LI260 Linux Security & Hardening

Kurzbeschreibung:

Im 5-tägigen Kurs **LI260 Linux Security & Hardening** erhalten Linux-Systemadministratoren eine praxisnahe Einführung in Sicherheitskonzepte und den Schutz von Linux-Systemen. Die Teilnehmenden lernen, Sicherheitsrichtlinien zu entwickeln und verschiedene Bedrohungen sowie Schutzmaßnahmen zu verstehen – von physischer Sicherheit über Kryptografie, Zugriffskontrolle und Benutzerverwaltung (inkl. PAM, Zwei-Faktor-Authentifizierung, SELinux, AppArmor) bis hin zu Methoden der Protokollierung, Integritätsprüfung und Intrusion Detection.

Praktische Übungen vertiefen die sichere Konfiguration von Netzwerkdiensten, Berechtigungen und Verschlüsselungstechniken. Theoretische Einblicke in Penetration Testing runden das Programm ab. Voraussetzung sind Grundkenntnisse in der Linux-Systemadministration. Nach dem Kurs sind die Teilnehmer in der Lage, ihre Systeme wirkungsvoll gegen aktuelle Bedrohungen abzusichern.

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)**