SSL und TLS Sicherheit

Kurs in Bern

22./23. Oktober 2020

Die SSL/TLS-Protokolle sind für die Sicherheit im Internet von zentraler Bedeutung. Entsprechend vielen und vielfältigen Angriffen sind sie ausgesetzt (z.B. BEAST, POODLE, CRIME, TIME, BREACH, Lucky 13, FREAK und Logjam). Die meisten dieser Angriffe können zwar mit geeigneten Konfigurationseinstellungen und Gegenmassnahmen technisch verhindert werden, allerdings sind diese Gegenmassnahmen zum Teil 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 der eSECURITY Academy bietet Prof. Dr. Rolf Oppliger einen 2-tägigen Kurs an, um dieses Verständnis zu vermitteln.

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 Kurs auch die Neuerungen im TLS 1.3 Protokoll aufgezeigt.

Der Kurs 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 Kursteilnehmenden abgegeben.

Der Kurs findet am Donnerstag und Freitag, 22./23. Oktober 2020, in Bern statt (Ort und genaue Zeit werden noch bekanntgegeben).

Die Teilnahmegebühren betragen CHF 1‘960.00 (inkl. MWST, Buch, Unterlagen und Verpflegung).

Melden Sie sich bitte bis am 22. September 2020 per E-Mail an registration@esecurity.academy an.

Für Fragen stehen wir Ihnen telefonisch unter +41 79 654 84 37 oder per E-Mail unter info@esecurity.academy bzw. rolf.oppliger@esecurity.ch jederzeit sehr gerne zur Verfügung.