INSTITUTSTEIL ANGEWANDTE SYSTEMTECHNIK AST

# PRESSEMITTEILUNG



## Cyber-Resilienz in der Energiewirtschaft durch innovative Schulungsformate stärken

Flexible Weiterbildungsangebote des Lernlabor Cybersicherheit für die Energie- und Wasserversorgung erhöhen die Cyberfitness von Fachkräften und Entscheidungsträgern in der Branche.

**Ilmenau, 10. Februar 2025: Auch wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem aktuellen Lagebericht den Betreibern kritischer Infrastrukturen einen positiven Trend bei der Nutzung von Informationssicherheits-Managementsystemen bescheinigt, bleibt die IT-Sicherheitslage in Deutschland im Berichtszeitraum angespannt. Umso wichtiger ist das breite Spektrum der Cybersicherheit für die gesamte Energiebranche: Das Fraunhofer IOSB-AST unterstützt Unternehmen mit passenden Trainingsangeboten.**

*Mobile Schulungsdemonstratoren im Lernlabor Cybersicherheit für die Energie- und Wasserversorgung. Foto: Martin Käßler, Fraunhofer IOSB-AST*

Public

**Head of Corporate Communication & Marketing** - **Fraunhofer IOSB-AST**
**Martin Käßler** | Telefon +49 3677 461-128 | martin.kaessler@iosb-ast.fraunhofer.de | Institutsteil Angewandte Systemtechnik AST | Am Vogelherd 90 | 98693 Ilmenau | www.iosb-ast.fraunhofer.de | https://www.linkedin.com/company/fraunhofer-iosb-ast/

Das Schulungsangebot des Lernlabor Cybersicherheit für die Energie- und Wasserversorgung deckt dabei ein weites Feld der aktuellen Cybersicherheits-Themen ab:

Im Rahmen von *Cyber-Awareness-Trainings* werden beispielsweise typische Angriffsszenarien erläutert, rechtliche Rahmenbedingungen sowie Standards und Normen skizziert und die Sensibilisierung der Mitarbeiter thematisiert.

In eine andere Richtung zielen die *Schulungen zur Cyber-Resilienz*: Angesichts der Tatsache, dass Cyberangriffe kaum vollständig zu verhindern sind, liegt hier der Schwerpunkt darauf, schnell und effektiv auf Cyberangriffe zu reagieren – bei Aufrechterhaltung des laufenden Geschäftsbetriebs. Dabei werden alle fünf Phasen des so genannten Cyber-Resilienz-Zyklus vorgestellt sowie für jede Stufe passende Maßnahmen und Werkzeuge präsentiert. Das Training wird mit aktuellen Forschungserkenntnissen und realen Praxisbeispielen verknüpft.

Zwei weitere Schulungen adressieren das Spektrum der so genannten OT-Sicherheit: Im Gegensatz zur IT, die sich hauptsächlich mit dem Einsatz von Software und Internet befasst, liegt hier der Fokus etwa auf physischen Überwachungs- und Steuerungssystemen im industriellen Kontext.

Das Format *Hack the Grid - Mission OT-Sicherheit* ist dabei für fortgeschrittene Teilnehmende gedacht, die im spielebasierten Trainingsansatz „Capture the flag" die unterschiedlichen Perspektiven von Angreifenden und Verteidigenden einnehmen können, um Schwachstellen einer fiktiven Anlage zu ermitteln, Bedrohungen präventiv zu erkennen und geeignete Abwehrstrategien zu entwickeln.

Im *Präventionstraining OT-Sicherheit in Energie- und Wasserversorgung* wird die Vorgehensweise von Angreifern auf die Energieautomatisierung erläutert und die Gefahrenpotentiale durch unsichere Konfigurationen skizziert. Die sichere Konfiguration und Vernetzung von Automatisierungskomponenten sowie geeignete Absicherungsstrategien runden das Training ab.

Präsentiert wird das Leistungsspektrum des Lernlabor Cybersicherheit für die Energie- und Wasserversorgung u.a. vom 11. – 13. Februar 2025 auf der E-world energy & water 2025 – Europas größter Energiefachmesse – am Stand von Eviden Germany GmbH in Halle 3 / E131. Weiterführende Fragen zum Thema beantwortet Ihnen gerne Martin Käßler, martin.kaessler@iosb-ast.fraunhofer.de oder telefonisch unter 03677 461 128.