Neue Zürcher Zeitung

Gegenseitige Hilfe in einer Mangellage

Der Bund erteilt der Handelsplattform für Strom- und Gaskontingente grünes Licht – mit Einschränkungen

Leeren sich die Gasspeicher, wollen die Wirtschaftsverbände gewappnet sein (im Bild ein Biogasspeicher in Niedergösgen). C. BEUTLER / KEYSTONE

DAVID VONPLON

Drohen in diesem Winter Energieengpässe in Europa? Diese Woche teilte die EU-Kommission mit, dass sie grossflächige Stromunterbrüche für möglich hält. Zwar sind die Gasspeicher in Europa gut gefüllt, jedoch reichen sie nicht aus, um eine Unterversorgung von Gaskraftwerken auszuschliessen. Dies erst recht, weil Kreml-Herrscher Wladimir Putin auch noch die letzten verbliebenen Gaslieferungen nach Europa stoppen könnte und Experten Anschläge und Cyberattacken auf Energieanlagen befürchten. Damit wächst auch hierzulande die Furcht, dass Gas und Strom bald rationiert werden müssen.

Um die Schäden bei einem solchen Szenario in Grenzen zu halten, haben sich der Wirtschaftsdachverband Economiesuisse und die Branchenverbände Swissmem (MEM-Industrie) und Scienceindustries (Chemie- und Pharmaindustrie) bereits Ende Juli zusammengeschlossen. Gemeinsam mit dem Energie-Treuhänder Enerprice sind sie daran, eine Internet-Plattform für Grossbezüger von Strom und Gas aufzubauen, die den Handel mit Energie-Kontingenten möglich macht.

Arbeitsplätze erhalten

Die Idee dahinter: Wird in einer Mangellage der Strom rationiert, verkaufen Firmen nicht benötigte Kontingente für den Bezug von Strom oder Gas an andere weiter. So könnte ein Betrieb die Revision der Maschinen in den Winter vorziehen. Seine nicht beanspruchten Kontingente tritt er an ein anderes Unternehmen ab, das seine Produktion nicht herunterfahren kann. Im Ergebnis könnten die Arbeitsplätze in beiden Unternehmen erhalten bleiben.

In der ersten Oktoberwoche sollte die Plattform mit der Web-Adresse mangellage.ch gemäss Plan ihren Betrieb aufnehmen, und die ersten Unternehmen sollten ihre Inserate für den Kauf und Verkauf von Strom und Gas aufschalten. Doch daraus wird jetzt nichts. Weil die Hürden für die Realisierung des Selbsthilfeprojekts höher sind als gedacht, verzögert sich beim Strom die Lancierung. Auch sonst muss die Wirtschaft zurückbuchstabieren. An einem Treffen mit dem Bund und der Organisation für Stromversorgung in ausserordentlichen Lagen (Ostral) am Dienstag wurde beschlossen, dass die Handelsplattform vorerst bloss in einem eingeschränkten Pilotbetrieb laufen soll.

Der Grund: Das Bundesamt für wirtschaftliche Landesversorgung (BWL) sowie die Ostral befürchten, dass der Handel mit den Stromkontingenten die 630 Verteilnetzbetreiber in der Schweiz administrativ überfordern könnte. Gerade grössere Netzbetreiber mit einer Vielzahl von Grosskunden könnten den Überblick darüber verlieren, ob die Sparvorgaben von den Unternehmen korrekt eingehalten werden. Das könnte zu Störungen im Netz führen – und auch das Krisenmanagement der Behörden stark erschweren.

Obwohl der Bund auf die Bremse tritt, hält man sich bei den Verbänden mit Kritik zurück. «In einer akuten Krise müssen immer Abstriche gemacht werden», sagt Alexander Keberle, Leiter Energie bei Economiesuisse. Er ist optimistisch, dass der Handel mit Stromkontingenten im Winter zumindest zu grossen Teilen möglich sein wird. Mit dem Pilotbetrieb könne man überdies die Möglichkeiten und Grenzen des Handels ausloten.

Kritik zeigt Wirkung

Bei den Verbänden ist die Erleichterung zu spüren, dass die Plattform überhaupt realisiert werden kann. Noch vor wenigen Tagen befürchteten die Wirtschaftsvertreter, dass der Bund den Handel mit den Kontingenten beim Strom ganz unterbindet. «Im BWL scheint die Meinung vorzuherrschen, dass ein Handel, wie beim Erdgas vorgesehen, beim Strom nicht möglich sein soll», heisst es in einem Brief an den Bund, datiert auf den 28. September.

In der Wirtschaft löste die Abwehrhaltung der Behörden grosse Irritation aus. «Vor dem Hintergrund der immensen wirtschaftlichen Schäden einer Kontingentierung darf der Handel nur eingeschränkt werden, wenn diesem harte technische Fakten entgegenstehen», heisst es im Schreiben weiter. Nun nehme man verwundert zur Kenntnis, dass vonseiten des Bundes bisher keine solchen Fakten zutage geführt worden seien.

Der scharfe Brief der Verbände hat offenbar Wirkung gezeigt. Man sei froh, dass man nun einen pragmatischen, konstruktiven Weg gefunden habe, beteuern nun alle Beteiligten – so auch Lukas Küng, der Chef der Krisenorganisation Ostral. Die Vorbehalte gegenüber dem Handel mit den Kontingenten sind für ihn nachvollziehbar. «Kann die Kontingentierung des Stroms nicht sauber durchgeführt werden, verliert sie ihre Wirksamkeit», sagt er. «Es könnten dann drastischere Massnahmen notwendig werden – wie die temporäre Abschaltung des Stromnetzes.» Gleichzeitig sei bei allen involvierten Akteuren der Wille spürbar, alles zu unternehmen, damit der wirtschaftliche Schaden einer Stromrationierung minimiert werde.

Keine Stellung zum Seilziehen über den Handel mit Kontingenten nehmen die Bundesbehörden. «Wir stehen mit den Exponenten der Plattform im Austausch», erklärt der BWL-Sprecher Thomas Grünwald. Inhaltlich könne man keine Auskunft geben.

> Wird der Strom rationiert, sollen Firmen nicht benötigte Strom- und Gaskontingente an andere weiterverkaufen können.

Noch sind bei der Realisierung der Handelsplattform einige Fragen ungeklärt. So ist offen, ab welchem Schwellenwert der Handel von Kontingenten für den Bezug von Strom erlaubt werden soll. Setzt der Bund die Latte hoch an, schliesst er damit einen Grossteil der Unternehmen vom Handel mit Kontingenten aus. Bei einem tiefen Grenzwert dagegen riskiert er, dass die Netzbetreiber den Überblick verlieren – dann droht in der Mangellage ein Chaos.

Ebenso ist ungewiss, wann es mit dem Handel von Stromkontingenten funktionieren soll. Einen fixen Starttermin kann derzeit keiner der Beteiligten nennen.

Die Information über Cyberangriffe erfolgt nur stockend

Rasches Handeln ist bei Hackerangriffen wichtig – aber in der Bundesverwaltung haben das noch nicht alle erkannt

LUKAS MÄDER

Wenn ausländische Spione in die Computer eindringen, muss es schnell gehen. Denn kann sich ein staatlicher Angreifer erst einmal im Netzwerk festsetzen oder gar ausbreiten, ist es viel schwieriger, ihn aufzuspüren. Und der angerichtete Schaden ist umso grösser. Es ist deshalb wichtig, rasch Spezialisten beizuziehen oder andere Stellen zu warnen.

Dass rasches Handeln bei Cyberangriffen wichtig ist, haben in der Bundesverwaltung noch nicht alle Stellen erkannt. Die Meldungen über sicherheitsrelevante Vorfälle erfolgen zu langsam. Und nicht alle Ämter melden dieselben Ereignisse.

Mit dem Nationalen Zentrum für Cybersicherheit (NCSC) hat die Bundesverwaltung eigentlich eine zentrale Anlaufstelle, die seit zwei Jahren auch für die Bewältigung von grösseren Sicherheitsvorfällen zuständig ist. Das war ein wichtiger Schritt, lag die IT-Sicherheit bis dahin doch einzig in der Verantwortung der Departemente.

Doch der Informationsfluss zwischen den Bundesämtern, den Departementen und dem NCSC hat noch grosse Mängel. Das zeigt ein neuer Bericht der Eidgenössischen Finanzkontrolle, für den die unabhängige Aufsichtsbehörde unter anderem zwei konkrete Cybervorfälle angeschaut hat. Das Fazit ist eindeutig: Die Meldungen müssen rascher erfolgen.

Erst nach Wochen gemeldet

In der Tat erstaunen die Abläufe, die die Finanzkontrolle beschreibt. In einem Fall dauerte es volle dreizehn Tage, bis die Sicherheitsprobleme dem NCSC gemeldet wurden. Die Abteilung der Bundesverwaltung ging anfangs davon aus, «dass nur ihr Netz betroffen sei», heisst es im Bericht. Später zeigte sich, dass auch ein externer IT-Dienstleister kompromittiert war.

> In der Vergangenheit haben sich zahlreiche Ämter nicht einmal an die minimalen Sicherheitsvorgaben gehalten.

Unter diesen Voraussetzungen ist es für das NCSC schwierig, seine Rolle als Kompetenzzentrum für Cybersicherheit wahrzunehmen. Denn nur mit Meldungen aus der Verwaltung und der Privatwirtschaft kann das NCSC ein gutes Bild der Bedrohungslage erhalten. Zudem braucht es weitere Informationen über Angriffe, um den Schutz der Bundesverwaltung insgesamt zu stärken.

Eine zusätzliche Baustelle besteht bei den externen IT-Dienstleistern. Die Bundesverwaltung ist in der Informatik stark auf Privatunternehmen angewiesen. Ihre Produkte sind mit den Systemen des Bundes vernetzt, und ihre Mitarbeiter haben Zugriff auf gewisse Anwendungen. Wenn einer der zahlreichen Dienstleister angegriffen wird, ist auch die Bundesverwaltung in Gefahr.

Die Sicherheit der IT-Lieferketten, der sogenannten Supply-Chain, ist in den letzten Jahren zu einem wichtigen Thema geworden. Spätestens seit dem Fall von Solarwinds, bei dem sich mutmasslich russische Spione über eine Software Zugang zu amerikanischen Behörden verschafften, ist das Vorgehen auch einer breiten Öffentlichkeit bekannt.

Deshalb wäre es für das NCSC wichtig, eine Übersicht zu haben über alle externen IT-Unternehmen, die für den Bund Dienstleistungen erbringen. Doch eine solche Liste für die gesamte Verwaltung existiert nicht. Selbst innerhalb der einzelnen Bundesämter sind solche Aufstellungen nicht einfach vorhanden, sondern müssen laut Finanzkontrolle mit grossem Aufwand erstellt werden. Dieser Mangel hat konkrete Folgen. Im Falle eines Cyberangriffs könne «nicht innerhalb nützlicher Frist erhoben werden», welche weiteren Abteilungen oder Applikationen möglicherweise ebenfalls betroffen seien, heisst es im Bericht. Es gehe «viel wertvolle Zeit verloren». Eine effiziente Abwehr der Attacke ist so nicht möglich.

Keine Meldepflicht für Externe

Schliesslich ist der Bund auch unwissend, wenn es um die Sicherheit der externen IT-Zulieferer geht. Werden diese Drittfirmen Opfer eines Cyberangriffs, müssen sie diesen der Bundesverwaltung als Kunden meist nicht melden. Eine entsprechende Pflicht fehlt in den meisten Verträgen. Immerhin sehen die Musterverträge inzwischen entsprechende Klauseln vor.

Das NCSC widerspricht der Darstellung im Bericht nicht. Es akzeptiert die Empfehlungen der Finanzkontrolle, die hohe Priorität haben. Das erstaunt nicht, hat das NCSC doch selbst ein Interesse daran, rascher mehr Informationen zu erhalten.

Entscheidend wird sein, ob die Bundesämter und Departemente im Bereich Cybersicherheit künftig stärker kooperieren. Dazu gehört auch, dass sie sich zu einem gewissen Masse der Kontrolle des NCSC unterordnen müssen. In der Vergangenheit haben sich zahlreiche Ämter nicht einmal an die minimalen Sicherheitsvorgaben gehalten. Die Armee verschwieg Schwachstellen gar bewusst – trotz der vorgesehenen Pflicht, diese der zentralen Stelle zu melden.