

## SC430-WS Digitale Forensik, Spurensuche Ransomware

### Kurzbeschreibung:

Cyberkriminelle stellen durch Phishing, Hacking oder Scamming eine hohe Gefahr **für Krankenhäuser** und deren hoch sensiblen Daten dar. Nicht nur Konzerne sondern auch Kliniken und Krankenhäuser in Deutschland sind massiv betroffen!

Die **Beweissicherung** und der **Nachweis** strafbarer Handlungen bei IT-Sicherheitsvorfällen stellt Krankenhäuser häufig vor große Herausforderungen. Um den drohenden Gefahren eines Angriffs vorzubeugen bzw. im Falle einer **Ransomware-Attacke** die von Tätern hinterlassenen Spuren zu analysieren und gerichtsverwertbar zu sichern, bedarf es **IT-forensischer Kenntnisse**.

### Zielgruppe:

Das kostenlose Web-Seminar ist interessant für denjenigen, der sich u.a. folgende Fragen stellt:

- Hackerangriff - was soll ich/wir nun tun?
- Hackerangriff - kann das mir/unsrem Krankenhaus passieren?
- Hackerangriff - habe ich/wir im Krankenhaus dafür einen Plan?
- Hackerangriff - ist mir/den Mitarbeitern im Krankenhaus die Tragweite wirklich bewusst?
- Hackerangriff - wie kann ich/wir im Krankenhaus jetzt Beweise sichern?
- Ihre Fragen?

Wertvolle Tipps, Ratschläge und Antworten auf diese Fragen gibt es im Online-Kurs.

### Voraussetzungen:

IT-Experten im Krankenhaus-Umfeld.

### Sonstiges:

**Dauer:** 1 Tage

**Preis:** 0 Euro plus Mwst.

### Ziele:

**Profitieren Sie von den Erfahrungen und Kenntnissen einer Kriminalkommissarin und erfahren Sie mehr über:**

- Prävention.
- Detektion.
- Reaktion.

#### Inhalte/Agenda:

- **◆ Der Fokus liegt auf der praktischen Anwendung IT-forensischer Vorgehensweisen, Prozessen und Analysen.**
  - ◆ **Hierzu gehören alle Leistungen im Bereich der Digital Forensics:**
    - ◆ Digitale Forensik und Incident Response (DFIR)
    - ◆ Vorbeugung von IT-Sicherheitsvorfällen (Prävention)
    - ◆ Erkennung und Einschätzung von Sicherheitslücken (Detektion)
    - ◆ Bearbeitung von IT-Sicherheitsvorfällen in der IT-Forensik (Reaktion)
  - ◆ **Fallbeispiele & Incident Response**
    - ◆ Anhand von Fallbeispielen werden z. B. die Phasen des Incident Response-Prozesses nähergebracht, sowie die einzelnen Schritte einer IT-forensischen Analyse von Windowssystemen durchgeführt, um umfassend Benutzerinteraktionen nachweisen und interpretieren zu können.