DE =	EN =	PT =	VN =
Sicherheit 1/2			

Firmen gegen NSA: Wie sich deutscher Mittelstand vor Industriespionage schützt

Kuppel der ehemaligen Abhörstation der NSA in Berlin: Weckruf für Unternehmen

Prism, Tempora, XKeyscore: Edward Snowdens Enthüllungen über die Geheimdienst-Spionage schrecken Deutschlands Wirtschaft auf. Gerade der Mittelstand will sich jetzt besser gegen Datenklau wappnen. Die hiesige Sicherheitsindustrie wittert gute Geschäfte.

Markus Stäudinger ist ein misstrauischer Mensch - ganz besonders vor dem Computer. Seine Mails etwa verschlüsselt der IT-Sicherheitsbeauftragte der traditionsreichen baden-württembergischen Maschinenfabrik Gustav Eirich schon seit Jahren. "Trotzdem habe ich beim Schreiben immer im Hinterkopf", erzählt Stäudinger, "dass sie am Ende doch geknackt werden könnten." Und diese Denke versucht der 48-Jährige auch in seinem Unternehmen zu verankern.
Jahrelang hat Stäudinger für Datensicherheit bei Eirich gekämpft. Hat seinen Kollegen wieder und wieder eingetrichtert, sorgsam mit sensiblen Informationen umzugehen. Hat Notebooks und Smartphones extra schützen lassen, ehe sie das Unternehmen verlassen. Manch einer der 750 Mitarbeiter in der mittelständischen Firma hat wohl den Kopf geschüttelt über die vermeintliche Paranoia. Aber nun, nach Edward Snowdens Enthüllungen, ahnen sie alle: Stäudinger hatte recht. "Uns war immer bewusst, dass in den USA die Geheimdienste und die Wirtschaft eng zusammenarbeiten", sagt der IT-Sicherheitschef. "Als wir das jetzt gehört haben, sind wir nicht aus allen Wolken gefallen."
Andere Unternehmen schon. Prism, Tempora, XKeyscore: Die Berichte über elektronische Massenüberwachung, angezapfte Internet-Knotenpunkte und transatlantische Datenleitungen haben Deutschlands Wirtschaft aufgeschreckt. Viele Firmen fürchten nun, dass die Geheimdienste nicht nur Terroristen ausspionieren wollen, sondern vor allem ihre Betriebsgeheimnisse. Sie bangen um ihren Know-How-Vorsprung gegenüber amerikanischen, britischen, französischen Konkurrenten.
Und werden sich schlagartig bewusst, dass sie selbst etwas tun müssen gegen den organisierten Datenklau.
Die Berichte über die Aktivitäten der Geheimdienste sind ein Weckruf für viele Unternehmen. Da sind einige Alarmglocken angegangen", sagt Rainer Glatz, Geschäftsführer der Arbeitsgemeinschaft Produkt- und Know-how-Schutz beim Verband Deutscher Maschinen- und Anlagebauer (VDMA). In der Vergangenheit seien Mahnungen vor Hacker-Angriffen und IT-Spionage oft verpufft. Jetzt aber seien gerade mittelständische Betriebe hellhörig geworden. "Die Sensibilität steigt", sagt Glatz.
Vielerorts wird nun auch auf Chefebene nachgedacht, wie man sich besser schützen kann.

DE =	EN =	PT =	VN =
Sicherheit 2/2			

Jährlicher Schaden durch Spionage beträgt Milliarden

Es tut dringend not. Höchstens jeder vierte Mittelständler habe bislang überhaupt eine IT-Sicherheitsstrategie, sagt Christian Schaaf, Gründer der Münchener Beratungsfirma Corporate Trust. Viele beschränken sich auf eine einfache Firewall und ein paar Anti-Virenprogramme. Das aber reicht nicht gegen professionelle Hacker, ganz zu schweigen gegen Angreifer vom Kaliber NSA. "Viele Unternehmen werden sich gerade bewusst, dass sie ein Sicherheitsnetz über ihre Daten legen müssen", sagt Schaaf.

Auszuspionieren gibt es allerhand im deutschen Mittelstand mit seinen Tausenden High-Tech-Unternehmen: von Neuentwicklungen über Produktionsverfahren und Steuerungssysteme bis hin zu Kundenlisten und Preisangeboten bei Ausschreibungen. Der Verfassungsschutz schätzt den Schaden durch Industriespionage auf 30 bis 60 Milliarden Euro pro Jahr. Genau weiß das niemand. Denn bislang herrschte beim Thema Geheimnisverrat das Gesetz des Schweigens in der deutschen und europäischen Wirtschaft. So gut wie nie haben sich ausspionierte Firmen an die Öffentlichkeit gewagt. Weil sie Angst haben vor Nachahmern. Weil sie keinen potentiellen Angreifer wissen lassen wollen, wo ihre Schwachstellen sind und wie sie sich gegen Attacken wappnen. Oder weil sie befürchten, ihnen könnten Kunden abspringen, wenn die Datenlecks publik werden.

Auch die Maschinenfabrik Gustav Eirich wäre ein begehrtes Angriffsziel. Das 150 Jahre alte Familienunternehmen aus Hardheim im Odenwald ist ein typischer deutscher "Hidden Champion", einer der Weltmarktführer für Mischanlagen. Eirichs Maschinen können Chemikalien und Stoffe aller Art schneller, gründlicher, effizienter vermixen als die der internationalen Konkurrenz: dank zahlreicher Erfindungen und Entwicklungen der Ingenieure, die sich die Firma hat patentieren lassen. Unser Know-how ist unser großer Wettbewerbsvorteil, sagt Sicherheitschef Stäudinger. Und den schützt Eirich mit allen erdenklichen Maßnahmen.

"Wir setzen nationale Produkte ein, wo immer es geht"

So lagert das Unternehmen gar keine Informationen in fremde Rechenzentren aus. Videokonferenzen, Datenübertragung, E-Mails - all das erledigt Eirich über seine hauseigenen Cloud-Server. Skype ist verboten, Facebook ungern gesehen. Alle Mitarbeiter werden intensiv geschult, keine sensiblen Daten versehentlich preiszugeben. E-Mails nach außen verschlüsselt die Firma grundsätzlich, sofern die Kunden mitspielen - bevorzugt mit deutscher Software. "Bei US-Programmen hat der Geheimdienst sicher den Generalschlüssel", sagt Stäudinger. "Wir versuchen deshalb, nationale Produkte einzusetzen, wo immer es geht." Schließlich bekommen Sicherheitsbehörden hierzulande in der Regel keinen Zugriff auf die Algorithmen der Verschlüsselungsanbieter.

Der vergleichsweise strenge Datenschutz könnte zum Standortvorteil für deutsche Anbieter von IT-Sicherheit werden. So seien hiesige Rechenzentren neuerdings stark gefragt, berichtet VDMA-Experte Glatz. Private-Cloud-Anbieter wie Demando, eine Tochter der Stadtwerke Kaiserslautern, bieten den Kunden eigene Serverschränke oder sogar exklusive Glasfaserleitungen vom Unternehmen zu ihrer Serverfarm, damit sensible Daten erst gar nicht durchs Internet geschickt werden müssen.

Am Ende können auch diese Leitungen angezapft, fast alle Verschlüsselungscodes geknackt werden. "Sicherheit lässt sich nie hundertprozentig garantieren", sagt Stäudinger. "Wir wissen, dass es ein Restrisiko gibt. Aber wir machen die Hürden so hoch wie möglich." Damit die Angreifer vielleicht weiterziehen: zu anderen, schlechter geschützten Unternehmen mit weniger misstrauischen Sicherheitschefs.

gezeichnet:	hpw	Datum:		eduction project	Sicherheit	translate/en_ds/p_ct/vn_ro	orign: http://www.spiegel.de/wirtschaft/u
Aenderung:	an	Datum:	24.07.2015	WIAP KFKOK	Safety	r1	datei_Wi_8_f_57_c1_r1_Sicherheit_de
Aenderung:	control 2	Data:		Safenwil Schweiz	spear 2	www.wiap.ch	idee of / from HPW