Kraftwerke zählen zur kritischen Infrastruktur und unterliegen besonderen Anforderungen an die Cyber-Sicherheit

Schutz durch Cyber-Sicherheit

Ob Stromversorgung, Wassernetze oder internationale Großveranstaltungen – digitale Angriffe können weitreichende Folgen haben. Auditorinnen und Auditoren des Innenministeriums tragen dazu bei, kritische Einrichtungen vor Cyber-Bedrohungen zu schützen und die Resilienz Österreichs im digitalen Raum zu stärken.

Während körperliche Übergriffe oder Verkehrsunfälle für viele Menschen greifbare Gefahren des Alltags darstellen, bleiben Cyber-Angriffe oft im Hintergrund. Treffen sie Elektrizitätswerke, Wasserversorger oder andere kritische Einrichtungen, können die Auswirkungen Millionen Menschen betreffen. Auch bei Großveranstaltungen wie dem Eurovision Song-Contest ist die Expertise der Cyber-Sicherheitsspezialistinnen und -spezialisten des Innenministeriums ein wichtiger Bestandteil der Sicherheitsplanung.

Die Abteilung IV/S/2 für Netz- und Informationssystemsicherheit gewährleistet ein hohes Cyber-Sicherheitsniveau bei Betreibern kritischer Infrastruktur. Schutzmaßnahmen werden bewertet und bei Bedarf verbessert. Eine zentrale Rolle spielen hierbei die Auditorinnen und Auditoren des Referats „Aufsicht und Durchsetzung“. Einer von ihnen ist Christian Gaisbauer. Durch Studien der Ingenieurwissenschaften, Business-Administration und IT-Security sowie Forschungsaufenthalte in Australien und den USA verfügt er über ein breites fachliches Fundament. Seine Laufbahn führte ihn zunächst in die Satellitennavigation, Satellitenkommunikation und Sicherheitsakkreditierung. Darüber hinaus beschäftigte er sich mit Fragen der europäischen Raumfahrtpolitik und war sowohl in der österreichischen Bundesverwaltung als auch für Institutionen der Europäischen Union in Wien, Brüssel und Prag tätig. Seit 2022 arbeitet Gaisbauer als Auditor im Innenministerium und wirkt am Vollzug des Netz- und Informationssicherheitsgesetzes (NISG) mit.

Sicherheitsniveau bewerten und verbessern. Rund 100 Betreiber kritischer Infrastruktur sind nach dem NISG verpflichtet, ihre Cyber-Sicherheitsmaßnahmen regelmäßig überprüfen zu lassen. Die Prüfungen werden von externen, von der NIS-Behörde zugelassenen Stellen durchgeführt. Die Berichte werden an die Behörde übermittelt und dort bewertet. Auf Grundlage dieser Berichte beurteilt Christian Gaisbauer, ob die bestehenden und geplanten Sicherheitsmaßnahmen den Risiken angemessen sind. „Dabei erhalten wir einerseits einen tiefen Einblick in die Sicherheitsarchitektur einzelner Unternehmen, andererseits einen sektorübergreifenden Überblick über die kritische Infrastruktur in Österreich“, erklärt Gaisbauer. Geprüft werden organisatorische, technische und physische Schutzmaßnahmen. Dazu zählen elektronische Zutrittskontrollen, Firewall- und Netzwerkeinstellungen, Sicherheitsrichtlinien für Mitarbeiterinnen und Mitarbeiter sowie Notfall- und Krisenpläne für Cyber-Vorfälle.

Christian Gaisbauer, Auditor im BMI

Empfehlungen als zentrales Instrument. Werden Schwachstellen erkannt, sprechen die Auditorinnen und Auditoren Empfehlungen aus und legen Verbesserungsmaßnahmen fest. Je nach Risikobewertung müssen diese innerhalb bestimmter Fristen umgesetzt werden. Reichen die vorliegenden Informationen nicht aus oder bestehen Zweifel an der Umsetzung, führen die Auditoren Vor-Ort-Überprüfungen durch. Dabei werden Sicherheitskonzepte, technische

FOTOS: RICHARD GANSTERER, EGON WEISSHEIMER

Systeme, Netzwerkeinstellungen und physische Schutzmaßnahmen eingehend kontrolliert. „Je nach Anlassfall kann eine Einschau einige Stunden oder auch mehrere Tage dauern“, sagt Gaisbauer. Erst wenn Unternehmen ihren Verpflichtungen trotz entsprechender Maßnahmen nicht nachkommen, wird eine Sachverhaltsdarstellung wegen möglicher Verwaltungsübertretungen nach dem NISG an die zuständige Behörde übermittelt.

Messbare Fortschritte. Die behördliche Aufsicht zeigt Wirkung. „Im ersten Prüfzyklus nach Einführung des NISG wurden 2.400 Empfehlungen ausgesprochen, die in etwa 50 Sachverhaltsdarstellungen mündeten. Zur Halbzeit des zweiten Prüfzyklus waren es nur noch 400 Empfehlungen und eine einzige Sachverhaltsdarstellung“, berichtet Gaisbauer. Diese Entwicklung verdeutliche den deutlichen Reifegewinn der betroffenen Unternehmen in der Cyber-Sicherheit. Für Gaisbauer ist genau dieser Beitrag zur Stärkung der digitalen Resilienz eine wesentliche Motivation seiner täglichen Arbeit.

Arbeit mit internationaler Perspektive. Neben der nationalen Aufsicht ist die Abteilung IV/S/2 in zahlreichen europäischen Gremien vertreten. Dort werden technische, organisatorische und rechtliche Entwicklungen abgestimmt sowie gemeinsame Standards weiterentwickelt. Dienstreisen, internationale Konferenzen und Facharbeitsgruppen gehören zum Berufsalltag wie die Bewertung von Prüfberichten. „Die Cyber-Sicherheit ist ein vergleichsweise junges regulatorisches Themenfeld. Dadurch ergeben sich große Gestaltungsmöglichkeiten – sowohl bei der Weiterentwicklung der rechtlichen Rahmenbedingungen als auch bei der Arbeit der Behörde selbst“, betont Gaisbauer.

Bundesamt für Cyber-Sicherheit. Die rasante Entwicklung der Cyber-Sicherheit führte im Dezember 2025 zu einer umfassenden Novellierung des Netz- und Informationssicherheitsgesetzes (NISG). Diese tritt mit 1. Oktober 2026 in Kraft. Dadurch wird der Anwendungsbereich von derzeit rund 100 Unternehmen auf mehrere Tausend Einrichtungen ausgeweitet. Erfasst werden künftig auch zahlreiche Stellen der Bundes- und Landesverwaltung. Gleichzeitig wird die bisherige Abteilung IV/S/2 zum Bundesamt für Cyber-Sicherheit als neue Cyber-Sicherheitsbehörde ausgebaut. „Die zusätzlichen Aufgaben und die deutlich höhere Zahl an betroffenen Einrichtungen werden eine Herausforderung darstellen. Gleichzeitig freut es uns, dass die Bedeutung unserer Arbeit erkannt und entsprechend gestärkt wird“, sagt Gaisbauer.

Richard Gansterer

AUDITOREN

Aufgaben und Bilanz

- Bewertung von Prüfberichten
- Ableitung von Sicherheitsmaßnahmen
- Vor-Ort-Kontrollen und Einschauen
- Rund 3.000 Empfehlungen ausgesprochen
- Etwa 50 Sachverhaltsdarstellungen erstellt
- Deutliche Verbesserung des Cybersicherheitsniveaus bei den betroffenen Unternehmen