VPS - 14 Sicherheit und Isolation

Ziel

Du kannst die Sicherheitsrelevanz des Virtualisierungslayers benennen und Grundmassnahmen ableiten.

Es kann sinnvoll sein, im Nachschlagedokument das Kapitel Sicherheit und Isolation zu lesen.

Inhalt

Der Hypervisor ist eine zentrale Sicherheitskomponente. Wenn er kompromittiert wird, können viele VMs betroffen sein.

Wichtige Massnahmen:

- Hypervisor regelmässig patchen
- Managementzugänge absichern
- Rechte nach dem Least-Privilege-Prinzip vergeben
- Netzwerke und Mandanten trennen
- unnötige Dienste deaktivieren
- Logging und Monitoring aktivieren
- Backups vor Manipulation schützen

VM-Escape beschreibt das Konzept, dass ein Angreifer aus einer VM auf den Hypervisor oder andere VMs ausbrechen könnte.

Auftrag

1. Erstelle eine Liste mit Sicherheitsrisiken einer Virtualisierungsplattform.
2. Ordne jedem Risiko eine geeignete Grundmassnahme zu.
3. Beschreibe, warum Administrationsrechte auf dem Hypervisor besonders sensibel sind.

Lernzielkontrolle

1. Warum ist der Hypervisor sicherheitskritisch?
2. Was bedeutet VM-Escape?
3. Warum sind Patches für den Hypervisor wichtig?
4. Was bedeutet Least Privilege?
5. Warum müssen Managementzugänge geschützt werden?
6. Warum ist Netzwerksegmentierung eine Sicherheitsmassnahme?
7. Welche Rolle spielt Logging?
8. Warum müssen Backups geschützt werden?
9. Nenne zwei Risiken bei zu vielen Administratorrechten.
10. Welche Grundmassnahmen würdest du für ein Lab trotzdem umsetzen?