eSECURITY EDUCATION CENTER

https://education.esecurity.ch

SSL und TLS Sicherheit

Seminar in Bern

3./4. Mai 2018

Die SSL/TLS-Protokolle sind für die Sicherheit im Internet von zentraler Bedeutung. Entsprechend vielen und vielfältigen Angriffen sind sie ausgesetzt, wie z.B. BEAST, POODLE, CRIME, TIME, BREACH, Lucky 13, FREAK, Logjam, DROWN, SLOTH und HEIST. Die meisten dieser Angriffe können mit geeigneten Gegenmassnahmen verhindert werden, allerdings sind diese Massnahmen auch wieder Ziel neuer Angriffe.

Damit die SSL/TLS-Protokolle sinnvoll und sicher eingesetzt werden können, ist ein tiefgreifendes Verständnis sowohl der Protokolle als auch der Angriffe, Gegenmassnahmen und Gegenangriffe erforderlich.

Im Rahmen des eSECURITY EDUCATION CENTER bietet Prof. Dr. Rolf Oppliger ein 2-tägiges Seminar an, das dieses Verständnis vermittelt.

Inhaltsübersicht:

1. Einführung
2. SSL Protokoll
3. TLS Protokolle
4. DTLS Protokoll
5. Firewall Traversierung
6. Public Key Zertifikate und PKI
7. Zusammenfassung und Ausblick

Insbesondere werden im Seminar auch die Neuerungen in TLS 1.3 aufgezeigt.

Das Seminar basiert auf dem 2016 im Artech House Verlag erschienenen Buch «SSL and TLS: Theory and Practice, Second Edition» (ISBN 978-1-60807-998-8). Das Buch wird – zusammen mit den verwendeten Folien – an die Seminarteilnehmenden abgegeben.

Das Seminar findet am Donnerstag und Freitag, 3./4. Mai 2018, in Bern statt (Ort und Zeit werden noch bekanntgegeben).

Die Teilnahmegebühren betragen CHF 1‘790.00 (inkl. MWST, Buch und Verpflegung).

Die Anmeldefrist läuft bis am 3. April 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.