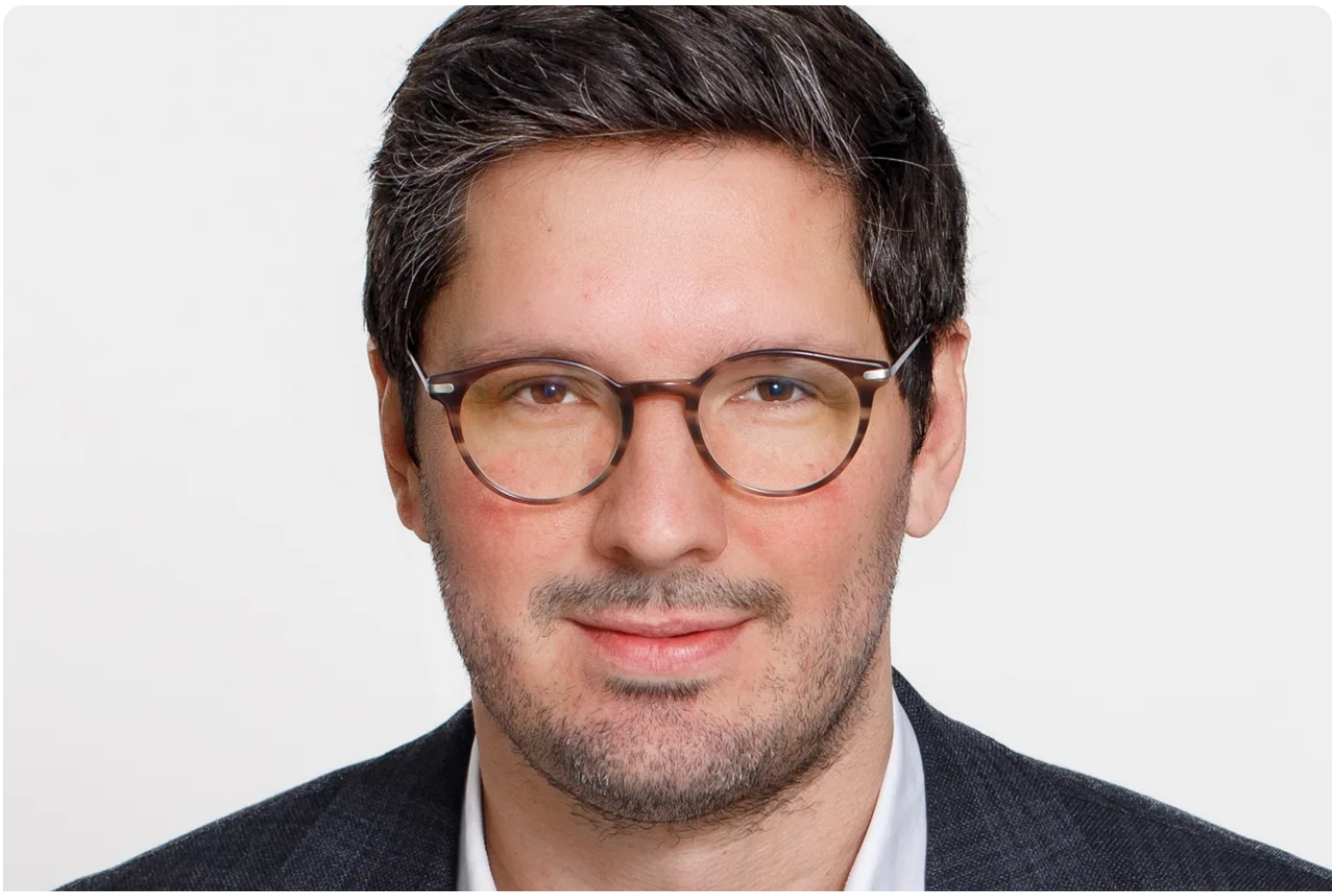
Vorausblick 2026

Zwischen Dezentralität und Angriffslage: Sicherheit entscheidet

BET-Consulting-Partner Sören Patzack warnt: Mit wachsender Dezentralität wird Cybersicherheit 2026 zentrale Voraussetzung für sicheren Netzbetrieb. Hinzu kommen sicherheitspolitische Risiken.

Artikel von Stephanie Gust

19.01.2026, 12:18 Uhr



"IT-Sicherheit beginnt mit Führung, Klarheit und Awareness – nicht mit Technik", sagt Sören Patzack von BET Consulting. Bild: © BET Consulting

2026 wird Cybersicherheit im Energiesystem endgültig zur Betriebsfrage. Die Netze werden dezentraler, digitaler und stärker vernetzt. Damit wächst die Angriffsfläche. Sören Patzack, Partner Digitalisierung bei BET Consulting, analysiert für die ZFK, wo die größten Risiken liegen und was jetzt nötig ist.

Dezentral heißt sicher – aber nicht automatisch

Patzack widerspricht der These, Dezentralität sei per se riskanter. Ein erneuerbares, dezentrales Energiesystem sei "klimafreundlicher, effizienter und widerstandsfähiger" als ein zentrales, fossiles System. Lokale Erzeugung senke Importabhängigkeiten, stärke regionale Wertschöpfung und erhöhe Versorgungssicherheit. Gleichzeitig entstünden neue Risiken. Immer mehr Komponenten seien vernetzt. Damit wachse die Angriffsfläche. Steuernde Systeme bis in die unteren Spannungsebenen würden zum Standard. Sie würden damit auch zu potenziellen Zielen für Cyberangriffe mit direkten Folgen für den Netzbetrieb.

Sein Fazit ist klar. Eine sichere IT- und OT-Architektur werde "zur unverzichtbaren Grundvoraussetzung für den sicheren Netzbetrieb". Richtig ausgestaltet könne Dezentralität die Resilienz sogar erhöhen. Störungen ließen sich dann lokal begrenzen.

Strategische Abhängigkeiten rücken ins Zentrum

Patzack warnt vor neuen sicherheitspolitischen Risiken. Wenn zentrale Komponenten überwiegend aus dem Ausland stammen, entstünden nicht nur Lieferkettenprobleme. Es entstünden auch Machtfragen. PV-Wechselrichter, Wallboxen und Speicher seien steuerbare Komponenten mit systemischer Relevanz. "Ihre Kontrolle ist eine sicherheitspolitische Frage", sagt Patzack. In einem vernetzten System müsse klar geregelt sein, wer diese Kontrolle ausübe – und wer nicht.

Politisch bewege sich etwas. Mit NIS 2, dem geplanten KRITIS-Dachgesetz und neuen IT-Sicherheitskatalogen rücke das Thema nach oben. "Das ist längst überfällig", so Patzack.

Vernetzung verlangt Ende-zu-Ende-Sicherheit

Das intelligente Messsystem sei eine sichere Haustür. Doch ein offenes Fenster könne das ganze Haus gefährden. IT-Sicherheit müsse im gesamten Steuerprozess gedacht werden. Es gehe nicht nur um den Kanal zum Messstellenbetreiber. Es gehe auch um Verbindungen zu Herstellern, Dienstleistern und Plattformen. Alle Kommunikationswege müssten verschlüsselt sein. Für alle Datenflüsse brauche es belastbare Sicherheitsmechanismen. Kurz gesagt: Sicherheit müsse über alle Systeme, Komponenten und Akteure hinweg funktionieren.

NIS 2 hebt das Sicherheitsniveau

NIS 2 ist inzwischen in deutsches Recht überführt. Patzack nennt das einen "unheimlich wichtigen Schritt". Für besonders wichtige Unternehmen und wichtige Unternehmen gelten nun verbindliche Sicherheitsanforderungen. Unternehmen müssen Notfallpläne vorhalten. Geschäftsleitungen müssen sich regelmäßig fortbilden. Die Umsetzung sei anspruchsvoll. Sie schaffe aber ein höheres Sicherheitsniveau in ganz Europa. Wer Cybersicherheit schon ernst genommen habe, habe jetzt einen Vorteil. Das treffe auf viele Energieversorger zu.

Cloud braucht klare Regeln

Cloud-Lösungen werden 2026 weiter an Bedeutung gewinnen. Für Patzack ist entscheidend, dass sie sicher gestaltet sind. Es brauche klare Verantwortlichkeiten, transparente Datenhoheit und überprüfbare Sicherheitsarchitekturen. Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten müssten jederzeit gewährleistet sein. Gleichzeitig nehme die Zahl der Cyberangriffe auf kritische Infrastrukturen weiter zu. Die Branche bleibe ein attraktives Ziel.

Mit NIS 2 kämen zusätzliche Anforderungen hinzu. Sie beträfen auch die Cloud-Nutzung.

IT-Sicherheit beginnt mit Führung

Gerade kleine und mittlere Stadtwerke stehen unter Druck. Patzack sagt klar: "IT-Sicherheit beginnt mit Führung, Klarheit und Awareness – nicht mit Technik." Entscheidend sei ein gemeinsames Problembewusstsein in der gesamten Belegschaft. Jede und jeder trage Mitverantwortung. Gleichzeitig müsse das Thema auf Managementebene verankert sein.

Sicherheit koste Geld. Unterlassene Sicherheit könne aber teurer werden. Kleinere Unternehmen sollten risikobasiert vorgehen. Ein schlankes ISMS, klare Verantwortlichkeiten, regelmäßige Risikoanalysen und eingeübte Notfallprozesse seien zentral. Wo interne Ressourcen fehlten, seien Kooperationen mit externen Dienstleistern sinnvoll. Patzacks Botschaft ist eindeutig. Die Energiewende wird digital. "Aber sie wird nur erfolgreich sein, wenn sie auch sicher ist."

MEHR ZU DIGITALISIERUNG

Softwarelösung

Energievertrieb ohne Mittelsmänner

Kraftwerk Software zeigt auf der E-World 2026 eine direkte Vertriebsplattform, die Energieversorger und Vertriebspartner ohne Mittelsmänner verbindet.

Autor Stephanie Gust