

SC510 Cyber Security - Emergency Training für CISOs und Security Professionals

Kurzbeschreibung:

CISOs sind für die Informationssicherheit in Unternehmen verantwortlich, und ihre Funktionen und Zuständigkeiten sind in einer Welt mit rasant ansteigenden Cyberbedrohungen äußerst wichtig. Tendenziell werden die Angriffe immer aggressiver und die Aufgaben eines CISOs somit immer anspruchsvoller.

Wird ein Unternehmen angegriffen, ist der CISO gefragt. Er muss die Abwehrmaßnahmen leiten, indem er die Bemühungen des Cybersicherheitsteams und anderer relevanter Abteilungen innerhalb und außerhalb der Organisation koordiniert. Er muss Maßnahmen zur Eindämmung und Beseitigung des Hackerangriffs ergreifen, den Umfang des Vorfalls definieren, die Folgen und den Schweregrad bewerten und unter großem Druck wichtige Entscheidungen treffen, um den Schaden zu minimieren und mit der Wiederherstellung fortzufahren. Es ist wichtig, dass der CISO während des Vorfalls Ruhe und Effizienz bewahrt.

Im Falle einer Cyberattacke zählt jede Minute. Es kommt auf präzise aufeinander abgestimmte Prozessabläufe und Koordination an – und da ist Übung gefragt. Krisenstabsübungen werden in der Regel häufig durchgeführt, Übungen im Cybersecurity-Bereich sind eher die Ausnahme. Das wollen wir ändern!

Im Workshop **SC510 Cyber Security - Emergency Training für CISOs und Security Professionals** werden Sie von **einem langjährigen Krisenstab-Experten** und **einer erfahrenen Psychologin** angeleitet. Wo immer möglich, werden die Aspekte der Schulung nicht nur theoretisch behandelt, sondern anhand von Praxiserfahrungen und Fallbeispielen lebendig gemacht. Dabei gehen wir besonders auf das Verhalten der CISOs in der Gruppendynamik ein und beleuchten den Aufbau von Kommunikation in ihren formellen und informellen Aspekten. Durch Praxisübungen entwickeln Sie Routine, um bei einem Angriff souverän agieren und reagieren zu können. Übungen, in denen Vor- und Nachteile von einzelnen Vorgehensweisen erlebbar werden, lassen die Problematiken erkennen, die sich in solchen Situationen stellen - sie schaffen Awareness und die Befähigung, mit Situationen, die allerhöchsten Stress mit sich bringen, umzugehen.

Zielgruppe:

Die Schulung richtet sich an:

- Verantwortliche im Bereich Informationssicherheit
- Security Professionals
- CISOs (Chief Information Security Officer)

Voraussetzungen:

Für die Teilnahme am Kurs **SC510 Cyber Security - Emergency Training für CISOs und Security Professionals** wird eine langjährige Berufserfahrung in einem informatiknahen Bereich, mehrjährige Erfahrungen im IT-Security-Bereich sowie in einer Leitungsfunktion vorausgesetzt.

Sonstiges:

Dauer: 2 Tage

Preis: 1950 Euro plus Mwst.

Ziele:

Im Workshop **SC510 Cyber Security - Emergency Training für CISOs und Security Professionals** behandeln wir das Management von Notfällen und Krisen. Sie erfahren, wie Sie sich bei IT-Sicherheitsvorfällen richtig verhalten, um Schäden zu minimieren und die Geschäftskontinuität des Unternehmens sicherzustellen.

Folgende Themen werden behandelt:

- Identifizierung von Vorfällen
- Koordination der Reaktion
- Bewertung der Risiken
- Eindämmung des Vorfalls
- Kommunikation und Berichterstattung

Inhalte/Agenda:

- **◆ Alarmierungsprozeduren und Fallstricke**
- **◆ Steuerung von Krisen und Notfällen aus CISO-Sicht**
 - ◆ Organisation von Notfallteams, Krisenstäben und Task Forces
 - ◆ Ablauf- und Aufbau-Organisation von Notfallteams und Krisenstäben
 - ◆ Lagebesprechungen und Dokumentation
 - ◆ Lagebilddarstellung
 - ◆ Zusammenarbeit der Beteiligten im Stab
 - ◆ Kommunikation im Stab sowie mit anderen internen und externen Beteiligten, inkl. Kommunikation mit Behörden
 - ◆ Bewertung von Informationen
- **◆**
- **◆ Empfehlungen und Erfahrungen aus Stabsübungen aus CISO-Sicht**
- **◆ Professionelle Krisenstabsübung**
 - ◆ Herausforderung Stabsaufbau, Aufgaben im Stab
 - ◆ Herausforderung Herstellung Lagebild
 - ◆ Kommunikationsfallen, Druck und emotionale Belastung
 - ◆ Reaktionsmuster, Gruppendynamiken und Bewältigungsstrategien