Cybersicherheit: Herausforderung für kritische Infrastrukturen

25.03.2025, 07:46 Uhr
Kommentare: 0
Sicher arbeiten

Cyberangriffe auf kritische Infrastrukturen sind eine reale Gefahr. (Bildquelle: Traitov/iStock/Getty Images Plus)

Die Sicherheitsanforderungen an Kritische Infrastrukturen (KRITIS) haben sich in den letzten Jahren deutlich verschärft. Die EU-weite NIS-2-Richtlinie sollte bis Oktober 2024 in deutsches Recht umgesetzt werden, was sich allerdings erheblich verzögert. Obwohl die EU-Mitgliedsstaaten verpflichtet waren, die Richtlinie bis zum 17.10.2024 in nationales Recht zu überführen, hat Deutschland diese Frist nicht eingehalten. Das Bundesministerium des Innern und für Heimat (BMI) legte im Juli 2023 einen Referentenentwurf für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vor. Nach mehreren Überarbeitungen wurde am 24.07.2024 der Regierungsentwurf veröffentlicht. Dennoch konnte das parlamentarische Verfahren aufgrund vorgezogener Bundestagswahlen im Februar 2025 nicht abgeschlossen werden.

Daher muss die neue Bundesregierung das Gesetzgebungsverfahren neu initiieren. Es wird erwartet, dass das NIS2UmsuCG frühestens im 2. Quartal 2025 verabschiedet wird. Diese Verzögerung betrifft schätzungsweise 30.000 deutsche Institutionen und Unternehmen, die unter die erweiterten Cybersicherheitsanforderungen der NIS-2-Richtlinie fallen. Die Betreiber müssen höhere Sicherheitsstandards erfüllen, etwa durch Cybersicherheitskonzepte, Meldepflichten und Notfallpläne. Bei Nichteinhaltung drohen Strafen von bis zu 20 Mio. Euro. Bereiche wie Energie, Luftfahrt und Telekommunikation werden auf Bundesebene reguliert, Wasser- und Gesundheitsversorgung sind Ländersache. Das führt zwangsläufig zu uneinheitlichen Sicherheitsstandards.

Zunehmende Bedrohung durch Cyberangriffe und hybride

Kriegsführung

Seit Beginn des Ukrainekriegs hat sich die Zahl der Cyberangriffe auf KRITIS-Betreiber verdreifacht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert in Deutschland täglich rund 250.000 neue Varianten von Schadprogrammen. Die Bedrohung ist nicht nur digital: Cyberangriffe werden zunehmend mit physischer Sabotage kombiniert. In den Jahren 2023 und 2024 ereigneten sich in Deutschland und der Ostseeregion mehrere Vorfälle, die die Verwundbarkeit kritischer Infrastrukturen, insbesondere im Energiesektor, verdeutlichen. Am 25.12.2024 wurden mehrere Unterseekabel in der Ostsee beschädigt, darunter das Stromkabel Estlink 2 zwischen Finnland und Estland. Die finnische Küstenwache reagierte umgehend und nahm Ermittlungen auf, wobei ein fehlender Anker des verdächtigen Öltankers „Eagle S“ entdeckt wurde. Es besteht der Verdacht, dass Russland hinter diesen Sabotageakten steckt, um die europäische Wirtschaft zu destabilisieren und Unsicherheit zu verbreiten (www.welt.de).

Das Bundesamt für Verfassungsschutz warnte im Januar 2025 vor einer neuen Bedrohung durch Sabotageakte fremder Nachrichtendienste, die kritische Infrastrukturen in Deutschland ins Visier nehmen könnten. Diese Sabotagehandlungen umfassen Cyberattacken, Sachbeschädigungen und Brandsätze, die eine Gefahr für Gesellschaft, Politik und Wirtschaft darstellen (www.verfassungsschutz.de). Bereits 2024 kam es vermehrt zu Sabotageakten auf maritime Infrastrukturen in der Ostsee, darunter die Beschädigung von Pipelines und Unterseekabeln. Diese Vorfälle zeigten die Verwundbarkeit kritischer Infrastrukturen und führten zu verstärkten Sicherheitsmaßnahmen in der Region (www.ndr.de).

Diese Ereignisse unterstreichen die Notwendigkeit, die Resilienz kritischer Infrastrukturen in Deutschland und Europa zu erhöhen, um zukünftigen Bedrohungen effektiv begegnen zu können. Angriffe auf solche Infrastrukturen können immense wirtschaftliche und sicherheitspolitische Folgen haben, insbesondere wenn sie mit gezielten Cyberangriffen kombiniert werden.

Technische Schwachstellen und Risikofaktoren

Viele Umspannwerke in Deutschland sind veraltet und enthalten Komponenten, die seit mehr als 30 Jahren in Betrieb sind. Diese Systeme wurden häufig nicht für eine vernetzte Steuerung entwickelt und können Schwachstellen aufweisen, für die keine aktuellen Sicherheitsupdates zur Verfügung stehen. Durch die zunehmende Digitalisierung und

Fernsteuerung sind diese Umspannwerke neuen Angriffsmöglichkeiten ausgesetzt.

Ein weiteres Risiko ist die unzureichende Notstromversorgung in vielen KRITIS-Bereichen. So sind beispielsweise Krankenhäuser gesetzlich verpflichtet, eine autarke Energieversorgung für mindestens 24 Stunden sicherzustellen. Doch schon nach einem Tag können wichtige Kühlketten für Medikamente ausfallen. Auch Tankstellen sind nicht flächendeckend mit Notstromaggregaten ausgestattet, sodass die Treibstoffversorgung im Krisenfall unsicher ist. Zudem fallen weniger als 1 % der deutschen Wasserversorger unter die KRITIS-Regelungen, so dass viele kleine und mittlere Versorgungsunternehmen keine höheren Sicherheitsstandards einhalten müssen.

Internationaler Einfluss auf die deutsche Energieinfrastruktur

Besondere Aufmerksamkeit verdient der hohe Anteil ausländischer Investoren in der deutschen Offshore-Windenergie. Derzeit befinden sich laut Recherchen des ZDF-Magazins „frontal“ 82,8 % der Offshore-Windkraftkapazitäten in ausländischem Besitz, davon 48 % außerhalb der EU. Besonders brisant ist die Kontrolle durch China: Das Staatsunternehmen China Three Gorges hält 80 % an der WindMW GmbH und damit wesentliche Teile der Offshore-Stromproduktion in Deutschland. Das US-Verteidigungsministerium führt China Three Gorges als Unternehmen mit Verbindungen zur militärischen Modernisierung Chinas.

RWE hat inzwischen 104 Stahlpfähle für mehrere Offshore-Windparks in China statt in Deutschland bestellt. Die Bundesnetzagentur hat 2024 neue Offshore-Windflächen ohne die von der EU geforderte Mindestbeteiligung europäischer Unternehmen vergeben. Dies führt zu einer zunehmenden Abhängigkeit von außereuropäischen Anbietern, insbesondere aus China.

Maßnahmen zur Erhöhung der Sicherheit

Forschungsinstitute wie die Fraunhofer-Gesellschaft entwickeln verschiedene Lösungen zur Abwehr von Cyberangriffen. Das Fraunhofer IOSB setzt auf künstliche Intelligenz (KI), um Anomalien in Netzwerkdaten frühzeitig zu erkennen. Parallel dazu erforscht das Fraunhofer IOF den Einsatz von Quantenkryptosystemen (QKD), um die Kommunikation zwischen Netzleitstellen und KRITIS-Betreibern vor Spionage zu schützen.

Eine wichtige Sicherheitskomponente ist das exklusive 450-MHz-Funknetz für KRITIS-Betreiber. Dieses Netz wurde speziell für den Notfallbetrieb entwickelt und bietet eine garantierte Notstromversorgung von 72 Stunden. Damit bleibt die Kommunikation auch bei großflächigen Stromausfällen erhalten. Ergänzend entwickelt das Fraunhofer FKIE ein digitales Lagebild, das den Einsatzkräften eine priorisierte Bearbeitung von Hilfeersuchen ermöglicht.

Netzwiederaufbau nach Blackout

Der Wiederaufbau der Stromversorgung nach einem Blackout ist komplex und erfordert speziell ausgerüstete Kraftwerke. Deutschland verfügt über 174 schwarzstartfähige Kraftwerke, die ohne Fremdenergie wieder angefahren werden können. Eine der wichtigsten Anlagen ist das Pumpspeicherkraftwerk am Schluchsee. Es gehört zu den 26 zentralen Kraftwerken, die für den Netzwiederaufbau unverzichtbar sind (www.kyon-energy.de). Mit diesen Kraftwerken kann das Stromnetz nach einem Totalausfall schrittweise stabilisiert werden.

Krisenmanagement und Katastrophenvorsorge

Um die Kommunikation im Krisenfall sicherzustellen, werden sog. Katastrophenleuchttürme eingerichtet. Feuerwehrhäuser dienen als Anlaufstellen für die Bevölkerung, da sie mit Notstrom versorgt werden. Ergänzend erhalten die kommunalen Krisenstäbe mobile Notfallkommunikationskoffer, die eine autarke Funkverbindung für mindestens 8 Stunden gewährleisten.

In Meißen wurde bereits viel in das Krisenmanagement investiert, u.a. durch regelmäßige Übungen der Einsatzkräfte. Viele andere Kommunen sind jedoch noch nicht ausreichend vorbereitet. Oft fehlen Notstromaggregate oder Treibstoffreserven, um eine länger anhaltende Krisensituation zu bewältigen. Der Einzelhandel hat keine einheitlichen Notfallpläne für die Lebensmittelversorgung. Die staatlichen Notfallreserven an Getreide, Reis und Linsen werden erst freigegeben, wenn ein Bundesstaat offiziell den Notstand ausruft.

Herausforderungen und Ausblick

Obwohl Deutschland über eine vergleichsweise stabile Energieversorgung verfügt, zeigen sich zahlreiche Schwachstellen in der Krisenvorsorge. Cyberangriffe, physische Sabotage und internationale Einflussnahme stellen wachsende Herausforderungen dar. Die Maßnahmen zur Absicherung von KRITIS werden kontinuierlich weiterentwickelt, die Umsetzung der gesetzlichen Vorgaben bleibt jedoch eine zentrale Aufgabe für Betreiber und Politik.

Unternehmen, die unter die KRITIS-Regelungen fallen, müssen sich gezielt auf Stromausfälle vorbereiten, um Betriebsunterbrechungen zu minimieren. Neben einer funktionierenden Notstromversorgung sind die Entwicklung umfassender Krisenpläne, regelmäßige Notfallübungen und die Reduzierung von Versorgungsabhängigkeiten wichtige Faktoren. Insbesondere die Implementierung von Inselnetzfähigkeiten ermöglicht

es Unternehmen, kritische Systeme unabhängig vom öffentlichen Netz weiter zu betreiben. Darüber hinaus sollten redundante Kommunikationssysteme aufgebaut werden, um auch bei großflächigen Ausfällen die Koordination mit Behörden und Partnern sicherzustellen.

Auch die Bevorratung wichtiger Betriebsmittel wie Treibstoff für Notstromaggregate oder Ersatzteile für Netztechnik muss in die Notfallstrategie integriert werden. Eine enge Abstimmung mit Netzbetreibern und Behörden trägt dazu bei, Wiederanlaufstrategien effizient umzusetzen und die Betriebsprozesse nach einem Blackout schnellstmöglich wiederherzustellen.

Neben der technischen Absicherung der Energieversorgung sollten KRITIS-Unternehmen umfassende physische Schutzmaßnahmen umsetzen. Dazu gehören verstärkte Zugangskontrollen, Überwachungssysteme und bauliche Schutzmaßnahmen gegen Sabotage. Insbesondere für hochkritische Infrastrukturen wie Netzleitstellen und Kommunikationszentralen wird der Schutz vor elektromagnetischen Angriffen (EMP) immer relevanter. Darüber hinaus spielt die redundante Datenhaltung eine wichtige Rolle, um nach einem Angriff oder Ausfall schnell wieder handlungsfähig zu sein. Um die Resilienz zu erhöhen, müssen Betreiber zudem eng mit Behörden, Netzbetreibern und Forschungseinrichtungen zusammenarbeiten, damit aktuelle Bedrohungsszenarien frühzeitig erkannt und geeignete Gegenmaßnahmen ergriffen werden können.

Weitere Beiträge zum Thema

Analyse von Cybersicherheitsbedrohungen in modernen elektrischen Steuerungssystemen

Internet of Things (IoT)

Sicherheit und Optimierung der betrieblichen Stromversorgung

Basiswissen Cybersecurity – die Bandbreite der Bedrohungen

Einsatz von Künstlicher Intelligenz zur Fehlerdiagnose in elektrischen Anlagen

Autor:

Thomas Joos

freiberuflicher Publizist

Thomas Joos ist freiberuflicher Publizist und veröffentlicht neben seinen Büchern auch Artikel für verschiedene Medien wie dpa, Computerwoche und C’t.

Seit seinem Studium der medizinischen Informatik berät er auch Unternehmen im Bereich IT, Security und Absicherung von Rechenzentren.