Malware und Ransomware – Hintergründe, Erkennung, Schutz und Reaktion

Malware und Ransomware haben sich zu einer allgegenwärtigen Bedrohung entwickelt. Immer mehr Unternehmen sind betroffen, werden erpresst und können nicht mehr arbeiten.

Die Schulung vermittelt das nötige Wissen über die Angreifer, ihre Techniken und Vorgehensweisen sowie sinnvolle Sicherheitsmaßnahmen, um sich wirksam schützen, Angriffe frühzeitig erkennen und richtig reagieren zu können.

In einem Rückblick auf die wichtigsten Vorfälle der vergangenen Jahre werden die verschiedenen Infektionsmechanismen, die Schritte zur Weiterverbreitung und Umgehung von Schutzmaßnahmensowie die Hintergründe und Tätergruppen erläutert.

Danach werden Strategien und Techniken zur Prävention von Vorfällen dargestellt und bewertet. Diese beinhalten sowohl die sinnvolle Nutzung der vorhandenen Bordmittel von Windows und der typischen Gateways als auch moderne Trends wie EDR, XDR und SASE sowie Strategien wie Zero Trust.

Ebenso werden Konzepte und Techniken zur frühzeitigen Erkennung von Angriffen und Infektionen erläutert und die Rolle von CERTs, SOCs und SIEM-Lösungen zusammen mit den heute relevanten Betriebsmodellen und Outsourcing-Optionen abgegrenzt.

Auch die richtige Reaktion auf Vorfälle, nötige Vorbereitung für das Incident Management und die Wiederherstellung sowie Möglichkeiten zur Analyse von Malware werden dargestellt.

In dieser Schulung erlernen die Teilnehmer nicht nur konkrete technische Maßnahmen und organisatorische, sondern auch die Herangehensweise zur Erstellung von Malwareschutzkonzepten.

Zielgruppe:
Sicherheitsverantwortliche, Administratoren, SOC-Mitglieder, CERTs

Voraussetzung:
Grundlegende Kenntnisse in der IT; von Vorteil sind Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern

Beginn:
Donnerstag, 30. November 2023, 09:00 Uhr

Ende:
Donnerstag, 30. November 2023, 18:00 Uhr

Veranstaltungsort:
Ludwigsburg
Deutschland

Website & Anmeldung:
Email nadine.eimuellner@cirosec.de

https://www.cirosec.de/trainings/malware-und-ransomware-hintergruende-erkennung-schutz