Event

Kommunales Cyber Krisenmanagement „Angriff auf KRITIS Infrastrukturen“

Kategorie	Datum	Zeit	Ort
Weiterbildung	23. Oktober 2019	14:00 - 17:00 Uhr	Meetingraum R13 (Ebene 3)

Der Workshop richtet sich ausschließlich an Vertreter von (kommunalen) Kritischen Infrastrukturen und KRITIS Betreiber aller Branchen. Die Teilnehmerzahl ist auf 24 Personen begrenzt.

Zur Anmeldung

Cyberbedrohungen, Regulierung, gesetzliche Anforderungen, Technologien und neue agile Organisationsformen führen an sich schon zu komplexen Herausforderungen. Digitale Risiken sind in den letzten Jahren stark angestiegen und alles und jeder steht heute im Visier der Täter – Staaten, kritische Infrastrukturen und Unternehmen jeglicher Größe sowie weite Teile der vernetzten Bevölkerung. Je nach Ziel bedienen sich die Täter verschiedener Straftaten wie Cybercrime, Cyberhacktivismus, Cyberspionage oder auch Cybersabotage zur Durchführung des Angriffes. Daher sollte Cybersicherheit eines der wichtigsten strategischen Ziele eines Unternehmens sein und damit ein integraler Bestandteil der Unternehmensstrategie. Ohne einen allumfassenden strategischen Ansatz, der die wesentlichen Leitlinien für den Umgang mit Cyberbedrohungen setzt, steigen die Eintrittswahrscheinlichkeit und das Schadensausmaß eines Cyberangriffs deutlich an.

Nach einer Einführung zu Kritischen Infrastrukturen, dem aktuellen Stand der Gesetzgebung und den jeweiligen branchenbezogenen Auflagen und vor allem der globalen Bedrohungslage, wird auf Basis reeller und auf die Anforderungen von Städten und Gemeinden ausgerichteter Szenarien ein Planspiel (Table Top Übung) durchgeführt und ein Cyberangriff auf strategischer Ebene simuliert. Durch ein, von den Moderatoren entwickeltes, methodisches Vorgehen können Rückschlüsse darauf gezogen werden, welche strategischen, organisatorischen, personellen und technischen Maßnahmen getroffen werden sollten. In Arbeitsgruppen bearbeitet werden die Bereiche:

- Prävention: Was hätte zur Vermeidung eines Angriffs getan werden können?
- Reaktion: Wie kommt man durch die aktive Phase?
- Stabilisierung/Wiederherstellung: Was kann getan werden, um die Wiederholung des letzten Angriffs zu vermeiden?

Anhand einer Fallstudie „Cyberangriff kommunale Infrastrukturen“ wird aufgezeigt, wie ein Cyberangriff durchgeführt und welche Aufgaben auf die jeweiligen Geschäftsbereiche von Städten und Gemeinden zukommen. Dabei geht es nicht um die Technologie eines Angriffs, sondern um das Verständnis warum ein Angriff durchgeführt wird, welche organisatorischen Vorbereitungen zu treffen sind, um die Kontinuität im Unternehmen sicherzustellen und wie Entscheidungen zu Stande kommen.

Die Teilnehmer müssen eine extrem komplexe Cyberkrise bearbeiten und die präventiven, reaktiven und stabilisierenden (Kontinuität) Maßnahmen und Mechanismen beschreiben, die sie benötigen, um die Cyberkrise abzuwenden. Die Analyse des Umfelds, die rechtlichen Grundlagen und die Möglichkeiten der Strafverfolgung werden dabei ebenfalls berücksichtigt.

Security Technologien Innovation

Speaker:

Michael Bartsch, Geschäftsführer, Deutor Cyber Security Solutions GmbH

Dr. Stefanie Frey, Geschäftsführerin, Deutor Cyber Security Solutions GmbH

bitkom Messe Berlin