Alles Zufälle? Nein – Cyberkrieg

IT-Experte warnt: Kritische Infrastruktur muss besser geschützt werden / Hacker-Angriffe auch im Norden

Was tun, wenn es passiert? Der Servicepoint Cybersecurity dient der Wirtschaft in Schleswig-Holstein als zentrale Anlaufstelle, um Beratung und akute Hilfe zur Prävention und Reaktion bei Cyberangriffen zu erhalten: servicepoint-cybersecurity.de

Inga Gercke

Wir haben einen Cyberkrieg und wir sind mittendrin.“ Das sagt IT-Sicherheitsexperte Thomas Holst, Inhaber der Firma BT-Nord in Husum. Mehr noch: „Und mich ärgert es, wenn Menschen in Schleswig-Holstein oder sonst wo denken, dass sie das nicht betrifft. Warum denn nicht? Wir leben in einer global vernetzten Welt, im IT-Bereich gibt es keine Grenzen“, sagt Holst.

Das Problem bei einem Cyberkrieg sei, dass es Hackern nun nicht mehr darum gehe, Daten von Computern zu stehlen – das nennt man Ransomware – und dafür ein Lösegeld zu fordern. „Bei einem Cyberkrieg geht es nur darum, Daten zu löschen und so möglichst viel Infrastruktur zu zerstören“, sagt Holst. Infrastrukturen wie Telekommunikation, Gesundheitswesen, Finanz- und Energieversorger – die sogenannte Kritische Infrastruktur.

Aktuell könne man das am Ausfall des „Ka-Sat“-Satellitennetzwerk sehen. Dessen Anbieter sitzt zwar in Kalifornien, doch seine Breitband-Satellitendienste werden auch hier für die Fernsteuerung und Wartung von Windkraftanlagen der Firma Enercon gebraucht. Das ist aktuell nicht möglich. „Wir sind und werden Kollateralschäden sein“, sagt er. Die Firma untersuche den Vorfall noch, heißt es von offizieller Seite.

Ein Zufall? „Zufälle gibt es nicht“, sagt Holst. Die Kritische Infrastruktur sei in Krisenzeiten wie jetzt besonders gefährdet.

Wie viele es von diesen sogenannten Kritischen Infrastrukturen in Schleswig-Holstein gibt, darüber macht das Innenministerium aus Sicherheitsgründen keine Aussage. Aber: „In den Jahren 2020 und 2021 sind dem Landeskriminalamt insgesamt sechs Cyberattacken auf systemrelevante Infrastrukturen mittels Ransomware bekannt gewor-

den“, teilt ein Sprecher des Innenministeriums mit. Eine Klinik sei darunter. Cyberattacken mittels Ransomware auf Behörden seien dem Landeskriminalamt (LKA) nicht bekannt. In den Jahren 2020 bis 2021 hätten sich 136 Firmen bei der Polizei gemeldet, die gehackt wurden. Doch diese Zahl könnte weitaus höher sein. Karsten von Borstel, Pressesprecher der Industrie- und Handelskammer (IHK) Schleswig-Holstein, sagt: „Leider ist die Datenlage beim Thema Cyberattacken auf Landes- und auf regionaler Ebene insgesamt dünn. Das hat auch mit der weiterhin sehr hohen Dunkelziffer zu tun.“
Doch warum melden sich die Opfer nicht? „Der Großteil der Unternehmen meldet sich schlichtweg aus Angst- oder Schamgründen nicht. Die Unternehmen fürchten, dass ein Bekanntwerden Image- und Vertrauensverlust der Kunden nach sich ziehen kann oder dass die Behörden Festplatten längere Zeit einziehen“, so von Borstel.
Nach dem BSI-Gesetz §8b müssen Betriebe der Kritischen Infrastruktur einen Angriff dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Tun sie das nicht, drohe eine hohe Geldstrafe, ähnlich wie bei einem Verstoß gegen die Datenschutz Grundverordnung (DSGVO). Bei kleineren Betriebe, die aufgrund ihrer Größe nicht zur Kritischen Infrastruktur zählen, gebe es das so nicht, sagt Holst.
Wie die Kritische Infrastruktur in puncto IT-Sicherheit aufgestellt ist: Auch dazu gibt es aus Sicherheitsgründen keine offiziellen Angaben. Holsts Einschätzung: „Mangelhaft! Es ist nicht ausreichend.“ Vor allem kleinere und mittlere Betriebe seien nicht ausreichend geschützt.
In Krankenhäusern laufen gleich mehrere Kritische Infrastrukturen wie Strom- und Wasserversorgung sowie Informationstechnologien zusammen. Auch das Uni-Klinikum Schleswig-Holstein (UKSH) wolle sich nicht zu konkreten Fragen äußern. Schriftlich heißt es aber: „Die Bedrohungslage für Krankenhäuser – und damit für Patientinnen und Patienten – ändert sich kontinuierlich und hat sich in den vergangenen Jahren und Monaten grundsätzlich verschärft. Angreifer legen immer häufiger ganze Kliniken lahm, Notaufnahmen müssen vom Netz und verhindern die Außenkommunikation. Derzeit ‚floriert‘ offenbar das Geschäft von Cyber-Erpressung mithilfe von Ransomware“, sagt Rudolf Dück von der UKSH-Stabsstelle Informationstechnologie.

Hacker fahren zweigleisig: Code kam per Post

Das Innenministerium beobachtet „ein breites Spektrum von Angriffsqualitäten. Professionell und oft mehrstufig durchgeführte Angriffsversuche nehmen sowohl in der Qualität als auch in der Quantität

im gesamten Internet zu, wie schon in den Vorjahren. Diese latente Gefährdungslage gilt grundsätzlich auch für Schleswig-Holstein“, heißt es auf Nachfrage. Täter agierten zunehmend professioneller, Arbeitsweisen werden häufig angepasst.

Ein besonders fieses Beispiel hat Thomas Holst: „Da kam ein Brief mit einem Code. Dieser Code war noch mal einzeln verpackt, so wie man es von Banken kennt. Nach diesem Code fragte dann einige Tage später ein Anrufer“, sagt Holst. Das war der Freifahrtschein auf den PC: gehackt.