Zertifizierter Kryptographie-Practitioner

Grundlagen kryptographischer Verfahren und Verschlüsselungstechniken

wecon.it-consulting
»we.secure-your.it«

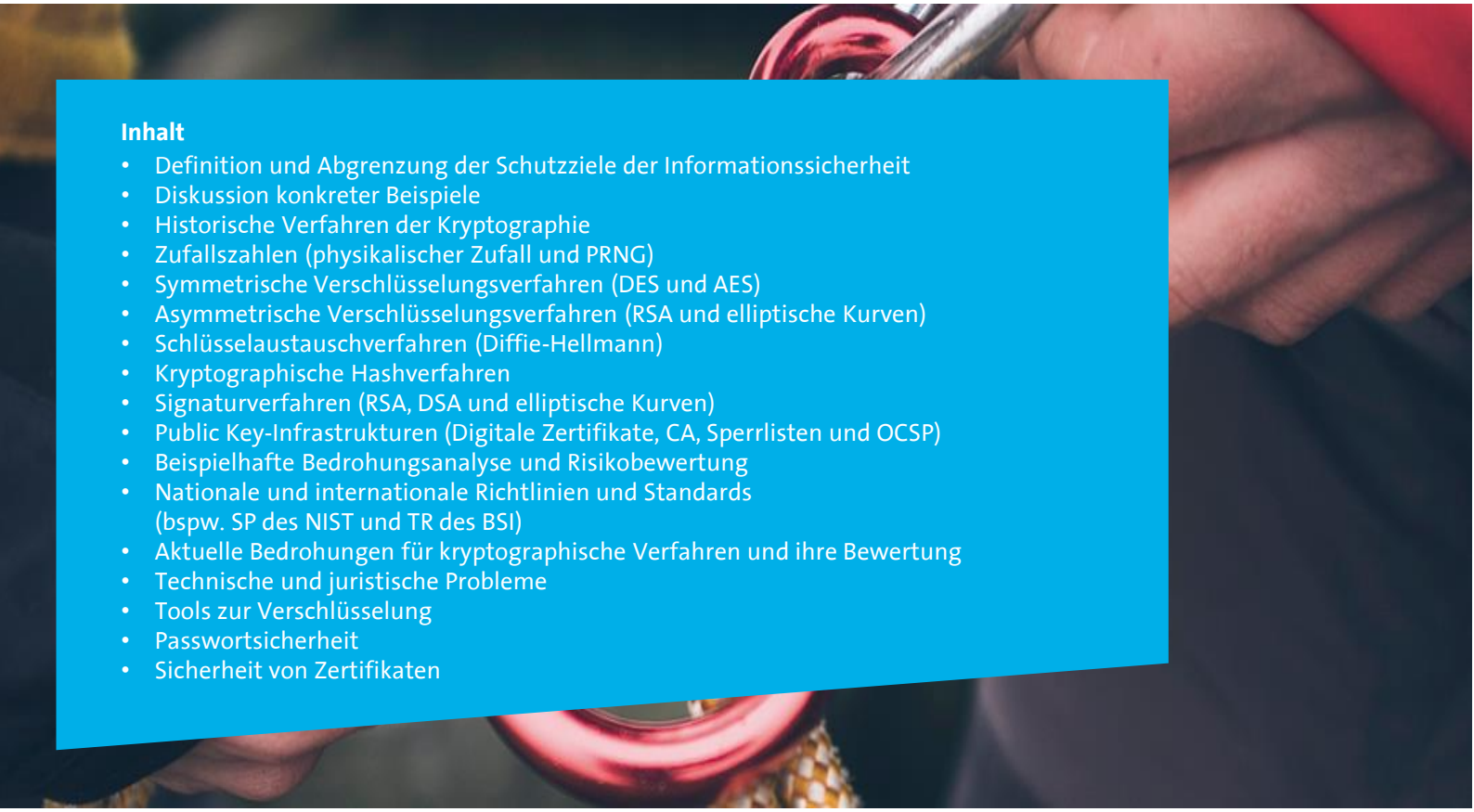
bitkom akademie

Zertifizierter Kryptographie-Practitioner

Grundlagen kryptographischer Verfahren und Verschlüsselungstechniken

Kurzbeschreibung

Kryptographie spielt in modernen Geschäftsprozessen eine immer größere Rolle und zählt bereits seit längerem zu den Standard-Maßnahmen in den Bereichen Informationssicherheit und Datenschutz. Zur Beurteilung der eingesetzten kryptographischen Verfahren ist aber ein Grundverständnis der Funktionsweise notwendig. Selbiges trifft zu, wenn -bspw. im Rahmen einer Risikobewertung- die Robustheit der eingesetzten Verfahren oder die Angemessenheit von Maßnahmen beurteilt werden soll.
Insbesondere da auch der Einsatz kryptographischer Verfahren gesonderte Risiken wie bspw. eine fehlerhafte Anwendung der Verfahren oder sich aus dem Einsatz ergebende zusätzliche Bedrohungen mit sich bringen kann, sind Kenntnisse aktueller Verschlüsselungstechniken, der Vor- und Nachteile Digitaler Signaturen sowie der Grundlagen von Public Key-Infrastrukturen (PKI) für eine angemessene Bewertung unerlässlich.



Inhalt

- Definition und Abgrenzung der Schutzziele der Informationssicherheit
- Diskussion konkreter Beispiele
- Historische Verfahren der Kryptographie
- Zufallszahlen (physikalischer Zufall und PRNG)
- Symmetrische Verschlüsselungsverfahren (DES und AES)
- Asymmetrische Verschlüsselungsverfahren (RSA und elliptische Kurven)
- Schlüsselaustauschverfahren (Diffie-Hellmann)
- Kryptographische Hashverfahren
- Signaturverfahren (RSA, DSA und elliptische Kurven)
- Public Key-Infrastrukturen (Digitale Zertifikate, CA, Sperrlisten und OCSP)
- Beispielhafte Bedrohungsanalyse und Risikobewertung
- Nationale und internationale Richtlinien und Standards (bspw. SP des NIST und TR des BSI)
- Aktuelle Bedrohungen für kryptographische Verfahren und ihre Bewertung
- Technische und juristische Probleme
- Tools zur Verschlüsselung
- Passwortsicherheit
- Sicherheit von Zertifikaten

wecon.it-consulting
»we.secure-your.it«

bitkom akademie

Was lernen Sie in diesem Seminar?

Ziel des Zertifikatslehrgangs ist die Vermittlung der für die praktische Anwendung und Beurteilung kryptographischer Verfahren notwendigen Grundkenntnisse; dazu gehört das Wissen über aktuelle Verschlüsselungstechniken, Digitale Signaturen und den Aufbau von Public-Key-Infrastrukturen (PKI). Zudem werden Sie über aktuelle Bedrohungen und Risiken bei der Nutzung moderner kryptographischer Verfahren, wie z. B. SSL/TLS und S/MIME, informiert und lernen, wie der Einsatz von kryptographischen Mechanismen in der Praxis zu beurteilen ist. Darüber hinaus erfahren Sie auch, welche nationalen und internationalen Richtlinien und Standards im Bereich der Kryptographie existieren und wie sich diese in der Praxis einsetzen lassen.

An wen richtet sich der Lehrgang?

- Personen, die kryptographische Verfahren bewerten oder anwenden müssen
- IT-Sicherheitsbeauftragte
- Chief Information Security Officer
- Datenschutzbeauftragte
- Verantwortliche in der Informationssicherheit

Sie entscheiden – wir bieten diesen Lehrgang in zwei Formaten an

Online-Lehrgang

- Der Online-Lehrgang ist eine reines Remote-Format und wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie hier einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) finden Sie hier einen zusätzlichen Vergleich zu den jeweiligen Eigenschaften.
- Bitte beachten Sie, dass die Stornofrist für Online-Lehrgänge **zwei Wochen** beträgt.

Präsenz-Lehrgang

- Der Präsenz-Lehrgang findet vor Ort an einem der Veranstaltungsorte der Bitkom Akademie statt. Die jeweiligen Veranstaltungsorte entnehmen Sie bitte der Website der Bitkom Akademie.
- Teilnehmerseitig ist keine spezielle Technik oder Software erforderlich.
- Bitte beachten Sie, dass die Stornofrist für Präsenzlehrgänge **vier Wochen** beträgt.

wecon.it-consulting
»we.secure-your.it«

bitkom akademie

Ihr Referent

Dr. Christoph Wegener

Experte für Informationssicherheit und Datenschutz
wecon.it-consulting

Christoph Wegener ist promovierter Physiker und seit 1999 als freiberuflicher Berater mit der wecon.it-consulting in den Bereichen Informationssicherheit, Datenschutz und Open Source aktiv. Zu seinen Arbeitsschwerpunkten zählen die Konzeption und Bewertung sicherheitsrelevanter Prozesse und Verfahren sowie insbesondere der Querschnittsbereich Recht und Technik. Neben seiner freiberuflichen Tätigkeit war er an der Ruhr-Universität Bochum zunächst als Projektkoordinator am Horst-Görtz-Institut für IT-Sicherheit (HGI) und später als IT-Leiter an der dortigen Fakultät für Elektrotechnik und Informationstechnik tätig. Herr Wegener ist Fachbuchautor, hat zahlreiche Beiträge in relevanten Fachzeitschriften veröffentlicht, ist Sprecher auf nationalen und internationalen Konferenzen sowie Mitglied des Beirats der Fachzeitschrift „Datenschutz und Datensicherheit – DuD“ und engagiert sich in der Ausbildung im Bereich der Informationssicherheit.

Shortfacts

Termine, Preise und Veranstaltungsorte

Bitte entnehmen Sie aktuelle Informationen hierzu Website der Bitkom Akademie.

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie