Systemhärtung

Schwachstellen

- Lieferwege (physisch, aber vor allem elektronisch)
- Software-Voreinstellungen (Defaults)
- Funktionale Fehler der Software Ausnutzbarkeit von Nebeneffekten
- Nicht getestete oder nicht autorisierte Aenderungen
- Fremd-/Fernzugriffe oder Auslagerung aus dem Sicherheits-Kontext
- Der Benutzer
- Der Administrator

Ursachen

- Komplexes Zusammenwirken verschiedener Effekte
- Ungerechtfertigtes Vertrauen ("es sah aber echt aus")
- Gutwillikgkeit der Beteiligten ("Wird schon stimmen")
- Fehlerhafte Ausführung und/oder Kontrolle (insbes. unter Zeitdruck)
- Böswilligkeit / Vorsatz (Innen- oder Aussentäterschaft)

Methoden und Prozeduren zur Härtung von ICT-Systemen

- Identifikation relevanter Systeme oder Applikationen Technische Überprüfung (Security Scan, Penetration Testing, Application Security Audit, Ethical Hacking)
- Organisatorische Überprüfung (ICT Bedrohungs- und Risiko analyse)

Definition des Massnahmenkatalog zur Erhöhung des Sicherheits niveaus:

- Default-Installationen kritisch hinterfragen --> ggf. eigener Default
- Konfigurationsänderungen (Rechte, Rollen, Prozesse, ...)
- Einspielen von Security-relevanten Updates
- Entfernen nicht benötigter HW/SW-Komponenten oder Schnittstellen
- Installation von sicherheitsspezifischer Zusatzsoftware
- Zyklische Neuüberprüfung von aussen (Scan) oder innen (z.B. Secunia)
- Veränderungen / Verbesserungen im Betriebsablauf oder Überwachung
- Auswertung "echter" Angriffsversuche oder Kollateralinformation

Back