eSECURITY®

EDUCATION CENTER

https://education.esecurity.ch

TLS 1.3

Seminar in Bern

30. November 2018

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

Im Rahmen des eSECURITY EDUCATION CENTER bietet Prof. Dr. Rolf Oppliger ein 1-tägiges Seminar an, um TLS 1.3 im Detail vorzustellen, und dabei insbesondere auch zu erklären, worin die hauptsächlichen Unterschiede zu den Vorgängerversionen liegen.

Das Seminar setzt elementare Grundkenntnisse über die Funktionsweise der SSL/TLS-Protokolle 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 Seminarteilnehmenden abgegeben.

Das Seminar findet am Freitag, 30. November 2018, in Bern statt (Ort und Zeit werden noch bekanntgegeben).

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

Die Anmeldefrist läuft bis am 30. Oktober 2018. Anmeldungen bitte per E-Mail an seminar@esecurity.ch.

Für Fragen stehen wir Ihnen gerne per E-Mail oder telefonisch unter 079 654 84 37 zur Verfügung.