Introdución a Seguridade Informática

Confidencialidade, Integridade e Dispoñibilidade

Principios Básicos

- Un sistema informático é seguro si:
  - A información so e accesible polos sistemas e persoal autorizados (Confidencialidade)
  - Se garante que a información non sufriu ningún tipo de alteración de xeito non autorizado (Integridade)
  - Se garante a autoría da información (Non repudio en orixe)
  - Se garante a identidade do receptor da información e se ten constancia de que foi entregada (Non repudio en destino)
  - Se garante que a información está dispoñible cando é necesario (Dispoñibilidade)

Compoñentes Clave

- Seguridade nas Redes
  - Protección contra accesos non desexados
    - Firewalls de Rede e Aplicación
  - Protección contra a filtración de datos
    - DLP: Data Loss Prevention – Etiquetado e categorización da información, rexistro de movementos de información
    - SIEM: Security Information and Event Management) – Logs, sistemas de alerta, analese forense, Detección de Eventos e intrusións
- Seguridade nos Sistemas e Dispositivos
  - Seguridade dos elementos hardware
  - Fontes seguras de software
  - Antivirus
  - IDS / IDPS
- Destrución Segura de Datos

Seguridade Física e Seguridade Lóxica

- Seguridade Física
  - Seguridade dos elementos hardware
  - UPS (SAI), Protección ante incendios ou inundacións, protección do acceso físico...
- Seguridade Loxica
  - Software e Datos dos sistemas
  - Protección contra accesos non autorizados, denegacións de servizo, perda e alteración de información...

Medidas de Seguridade Física

- Aloxamento en CPD
  - Seguridade de acceso Físico
  - Protección contra desastres
  - Redundancia
- Os UPS / SAI
  - Offline
  - Line-Interactive
  - Online

Medidas de Seguridade Loxica

- Boas prácticas na xestión do software
- Deseño axeitado da estrutura de rede
- Sistemas Firewall / IDPS / Antimalware
- Adopción da política do mínimo privilexio

Ameaza, Vulnerabilidade, Ataque, Risco e Impacto

- Ameaza
  - Existe a posibilidade de que se vulnere a seguridade
- Ataque
  - Intento de vulnerar a seguridade
  - Existen moitas técnicas de ataque: MiM, DoS, Phising, KeyLogging, Sniffing, Ramsonware, Enxeñería Social, DNS Spoofing, Escalada de Privilexios, Ataques de forza bruta, ARP Spoofing...
- Vulnerabilidade
  - Existe unha falla no deseño e implementación dos sistemas que fai posible o éxito dun ataque.
  - Vulnerabilidades típicas son XSS, SQL Injection, Buffers Overflow, Software desactualizado, Malas configuracións ou erros...
- Impacto
  - O Impacto mide as consecuencias sobre os sistemas de datos e a empresa dun ataque exitoso.
  - Existen varias calificacións, como “Baixo”, “Medio” e “Alto”, ou pode medirse segundo o impacto legal ou económico.
- Risco
  - O Risco mide a posibilidade de que se de un ataque e de que ese ataque teña éxito xunto co impacto que ese ataque produciría. Un xeito é asignar ao impacto Baixo, Medio e Alto un valor numérico e multiplicalo pola probabilidade estimada de éxito dun ataque.

Confidencialidade e Integridade

- Criptografía e Cifrado
- Cifrado Simétrico e Asimétrico
- Criptografía mixta
- Sinadura Electrónica: PGP e X509
- Protocolos Seguros: HTTPS e as CA
- Creación de certificados HTTPS
- PKI X509

Dispoñibilidade

- Redundancia de Alimentación
- Redundancia no Almacenamento
- Redundancia dos datos
- Balanceo e Dispoñibilidade

Seguridade Activa e Pasiva

- Seguridade Activa: Medidas tomadas para prever, detectar e impedir as fallas na confidencialidade, integridade e dispoñibilidade
  - Antivirus / IDPS / Firewall
  - Sistemas de monitorización e control de integridade
  - Actualización de aplicacións e sistemas
  - Autenticación multifactor
  - Boas Prácticas
- Seguridade Pasiva: Medidas tomadas para disminuír o impacto dunha incidencia de seguridade
  - Backups
  - Cifrado
  - Segmentación da Rede