31. Cyber-Sicherheits-Tag der Allianz für Cyber-Sicherheit in Kooperation mit dem Mittelstand 4.0-Kompetenzzentrum Hamburg

19.03.2020 in der Handelskammer Hamburg

Session-Informationen (Stand 04.02.2020)

Genaue Angaben zu den Räumen werden noch bekannt gegeben.

10:00 – 10:30 Uhr

Erkennung IT/OT - Anomalieerkennung bei Produktionsnetzwerken der Unternehmenspraxis

Die Unterscheide in der Risikolage und möglicher CS-Maßnahmen in Bezug auf IT und OT (operational Technology) werden aufgezeigt. Auf die Bedeutung von Monitoring/Detektion/Anomalieerkennung (größtenteils synonym) für die Corporate Security (CS) wird eingegangen. In diesem Kontext werden Grundlegende Arten/Facetten der Anomalieerkennung vorgestellt.

10:40 – 11:30 Uhr

Information Security Management - Nachhaltig Cyber-Sicherheit gestalten anhand von Standards

Wer ganzheitlich und nachhaltig CS gestalten will, kommt langfristig um ein Management-System für Informationssicherheit (ISMS) nicht herum. Der Einsatz von Management-Systemen bedeuten auch, dass mindestens 50% der Ressourcen in nicht- technische Maßnahmen fließen. Der Aufbau und Betrieb eines ISMS ist ressourcenintensiv, allerdings können gerade die Maßnahmen zu dessen Einführung große Potenziale für Effizienzsteigerung entfalten, weil Prozesse analysiert und angepasst werden.

10:40 – 11:30 Uhr

Automatisiertes Schwachstellen-Management für Jedermann?

In dieser Session werden wichtige Fragen beantwortet: Wie kann ich möglichst automatisiert mein Netzwerk auf technische Schwachstellen untersuchen? Was können diese Tools (z.B. Open VAS) leisten, was nicht? Wie ergänzt diese Möglichkeit die eigene Bestrebung für mehr CS?

11:20 – 12:00 Uhr

Routenplaner Teil I – Cyber-Sicherheit für Handwerksbetriebe und KMU durch IT-Grundschutz-Profile

Ein anhand des IT-Grundschutzes des BSI entwickeltes ISMS ist die Basis für ein IT-Grundschutz-Profil für Handwerksbetriebe gewesen. Aufbauend auf diesem Profil wurde der Routenplaner für Handwerksbetreibe entwickelt. Dieser Routenplaner beantwortet die Frage, inwieweit sich der ISMS Ansatz auf KMU und Handwerksbetriebe herunterbrechen lässt. Betriebe, die den Routenplaner probiert haben, berichten von ihren Erfahrungen, ihren Learnings und geben einen Ausblick, was ggf. noch zu tun bleibt.

11:20 – 12:00 Uhr

Cyber-Angriff auf Bestellung: Wie Pentesting die Cyber-Sicherheit erhöhen kann

Was genau ist Pentesting? Wie kann Pentesting erfolgreich gestaltet und genutzt werden? An welcher Stelle im CS-Prozess ist diese mögliche Maßnahme zu setzen und worauf kann man dabei achten? Lassen Sie andere die Schwachstellen in Ihren Systemen finden und erfahren Sie dadurch mehr über mögliche Angriffsszenarien, gegen die Sie Ihr Unternehmen schützen sollten.

13:00 – 13:40 Uhr

Routenplaner Teil II – Interaktiver Erfahrungsaustausch und Lessons Learned für Handwerksbetriebe und KMU

Aufbauend auf Teil I sollen in diesem Teil die Erfahrungen der Betriebe diskutiert werden und mit dem Publikum ein Austausch zu erfahrenen und möglichen Ansätzen stattfinden. Der Austausch wird gemeinsam durch KDH und BSI moderiert.

13:00 – 13:40 Uhr

Threat Intelligence – Was ist das und wo werden diese Informationen in einem Sicherheits-Konzept eingeordnet?

Threat Intelligence bezeichnet die Informationen bzw. das Wissen über aktuelle Bedrohungslagen im Bereich von Cybersicherheit. Wie Unternehmen in diesem Bereich sinnvoll arbeiten sollten und welche möglichen Produkte (IoC) und Integration in Monitoring-Maßnahmen dabei helfen können werden vorgestellt. Dabei wird u.a. auf APT-Angriffe (Advanced Persistence Threat) eingegangen, sowie darauf, wie diese einzuordnen sind und für wen diese Informationen Relevanz haben?

13:40 – 14:10 Uhr

Cyber-Sicherheit für Industrie 4.0

Wie kann langfristig die Cyber-Sicherheit im Hinblick auf Industrie 4.0 und IoT gewährleistet werden? In diesem Beitrag werden durch das BSI Forschungsansätze und aktuelle Entwicklungen dargestellt, die zukünftig by-default Cyber-Sicherheit ermöglichen sollen.

14:10 – 14:50 Uhr

Anti-Virus-Software – Überholt oder weiterhin essentiell?

In dieser Session soll auch der Wert von Anti-Virus-Programmen diskutiert und dabei folgende Fragen beantwortet: Welche Rolle spielen Cybersicherheitsprodukte, insbesondere Virenscanner heute? Wie gelingt der Schutz vor Malware richtig? Ersetzen CS-Produkte die anderen Cyber-Sicherheits-Maßnahmen? Kann man nicht Firewall und Virenscanner statt ISMS „machen“?

15:15 – 15:45 Uhr

IT-Sicherheit mit knappen Ressourcen – wie anfangen?

Trotz der Herausforderungen – insbesondere für KMU - (Ressourcenmangel: kein Geld, keine Zeit, kein Know-How, in unterschiedlichen Konstellationen) wird es immer wichtiger, die möglichen „richtigen“ Schritte für mehr Cyber-Sicherheit zu gehen. Ziel ist es, kein Opfer von gezielten – und schon gar nicht von ungezielten - Cyberbedrohungen zu werden. Die verschiedenen Aspekte des Tages werden zu einem entsprechenden Gesamtbild zusammengefasst.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages