IT-Sicherheitsmanagementsystem & IT-Notfallplan

Kurs zum Aufbau einer sicheren IT-Infrastruktur inkl. Cyber-Risiken

Seminar-ID: **22143**

Veranstaltungsformat: **Seminar**

Das nehmen Sie mit

- Unternehmen, die bereits ein Informationssicherheitsmanagementsystem (ISMS) etabliert - haben, können besser & schneller auf Cyber-Risiken reagieren
- Der Workshop vermittelt Ihnen das nötige Bewusstsein über aktuelle Bedrohungsbilder und wie rasant sich Schadsoftware ausbreiten kann
- Lernen Sie, wie ein IT-Notfallplan beschaffen sein muss, um einen effizienten Disaster-Recovery-Prozess zu ermöglichen
- Anhand praktischer Beispiele erfahren Sie, wie man ein ISMS erfolgreich implementiert
- Anschaulich & praxisnah durch Live-Demonstrationen

METHODEN

- Workshop mit Praxisthemen zur IT Notfallplanung. Im Zuge des Workshops wird ein Protokoll erstellt, welches nachträglich per E-Mail an die Teilnehmer übermittelt wird.

Die COVID-19 Pandemie hat viele Unternehmen plötzlich vor eine gänzlich neue Situation gestellt. Plötzlich mussten altbewährte IT Mechanismen ohne ausreichende Planung angepasst oder erweitert werden, um den Betrieb überhaupt aufrecht erhalten zu können. Viele der Seminarthemen können Unternehmen mit entsprechender Notfallvorsorgeplanung und gutem IT-Management frühzeitig abfedern, sodass dies nicht zu einer zusätzlichen Bedrohung wird. Der Seminarteil zur Notfallplanung geht dabei auf technische und organisatorische Anforderungen ein, die Unternehmen vorbereiten können, um – sollte es tatsächlich zu einer zweiten COVID-19 Welle kommen – diese besser überstehen zu können.

Ihr Programm im Überblick

- Standards und relevante Sicherheitsnormen (mit Fokus auf Notfallplanung und ISMS) & Best-Practice-Ansätze (z. B. ISO27001)
- Aktuelle Cyber-Bedrohungsbilder und warum ein IT-Notfallplan erforderlich ist
- Was ist ein ISMS? (Informationssicherheitsmanagementsystem)
  - IT-Notfallplanung, generelles Risikomanagement etc.
- Welche spezifischen Anforderungen an die Notfallplanung sind bei Cyber-Attacken erforderlich?
- Vorbereitende Aufgaben/Prozesse für die Notfallplanung (z. B. Risk Management, BIA, Aufbau einer Notfallorganisation)

COVID-19 „Special"

- Firewall Systeme waren nicht für die große Anzahl von gleichzeitigen VPN Sessions ausgelegt oder es gab nicht genügend VPN Lizenzen für alle Mitarbeiter
  - Lieferengpässe in der Beschaffung von Notebooks / Zugriff auf Unternehmensdaten von privaten PCs
  - Störung bei IT Infrastrukturkomponenten führte zu Ausfällen der Verfügbarkeit von IT-Systemen
  - Cloud Dienste oder Video Kollaboration Dienste musste rasch – ohne eine entsprechende Risikobetrachtung – eingeführt werden, u. s. w.
- Lessons Learned aus der COVID-19 Krise - welche Maßnahmen im Bereich IT Notfallplanung haben sich bewährt?
- Praxistipps zum Thema sicheres Arbeiten im Home Office - und was ist bez. IT Notfallplanung vorzubereiten, falls doch ein Sicherheitsvorfall eintritt?
- Welche IT Notfallplanungs- und Business Continuity Maßnahmen sind bei Ransomware Angriffen zu beachten, wie kann man als Unternehmen Ransomware Angriffe wirklich überstehen?

Interessant für

- CIO, CISO | Information-Security-Beauftragte

- IT-Leiter | Datenschutzbeauftragte
- Geschäftsführer, CEO
- IT-Anwender von Banken & Versicherungen
- IT-Projektleiter, IT- und EDV-Berater
- System- & Netzwerkadministratoren, Datenverarbeitung
- Führungskräfte & MA in Rechtsabteilungen, Einkauf / Verkauf

Referent*in

Ing. Thomas Mandl

Cyber Defense Consulting Experts e.U.

Mag. Manfred Spanner MSc.

Head of Department Group Data Protection Office

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
06.03.2023	1 Tag	Wien	Präsenz	€ 580,-
22.05.2023	1 Tag	Wien	Präsenz	€ 580,-
09.10.2023	1 Tag	Wien	Präsenz	€ 580,-