relações pessoais

Não fazem parte do âmbito de Sistemas Operativos!

Ameças que nos interessam – Malware

- Vírus
- Spyware
- Trojans

Podem custar milhões em prejuízo, no melhor dos casos custam produtividade.

Vírus

- Consomem recursos
- Danificam ficheiros
- Não são tão distrutivos como a publicidade faz querer
- Conseguem reproduzir-se

- Cópias de segurança actualizadas
- Anti-vírus quando se justifica
- Formação adequada aos utilizadores – O mais importante
- Actualizações constantes – O segundo mais importante

Spyware

- Registam a actividade do utilizador
- Não se reproduzem
- Pretendem seguir os hábitos do utilizador

- Mesmas protecções que no caso dos anti-vírus

Trojan

- Abrem portos de acesso ao exterior
- Permitem a um utilizador mal intencionado controlar o sistema
- São usados para criar botnets
- Não se conseguem reproduzir

- Uso de firewalls pode limitar o acesso ao computador.
- Controlo constante de todo o tráfego na rede.
- Remoção de permissões ao nível do computador (ex: um computador de impressão não deve poder aceder ao servidor de ficheiros)

Receita comum

- Formar os utilizadores
- Manter o software actualizado e legal
- Controlar todos os recursos seguindo a regra de “menos permissões possíveis” - tanto para máquinas como para utilizadores
- Não há soluções infalíves – ter planos de contingência
- Testar tudo e nunca confiar
- Qualquer solução colide com a liberdade do utilizador!

Exemplos

- ILOVEYOU
  - Dependia de eng. Social;
  - Usava uma falha do SO (extensões de ficheiros);
  - Causou 5.5 mil milhões de dólares em danos;
  - Infectou mais de 50 milhões de utilizadores em 8 dias
  - Obrigou ao fecho de redes completas – CIA e Pentágono desligaram sistemas.
- Storm Worm
  - Envia 1800 e-mails em cerca de 5 minutos
  - Criar uma botnet P2P
  - Actualmente entre 5000 a 40000 nós com 10 milhões de computadores infectados
  - Em constante actualização

Conclusão

A única defesa é a correcta formação dos utilizadores e dos seus hábitos na utilização de computadores. Tudo o resto é acessório.
constante actualização