LI260 Linux Security & Hardening

Kurzbeschreibung:

Linux-Systemadministratoren erhalten eine praxisnahe Einführung in Sicherheitskonzepte und Hardening von Linux-Systemen. Vermittelt werden Sicherheitsrichtlinien, Kryptografie, Zugriffskontrolle und Benutzerverwaltung (inkl. PAM, 2FA, SELinux, AppArmor). Behandelt werden Protokollierung, Intrusion Detection, sichere Konfiguration von Netzwerkdiensten sowie Penetration-Testing-Grundlagen.

Zielgruppe:

Das Seminar **LI260 Linux Security & Hardening** richtet sich an Linux-Systemadministratoren.

Voraussetzungen:

Um Kursinhalten und dem Lerntempo im Workshop **LI260 Linux Security & Hardening** gut folgen zu können, sind Grundkenntnisse der Linux-Systemadministration erforderlich.

Sonstiges:

Dauer: 5 Tage

Preis: 2890 Euro plus Mwst.

Ziele:

Teilnehmende des Kurses **LI260 Linux Security & Hardening** lernen verschiedene Aspekte der Computersicherheit kennen, welche möglichen Bedrohungen lauern und wie man sich gegen diese schützt. In praktischen Übungen werden diese Mechanismen selbst umgesetzt, sodass den Teilnehmenden ermöglicht wird, die eigenen Systeme effektiver zu schützen.

Inhalte/Agenda:

- ♦ **Physische Sicherheit**

♦ **Einführung in Kryptographie & Verschlüsselung**
♦ ◊ Hardwareverschlüsselung
◊ Dateiverschlüsselung
◊ · Transportverschlüsselung

♦ **Absicherung von Netzwerkdiensten**

♦ **Zugriffskontrolle**

♦ **Sichere Benutzererstellung**
♦ ◊ PAM
◊ Zwei-Faktor-Authentifizierung
◊ Privilege Escalation

♦ **Berechtigungen und ACLs**
♦ ◊ Unix Permissions
◊ SELinux
◊ Apparmor

♦ **Erkennen von Problemen**
♦ ◊ Logging
◊ Integritätschecks
◊ Intrusion Detection

♦ **Penetration Testing (nur Theorie)**
♦