Illustrationen: Mathis Rekowski

SERIE
1 JAHR NSA-SKANDAL

Teil 1: Leben im Glashaus
Nach dem ersten Schock haben sich die privaten Internet-User schnell an die Überwachung gewöhnt.

TEIL 2: GESCHÄFT IST (CYBER)-KRIEG
Wie reagieren Unternehmen auf die globale Überwachung des Internets?

Teil 3: Der Staat im Staat
Hat die Politik die Geheimdienste noch unter Kontrolle? Oder ist es längst umgekehrt?

WER TRAUT NOCH DER CLOUD?

Die Spähaffäre hat die Wirtschaft alarmiert. **IT-Sicherheit und Datenschutz** sind plötzlich Dauerbrenner in den Chefetagen. Doch nur ein Teil der Unternehmen zog die richtigen Konsequenzen.

VON ULRICH HOTTELET

Die NSA mag nach wie vor beteuern, keine Wirtschaftsspionage zu betreiben – die Ereignisse des vergangenen Jahres legen einen anderen Schluss nahe. Denn die Kontakte zwischen Geheimdienst und Unternehmen bestehen. Ex-NSA-Chef Michael Hayden räumte in einem ZDF-Interview ein, dass „es Transaktionen in der Wirtschaft gibt, die von hoher Bedeutung sind“. Wenn beispielsweise Siemens „programmierfähige, logische Steueranlagen für die Uranverarbeitung“ herstelle, sei das für Nachrichtendienste relevant. Beim Verband Deutscher Maschinen- und Anlagenbau (VDMA) weiß man von einem Marktführer im Hightech-Bereich, der von den Amerikanern ausspioniert wird. Das Unternehmen will damit allerdings nicht an die Öffentlichkeit gehen.

Aber nicht nur für Großunternehmen, auch für den Mittelstand ist Wirtschaftsspionage ein „sehr ernstes Problem“, sagt der Präsident des Bundesverbands mittelständische Wirtschaft (BVMW), Mario Ohoven. „Es trifft uns an unserer empfindlichsten Stelle, unserer Innovationsleistung. Von den 2700 Weltmarktführern kommen über 1300 aus dem deutschen Mittelstand.“ Besonders bedroht sieht er Maschinenbau, Metallverarbeitung, Automobilbau sowie Luft- und Raumfahrt. Für Steffen Zimmermann, verantwortlich für Know-how-Schutz beim VDMA, hat es sich zwar „nicht bewahrheitet, dass die NSA deutsche Unternehmen im großen Stil ausspioniert“. Er macht jedoch drei wichtige Ausnahmen: Luftfahrt, Rüstung und Energietechnik. Seit der Spähaffäre verzichtet daher so mancher Maschinenbauer lieber auf den Austausch von Konstruktionsdaten.

Die NSA versichert zwar nach wie vor, die Daten von ausländischen Unternehmen nicht an US-Konkurrenten weiterzugeben, um ihnen einen Wettbewerbsvorteil zu verschaffen. Aber selbst wenn das zutrifft, ist die Gefahr der Industriespionage keineswegs gebannt.

Denn zum einen könnten die Betriebsgeheimnisse jenseits des offiziellen Wegs in die Hände von Konkurrenten gelangen. Der frühere technische Direktor der NSA, William Binney, erklärte auf den European Data Protection Days im Mai, ein großes Risiko für Industriespionage bestehe darin, dass viele US-Unternehmen, wie zum Beispiel Booz Allen Hamilton, bei dem Edward Snowden bis Juni 2013 beschäftigt war, die Überwachungsprogramme ausführten. Sie hätten dadurch Zugang zu allen Daten, was dem Missbrauch Tür und Tor öffne. Außerdem gebe es in einer Behörde wie der NSA, in der derartig viele sensible Daten zusammenfließen, ein hohes Korruptionsrisiko – noch dazu sei die NSA eine der wenigen US-Behörden, die keiner Revision unterliege. Thomas Endres, Präsident des IT-Anwenderverbands Voice, sorgt ein weiterer Aspekt: dass mit der Zeit auch Cyberkriminelle die technischen Mittel der NSA nutzen werden. Besonders problematisch findet der ehemalige Lufthansa-IT-Chef zudem, dass die USA de facto ihre Rechtsauffassung durch die Überwachungstechnik exportiert.

Umso ernüchternder ist die Bilanz der Gegenmaßnahmen. Einer repräsentativen Studie des Hightech-Verbands Bitkom zufolge nahmen lediglich 36 Prozent der Unternehmen die NSA-Affäre zum Anlass, ihre IT-Sicherheitsmaßnahmen zu verstärken. Zwei Drittel dieser Firmen haben ihre Organisation verbessert, zum Beispiel durch Zugriffskontrollen für bestimmte

Daten. 43 Prozent haben Firewalls und 35 Prozent Virenschutzprogramme eingeführt oder erneuert. Und das, obwohl fast 80 Prozent der Unternehmen die Betroffenheit der deutschen Industrie durch die Abhörmaßnahmen als hoch oder sehr hoch einschätzten. So jedenfalls das Ergebnis einer Umfrage des Bundesverbands der deutschen Industrie (BDI).

Woher kommt die Diskrepanz? Die Dax-Konzerne zumindest sind „sehr gut aufgestellt bei der Cybersicherheit", betont Matthias Wachter, beim BDI Abteilungsleiter für Sicherheit. Der Skandal hat dazu geführt, dass die von BSI und Bitkom initiierte „Allianz für Cyber-Sicherheit" großen Zulauf bekam, sodass jetzt 700 Unternehmen daran teilnehmen. Was genau die Konzerne in diesem Rahmen unternehmen, will jedoch keiner verraten. Siemens beispielsweise hält sich in Sachen NSA bedeckt und lehnte eine Stellungnahme ab. „Wir wollen keinen Einblick geben, welche Gefahren wir sehen und wie wir uns dagegen verstärkt haben", teilte ein Pressesprecher mit. Möglicherweise will man es sich mit den Amerikanern auch nicht verscherzen, denn die US-Tochter Siemens Government Technologies zählt US-Streitkräfte und -Geheimdienste zu ihren Kunden. Auch SAP hat wohl den wichtigen amerikanischen Markt im Blick, denn Pressesprecher Marcus Winkler wiegelt ab: „Das ist kein Thema mehr für uns. Wir waren von der NSA-Spionage nicht betroffen." Natürlich bleibe aber Sicherheit sehr wichtig für SAP, beeilt er sich zu versichern.

Deutlich schwerer mit Gegenmaßnahmen tun sich dagegen die Mittelständler, immerhin 99 Prozent aller Betriebe in Deutschland. Einen möglich Grund verrät die Bitkom-Studie: Kosten. Nur ein Viertel aller Unternehmen erhöhte infolge der NSA-Affäre die Ausgaben für IT-Sicherheit. Die größte Auswirkung hatten die Snowden-Enthüllungen denn auch auf eine Maßnahme, die rasch und günstig umzusetzen war: der Verzicht auf Cloud Computing. Der „Cloud-Monitor 2014", eine Umfrage des Bitkom unter 403 Unternehmen mit über 20 Mitarbeitern, zeigte: Vor allem Mittelständler sahen sich in ihrer Zurückhaltung bestätigt, ihre Unternehmensdaten in die Wolke auszulagern. Demnach haben 13 Prozent der Firmen geplante Projekte zurückgestellt und elf Prozent sogar ihre Cloud-Lösungen aufgegeben. 23 Prozent nehmen dieses Jahr aus Sicherheitsbedenken keine Dienste aus der Wolke in Anspruch.

Das ist die defensive Haltung. Aber es geht auch anders. Fachleute plädieren für einen differenzierten Umgang mit dem Thema Cloud, je nach Geschäftszweck und Unternehmensbereich. Man kann zum Beispiel eigene IT-Systeme mit Cloud-Diensten verknüpfen und sie in einer hybriden Umgebung als Mix betreiben. Geschäftsgeheimnisse sollte man allerdings auf keinen Fall der Wolke anvertrauen, lautet unisono der Rat. Dem Bitkom-Monitor zufolge gehen 31 Prozent der befragten Mittelständler tatsächlich offensiv mit den Sicherheitsproblemen um: Sie nutzen die Cloud, haben jedoch die Sicherheitsanforderungen an die Dienstleister deutlich erhöht. Viele von ihnen bevorzugen zudem die Private Cloud, weil sie geschützter ist als die Public Cloud.

Stellvertretend für diese Mischung aus Reserviertheit und Gegenmaßnahme kann Kolbus aus Ostwestfalen gelten, der Weltmarktführer im Bau von Buchbindereimaschinen. IT-Bereichsleiter Wolfgang Bokämper erklärt: „Wir lassen unternehmensrelevante Daten nicht aus dem Haus. Statt der Cloud nutzen wir eigene FTP-Server. Wenn wir Modelldaten mit Lieferanten oder Kunden austauschen müssen, werden sie nie im Komplettzusammenhang zur Verfügung gestellt."

Die Sorge vor Zugriffen amerikanischer Sicherheitsbehörden auf die Daten führte

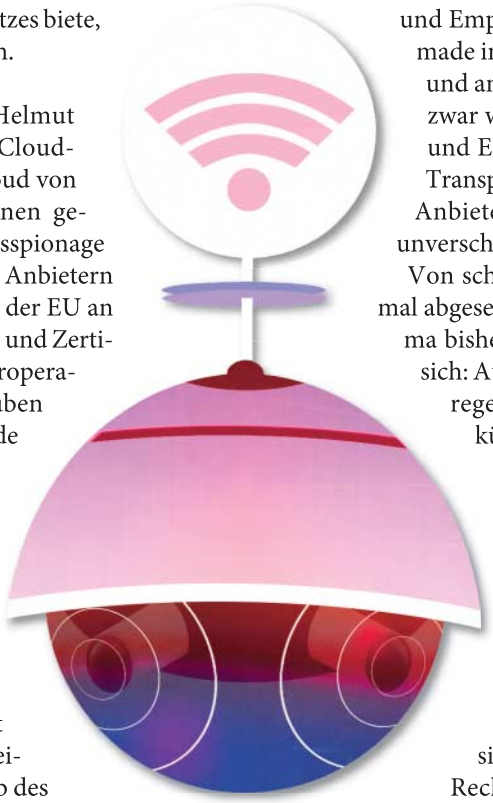
WELTREKORD MIT IT-SICHERHEIT

Das Hamburger Start-up Protonet will den Cloud-Markt für Selbstständige und mittelständische Unternehmen revolutionieren. Das Versprechen: Der Nutzer behält die Kontrolle über seine Daten, kann sie aber wie bei herkömmlichen Cloud-Diensten mit Mitarbeitern oder Kunden teilen. Die Idee zündete. Innerhalb von nur dreieinhalb Stunden kamen über die Crowdfunding-Plattform Seedmatch über eine Million Euro zusammen: Weltrekord! Schon nach zehn Stunden war das Finanzierungsziel von 1,5 Millionen Euro erreicht. Mit dem Geld will Protonet den Bau eines orangefarbenen Servers namens Maya finanzieren, einen persönlichen Cloud-Speicherdienst mit bis zu einem Terabyte Kapazität für Selbstständige und kleine Unternehmen.

Die Version soll 1200 Euro kosten. Dafür verspricht der Hersteller eine leichte Inbetriebnahme, Nutzung und Wartung. Teure IT-Dienstleister seien nicht erforderlich. Das Versprechen konnte das Computermagazin „c't" zumindest für die leistungsstärkere erste Speicherbox der Firma bestätigen. Auch mit diesem Modell hatte Protonet einen Crowdfunding-Rekord aufgestellt.

dazu, dass viele deutsche Cloud-Anbieter zu Lasten der US-Konkurrenz einen Zulauf im zweistelligen Prozentbereich verzeichneten. „Kritische Amerikaner geben den Rat, noch mehr Aufträge aus den USA abzuziehen. Wenn die Verluste die Wirtschaft schmerzen, ändert die US-Regierung am ehesten etwas“, sagt Michael Rotert, Vorstandsvorsitzender des Internet-Wirtschaftsverbands eco. Matthias Wachter vom BDI berichtet: „Vielen Unternehmen ist erst durch den Skandal bewusst geworden, dass ihre Daten in den USA lagern und damit einer anderen Rechtsordnung unterliegen.“ Das hohe deutsche Datenschutzniveau hat sich so zu einem veritablen Pluspunkt entwickelt. „Unsere Rechtslage ist ein Wettbewerbsvorteil“, so Holger Mühlbauer, Geschäftsführer des Bundesverbands IT-Sicherheit Teletrust. Die Vertrauenskrise sei eine Steilvorlage für deutsche IT-Sicherheitstechnik und ihr Qualitätszeichen „IT Security made in Germany“. Einhellig fordern Fachleute daher, eine EU-Datenschutzreform, die das hohe Niveau des Bundesdatenschutzgesetzes biete, zu erarbeiten und zügig zu verabschieden.

Dazu passt das Ansinnen von Helmut Fallmann, Chef des österreichischen Cloud-Anbieters Fabasoft. Er hat sich eine „Cloud von Europäern für Europäer“ auf die Fahnen geschrieben. Sie soll besser vor Wirtschaftsspionage schützen, da die Daten bei europäischen Anbietern gespeichert sind. Zurzeit arbeitet man in der EU an gemeinsamen Standards, Spezifikationen und Zertifikationen, die eine „größtmögliche Interoperabilität verschiedener Plattformen“ erlauben soll. Nationale Initiativen à la „Cloud made in Germany“ sieht der Unternehmer, der auch die EU-Kommission in ihrer Cloud-Strategie berät, dagegen kritisch: „Zusammen können wir im Weltmarkt besser bestehen.“



Ex-Telekom-Chef René Obermann regte sogar eine noch grundlegendere Lösung an: das Schengen-Routing. Daten, die aus Europa kommen, sollen nicht über Knotenpunkte anderer Länder geleitet werden, sofern auch ihr Ziel innerhalb des Schengen-Raums liegt. So würde das Ausspähen zumindest erschwert. Darüber kam es im Branchenverband Bitkom zum handfesten Streit zwischen der Telekom und den amerikanischen IT-Riesen, die den Plan rundheraus ablehnen.

Die Kritiker halten das europäische Routing technisch für schwer umsetzbar und zu teuer. Gravierender noch: Sie wittern dahinter in erster Linie Geschäftsinteressen der Telekom. Deren Pressesprecher Philipp Blank verteidigt die Grundidee: Der Vorwurf der Geldmacherei sei „Unsinn“: „Der Datenverkehr verteuert sich dadurch nicht. Man muss keine neuen Ressourcen schaffen, sondern lediglich die Routing-Tabellen ändern.“ Michael Rotert vom Internet-Wirtschaftsverband eco hält dagegen: Die Telekom beteilige sich schon jetzt nicht am Datenaustausch mit anderen deutschen Internetprovidern am zentralen Internetknoten DE-CIX in Frankfurt. Das sei nicht nur teurer für die Nutzer – sondern bedeute zudem, dass ihre Daten auch über Großbritannien laufen. Der britische Geheimdienst arbeitet in der massiven Überwachung der Netze eng mit der NSA zusammen. „Es ist schwer zu kontrollieren, ob die Daten in Europa nicht durch Kabel geleitet werden, die amerikanischen oder britischen Betreibern gehören.“ Telekom-Sprecher Andreas Middel betont dagegen, sein Unternehmen nutzt direkte Schaltungen mit anderen Netzbetreibern statt des DE-CIX, weil das günstiger ist und besser vor Ausfällen schützt.

Statt der Umgehung von US-Servern fordern die Kritiker des Telekom-Vorschlags den Ausbau der sogenannten Ende-zu-Ende-Verschlüsselungen. Nur hierbei werden die Daten komplett verschlüsselt, sodass nur Sender und Empfänger sie lesen können. Bei der „E-Mail made in Germany“ von Telekom, Web.de, GMX und anderen Partnern dagegen werden E-Mails zwar während des Transports zwischen Sender und Empfänger verschlüsselt – die sogenannte Transportsicherung. Auf dem Server des E-Mail-Anbieters liegen die Mails aber immer noch unverschlüsselt.

Von schärferen Datenschutzbestimmungen einmal abgesehen: Aus der Politik war bei diesem Thema bisher wenig zu hören. Aber auch das ändert sich: Aufgrund einer Verschärfung der Vergaberegeln durch die Bundesregierung müssen künftig Bieter um einen sensiblen IT-Auftrag des Bundes versichern, dass sie sich nicht zur Weitergabe vertraulicher Daten an ausländische Geheimdienste und Sicherheitsbehörden verpflichtet haben. Wer das nicht zusichert, darf am Vergabeverfahren nicht teilnehmen. Bisher kann die NSA relativ problemlos amerikanische Firmen zur Herausgabe von Daten zwingen. Mühlbauer freut sich: „Das ist jetzt eine Denkaufgabe für die Rechtsabteilungen in ausländischen Unternehmen.“

Und es könnte den Druck aus der Wirtschaft, die US-Abhörpraxis zu überdenken, deutlich erhöhen. Microsoft kniffelt bereits an einem Urteil eines New Yorker Bundesgerichts. Danach müssen US-Unternehmen ihren Behörden bei Vorlage eines Durchsuchungsbefehls auch dann Zugang zu Mails und anderen Daten geben, wenn die betroffenen Server im Ausland stehen. Damit könnte die Justiz die Taktik amerikanischer Cloud-Anbieter durchkreuzen, verloren gegangenes Vertrauen durch neue Rechenzentren in Europa wiederzugewinnen. Microsoft will in Revision gehen. Scheitert es vor Gericht, könnte der Konzern nur versuchen, öffentlichen Druck aufzubauen, damit das Recht geändert wird. Es wäre zum Nutzen aller.