



# MOBILE FORENSICS WORKSHOP I WEBINAR

Wirtschaftskriminalität und gezielte Hacker-Angriffe wie z.B. Advanced Persistent Threats können ein Unternehmen schwer treffen. Damit ein solcher Vorfall gerichtlich aufgeklärt werden kann, ist eine IT-forensische Untersuchung notwendig. Im Rahmen des Mobile Forensics Workshops schlüpft der Teilnehmer/die Teilnehmerin in die Rolle eines IT-Forensikers und klärt unter der Anleitung von Herrn Ludwig Englbrecht einen IT-Sicherheitsvorfall mit forensischen Tools auf. Neben kurzen theoretischen Einheiten zur Vermittlung von Hintergrundinformationen kann der Teilnehmer/die Teilnehmerin mit einem virtuellen System tatkräftig bei der Aufklärung eines Social-Engineering Vorfalles helfen, welches dem fiktiven Unternehmen die Marktführerschaft gekostet hat.

## Motivation

Die Bedrohungslage für Unternehmen im Bereich IT-Sicherheit nimmt seit Jahren stetig zu. Dabei steigt sich nicht nur die Anzahl der erkannten und gemeldeten IT-Sicherheitsvorfälle - auch die Schlagkraft der Angriffe erhöht sich. Dabei werden z.B. gezielt Mitarbeiter/-innen eines Unternehmens mit einer Schlüsselrolle adressiert und somit zur Zielscheibe eines Hackerangriffs. Es gibt viele Maßnahmen um die IT-Sicherheit in einem Unternehmen zu erhöhen. Die Schulung der Mitarbeiter/-innen ist dabei ein entscheidender Faktor. Dieser Workshop vermittelt ein tiefes Verständnis über moderne Angriffsmöglichkeiten und lässt den Teilnehmer/die Teilnehmerin durch eine IT-forensische Herangehensweise einen fiktiven Fall aufklären. Anders als innerhalb gängiger Schulungen und Trainings im Bereich IT-Security, erkundet und analysiert der Teilnehmer/die Teilnehmerin in diesem Workshop Schritt für Schritt in die Vorgehensweise des Angreifers.

## Ziel des Workshops

- ▶ Bewusstsein für IT-Sicherheit und IT-Forensik durch Verständnis fördern
- ▶ Einen fiktiven Social Engineering Angriff mit IT-Forensik Tools aufklären
- ▶ Whats-App Chat und andere Daten auf einem Android Smartphone wiederherstellen
- ▶ Eine echte Android-Malware analysieren



## Workshop Methoden

Der Workshop vermittelt theoretisches Wissen im Bereich IT-Sicherheit und der digitalen Forensik. Durch hands-on Aufgaben analysiert der Teilnehmer/die Teilnehmerin schrittweise einen Vorfall und reflektiert die Erkenntnisse in der Gruppe.

Dieses Konzept basiert auf dem wissenschaftlichen Konzept der peer-instruction basierten Lehrmethode. Der übergeordnete Rahmen des Workshops ergibt sich aus weiteren Forschungsergebnissen zur Etablierung und Steigerung der Digital Forensic Readiness von Unternehmen. Der Workshop wird geleitet und durchgeführt von Herrn Ludwig Englbrecht, M.Sc. (ludwig.englbrecht@ur.de)

## Kontakt

Benedikt Putz, M.Sc.  
(Projektverantwortlicher)  
benedikt.putz@ur.de  
TRIO – Transfer und Innovation Ostbayern  
Universität Regensburg