BERUFSINFO | Berufsbereich: Recht / Sicherheit / Verwaltung | Bildungsweg: Akademische Ausbildung

IT-Forensiker*in

BERUFSBESCHREIBUNG

Die IT-Forensik bzw. Computer-Forensik befasst sich mit der Untersuchung von kriminellen Vorgängen und Tathandlungen im Internet und in IT-Systemen (wie z. B. Cybercrime, Hacking, Phishing) sowie mit der 'digitalen Spurensuche' im Rahmen von Wirtschaftskriminalität, Steuerhinterziehung und anderen kriminellen Handlungen.

IT-Forensiker*innen führen forensische Datenanalysen durch, in denen sie IT-Systeme wie Computer, Server, Datenbanken, Netzwerke und dergleichen zur Feststellung von kriminellen Tatbeständen und zur Identifizierung von Täter*innen untersuchen und analysieren. Sie werten die vorgefundenen Daten und Informationen (in der Regel aus beschlagnahmten Geräten) aus und stellen deren Gerichtsfestigkeit als digitale Beweismittel fest. Zu diesem Zweck erstellen sie eine lückenlose und umfassende Dokumentation, welche sie gemeinsam mit Kriminolog*innen, Kriminalbeamt*innen usw. besprechen und evaluieren.

Infos dazu findest du auch beim Beruf:

Forensiker*in (Spurensicherungsexpert*in)

Ausbildung

Für die Tätigkeit IT-Forensiker*in ist in der Regel ein abgeschlossenes Studium (Fachhochschule, Universität) in den Bereichen Informatik, Computertechnik, Datentechnik usw. und Weiterbildungen im Bereich der Forensik erforderlich. Mitunter kann auch der Abschluss einer facheinschlägigen berufsbildenden Schule (z. B. HTL im Bereich IT) den Berufseinstieg ermöglichen.

Wichtige Aufgaben und Tätigkeiten

- Festplatten aus beschlagnahmten PC- und Serversystemen sichern
- Festplatten von Laptops und Tablets sichern
- digitale Spuren von Smartphones sichern
- Cloudspeicher sichern und analysieren
- vorgefundene Daten sichern, forensische Datenanalysen durchführen
- Daten aufbereiten und präsentieren
- Gerichtsfestigkeit der Daten wie z. B. E--Mails, Korrespondenzen, Transaktionen als Beweismittel feststellen
- Tatbestand, Tathergang und Identität der Täter*innen ermitteln
- Umfang und Zeitraum der Tat feststellen (Erstellung einer „Timeline“)
- umfassende Berichte und Dokumentationen zur Vorlage vor Gericht erstellen
- mit anderen kriminaldienstlichen Spezialist*innen zusammenarbeiten
- IT-forensische Dokumentationen, Archive und Datenbanken führen

Anforderungen

- Anwendung generativer KI und von KI-Assistenzsystemen
- Anwendung und Bedienung digitaler Tools
- Datensicherheit und Datenschutz
- gute Beobachtungsgabe
- gutes Gedächtnis
- technisches Verständnis
- wirtschaftliches Verständnis
- Zahlenverständnis und Rechnen

- Argumentationsfähigkeit / Überzeugungsfähigkeit
- Kommunikationsfähigkeit
- Konfliktfähigkeit

- Aufmerksamkeit
- Ausdauer / Durchhaltevermögen
- Belastbarkeit / Resilienz
- Beurteilungsvermögen / Entscheidungsfähigkeit
- Flexibilität / Veränderungsbereitschaft
- Konzentrationsfähigkeit
- Sicherheitsbewusstsein
- Verschwiegenheit / Diskretion

- gepflegtes Erscheinungsbild

- Informationsrecherche und Wissensmanagement
- komplexes / vernetztes Denken
- Koordinationsfähigkeit
- kritisches Denken
- logisch-analytisches Denken / Kombinationsfähigkeit
- Planungsfähigkeit
- Problemlösungsfähigkeit
- Prozessverständnis
- systematische Arbeitsweise

WIRTSCHAFTSKAMMER ÖSTERREICH