Fraunhofer IOSB
Institutsteil Angewandte Systemtechnik AST

Cybersecurity Assessment

Den eigenen Sicherheitsstandard bewerten und verbessern

Das Lernlabor Cybersicherheit für die Energie- und Wasserversorgung trägt wesentlich zur Gewährleistung der Cybersicherheit in der deutschen Energie- und Wasserversorgung bei. Durch die enge Verzahnung mit der Vorlaufforschung sowie die Nutzung modernster Laborinfrastruktur bietet es Qualität und Expertise. Auf dieser Grundlage entwickelt das Lernlabor praxisnahe Weiterbildungen, um die gesamte Bandbreite der Cybersicherheit in IT- und OT-Systemen der Energie- und Wasserversorgung abzudecken.

Vorausschauende Cybersicherheit: Identifikation und Abwehr von Bedrohungen in der Energieinfrastruktur

Angriffe auf Energieversorger und deren Infrastrukturen, sogenannte Cyberangriffe, haben sich zu einer permanenten und gefährlichen Bedrohung entwickelt. Sowohl ihr Schadenspotential als auch ihr Auftreten nehmen immer weiter zu. Es ist nicht die Frage ob, sondern wann die nächste Angriffswelle auch Sie trifft.

Daher ist es unerlässlich, eine umfassende Sicherheitsbewertung für Ihre IT-Systeme, Netzwerke und ICS-Anlagen durchzuführen, um Schwachstellen zu identifizieren und sich bestmöglich vor potentiellen Gefahren zu schützen.

Seien Sie den Angreifern immer einen Schritt voraus und erkennen Sie potentielle Risiken, bevor sie sich negativ auf Ihre Unternehmenssicherheit auswirken können. Bestimmen und bewerten Sie mit Hilfe unserer Experten Ihre aktuelle Bedrohungslage, basierend auf dem Stand der Technik sowie aktuellen Forschungsergebnissen. Ermitteln Sie anhand von ausführlichen Berichten den notwendigen Handlungsbedarf, um die Verfügbarkeit und Zuverlässigkeit Ihrer Betriebsabläufe auch weiterhin zu gewährleisten.

Lernlabor Cybersicherheit für die Energie- und Wasserversorgung

Wie gut ist Ihr Unternehmen aufgestellt?

- Welche Cyber-Security-Schwachstellen lauern in Ihrem Unternehmen?
- Wie sicher sind Ihre IT-Infrastruktur und ICS-Anlagen?
- Sind Ihre Mitarbeitenden ausreichend sensibilisiert?
- Wie gut würde Ihr Unternehmen einem Cyberangriff widerstehen?
- Verfügt Ihr Unternehmen über wirksame Systeme zur Angriffserkennung?

Konzeptbewertung

Für die Beachtung von Sicherheitsaspekten in IT-Netzwerken, ICS-Anlagen sowie der Absicherung der Kommunikationswege existieren zahlreiche, mitunter komplexe Richtlinien und Normen. Diese im Rahmen der Planung und Konzeption im Überblick zu behalten, kann eine Herausforderung darstellen. Wir prüfen und bewerten Ihre Konzepte hinsichtlich der Einhaltung der gewünschten Standards und geben Empfehlungen für mögliche Anpassungen.

Bewertung der Netzwerksicherheit

Die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit sind sowohl die obersten Schutzziele der Netzwerksicherheit als auch die primären Angriffsziele von Schadprogrammen und Cyberkriminellen. Ob Ihr Netzwerk den neuen Bedrohungen und steigenden Gefahrenquellen noch gewachsen ist, erfahren Sie anhand unserer Sicherheitsanalyse. Basierend auf bekannten Schwachstellen sowie potentiellen Angriffsvektoren erhalten Sie darin eine Bewertung Ihrer aktuellen Netzwerksicherheit.

Penetrationstests

Bei einem Penetrationstest werden Ihre IT-Systeme und IT-Netzwerke ausführlich geprüft, um festzustellen, wie empfindlich diese auf Cyberangriffe reagieren. Dabei kommen Schwachstellenscans sowie Methoden und Techniken zum Einsatz, die auch von Angreifern genutzt werden. Als Ergebnis erhalten Sie einen ausführlichen Bericht mit den erkannten Schwachstellen und möglichen Lösungsansätzen als Grundlage für weitere eigene Schritte.

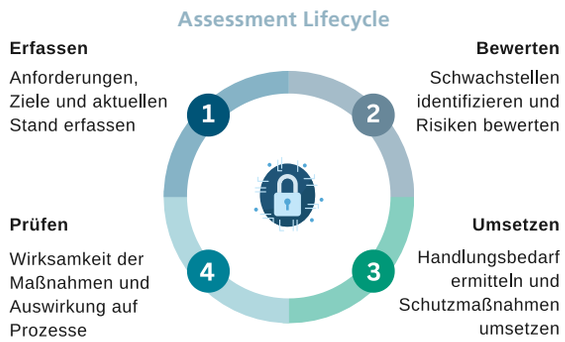
Hardware- und Konfigurationstests

Aktuelle IT und ICS Systeme sind nicht nur bei der Einrichtung, sondern auch im Betrieb immer komplexer zu handhaben. Wir prüfen Ihre Hardware- sowie Ihre Systemkonfiguration umfassend und intensiv auf mögliche Schwachstellen und potentiell gefährliche Fehlkonfigurationen. Dabei werden die Verteidigungsmechanismen gegen Cyberangriffe anhand unterschiedlicher Sicherheitsaspekte bewertet und konkrete Handlungsempfehlung für das weitere Vorgehen abgeleitet.

Unsere Prüfungen sind darauf ausgerichtet, nicht nur vorhandene Schwachstellen zu erkennen, sondern auch präventive Maßnahmen zu entwickeln, um zukünftige Bedrohungen abzuwehren. Wir unterstützen Sie bei der Implementierung dieser Schutzmaßnahmen und sorgen dafür, dass Ihre Systeme den neuesten Sicherheitsstandards entsprechen.

Security Awareness - Faktor “Mensch”

Durch die zunehmende Digitalisierung und steigende komplexität der Arbeitswelt stehen Mitarbeitende vor großen Herausforderungen und müssen über umfangreiche Kompetenzen im Umgang mit den IT-Lösungen verfügen. Mit unserer Unterstützung sind Sie in der Lage, die notwendigen Voraussetzungen für Security Awareness in Ihrem Unternehmen zu schaffen, aufrecht zu erhalten und zu messen.



Lernlabor Cybersicherheit für die Energie- und Wasserversorgung

Standort Ilmenau

Dipl.-Ing. Steffen Nicolai
Tel. +49 3677 461-188
Mobil +49 170 2981 852
steffen.nicolai@iosb-ast.fraunhofer.de

Fraunhofer IOSB, Institutsteil
Angewandte Systemtechnik (AST)
Am Vogelherd 90
98693 Ilmenau

Standort Görlitz

Prof. Dr.-Ing. Jörg Lässig
Tel. +49 3581 7925354
Mobil +49 173 7366285
joerg.laessig@iosb-ast.fraunhofer.de

Fraunhofer IOSB, Institutsteil
Angewandte Systemtechnik (AST)
Wilhelmsplatz 11
02826 Görlitz