Cybersicherheit

Den Ernstfall trainieren

[18.05.2026] Ein Übungskonzept soll die Sicherheit Kritischer Infrastrukturen erhöhen. Das Konzept für KRITIS-Betreiber wurde Fraunhofer IOSB-AST mit dem Future Energy Lab der Deutschen Energie-Agentur entwickelt.

Das Fraunhofer IOSB-AST hat ein neues Übungskonzept für Betreiber Kritischer Infrastrukturen entwickelt. Nach Angaben des Instituts sollen damit Reaktionsabläufe bei Cyber-Angriffen auf industrielle Steuerungssysteme praxisnah trainiert werden. Das Konzept entstand im Projekt EnerCise III im Auftrag des Future Energy Labs der Deutschen Energie-Agentur (dena). Cyber-Angriffe auf industrielle Steuerungssysteme in der Energie- und Wasserversorgung werden immer komplexer und zielgerichteter, teilt das Fraunhofer IOSB-AST mit. Gleichzeitig nähmen die Abhängigkeiten zwischen Informationstechnik (IT) und Betriebstechnik (OT) zu. Sicherheitsvorfälle an den Schnittstellen beider Bereiche träten deshalb häufiger auf.

Übung als ganztägige Simulation

Das entwickelte Trainingsformat soll technische und organisatorische Abläufe gemeinsam abbilden. Bisherige Schulungen hätten oft nur einzelne Aspekte der Vorfallbewältigung behandelt, heißt es. Das neue Konzept simuliere dagegen das Zusammenspiel von Leitwarte, OT-Betrieb, IT-Administration, Informationssicherheitsmanagement und Geschäftsführung. Die Übung ist als ganztägige Simulation angelegt. Sie orientiert sich an den fünf Phasen des Incident-Response-Prozesses nach der Norm ISO/IEC 27035: Vorbereitung, Erkennung und Meldung, Bewertung und Entscheidung, Reaktion sowie Auswertung. Im Mittelpunkt stehen laut Fraunhofer Entscheidungsprozesse, Kommunikation und Zusammenarbeit unter Bedingungen unvollständiger Informationen.

Angriff auf die Lieferkette

Das Szenario simuliert einen Angriff auf die Lieferkette eines Geräteherstellers. Dabei manipulieren Angreifer nach Angaben des Instituts den Firmware-Update-Prozess. Nach der Installation der kompromittierten Software auf Steuerungskomponenten komme es zeitversetzt zu Störungen und Schutzabschaltungen. Die Anzeichen seien bewusst so gestaltet, dass sie zunächst wie gewöhnliche Betriebsprobleme wirkten. Technische Grundlage der Übungen sind mobile Schulungsplattformen sowie Leit- und Angriffserkennungssysteme aus dem Lernlabor Cybersicherheit Energie- und Wasserversorgung am Fraunhofer IOSB-AST.

Das Konzept verbindet drei Trainingsansätze: technische Übungen an Trainingsplattformen, sogenannte Tabletop-Übungen zur Lagebewertung sowie einen Capture-the-Flag-Ansatz als Feedback- und Motivationselement. Bis zu acht Rollen können dabei besetzt werden, darunter Leitstellenpersonal, OT-Sicherheitsanalystinnen und -analysten, Einsatzkoordinatoren und Krisenstäbe. Die Übungen seien für elf bis 25 Teilnehmende ausgelegt und orientierten sich an gesetzlichen Vorgaben des IT-Sicherheitsgesetzes sowie an Standards des Bundesamts für Sicherheit in der Informationstechnik.

Übungen für Energieversorger geplant

„Die Besonderheit der EnerCise-Übungen liegt darin, dass Personen aus verschiedenen Organisationen und Positionen zusammenkommen und gemeinsam für den Ernstfall trainieren. Dadurch entstehen branchenweite Austausche und neue Netzwerke, die auch nach den Übungen bestehen bleiben“, erklärt Marius Dechand von der Deutschen Energie-Agentur. Thomas Bauer vom Fraunhofer IOSB-AST sagt: „Hybride Bedrohungen erfordern hybride Übungsformate. Wer Incident Response nur am Schreibtisch plant, wird im Ernstfall an den Schnittstellen zwischen Technik und Organisation scheitern.“ Im weiteren Verlauf des Projekts sollen die Übungen mit Betreibern aus der Energie- und Wasserversorgung durchgeführt werden. Die Ergebnisse würden wissenschaftlich ausgewertet, teilt das Fraunhofer IOSB-AST mit.

(al)

Kostenfreie Anmeldungen für die EnerCise III – Cybersicherheitsübung am 23. Juni 2026 in Berlin sind noch möglich

Stichwörter: Informationstechnik, Cyber-Sicherheit, Deutsche Energieagentur (dena), Fraunhofer IOSB-AST, Future Energy Lab