UD01 – Adopción de pautas de seguridade informática

Introdución á seguridade Informática

Conceptos Básicos

Conceptos Básicos de Seguridade Informática (ISO 27002)

Podemos decir que un sistema informático é seguro si garante:

- Confidencialidade
- Integridade
- Dispoñibilidade
- Non Repudio (Orixe -sinatura dixital, trazabilidade, logs-, Destino -terceiros de confianza-)

Elementos Vulnerables

Un **sistema vulnerable** é aquel no que existe algunha probabilidade de que se vexa comprometida a dispoñibilidade, confidencialidade ou integridade da información.

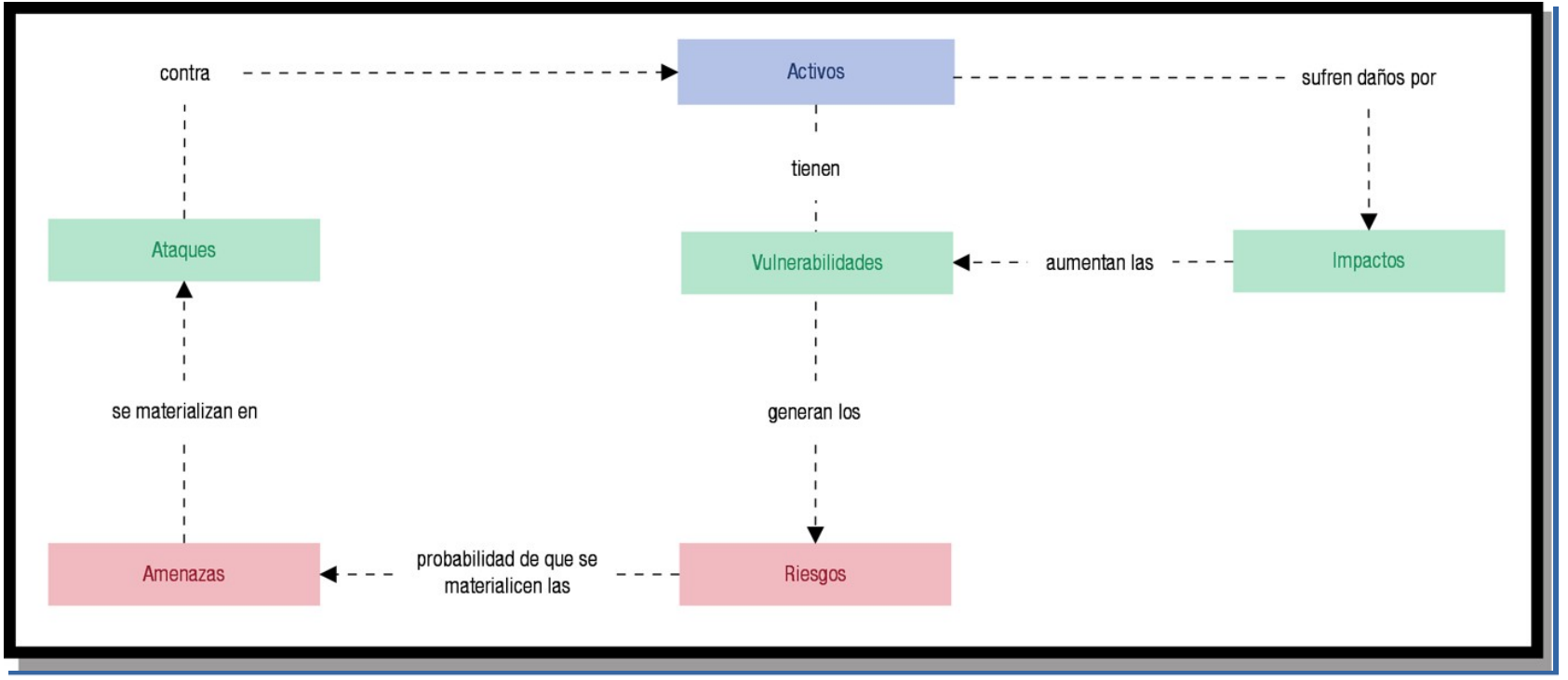
Realmente, todos os sistemas son vulnerables en maior ou menor grao

Os elementos vulnerables nos sistemas informáticos poden ser: Hardware, Software e Datos.

Outros conceptos importantes son:

- Ameaza - Posibles intentos de vulneración da seguridade.
- Risco - Posibilidade de que unha ameaza teña éxito.
- Ataque - Intento de vulnerar a seguridade.
- Impacto - Posibles consecuencias dun ataque con éxito.

Vulnerabilidades,Ameazas,Ataques e Impacto



Elementos vulnerables

Activos dun Sistema de información

- Datos
- Software
- Hardware
- Redes
- Soportes
- Instalacións
- Persoal
- Servizos

Activos dun Sistema informático

- Datos – Acceso non autorizado (Seguridade da información)
- Software – Erros nas aplicacións
- Hardware – Fallos no deseño, fallos elécrricos
- Persoal – Preparación e organización

Un sistema de información pode ter como compoñente un sistema informático. Cada un dos distintos activos presentan distintas vulnerabilidades. As máis claras e importantes son as asociadas ao persoal

Análise de vulnerabilidades

E moi importante coñecer as vulnerabilidades presentes nos sistemas de información, para o que se realizan auditorías de seguridade. O proceso a seguir comprende varios pasos:

- **Identificar os activos do sistema** (Hardware e software) – Existen ferramentas especializadas, algunhas que nos sirven como xestión de activos/inventario (nmap, GLPI / Rudder).
- **Identificar as medidas de seguridade existentes**
- **Atopar as vulnerabilidades** – O proceso de busca de vulnerabilidades se coñece como **Pentesting** (Penetration Testing). Existen ferramentas automatizadas que o permiten. (nmap, Metasploit, Nexpose, metasploit, Nessus / OpenVAS, nmap -sC, nikto, fierce, wapiti…). Tamén podemos facer uso de ferramentas OSINT (Open Source InTelligence) como Google Dorks, Bing Dorks, Shodan, Maltego, TheHarvester, Recon-ng, crt.sh, Creepy, dnsdumpster.com, spyse, foca, Ipinfo, waybackmachine, google imaxes …

  As vulnerabilidades coñecidas se publican no CVE (common vulnerabilities and exposures) e son utilizadas por moitas das ferramentas anteriores.
- **Valorar as posibles ameazas** – Dependerá da exposición (risco) dos diferentes activos e do posible impacto que pode producir un ataque.
- **Seleccionar as medidas de protección necesarias** – Normalmente se establece unha clasificación das medidas en función da súa urxencia, determiñadas pola valoración obtida no punto anterior.

https://www.osi.es/es/conan-mobile (INCIBE, Instituto Nacional de Ciberseguridade)

Vulnerabilidades

Unha vulnerabilidade é un erro no desenvolvemento ou xestión dos sistemas:

- **Fallos de implantación** : Uso de software non apropiado ao contorno, como telnet en lugar de ssh
- **Fallos de deseño**: Como erros na construción do software (buffer overflow), ou o deseño de formatos de audio / video / texto pouco apropiados.
- **Fallos de configuración**: Como a instalación de servicios non necesarios, ou deixar as configuracións por defecto do software.

As vulnerabilidades poden darse en distintos ámbitos:

- **Ámbito físico**: Salas non seguras, BIOS sen protección, falta de control de acceso…
- **Ámbito organizativo**: Persoal pouco preparado, falta de revisións das políticas de seguridade e dos sistemas/software/servicios instalados…
- **Ámbito tecnolóxico**: Falta de actualizacións, descontrol das aplicacións instaladas, falta de supervisión dos incidentes, falta de rendundancia, redes sen protección, mal uso do correo e da navegación … etc.

Ciclo dunha vulnerabilidade

Existen investigadores de seguridade encargados de buscar fallos de deseño no software, normalmente cando se atopa unha vulnerabilidade se poden tomar tres decisións distintas:

- **Divulgación coordinada**
- **Divulgación completa**
- **Non divulgación (zero day)**

Unha vez publicadas, as vulnerabilidades pasan a formar parte de bases de datos públicas (como CVE) xunto co ***exploit*** que demostra a súa existencia. CVE (Common Vulnerabilities and Exposures) é un estándar desenvolto polo MITRE (https://cve.mitre.org) onde se almacenan as vulnerabilidades xunto cunha nomenclatura identificativa, enlaces a fontes de información e os parches / solucións / mitigacións existentes.

Ameazas

Unha ameaza é alguén ou algo que pode explotar unha vulnerabilidade. Podemos distinguir entre:

- **Ameazas Físicas** – As ameazas físicas afectan á organización, como accesos non autorizados ou ataques físicos a equipos e instalacións.
- **Ameazas Lóxicas** – As ameazas lóxicas afectan á información, como impedir ou dar acceso indebido a programas ou datos.

Podemos clasificar as ameazas en:

- **Deliberadas**: Roubo de datos, virus, incendios,sabotaxes, alteración de datos, accesos non autorizados…
- **Naturais ou ambientais**: Terremotos, inundacións, cortes de subministro eléctrico, incendios…
- **Accidentais**: Erros de uso…
- **Fallos Técnicos**: Fallo no hardware ou no software….

Ameazas Físicas

As ameazas físicas máis comúns son:

- Roubos
- Sabotaxes
- Incendios
- Inundacións
- Humidade do aire
- Fallos no subministro eléctrico
- Desastres naturais (terremotos, inundacións…)

Ameazas Lóxicas

As ameazas lóxicas están relacionadas co software, as máis importantes son:

- Malware (Troianos, Backdoors, Virus, Bombas lóxicas, Worms, Spyware, Ramsonware)
- Enxeñería social
- DoS
- MiM
- Suplantación (Phising)
- Modificación
- Botnets

Estas ameazas empregan varios sistemas para materializarse (ataques), normalmente aproveitándose de ***bugs*** no software ou dunha deficiente configuración dos sistemas:

- Buffer Overflow
- Syn Flood
- Force Brute Attack
- XSS
- SQL Injection
- ARP poisoning
- Roubo de cookies
- Eavesdropping / Sniffing (intercepción de tráfico de rede)

Seguridade Física

A seguridade física e ambiental establece normas para evitar os accesos non autorizados, os danos e as interferencias nos sistemas de información da organización. Únicamente as persoas autorizadas deben ter acceso e se deben regular as condicións ambientais para o funcionamento óptimo dos sistemas.

Para todo esto, o óptimo e o uso de emplazamentos especializados chamados centros de procesamento de datos (CPD) que dispoñan de medidas contra incendios, inundacións e terremotos, control de acceso e liñas de comunicación e subministro eléctrico redundantes.

Para protexer o subministro eléctrico se recurre ao uso de SAI/UPS (Sistemas de alimentación ininterrumpida / Uninterrupted Power Supply). Os SAI poden ser:

- OFF-LINE: Uso doméstico. A batería toma o relevo do subministro en caso de corte. Entre o fallo de corte e o inicio de subministro da batería se produce un pico de tensión que pode ser problemático en equipamento sensible.
- ON-LINE: Uso empresarial. O subministro eléctrico sempre o proporciona a batería, polo que ailla ao equipamento de calquera problema no subministro como picos de tensión.
- INTERACTIVE: E similar ao OFF-LINE pero protexe os sistemas das imperfeccións do subministro eléctrico.

Tamén se recurre a grupos electróxenos que poden crear electricidad a partir de distintas fontes de enerxía, sendo o gasoil o máis común.

Seguridade Lóxica

A seguridade lóxica pretende impedir ou mitigar os danos producidos pola materialización das ameazas lóxicas. Polo tanto debe:

- **Impedir o acceso indebido a programas e datos**: Control de Acceso, Xestión da Autorización e Cifrado
- **Garantir a privacidade na transmisión e o almacenamento da información**: Cifrado a nivel de carpetas, de dispositivo e cifrado asimétrico
- **Garantir a integridade da información transmitida**: Cifrado asimétrico
- **Garantir a dispoñibilidade ante fallos no soporte ou liñas de transmisión da información**: Uso de RAID e Backups. Recuperación de datos.
- **Detectar funcionamentos anómalos que podan afectar a seguridade ou ao rendimento:** Uso de sistemas de detección de intrusos (SDI/IDS) ou de detección e prevención (SDPI/IDPS)

Para conseguir esto, se deben establecer medidas de seguridade que poden ser **activas** ou **pasivas**. As medidas de seguridade activas pretenden evitar o problema (RAID, Bonding, Control de acceso, autorización, cifrado, antivirus, firewall,IDPS….). As medidas de seguridade pasiva pretenden solventar a situación unha vez que o suceso se produce (Backups, Recuperación de datos, chkrootkit, ...)

Cifrado

O Cifrado consiste en transformar a información de xeito que únicamente o que coñeza a chave apropiada pode acceder a ela. Existen dous sistemas de cifrado:

- **Cifrado simétrico ou de chave única:** Se emprega a mesma chave para cifrar e descifrar. Ambas partes da comunicación deben coñecer a chave, polo que o problema de seguridade radica na comunicación da chave a outra parte da comunicación. E rápido, e polo tanto apropiado para cifrar grandes volumes de información. Algoritmos coñecidos son: ***DES*** (inseguro), ***3DES*** (lento), ***AES*** (o máis utilizado), ***RC4*** (o usa TLS e algunha ferramenta de cifrado de arquivos), ***RC5***
- **Cifrado asimétrico ou de chave pública:** Se emprega unha parella de chaves. A información que cifra unha das chaves so a pode descifrar a outra. Unha das chaves se conserva en segredo (chave privada) mentres que a outra se debe distribuír públicamente (chave pública). Se elimina o problema da comunicación da chave a outra parte, pero é un sistema lento apropiado para información pequena. Algoritmos coñecidos son Diffie-Hellman (se usa para distribución de chaves), ElGamal, RSA (o mais utilizado), DSA (se usa para firma)
- Cifrado unidireccional (hash): Este sistema consiste en crear unha “firma” única a partir dunha información. Se utiliza para o cifrado de contrasinais e para as verificacións de integridade de arquivos. **O fundamental é que non sexa posible crear información que produza unha saída hash concreta (colisión).** Algoritmos coñecidos son SHA2, SHA2-256, SHA2-384, SHA2-512, SHA2-254, MD5 (inseguro, se atoparon colisións).