Fraunhofer FOKUS

Cyber-Notfälle im Labor durchspielen

[18.11.2026] Das Fraunhofer-Institut FOKUS lässt Verantwortliche aus Verwaltungen und Unternehmen einen Cyber-Notfall aus verschiedenen Perspektiven erleben. Das neue Szenario im SIRIOS Lab soll helfen, Entscheidungen, Kommunikation und Abläufe für den Ernstfall zu erproben.

Im März hat das Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS mit dem SIRIOS Lab ein immersives Forschungslabor und einen Demonstrationsraum für vernetzte Sicherheit und Krisenbewältigung eröffnet. Dort lassen sich komplexe Krisen- und Sicherheitslagen mithilfe digitaler Zwillinge und immersiver Medientechnik realitätsnah simulieren, visualisieren und erproben. Nun wurde das Labor um ein Szenario zu Cyber-Angriffen erweitert.

Wie das Institut mitteilt, können Teilnehmende in dem immersiven Sicherheitslabor am Beispiel eines fiktiven Unternehmens nachvollziehen, wie sich ein IT-Sicherheitsnotfall entwickelt und welche Entscheidungen dann anstehen. Unternehmen und Verwaltungen sollen so technische und organisatorische Schwachstellen erkennen und sich gezielter auf den Ernstfall vorbereiten können. Die Teilnehmenden verfolgen den Verlauf eines Cyber-Angriffs sowohl aus der Perspektive der Angreifer als auch aus Sicht der betroffenen Mitarbeitenden. Dabei geht es um Spear-Phishing, Social Engineering und die schrittweise Kompromittierung von IT-Systemen. Das Szenario veranschaulicht Ransomware-Angriffe, Datendiebstahl und kompromittierte Benutzerkonten ebenso wie die Folgen für Arbeitsabläufe und Kommunikation. Im Mittelpunkt steht auch die Frage, wie sich die Handlungsfähigkeit nach einem Vorfall wiederherstellen lässt.

Das Angebot richtet sich insbesondere an Verantwortliche für IT- und Informationssicherheit, Business Continuity und Krisenmanagement sowie an Führungskräfte aus Wirtschaft und öffentlicher Verwaltung. In Workshops, Schulungen und Planspielen können sie nach Angaben des Instituts Maßnahmen zur Cyber-Resilienz praktisch erproben. Sebastian Breu, wissenschaftlicher Gruppenleiter bei Fraunhofer FOKUS, berichtet von einem Workshop, in dem alle Teilnehmenden die geltenden Regeln und Bestimmungen kannten. „Schnell wurde deutlich: Kommunikation und Organisation sind entscheidend. Genau deshalb müssen wir Vorfälle nicht nur theoretisch durchdenken, sondern wir müssen sie gemeinsam durchspielen und üben“, sagt Breu.

(sib)

Stichwörter: IT-Sicherheit, Fraunhofer FOKUS