LEHRGANGSZIEL | ZIELGRUPPEN

Viele Unternehmen wappnen sich mit meist hohem Aufwand auf technischem Wege gegen externe Angriffe. Doch Schwachpunkt Nr. 1 ist und bleibt der Mensch. Dies belegen Zahlen aus dem Jahr 2016; **danach flossen sensible Unternehmensdaten nur zu 20 % durch digitale Angriffe, jedoch 80 % durch menschliche Eingriffe ab**. Gutgläubigkeit, Hilfsbereitschaft und Hierarchiefragen werden gezielt genutzt, um unter Legenden und falscher Identität vertrauliche Informationen unter Umgehung sämtlicher Sicherungsvorkehrungen zu gewinnen.

Durch geschickte Manipulation und Täuschung durch die Angreifer ist das Datenleck „Mensch" die größte Bedrohung für Ihr Unternehmen. Sei es, dass durch geschickte Täuschung Geldüberweisungen (CEO-Fraud) vorgenommen werden oder unberechtigter Zugriff auf Systeme gewährt wird.

Ziel des Workshops ist es, Sicherheitsverantwortliche fit zu machen und die im Unternehmen vorhandenen Tools optimal und effektiv einzusetzen; und dies, ohne Neuinvestitionen in kostenintensive Hard- und/oder Software vornehmen zu müssen, können Tools, die in jedem Unternehmen als Basisschutz vorhanden sein müssen, wirkungsvoll und effektiv ein- und umgesetzt werden.

Um die Trainingsinhalte nachhaltig zu vermitteln und zu verankern, werden die perfiden Methoden des „Social Engineering" den Teilnehmern nicht nur in der Theorie, sondern auch in der Praxis vorgeführt. – Wir machen ausdrücklich darauf aufmerksam, dass bei der Schulung teilweise illegale, strafbewehrte Vorgehensweisen demonstriert werden, um so die verschiedenen Vorgehensweisen realistisch darstellen zu können.

Zielgruppe: Sicherheitsverantwortliche, Leitende Mitarbeiter aus Personalbereich, Verkauf, Vertrieb, Forschung und Entwicklung, IT-Bereich etc.

PROGRAMM | REFERENTEN

Donnerstag, 19. April 2018

09:00 Uhr	**Begrüßung/Einführung**
09:15 Uhr	Was bedeutet Social Engineering? Sensibilisierung für die eigene unbewusste Manipulation Welche Methoden benutzen die Angreifer? Was ist/wie funktioniert Identitätsmissbrauch? Welche Ziele verfolgt der Angreifer? Was sind schützenswerte Informationen (Kronjuwelen) im Unternehmen? Geändertes Bewusstsein beim Umgang/ der Weitergabe von Informationen Welchen realen Bedrohungen bin ich täglich unbewusst ausgesetzt? Wie anfällig bin ich für Angriffe dieser Art? Wie schütze ich mich und andere?
12:00 Uhr	Gemeinsames Mittagessen
13:00 Uhr	ISMS und Compliance – verständlich und lebbar machen Sicherheitskultur als wichtige Säule der Existenzsicherung **Darknet live – Die hochkriminelle Parallelwelt des Internet**
16:30 Uhr	**Abschlussdiskussion**

Ihr Referent:
Thomas Krauss – Ein vielfach gebuchter Referent/ Dozent, der vor Wirtschaftsverbänden, bei Unternehmen ebenso wie in diversen Universitäten im gesamten deutschsprachigen Raum auftritt. Er zeigt in seinen Vorträgen und Schulungen die hochkriminellen, jedoch effektiven Tricks Wirtschaftskrimineller auf.

Wir helfen Ihnen mit Sicherheit! Seit 49 Jahren

ORGANISATION

Datum **Donnerstag, 19. April 2018**

Anmeldung **www.asw-bw.com/8/Leistungen/SocialEngineering** oder mit Kennziffer **336/18** per E-Mail/Fax

bei
ALLIANZ FÜR SICHERHEIT
IN DER WIRTSCHAFT
BADEN-WÜRTTEMBERG e. V.
Postfach 50 11 43
70341 Stuttgart
Telefon 0711 954609-0
Telefax 0711 954609-20
anmeldung@asw-bw.com

bis zum **18. April 2018**

Teilnahmekosten

ASW-Mitglieder	**€ 450,–**
ASW-Nichtmitglieder	**€ 500,–**

Die Tagungskosten beinhalten die Tagungsunterlagen, das Mittagessen und die Getränke.

Seminarort

Geschäftsstelle der ASW-BW
Daimlerstraße 71, 70372 Stuttgart

Hotel MOTEL ONE
Badstraße 20, 70372 Stuttgart
Telelefon 0711 21840200
Internet: http://www.motel-one.com/de/hotels/stuttgart/hotel-stuttgart-bad-cannstatt
EZ ohne Frühstück zwischen € 69,-/€ 79,-
Bio-Frühstücksbuffet € 9,50
Gern sind wir Ihnen bei der Reservierung behilflich.