eSECURITY®

Academy

esecurity.academy

TLS 1.3

Kurs in Bern

28. März 2019

Die Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS) Protokolle stehen heute im Mittelpunkt aller Bemühungen, den Datenverkehr im Internet durchgehend kryptografisch abzusichern. In der Vergangenheit haben viele kryptanalytische Angriffe (z.B. BEAST, POODLE, CRIME und Lucky 13) die Schwächen und Verwundbarkeiten dieser Protokolle aufgezeigt, so dass die IETF TLS WG angetreten ist, eine neue und vollständig überarbeitete TLS-Protokollversion zu spezifizieren. Seit August 2018 liegt das Resultat als RFC 8446 vor, und ist in dieser Form in die Internet-Standardisierung eingereicht.

Im Rahmen der eSECURITY Academy bietet Prof. Dr. Rolf Oppliger einen 1-tägigen Kurs an, um TLS 1.3 im Detail vorzustellen, und dabei insbesondere auch zu erklären, worin die wesentlichen Unterschiede zu den Vorgängerversionen liegen.

Der Kurs setzt elementare Grundkenntnisse über kryptografische Sicherheitsprotokolle und SSL/TLS voraus, wie sie z.B. im Buch «SSL and TLS: Theory and Practice, Second Edition» (Artech House, 2016, ISBN 978-1-60807-998-8) vermittelt werden. Das Buch wird – zusammen mit den verwendeten Folien – an die Kursteilnehmenden abgegeben.

Der Kurs findet am Donnerstag, 28. März 2019, in Bern statt (Ort und genaue Zeit werden noch bekanntgegeben).

Die Teilnahmegebühren betragen CHF 950.00 (inkl. MWST, Buch, Unterlagen und Verpflegung).

Melden Sie sich bitte bis am 28. Februar 2019 per E-Mail an registration@esecurity.academy an.

Für Fragen stehen wir Ihnen gerne telefonisch (079 654 84 37) oder per E-Mail (info@esecurity.academy oder rolf.oppliger@esecurity.ch) zur Verfügung.