Sorge um die Netze

Besonders viele Strom- und Datenkabel kommen an den Küsten Schleswig-Holsteins an – doch sie sind unzureichend gegen Angriffe geschützt

Lisa Bohlander

Verbogener Stahl, eine weggesprengte Betonummantelung, eine zerstörte Röhre. Die Bilder der beschädigten Pipeline Nord Stream 1 südöstlich der dänischen Insel Bornholm zeigen: Hier, 79 Meter tief in der Ostsee, muss es eine wuchtige Explosion gegeben haben. Die Attacke

auf die Gasleitung im vergangenen September zeigt eine neue Größenordnung möglicher Angriffe auf die kritische Infrastruktur in Europa, Deutschland – und Schleswig-Holstein. Und sie zeigt, wie schwierig unser Netz aus Energie und Daten zu schützen ist.
„Wir haben das Problem in Deutschland, dass wir sehr viele neuralgische Punkte haben“, sagt Thomas Holst, IT-Unternehmer aus Husum und Vize-Präsident der IHK Flensburg. Dabei handelt es sich um besonders kritische und empfindliche Stellen wie Seekabelendstellen. „Sie sind durch die Zeitenwende, wie unser Bundeskanzler es ausgedrückt hat, mittlerweile ein bisschen anders zu betrachten.“ Die Sicherheit sei dort nicht so weit, wie sie sein sollte.

Neue Dimension durch Russlands Krieg

Unter anderem der russische Angriff auf die Ukraine habe dem ganzen eine neue Dimension gegeben: „Wir sind über den Punkt hinaus, an dem Cyberkriminelle nur Geld erpressen. Das ist mittlerweile staatlich organisiert und auf Zerstörung und Vernichtung ausgelegt“, sagt Holst. Es sei eine andere Lagebewertung nötig – und Verbesserungen. „Das beginnt mit Verteilerhäuschen, die mit Kameras, Stacheldraht und sichereren Schlössern ausgerüstet werden, damit sie geschützt sind.“
Politisch ist das Thema längst: In einer gemeinsamen Erklärung der Nato und der Europäischen Union vom Dienstag heißt es, man wolle sich beim Schutz kritischer Infrastrukturen enger abstimmen. Zudem richten die Institutionen eine gemeinsame Arbeitsgruppe dazu ein. Das Bundesamt für Verfassungsschutz warnt Unternehmen, Behörden und Industrieverbände davor, Daten, Karten und Baupläne ins Internet zu stellen. Diese lieferten Hinweise auf mögliche Anschlagziele. Ausländische Geheimdienste und andere mögliche Saboteure suchten das Internet vermehrt und systematisch nach Informationen über die deutschen Digital-, Strom- und Gasnetze ab. Thomas Holst bekräftigt: „IT-Sicherheit heißt für mich, dass so gut wie keine Informationen nach draußen dringen sollen. Denn es bedeutet, Leuten Informationen zu geben, die sie nicht haben sollten.“

Wichtige Standorte öffentlich im Internet

Informationen zu kritischen Punkten sind in Schleswig-Holstein teilweise relativ leicht zu finden. Da gibt es Stromtrassen wie die Mittelachse, erkennbar an Dutzenden Metern hohen überirdischen Strom-

masten. Und die klotzigen Umspannwerke, deren dunkle Metallspiralen hinter Zäunen im Nebel knistern. Ein Foto inklusive Pfeil verrät auf Wikipedia den genauen Punkt, an dem das Baltic Cable aus Schweden auf schleswig-holsteinischem Boden landet. Die Seite infrapedia.com zeigt den genauen Verlauf unzähliger Datenkabel weltweit – das Überseekabel AC-1 landet am Strandübergang Samoa auf Sylt an. Nur wie die Seekabelendstellen, die die Kabel mit dem deutschen Netz verbinden, genau aussehen, ist und bleibt geheim. Zuständig für die Seekabelendstelle auf Sylt ist die Telekom, wie das Unternehmen auf Nachfrage bestätigte. Da diese zur kritischen Infrastruktur zähle, wolle man sich dazu aber nicht weiter äußern.
Bereits Ende 2010 war die Sicherheit der Seekabel und ihrer Endstellen Thema: Damals hatte das Enthüllungsportal Wikileaks von Julian Assange auf die kritische Infrastruktur als potenzielle Terrorziele hingewiesen. Die Telekom teilte damals mit, dass die technischen Einrichtungen und die Infrastruktur höchste Sicherheitsstandards erfüllten. Weitere Details nannte die Telekom nicht.
Auch rechtlich wird die Sicherheit kritischer Infrastruktur mittlerweile ernster genommen: Die EU hat im vergangenen November die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) 2.0 auf den Weg gebracht. Sie legt Mindeststandards in der EU für die Regulierung kritischer Infrastrukturen fest und erweitert Betroffenheit und Pflichten. Spätestens im Herbst 2024 sollen Unternehmen in 18 Sektoren ab 50 Mitarbeitern und zehn Millionen Euro Umsatz die Pflichten umsetzen – in Deutschland sind etwa 20000 Unternehmen betroffen. In Schleswig-Holstein sind es hunderte, genaue Zahlen aus dem Land gibt es nicht. Maßnahmen können etwa ein anderes Risikomanagement und neue Notfallpläne sein. Ausgelöst hat der Krieg die neue Verordnung Holst zufolge zwar nicht, „aber das war alles längst fällig und hat das etwas beschleunigt“.

Gesetz zur Sicherheit nachschärfen

In Deutschland gilt das IT-Sicherheitsgesetz 2.0, das durch die EU-Verordnung wohl nachgeschärft werden muss. Das Gesetz wurde von Experten und Branchenkennern nach seiner Verabschiedung Ende 2020 als unzureichend und lückenhaft beurteilt.
Wie beurteilen Unternehmen der kritischen Infrastruktur die Lage nun? Bei Tennet heißt es, die zuständige Fachabteilung sei derzeit mit der Auswertung der neuen Richtlinie beschäftigt. Laut der SH Netz AG enthalte die neue Richtlinie „im Wesentlichen die Anforderungen aus

dem deutschen IT-Sicherheitsgesetz, das bei uns bereits länger umgesetzt ist“. Dazu gehöre eine unabhängige jährliche Prüfung und Zertifizierung des unternehmenseigenen Informations-Sicherheits-Management-Systems.
Durch die NIS-Richtlinie kämen an der einen oder anderen Stelle noch Aspekte hinzu – sie gingen aber letztlich nicht deutlich über das hinaus, was mit der Novelle 2.0 des IT-Sicherheitsgesetzes in Deutschland 2021 bereits verabschiedet wurde und in diesem Jahr umzusetzen ist. „Derzeit sind wir dabei – auch im Verbund mit anderen betroffenen Unternehmen des E.ON Konzernverbunds – diese im Detail zu analysieren“, heißt es von der SH Netz AG.

Diese Vorfälle gab es in Schleswig-Holstein

Strom- und Internetausfälle durch beschädigte Kabel gab es in der Vergangenheit bereits mehrfach – jedoch ohne Angriffe von außen. In der Nacht vom 16. zum 17. April 2016 trat am Baltic Cable auf der Halbinsel Priwall bei Lübeck-Travemünde ein Defekt auf. Das Kabel geriet in Brand, es gab eine meterhohe Stichflamme. Die herbeigerufene Feuerwehr konnte diese zuerst nicht löschen – die Flamme erstickte schließlich, als das Kabel abgeschaltet wurde.
Am 17. Dezember 2006 gab es einen Schaden am Unterseekabel CANTAT 3. Es waren einige hunderttausend Anschlüsse wie Telefon und Internetdienste von Síminn, Vodafone und HIVE betroffen. Die Reparaturzeit war mit zehn Tagen veranschlagt – dauerte aber ein halbes Jahr. Am 13. Januar 2007 begannen die Reparaturarbeiten und zogen sich bis zum 28. Juli 2007 hin. Erst am 29. Juli war das Kabel wieder voll funktionsfähig und erreichte seine volle Kapazität von 2,5 Gbit/Sekunde.