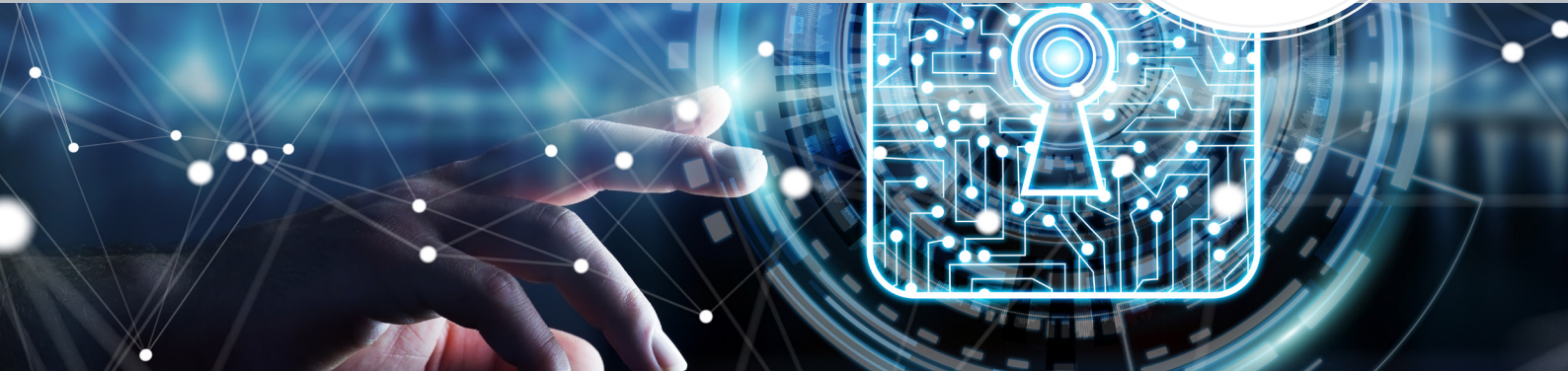




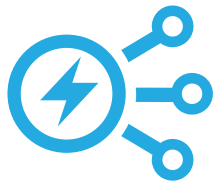
Fraunhofer

IOSB

Institutsteil Angewandte Systemtechnik AST



**LERNLABOR
CYBERSICHERHEIT
ENERGIE- UND
WASSERVERSORGUNG**



GESPRÄCHSPARTNER

Dipl.-Ing. Steffen Nicolai
Fraunhofer IOSB-AST
+49 3677 461-112
steffen.nicolai@iosb-ast.fraunhofer.de

M.Sc. Dennis Rösch
Fraunhofer IOSB-AST
+49 3677 461-188
dennis.roesch@iosb-ast.fraunhofer.de

Prof. Dr.-Ing. Jörg Lässig
Fraunhofer IOSB-AST
+49 3581 792-5354
joerg.laessig@iosb-ast.fraunhofer.de

SENSIBEL FÜR BEDROHUNGEN!

Gefahren frühzeitig erkennen und richtig reagieren

Durch die zunehmende Digitalisierung erhöht sich die Anfälligkeit von Versorgungsinfrastrukturen gegenüber **Cyberattacken**, während den Angreifern immer leistungsfähigere Werkzeuge und Methoden zur Verfügung stehen. Im besonderen Maße steigt die Abhängigkeit von automatisierten Prozessen und IT-Systemen immer weiter an, wodurch eine erhöhte **Bedrohungslage** resultiert. Um sich gegen die allgegenwärtigen Gefahren adäquat zu schützen ist ein Bewusstsein und die **Sensibilisierung** für Bedrohungen

sehr wichtig. Der Faktor Mensch spielt eine erhebliche Rolle in der IT-Sicherheit und der Vermeidung von Sicherheitsvorfällen. Vor allem die Frage nach Hilfsmitteln zur Umsetzung von IT-Sicherheit stellt viele Unternehmen vor Herausforderungen. Wir geben Ihnen einen Überblick über aktuelle Standards bzw. Regularien und erarbeiten mit Ihnen eine Einschätzung zur Umsetzung in Ihrem Unternehmen. Der **Awareness-Workshop** fördert nachhaltig ein vorausschauendes und sicherheitsrelevantes Verhalten in Ihrem Unternehmen.

AUF EINEN BLICK:

- Für Führungskräfte und Mitarbeiter
- Individuell gestaltbar
- Inhouse bei Ihnen oder im Lernlabor Ilmenau / Görlitz
- Dauer: ab 0,5 Tage
- Relevante Gefahren in der Energieversorgung
- Live-Hacking von Automatisierungstechnik
- Sichere Authentifizierung
- Unternehmenskultur der IT-Sicherheit



Lernziele

- Typische Angriffsabläufe verstehen
- Verschiedene Angriffsbeispiele und -szenarien kennen
- Rechtliche Rahmenbedingungen kennen und deren Auswirkungen verstehen
- Standards und Normen voneinander abgrenzen und einschätzen können
- Eigenes Handeln sicherer gestalten können
- Mitarbeiter für Themen der Cybersicherheit sensibilisieren können

Sie erwartet im Workshop

Während des Workshops werden verschiedene Cybersicherheit-Themen diskutiert und anhand vieler praxisnaher Beispiele und Vorführungen verinnerlicht. Dafür werden die einzelnen Phasen von Angriffen und die ausgenutzten technischen und organisatorischen Schwachstellen untersucht und aufgezeigt. Möglichkeiten der Verhinderung von solchen Angriffen stehen besonders im Vordergrund. Die Unterstützung von Richtlinien und Standards wird Ihnen Nahe gebracht und wir befähigen Sie, die geeigneten IT-Sicherheitsmaßnahmen entsprechend einzuleiten und umzusetzen.

Bei uns bekommen Sie Antworten auf die folgenden Fragen

- Welche Angriffe auf Kritische Infrastrukturen gab es bereits, und wie liefen diese ab?
- Welche Auswirkungen hatten diese Angriffe?
- Wie hätten die Angriffe verhindert werden können?
- Welche Standards und Normen existieren bereits, wie können sie umgesetzt werden?
- Welche Gesetze gelten für Kritische Infrastrukturen und die Energieversorgung?
- Welcher Aufwand muss, welcher sollte betrieben werden?
- Wie kann ich mich selbst vor Cyberangriffen schützen?
- Wie sensibilisiere ich meine Mitarbeiter nachhaltig?

Das sagen unsere Kunden über uns

„Das Seminar hat mich durch die sehr kompetenten Vorträge und erfrischenden Diskussionen überzeugt. Für meine strategische Arbeit konnte ich aus dem Tag viel mitnehmen und kann deshalb das Seminar sehr weiterempfehlen.“

Susanne Kufeld, Leiterin DB-Lagezentrum und globales Krisenmanagement, zivile Verteidigung

LERNLABOR CYBERSICHERHEIT...

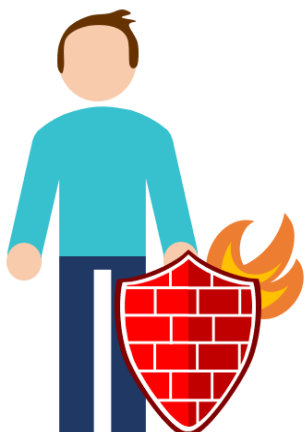
... ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen.

Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT- und OT-Infrastruktur.

www.iosb-ast.fraunhofer.de
www.cybersicherheit.fraunhofer.de/energie



Hochschule
Zittau/Görlitz
UNIVERSITY OF APPLIED SCIENCES



loading human firewall... 