»Die Souveränität erhalten«

INTERVIEW | **Cornelia Rogall-Grothe** Die Vorsitzende des Nationalen Cybersicherheitsrates will Cyberangriffe durch heimische Produkte in lebenswichtigen Infrastrukturen abwehren.

Frau Rogall-Grothe, die Bundesregierung will Unternehmen besser vor Cyberangriffen schützen. Für hochsensible Bereiche wie Strom- und Telekommunikationsnetze empfehlen Sie, stärker als bisher IT-Systeme und Produkte von Herstellern aus Deutschland oder Europa zu kaufen, die als vertrauenswürdig gelten. Was versprechen Sie sich von diesem Vorstoß?
Rogall-Grothe: Für den Wirtschaftsstandort Deutschland ist sehr wichtig, dass wir unsere technische Souveränität erhalten. In Deutschland traditionell starke Industriezweige wie der Maschinenbau wachsen immer enger mit der Informationstechnik zusammen. Deswegen benötigen wir eigenes IT-Know-how. Das gilt auch für besonders sensible und schutzbedürftige staatliche Stellen, die dem Geheimschutz unterliegen – und für lebenswichtige Infrastrukturen wie Strom- und Telekommunikationsnetze. Dort sollten Behörden und Unternehmen verstärkt vertrauenswürdige Produkte von Herstellern aus Deutschland oder Europa einsetzen.

In den neuen Sicherheitsanforderungen für Telekommunikationsnetze hat die Bundesnetzagentur erstmals den Passus aufgenommen, dass die Betreiber auf den Einsatz von Einrichtungen vertrauenswürdiger Hersteller achten sollten. Bislang gab es solch eine Vorschrift nicht. Dürfen Netzbetreiber jetzt nicht mehr bei chinesischen Ausrüstern einkaufen?
Rogall-Grothe: Die Unternehmen sollten sich bei der Beschaffung von ITK-Produkten für den Einsatz in öffentlichen Telekommunikationsnetzen jedenfalls auch Gedanken über die Vertrauenswürdigkeit der Hersteller dieser Produkte machen und diese – neben den Fragen der technischen Reife und der Kosten – in die Auftragsvergabeentscheidung mit einbeziehen.

Bei wichtigen Komponenten im Internet wie Computerchips, Betriebssystemen und Vermittlungsanlagen sind ausländische Anbieter Marktführer. Wie wollen Sie deren Vormachtstellung aufbrechen?
Rogall-Grothe: Bei Sicherheitschips gehören deutsche Unternehmen bereits mit zu den Marktführern. Wir wollen auch bei anderen Komponenten auf der globalen Ebene mitspielen. Deshalb diskutieren wir, welchen Beitrag der Staat leisten kann. Wir haben eine freie Wirtschaftsordnung. Trotzdem müssen wir uns geeignete Maßnahmen überlegen, wie der Staat die Industrie dabei unterstützen kann, sich in puncto IT-Sicherheit robust aufzustellen und dabei das in Deutschland vorhandene Potenzial zu nutzen.

Welche Sicherheitsrisiken schlummern denn in Produkten ausländischer Anbieter? Hinter vorgehaltener Hand warnen Sicherheitsbehörden, dass ausländische Geheimdienste gut getarnte Hintertüren in die Software einbauen, die zur Spionage und Sabotage genutzt werden können.
Rogall-Grothe: Die Hintertüren sind sicher ein Problem, das wir im Blick haben müs-

FOTO: DANUTA OTFINOWSKI FÜR WIRTSCHAFTSWOCHE

sen. Gut getarnte Hintertüren in Hardware, Software und ganzen IT-Systemen sind mit vertretbarem Aufwand kaum auffindbar. Aber genauso wichtig ist für uns die 100-prozentige Verfügbarkeit der Produkte. In einigen Staaten gibt es Ausfuhrkontrollen, ein Export der wichtigen Komponenten zum Betrieb einer kritischen Infrastruktur könnte also unterbunden werden. Die Produkte oder wichtige Ersatzteile wären dann nicht mehr lieferbar.

Für eine starke Cyberabwehr müsste Deutschland also eine autonome IT-Nation werden, die nicht vom Ausland abhängig ist. Wie wollen Sie das erreichen?

Rogall-Grothe: Autonomie ist nicht unser Ziel, sondern eine starke Stellung in der globalen IT-Welt, gerade im Kontext der Sicherheit. Hierfür gibt es nicht die einfache Lösung, damit die europäische IT-Industrie mithalten kann. Aber einiges lässt sich anschieben. Wir können es mittelbar steuern, wenn Behörden und Unternehmen beim Kauf von Produkten mit Verbindungen ins Internet stärker darauf achten, wer sie herstellt. Wir können uns als Nachfrager zusammenschließen, um eine größere Marktmacht zu bekommen. Die Stückzahlen steigen dann, und es wird für die europäische Industrie wieder interessant, in IT-Produkte zu investieren. Ich halte es auch für sinnvoll, dass die hiesige IT-Industrie gemeinsam sichere Produkte entwickelt und die hohen Kosten auf mehrere Schultern verteilt. Der Bund fördert in diesem Bereich bereits einige Forschungsprojekte.

Der Staat kauft selbst IT-Produkte aller Art. Bei öffentlichen Ausschreibungen ist es aber gar nicht so einfach, dass das sicherste und nicht das billigste Produkt den Zuschlag bekommt.

Rogall-Grothe: In sensiblen Bereichen müssen Sicherheitsprodukte eingesetzt werden, die den Vorgaben des BSI entsprechen. Wenn wir bei einer Ausschreibung dieses Kriterium aufnehmen, ist das eine wichtige Voraussetzung für die spätere Auftragsvergabe.

Europaweit gibt es diese Sicherheitsvorgaben in Ausschreibungen noch nicht. Müssen die Richtlinien harmonisiert werden?

Rogall-Grothe: Zumindest für den Bereich der kritischen Infrastrukturen brauchen wir Mindestsicherheitsvorgaben. Der Weg geht dahin, dies europaweit einheitlich zu verlangen. In der kürzlich vorgestellten Cybersicherheitsstrategie der EU-Kommission gibt es erste Ansätze. Wenn wir als Staat besonders sichere Produkte einsetzen wollen oder ihren Einsatz von den kritischen Infrastrukturen verlangen wollen, können wir das heute schon tun. Bisher gab es vergaberechtlich keine Probleme. Wir schließen ausländische Anbieter ja nicht aus.

Kritische Infrastrukturen werden in der Regel nicht vom Staat betrieben, sondern von privaten Unternehmen. Wie wollen Sie denn dafür Sorge tragen, dass Telekomunternehmen oder Energieversorger bei sicherheitsrelevanten Komponenten vertrauenswürdige Produkte einkaufen?

Rogall-Grothe: Wir vertrauen darauf, dass die Unternehmen selbst ein Interesse daran haben, nur Produkte einzusetzen, die die Sicherheitsanforderungen erfüllen. Zudem wissen wir aus zahlreichen Gesprächen, dass das Problembewusstsein mittlerweile in den betroffenen Branchen sehr ausgeprägt ist. Wir beobachten, dass das günstige Angebot nicht mehr das einzige Entscheidungskriterium ist. IT-Sicherheit ist ein relevantes Kriterium, das natürlich nicht zum Nulltarif zu haben ist.

Marc Elsberg hat in seinem Roman „Blackout“ sehr plastisch beschrieben, wie Saboteure in Steuerungscomputer eindringen und flächendeckend die Stromversorgung und das gesamte gesellschaftliche Leben lahmlegen. Muss der Staat nicht mehr Vorkehrungen treffen?

Rogall-Grothe: Angesichts der stetig steigenden Zahl von Cyberangriffen halte ich es für sinnvoll, dass wir in Zukunft den Betreibern kritischer Infrastrukturen schärfere Vorgaben machen. Einige Branchen sind hier bereits gut aufgestellt, andere müssen dringend nachbessern. Dass wir mit diesem Petitum nicht nur offene Türen einrennen, können Sie an der Diskussion um eine gesetzliche Meldepflicht von Cyberangriffen beobachten, die wir im neuen IT-Sicherheitsgesetz verankern wollen.

Auch Produktionsanlagen werden zunehmend über das Internet gesteuert; dort häufen sich ebenfalls die Angriffe. Werden Fabriken noch zu wenig als kritische Infrastruktur wahrgenommen?

Rogall-Grothe: Damit sprechen Sie in der Tat den Kern der Diskussion an. Was ist eine kritische Infrastruktur? Durch die Vernetzung der Maschinen und die verstärkte Kommunikation zwischen den Maschinen und den dahinterliegenden Produktionsprozessen und Lieferketten werden ganze Industriekomplexe über IT-Systeme gesteuert. Ich beobachte, dass dies den Unternehmen immer stärker bewusst wird. Es gibt aber auch hier Branchen, die noch Nachholbedarf haben.

Welche denn?

Rogall-Grothe: Darüber haben wir Stillschweigen vereinbart. Mit den Vertretern der wichtigsten Branchen haben wir das aber in den vergangenen Monaten erörtert. ■

juergen.berke@wiwo.de

CYBERABWEHR

Monokultur vermeiden

Neue Sicherheitsvorschriften sollen Abhängigkeit von China verhindern.

Die Bundesregierung greift mit verschärften Sicherheitsanforderungen stärker in die Investitionsentscheidungen von Betreibern lebenswichtiger Infrastrukturen wie Strom- und Telekommunikationsnetze ein. Im neuen Sicherheitskatalog für Telekommunikations- und EDV-Systeme nimmt die Bundesnetzagentur erstmals die Vorschrift auf, dass die Anbieter den „Aufbau von Monokulturen beim Einsatz von Hard- und Software und die Abhängigkeit von einzelnen Anbietern vermeiden“ sowie „auf den Einsatz von Einrichtungen vertrauenswürdiger Hersteller achten“ sollten.

Noch ist dies eine nicht verbindliche Empfehlung. Die Netzbetreiber tragen also selbst die Verantwortung, wie die Bundesnetzagentur erläutert, „bei der Auswahl vertrauenswürdiger Hersteller größtmögliche Sorgfalt walten zu lassen“. Doch der Entscheidung, welcher Ausrüster den Zuschlag bekommt, sind damit engere Grenzen gesetzt. Bisher kaufen Netzbetreiber meist gleichzeitig bei zwei Ausrüstern ein: einem europäischen (Ericsson, Nokia Siemens Networks, Alcatel-Lucent) und einem chinesischen (Huawei, ZTE). Weitere Marktanteilsgewinne von Huawei und ZTE könnten zu einer Abhängigkeit führen, die politisch nicht gewollt ist. Tritt dann ein Sicherheitsproblem auf, steigen auch auf Basis einer nicht verbindlichen Vorschrift die Haftungsrisiken. Betroffene könnten Schäden beim Netzbetreiber geltend machen, wenn eine nicht vertrauenswürdige Monokultur entstanden ist.