

## Die Autoren

**Michael Kofler** (<https://kofler.info>) ist einer der renommiertesten IT-Autoren im deutschen Sprachraum. Er ist außerdem als Administrator, Software-Entwickler und als Lektor an einer Fachhochschule tätig. Michael Kofler hat das Autorenteam zusammengestellt und für dieses Buch sieben Kapitel zu Grundlagenthemen sowie rund um Linux verfasst.

**Klaus Gebeshuber** (<https://fh-joanneum.at/hochschule/person/klaus-gebeshuber>) ist Professor für IT-Security an der FH JOANNEUM in Kapfenberg/Österreich. Seine Schwerpunkte liegen im Bereich Netzwerksicherheit, Industrial Security, Security-Analysen und Penetration-Tests. Er hält zahlreiche Industriezertifizierungen im Umfeld von IT-Security, Netzwerksicherheit und Penetration-Testing. In diesem Buch deckt er in vier Kapiteln die Themen Exploits, Sicherheit in Funknetzwerken (WLAN/-Bluetooth), Sicherheit in Webapplikationen sowie den Umgang mit Passwörtern ab.

**Thomas Hackner** (<https://www.hackner-security.com>) ist Senior Security Consultant und Geschäftsführer der Firma HACKNER Security Intelligence GmbH, die er 2010 nach seinem Studium für Sichere Informationssysteme in Hagenberg, Oberösterreich, gründete. Er arbeitet außerdem in internationalen Projekten mit, in denen sowohl IT-Netzwerke und Webanwendungen als auch SCADA-Systeme in Form von Penetration-Tests auf Sicherheit überprüft werden. In diesem Buch erläutert er in drei Kapiteln die Zielsetzung und Durchführung von Penetration-Tests.

**Peter Kloep** ist herausragender Experte für sichere Windows-Infrastrukturen im deutschsprachigen Raum. Seit 2002 ist er Microsoft Certified Trainer und hat zahlreiche technische Trainings zur Windows-Administration durchgeführt. Im vorliegenden Buch erklärt er die sichere Konfiguration von Windows-Server- und Active-Directory-Installationen.

**André Zingsheim** ist als Principal Security Consultant in der TÜV TRUST IT GmbH tätig. Neben technischen Sicherheitsanalysen/Penetration-Tests von IT-Systemen und -Infrastrukturen beschäftigt er sich intensiv mit der Sicherheit von mobilen Endgeräten. Er ist ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierter Penetration-Tester und *Certified Information Systems Security Professional* (CISSP®). Er bringt sein Hacking- und Security-Know-how im Bereich Smartphones in das Buch ein.

**Frank Neugebauer** (<https://pentestit.de>) blickt auf eine langjährige Tätigkeit als Offizier der Bundeswehr zurück. Dort arbeitete er über 25 Jahre lang auf dem Gebiet der IT-Sicherheit und war u. a. als IT-Sicherheitsbeauftragter, Systems Engineer eines NATO-Hauptquartiers und Leiter eines Incident Response Teams eingesetzt. Als Mitglied des Computer Emergency Response Teams wirkte er maßgeblich an Schwachstellenanalysen in vielen Netzwerken der Bundeswehr mit. Zuletzt war er als Incident Handler im Zentrum für Cybersicherheit der Bundeswehr tätig. Er wurde Ende 2017 in den Ruhestand versetzt und arbeitet derzeit als Berater und externer Mitarbeiter. Für dieses Buch hat er das Kapitel »Angriffsvektor USB-Schnittstelle« sowie Abschnitte zu den Themen »Empire«, »Koadic« und »Pwnagotchi« verfasst.

**Markus Widl** (<https://www.linkedin.com/in/markus-widl>) arbeitet seit rund 20 Jahren als Berater, Entwickler und Trainer in der IT. Sein Fokus liegt auf Cloud-Technologien wie Office 365 und Azure. Durch seine Expertenworkshops, Konferenzbeiträge und Autorentätigkeit hat er sich einen Namen gemacht. In »Hacking & Security« zeigt er, wie Sie Sicherheitsprobleme beim Einsatz von Microsofts Cloud-Produkten vermeiden.

**Roland Aigner** (<http://www.aignerdevelopment.com>) ist Experte für sichere IoT-Infrastrukturen. Er entwickelte Firmware und Software in der medizinischen In-vitro-Diagnostik, ist Mitautor in der Bluetooth SIG sowie ein Gründungsmitglied des NFC Forums, in dem er sich im Speziellen um Ticketing und Kommunikations-Security kümmerte. Er arbeitet als Software Manager im Zutrittskontrollbereich und ist als Consultant für IoT-Projekte tätig. Er hat zu dem Buch das IoT-Kapitel beigesteuert.

**Stefan Kania** (<https://www.kania-online.de>) ist seit 1997 freiberuflich als Consultant und Trainer tätig. Seine Schwerpunkte liegen in der sicheren Implementierung von Samba und LDAP sowie in Schulungen zu beiden Themen. Er hat das ebenfalls im Rheinwerk Verlag erschienene Samba-Handbuch verfasst und führt regelmäßig Schulungen und Consulting-Projekte durch. In diesem Buch zeigt er, wie Sie Samba-Server sicher in Windows-Netzwerke integrieren.