Deutor Cyber Security War Game – Vom Cyberangriff zur Cyberstrategie

Zielgruppe: Industrie/Unternehmen und Behörden

Die Cyberbedrohungen 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 des 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.

Die Entwicklung einer Cyberstrategie ist der erste Schritt in eine sichere und planbare Unternehmenszukunft. Egal in welcher Branche, ob Start-up, Mittelstand, Konzern oder Behörde – jeder sollte die Rahmenbedingungen setzen, die er benötigt, um den Cyberherausforderungen zu begegnen. Eine Cyberstrategie zu entwickeln ist, wenn die richtige Methode und die richtigen Instrumente angewendet werden, keine Zauberei.

Auf Basis reeller Szenarien wird ein Planspiel (Cyber War Game) durchgeführt und ein Cyberangriff auf ein Unternehmen/eine Behörde simuliert. Durch ein, von den Moderatoren entwickeltes, methodisches Vorgehen können Rückschlüsse darauf gezogen werden, welche strategischen, organisatorischen, personellen und technischen Maßnahmen getroffen werden sollten, damit Cyberangriffe mit so geringen Auswirkungen wie möglich überstanden werden können. Anhand der Ergebnisse des Cyber War Games wird die Struktur einer Cyberstrategie entwickelt.

Anhand einer Fallstudie wird aufgezeigt, wie ein Cyberangriff durchgeführt und welche Aufgaben auf den Vorstand / die Geschäftsleitung zukommen. Dabei geht es nicht um die Technologie eines Angriffs, sondern um das Verständnis warum ein Angriff durchgeführt wird, welche Vorbereitungen zu treffen sind und wie Entscheidungen zu Stande kommen.

Die Teilnehmer müssen eine extrem komplexe Cyberkrise bearbeiten und die die Maßnahmen und Mechanismen beschreiben die sie benötigen um die Cyberkrise abzuwenden. Die Analyse des Umfelds, die rechtlichen Grundlagen und die Möglichkeiten der Strafverfolgung / Nachrichtendienste werden dabei ebenfalls berücksichtigt.

Am Ende des Seminars sind Sie in der Lage einzuschätzen, welche Cyberbedrohungen es gibt und wie Tätermotivationen aussehen. Sie können beurteilen, wie gut Ihre Organisation auf Cyberangriffe vorbereitet ist, und erkennen Lücken und Schwachstellen. Sie verstehen die generischen Methoden und Instrumente, um in Ihrem eigenen Unternehmen eine Cybersicherheitsstrategie entwickeln und umsetzen zu können.

Voraussetzungen für die Teilnahme: Interesse an Cyber und digitalen Straftaten

Dauer: ca. 4 Stunden

Anmeldung: Vorabregistrierung auf der Homepage

Anzahl der Personen: ca. 20