Glasfaser gegen Pipeline-sprenger

Deutschland ist das Ziel von Sabotage und hybriden Angriffen auf kritische Infrastruktur. Der Schutz davor: schwer bis unmöglich. Ein Hightechmittelständler aus Böblingen hält mit Sensortechnik dagegen.

Sächsische Zeitung (Riesa & Großenhain) · 28 Juli 2025 · Von Felix Huesmann

Um zu zeigen, was seine Technik kann, schlüpft Bernd Drapp kurz in die Rolle des Einbrechers. Der promovierte Physiker tritt gegen den Zaun, der eine Trafostation des Böblinger Technologieparks umgibt, rüttelt daran und macht Anstalten, darüber zu steigen.

Einige Meter entfernt steht sein Kollege Daniel Gerwig, ein Tablet in der Hand, und überwacht die Inszenierung. Das System, das die beiden vorführen, erkennt Drapps Einbruchsversuch und schickt einen Alarm aufs Tablet – inklusive des genauen Standorts. Und auch seine Schritte neben dem Zaun erscheinen in Echtzeit auf dem Bildschirm. Dafür sind keine Bewegungsmelder oder Kameras am Zaun installiert. Der Böblinger Mittelständler AP Sensing, für den Gerwig und Drapp arbeiten, macht handelsübliche Glasfaserkabel zu Mikrofonen, Seismografen und Thermometern. Die Technik erkennt nicht nur Einbrecher an Zäunen. Mit ihr hätte möglicherweise der Anschlag auf die Nord-stream-pipelines verhindert werden können, sagt Gerwig.

Der Anschlag rüttelte im September 2022 viele in Deutschland und Europa wach. Vier Explosionen zerstörten nicht nur drei Stränge der Gaspipelines, sondern machten deutlich, wie verwundbar unsere Infrastruktur ist. Auch danach blieb es in der Ostsee nicht ruhig: Schiffe der sogenannten russischen Schattenflotte zerrissen mehrfach Unterseekabel mit

tonnenschweren Ankern. An bloße Unfälle glauben Sicherheitsexperten nicht. Unter westlichen Nachrichtendienstlern zitiert man dazu den sogenannten Ententest: „Wenn es aussieht wie eine Ente, schwimmt wie eine Ente und quakt wie eine Ente, dann ist es wahrscheinlich eine Ente.“Was wie ein Anschlag aussieht, dürfte auch ein Anschlag sein – gerade, wenn sich solche Fälle häufen.

Pipelines, Unterseekabel, Stromtrassen und Breitbandverbindungen sind die Schlagadern unserer vernetzten Gesellschaft. Sie nimmt Russland ins Visier. Aus Sicht von Militärs und Geheimdiensten führt das Land längst einen „hybriden Krieg“gegen alle westlichen Ukraine-unterstützer. Aber auch einheimische Extremisten schrecken teilweise nicht vor entsprechenden Angriffen zurück, wie linksextreme Brandanschläge auf Kabelschächte der Deutschen Bahn gezeigt haben.

Wie also lässt sich dieses weit verzweigte und lebenswichtige Netz schützen? In Böblingen wollen sie ihren Teil zur Antwort auf diese Frage beitragen. Seit 2007 stellt AP Sensing Glasfasersensortechnik her. Am Anfang waren sie nur eine Handvoll Leute, mittlerweile beschäftigt AP Sensing in Böblingen und an sieben weiteren internationalen Standorten mehr als 150 Mitarbeitende. In den Räumen im Technologiepark am Rand der schwäbischen Kreisstadt wird entwickelt, programmiert und geschraubt. Das Team ist international, die Arbeitssprache Englisch. „Was die Nerven für unseren Körper sind, sind Glasfasern für unsere Infrastruktur“, sagt Vertriebsleiter Daniel Gerwig. In den meisten Bereichen kritischer Infrastrukturen sei ohnehin längst Glasfaser verlegt, wenn nicht, lasse sie sich einfach nachrüsten.

Sensor erkennt Schüsse

Mit den Geräten, die AP Sensing herstellt, werden diese Fasern zu ultrasensiblen Sensoren. Sie schicken Lichtpulse hindurch, die mit der Faser selbst interagieren, wie Wirtschaftsinformatiker Gerwig erklärt. „Das zurückgestreute Licht analysieren wir millionenfach pro Sekunde hochpräzise. Je nach Auswertung erkennen wir daraus Temperatur, Dehnung oder Vibration.“Jede dieser Veränderungen sorgt für eine winzige Veränderung der Lichtrückstreuung. In Texas hat das Unternehmen ein Glasfaserkabel neben einem Weg im Erdboden ver

Was die Nerven für unseren Körper sind, sind Glasfasern für unsere Infrastruktur. Daniel Gerwig, Vertriebsleiter der Firma AP Sensing

Das Ziel muss sein, dass ein Angriff – selbst, wenn er erfolgreich ist – keinen gravierenden Schaden für das Gesamtsystem verursacht. Christian Dörr, Sicherheitsforscher

graben. In einem Test, von dem Gerwig und Drapp Videoaufnahmen zeigen, fährt ein Auto den Weg entlang – das System erkennt das Fahrzeug und seine Position. Als das Auto stoppt und keine Vibrationen mehr verursacht, verschwindet es kurz von der Überwachungskarte. Dann steigt ein Mann aus, geht ein paar Schritte, er wird sofort als „Person“erkannt. Schließlich bleibt er stehen, legt ein Gewehr an und gibt einen Schuss ab. „Gunshot“ist nun im Alarmsystem zu lesen.

Um aus den Vibrationsmustern im Boden zu erkennen, dass sie auf Schritte, ein Auto oder einen Schuss zurückzuführen sind, verwendet AP Sensing Künstliche Intelligenz. Die Glasfasersensorik wurde ursprünglich vor allem in der Öl- und Gasindustrie eingesetzt,

um Bohrlöcher zu kontrollieren. Dort kann sie zum Beispiel erkennen, wenn Wasser in einen Schacht eintritt, weil sich die Temperatur dadurch verändert. Ein anderer Einsatzzweck ist der Brandschutz. In Parkhäusern oder Autobahntunneln kann ein ausbrechendes Feuer mit gewöhnlichen Glasfaserkabeln in Sekundenbruchteilen erkannt werden.

Preise nennt die Firma nicht

Heute ist die Stromversorgung ein Haupteinsatzgebiet. „Netzbetreiber wissen mit unserer Technologie genau, wie viel Strom sie durch eine Leitung schicken können, ohne dass das Kabel überhitzt“, sagt Gerwig. Dadurch lasse sich die Kapazität oft um mehr als 30 Prozent steigern. Drapp, Innovationsdirektor bei AP Sensing, erklärt: „Bei unseren Anwendungen ging es ursprünglich nicht in erster Linie um den Schutz vor Sabotage, sondern um ein Monitoring, das dem Kunden einen betriebswirtschaftlichen Mehrwert bietet.“Der Sabotageschutz sei erst in den vergangenen Jahren hinzugekommen. Nachdem die Nordstream-pipelines gesprengt wurden, klingelten in Böblingen die Telefone. Doch in Deutschland werde in diesem Bereich noch eher zögerlich investiert, sagt Drapp. Was die Systeme genau kosten, möchte AP Sensing nicht öffentlich verraten. Doch so viel ist klar: Die Kosten sind deutlich geringer, als die Reparatur einer zerstörten Pipeline.

Unter Wasser funktioniert die

Technik im Grunde wie an Land: „An Pipelines in der Nord- und Ostsee hängen in aller Regel ohnehin Glasfaserkabel“, erklärt Vertriebsleiter Gerwig. „Wenn ich eine 100 Kilometer lange Pipeline überwachen will, kann ich deshalb einfach eine vorhandene Faser nehmen und unser Gerät anschließen. Dann braucht es nichts weiter entlang der gesamten Pipeline.“So könnten Schallwellen erkannt werden, die von Schiffsmotoren ausgehen. „Wir können nicht nur erkennen, dass ein Schiff über eine Pipeline fährt. Wir erkennen auch, wenn es sich über einen längeren Zeitraum in der Nähe aufhält“, ergänzt Drapp. Außerdem, erklärt Gerwig, ließen sich „diverse Unterwasseraktivitäten“erkennen. Wenn ein Taucher neben einer Pipeline auf den Meeresboden trete oder etwas an einem Kabel anbringe, mache das eindeutige Geräusche. „Außer Krebsen und Fischen gibt es da unten nicht viel. Wenn da jemand herumwerkelt, kann man das deshalb deutlich erkennen und lokalisieren“, sagt Gerwig. Solche Systeme könnten auch U-boote, Unterwasserdrohnen oder Unterwasserscooter finden, die von Tauchern verwendet werden. Die Hoffnung: Sicherheitskräfte könnten bereits alarmiert werden, wenn Saboteure eine Pipeline oder ein Unterseekabel erkunden oder dort Sprengstoff anbringen und nicht erst dann, wenn es knallt.

Hightech allein reicht nicht

Ist moderne Technik also die Lösung für das Problem der steigenden Sabotagegefahr? Sicherheitsforscher Christian Dörr ist skeptisch. „Das Erdgasfernleitungsnetz umfasst rund 40.000 Kilometer, die Bahnstrecken 33.000 Kilometer und allein das Glasfasernetz der Deutschen Telekom 750.000 Kilometer. Das entspricht fast 19-mal dem Erdumfang“, sagt der Professor für Cybersicherheit des Potsdamer Hassoplattner-instituts. Sein Fazit: „Das lässt sich schlichtweg nicht schützen.“Wo Unterseekabel, Gaspipelines oder Hochspannungsleitungen verlaufen und Umspannwerke stehen, das sei in öffentlichen Karten verzeichnet, sagt er. „Unterseekabel verlaufen durch internationale Seewege. Dort kann ich

keine Zugangsbeschränkungen
einführen, und es ist zu schwierig und zu teuer, sie wirklich zu schützen.“
Glasfasersensortechnik wie die von AP Sensing sei technisch beeindruckend, sagt Dörr. Der Wert dieser Sensorik hänge aber vom Anwendungsfall ab. Bei Unterseekabeln hält er den praktischen Nutzen für gering. „Ein Schiff, das seinen Anker über ein Kabel zieht, zerstört es in wenigen Sekunden – da hilft mir auch eine exakte Detektion nicht, weil die Reaktionszeit fehlt.“Einen hohen Stellenwert habe die Technik aber beim Schutz des Umfelds – etwa bei Militärgeländen, Industrieanlagen oder Unternehmensstandorten. Viele Sicherheitsprobleme entstünden erst, weil es eine große Asymmetrie zwischen Verteidigungs- und Angriffskosten gebe, erklärt der Sicherheitsforscher. „Ich muss zigtausende Kilometer kritische Infrastruktur schützen, der Angreifer braucht nur einen einzigen verwundbaren Punkt, an den ich nicht gedacht habe – und schon entsteht enormer Schaden.“
In so einer Situation könne man sich „tot rüsten“, warnt er: „Egal, wie viel ich investiere, die Angriffsseite bleibt im Vorteil, solange der Angriff weniger kostet als die Verteidigung. Das macht die Systeme grundsätzlich verwundbar.“Wenn sich diese Asymmetrie nicht auflösen lasse, müsse stattdessen an der Widerstandskraft angesetzt werden, sagt Dörr. „Das Ziel muss sein, dass ein Angriff – selbst, wenn er erfolgreich ist – keinen gravierenden Schaden für das Gesamtsystem verursacht. Wenn wir dafür sorgen, dass die kritische Infrastruktur so ausgelegt ist, dass sie bei Ausfall einzelner Komponenten weiter funktioniert, verliert der Angreifer einen Großteil seines Hebels.“Wenn ein Kabel sabotiert wird, muss also sichergestellt werden, dass Strom oder Daten ohne Aussetzer auf andere Wege umgeleitet werden. Bisher ist das an vielen wichtigen Stellen in Deutschland der Fall – doch längst nicht überall.
Dörr nimmt aber auch die Bevölkerung in die Pflicht: „Gesellschaftliche Resilienz heißt, dass nicht jede Störung sofort zum Chaos führt“, sagt er. „Wenn alle Menschen zu Hause für ausreichende Zeit Lebensmittel und Wasser vorrätig hätten, wäre unsere Gesellschaft im Fall eines Stromausfalls oder einer anderen Krise deutlich widerstandsfähiger.“Zumindest ein paar Tage könnten die Leute so überbrücken, ohne in Panik zu geraten, sagt Sicherheitsforscher Dörr. Der Wissenschaftler drückt es diplomatisch aus: Andernfalls könnten sich die Leute gezwungen sehen, „ihre Versorgung mit allen Mitteln zu sichern“. Man könnte auch sagen: Auf Panik folgt Chaos. Das wissen auch die Staatsfeinde von innen und außen.