Grundlagen der Systemhärtung

- Um Clientrechner und Server sicherer zu machen, können Sie, neben der Arbeit mit Richtlinien und einem konsistent geführten Konfigurationsmanagement durch die Pflege der Systeme viel zu deren Sicherheit beitragen.
- Durch unterschiedliche Massnahmen können Sie dabei die Sicherheit der Systeme verbessern, was, wie schon erwähnt, auch unter dem Begriff Systemhärtung (Hardening) zusammengefasst wird.
- Die Härtung der Systeme kann auf verschiedenen Ebenen erfolgen: auf Ebene der Hardware und Firmware, auf Ebene des Betriebssystems und auf der Ebene der Anwendungen.
- Dabei sollten Sie sich vor Augen halten, dass in einem Netzwerk meist nur wenige Server in Betrieb sind, aber ungleich viel mehr Arbeitsstationen.

Grundlagen der Systemhärtung

- Für einen potenziellen Angreifer ist es daher mitunter wesentlich einfacher, eine ungesicherte Arbeitsstation im Netzwerk zu finden und von dort aus weiter vorzudringen.
- Es lohnt sich also, auch die Arbeitsstationen sorgfältig zu behandeln! Ein besonderes Augenmerk sollten Sie dabei auf mobile Stationen (Tablets, Notebooks, Smartphones) richten, da diese durch ihren wechselnden Standort zusätzlichen Gefahren ausgesetzt sind.
- Best practices: Wenn ein System nicht gehärtet werden kann, sei es aus Gründen der Validierung beispielsweise bei Produktionsanlagen, dann müssen solch gefährdete Systeme in ein separiertes und vom restlichen Netzwerk getrenntes Netzsegment verschoben werden.

Grundlagen der Systemhärtung

- Das Härten auf Hard- und Firmware-Ebene kann folgende Aktionen umfassen:
  - Abschließen der Rechnergehäuse
  - Schutz des BIOS vor Systemzugriffen durch Passwörter
  - Harddisk-Verschlüsselung über den Controller (FDE)
  - Systemverschlüsselung über ein Hardware-Sicherheitsmodul (HSM)
  - Richtlinien für den Umgang mit externen Schnittstellen implementieren, z.B. Deaktivieren von USB-Schnittstellen oder SD-Kartenlesern
  - Nicht benötigte Laufwerke (z.B. CD/DVD) entfernen oder deaktivieren

Grundlagen der Systemhärtung

- Das zusätzliche Härten des Betriebssystems umfasst zudem:
  - Aktuell-Halten aller betriebsnotwendigen Dienste und Anwendungen
  - Deaktivieren von Standard-Accounts wie »Administrator« oder »Gast« oder Einrichten einer entsprechenden Berechtigungsstufe unter anderen Kontonamen
  - Benutzerkontensteuerung (UAC) bei Windows-Systemen auf sicherste Stufe einstellen
  - Entfernen nicht benötigter Dienste (Services) des Betriebssystems
  - Einspielen aktueller Sicherheitsaktualisierungen und Service Packs
  - Deinstallation nicht benötigter Betriebssystemfunktionen: je schlanker, desto weniger Angriffsfläche
  - Bei Servern zudem: Deinstallation nicht benötigter Rollen und Features

Grundlagen der Systemhärtung

- Das Härten der Arbeitsumgebung kann Folgendes beinhalten:
  - Entfernung nicht benötigter Software
  - Entfernen oder Deaktivieren nicht benötigter Funktionalitäten
  - Verschlüsselung der Datenverarbeitung mittels Software oder HSM
  - Aktuell-Halten aller installierten und eingesetzten Anwendungen
  - Passwortrichtlinien, Least-Privilege-Zugriffe für Daten und Anwendungen