DIHK Deutscher Industrie- und Handelskammertag

17 Newsletter 25.04.2013

Daten | Fakten | Argumente

THEMA DER WOCHE

IT-Sicherheitsgesetz – ja, aber mit Augenmaß!

Die meisten Unternehmen nutzen das Internet nicht nur zur Information und Kommunikation, sondern auch als Absatzkanal und Teil der eigenen Wertschöpfung. Mit der zunehmenden Vernetzung erhöhen sich auch die Bedrohungspotenziale. Nach einer Umfrage berichtet jedes fünfte Unternehmen von gezielten Cyber-Attacken. Dabei bemerken die Betriebe aber oft gar nicht, dass sie in das Visier von Kriminellen geraten sind. Schmerzhaft wird es insbesondere dann, wenn wettbewerbs- und sicherheitsrelevante Unternehmensdaten gestohlen werden, durch Sabotage betrieblicher Prozesse verloren gehen oder für das Gemeinwesen kritische Infrastrukturen betroffen sind. Staat und Unternehmen müssen sich mit diesen Risiken auseinandersetzen.

Die richtige Antwort auf Cyberangriffe?

■ Das Bundesinnenministerium hat jetzt einen Entwurf für ein IT-Sicherheitsgesetz vorgelegt. Er sieht Meldepflichten für IT-Sicherheitsvorfälle in den Sektoren Energie, Telekommunikation, Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen vor. Die betroffenen Unternehmen müssen als Betreiber kritischer Infrastrukturen zudem mittels Audits nachweisen, dass sie IT-Sicherheitsstandards einhalten. Telekommunikationsanbieter werden danach außerdem verpflichtet, Nutzer auf Sicherheitsmängel aufmerksam zu machen und sie dabei zu unterstützen, Störungen zu beseitigen. Und auch Telemedienanbieter, also jeder, der geschäftsmäßig eine Website betreibt, müssen künftig Mindest-IT-Sicherheitsstandards einhalten.

Klares politisches Signal im Grunde richtig, aber nicht so

■ Gesetzlich geregelte Mindeststandards für Betreiber kritischer Infrastrukturen sind angesichts der Bedrohungslage grundsätzlich richtig. Generell stellt sich aber die Frage, welchen Mehrwert eine gesetzliche Meldepflicht – zusätzlich zu den schon bestehenden freiwilligen Auskünften von Betreibern kritischer Infrastrukturen – bieten würde. Der Gesetzentwurf lässt zudem zu viele Fragen offen. Unklar ist derzeit, welche Unternehmen genau zu Betreibern kritischer Infrastrukturen zählen – eine Verordnung soll hier Klarheit schaffen. Diese muss nun möglichst zeitnah auf den Weg gebracht werden. Der Gesetzentwurf lässt auch offen, welche Vorfälle konkret zu melden sind und ob sich die geplanten Audits nur auf den Bereich kritischer Infrastrukturen in einem Unternehmen erstrecken sollen – oder auch darüber hinaus. Die vagen Vorgaben des Entwurfs bergen große Kostenrisiken für die Unternehmen. Außerdem müssen bei der geplanten Hinweis- und Supportpflicht von Telekommunikationsanbietern noch datenschutz- und haftungsrechtliche Aspekte geklärt werden.

Wirtschaft rät von Schnellschüssen ab

■ Angesichts der vielen Fragen und Diskussionspunkte kann von einer gesetzgeberischen Regelung in dieser Form nur abgeraten werden. Unternehmen haben ein vitales Eigeninteresse daran, ihre Unternehmenswerte zu sichern. Es bestehen bereits zahlreiche freiwillige Initiativen zur Verbesserung der IT-Sicherheit in der Wirtschaft wie z. B. kostenlose Website-Checks, Maßnahmen zur Beseitigung von Botnetzen, Allianz für Cybersicherheit etc. Der Gesetzgeber sollte diesen Instrumenten zuerst einmal Zeit lassen und deren Wirkung genauer analysieren, bevor er zu gesetzlichen Regelungen greift. Außerdem wird auf europäischer Ebene aktuell der Entwurf einer Richtlinie zur Netz- und Informationssicherheit diskutiert. Keinesfalls darf ein nationaler Alleingang vor einer europäischen Regelung erfolgen.

Ansprechpartner: *Dr. Katrin Sobania, DIHK Berlin, Tel. 030 20308-2109*
Axel Geiling, DIHK Berlin, Tel. 030 20308-2728