Disseny del perímetre

Disseny d'un perímetre segur per a una petita empresa

Objectiu

Haureu de dissenyar un perímetre de xarxa segur per a una petita empresa, tenint en compte les possibles amenaces, les necessitats de l'empresa i la ubicació dels dispositius.

Escenari

Una petita empresa vos ha contractat per millorar la seguretat de la seva xarxa. L'empresa té:

- 50 empleats.
- Un servidor web públic.
- Una VPN per a treballadors remots.
- Un servidor de fitxers intern amb dades confidencials dels clients.
- Un pressupost modest per a dispositius de seguretat.

L'empresa ha experimentat incidents menors, com intents de phising i accés no autoritzat al servidor web. La vostra tasca és dissenyar un perímetre segur i recomanar dispositius per protegir la xarxa.

Pas 1: Investigar i planificar

Amenaces a tenir en compte:

- Atacs externs (p. ex., DDoS, escaneig de ports i intents d'explotació).
- Amenaces internes.
- Malware/ransomware que ingressa a través del correu electrònic o el trànsit web.
- Accés remot no segur.

Dispositius/tecnologies a utilitzar:

- Tallafocs (amb estat, reconeixement d'aplicacions, etc.).
- Sistemes de detecció i prevenció d'intrusions (IDS/IPS).

- Tallafocs d'aplicacions web (WAF).
- Porta d'enllaç VPN.
- Eines de protecció i monitorització de punts finals.
- Zona desmilitaritzada (DMZ) per a serveis públics.

Pas 2: Tasques

1. **Dibuixar l'arquitectura del perímetre:**
   - Haureu de crear un diagrama de xarxa amb zones clarament diferenciades: pública, DMZ i xarxes internes.
   - Incloure la ubicació dels dispositius, com firewalls, IDS/IPS i balancejadors de càrrega.
2. **Elegir i justificar els dispositius:**
   - Els estudiants han de seleccionar almenys tres dispositius de seguretat per incloure al disseny. Exemples:
     - Un tallafocs d'última generació (p. ex., Palo Alto, Fortinet).
     - Un WAF per al servidor web (p. ex., ModSecurity, AWS WAF).
     - Un IDS/IPS (p. ex., Suricata, Snort).
     - Una solució VPN per a accés remot segur (p. ex., OpenVPN, Cisco AnyConnect).
     - Han d'explicar per què es van triar aquests dispositius i com mitiguen amenaces específiques.
3. **Abordar les limitacions pressupostàries:**
   - L'empresa vos a posat com a límí pressupostari total uns 20.000€. Així les coses, potser haureu de considerar software de codi obert o basat en el núvol, entre altres solucions.

Entregables

1. **Diagrama de xarxa:** Una representació visual del perímetre de la xarxa, que mostra les zones i la ubicació dels dispositius.
2. **Recomanacions de dispositius:** Una llista de dispositius o eines recomanats amb justificació per a cada opció, així com el preu.
3. **Pla de mitigació de riscos:** Una breu explicació de com el disseny proposat aborda les amenaces identificades.

Repte addicional i d'ampliació (opcional)

En un segon escenari, l'empresa s'expandeix per incloure una sucursal. Haureu d'ajustar el disseny del seu perímetre per incorporar una connexió segura de site-to-site.

Aquest exercici emfatitza la **planificació i el pensament crític**, que són habilitats essencials per dissenyar perímetres segurs.