Ostsee im Visier: Experten warnen vor Cyberangriffen auf Energieinfrastruktur

Experten diskutieren bei einem Forum in Berlin über den Schutz kritischer Infrastruktur und steigende Cyberbedrohungen in der Ostsee.

Berlin, Deutschland - Mit einem Blick auf die Ostsee zeigt sich, dass die Sicherheit kritischer Infrastruktur mehr denn je im Fokus steht. Am 9. Juli 2025 fand das Baltic Energy and Cyber Security Forum in Berlin statt, wo über 80 Fachleute aus Politik, Wirtschaft und Wissenschaft über die drängenden Herausforderungen diskutierten. Die Sorgen um wiederholte Sabotageakte auf Gas-, Strom- und Datenleitungen nehmen zu und die Bedrohung durch Cyberangriffe auf Energieversorger steht im Raum. dena berichtet, dass das Forum ein neu konzipiertes Austauschformat darstellt,initiiert von der dena, der polnischen Botschaft und der polnischen Akademie der Wissenschaften.

Die Debatte wurde von Polens Botschafter Jan Tombiński eröffnet, der die Bedeutung nationaler Energiepolitik für die Resilienz der Region hervorhob. „Hier geht es um weit mehr als nur um lokale Lösungen“, so Tombiński. Kristina Haverkamp, Geschäftsführerin der dena, ergänzte, dass eine stärkere regionale und europäische Koordinierung für den Schutz kritischer Energieinfrastrukturen unerlässlich sei. Dazu gehören nicht nur physische, sondern auch digitale Sicherheitsschutzmaßnahmen.

Bedrohungen im digitalen und physischen Raum

Eine besondere Herausforderung stellen die Unterseekabel dar, die über 90% des globalen Datenverkehrs transportieren. Sicherheitsexperte Johannes Peters vom Institut für Sicherheitspolitik warnte, dass der Schutz dieser Kabel unzureichend sei. Viele von ihnen liegen am Meeresboden und sind kaum geschützt. Die Zunahme hybrider Angriffe auf kritische Infrastrukturen verdeutlicht die Notwendigkeit für verbesserte Schutzmaßnahmen. Manuel Atug von der AG KRITIS betonte, dass während ein kompletter Sabotageschutz nicht möglich sei, es dennoch Lösungsvorschläge gibt, wie etwa die Verlegung der Kabel mehrere Meter unter dem Meeresboden oder die Geheimhaltung neu verlegter Kabel. Doch diese Ansätze haben ihre eigenen Fallstricke, wie etwa höhere Kosten und Schwierigkeiten bei Reparaturen, wie ZDF berichtet.

Die Sicherheitslage wird zudem beeinträchtigt durch die Rekordzahl an Cyberangriffen, insbesondere seit Ausbruch des Ukraine-Konflikts. Diese Gefahrenlage erfordert ein Umdenken: Eine effektive Gegenstrategie könnte die verstärkte NATO-Präsenz beinhalten sowie eine bessere Vernetzung und Zusammenarbeit zwischen EU-Staaten. Hierbei wird auch die Nutzung von Sensoren zur Verbesserung der Sicherheit in der Ostsee immer relevanter.

Die Rolle von Rechenzentren und Zertifizierungen

Über das unmittelbare Gefahrenumfeld hinaus spielen auch Rechenzentren eine tragende Rolle. Einige davon sind als kritische Infrastrukturen klassifiziert und werden regelmäßig auf ihre Sicherheit hin überprüft. Laut TÜV Nord erfolgt diese Prüfung meist freiwillig, oft aber in Form von Zertifizierungen, die von Kunden oder Aufsichtsbehörden gefordert werden. Dabei wird beispielsweise die Einbruchssicherheit von Fenstern und Türen, der technische Brandschutz sowie moderne Sicherheitssysteme wie Videokameras und Zugangskontrollen geprüft.

Insgesamt sind die Herausforderungen im Bereich der kritischen Infrastruktur vielschichtig und erfordern ein gemeinsames Vorgehen. Das Baltic Energy and Cyber Security Forum wird fortgesetzt, um die entstandenen Erkenntnisse zu vertiefen und neue Ansätze zur Verbesserung der Sicherheit zu entwickeln. Die nächsten Schritte in diesem Prozess beinhalten das Deutsch-Polnische Energiewendeforum im November sowie den Nordseegipfel im Januar 2026, die weitere Möglichkeiten zur Zusammenarbeit bieten.

Details	
Ort	Berlin, Deutschland
Quellen	• www.dena.de • www.zdfheute.de • www.tuev-nord.de

Besuchen Sie uns auf: wom87.de