IT-Sicherheitsgesetz – Bundesregierung muss europäische Einbettung sicherstellen

RA Oliver Süme, Hamburg

IT-Sicherheit ist ein Thema, das in der IT-Branche schon seit vielen Jahren ganz oben auf der Agenda steht und spätestens seit den Snowden-Enthüllungen und sich häufenden Nachrichten über spektakuläre Hackerangriffe auch in der öffentlichen Wahrnehmung als eine der größten Herausforderungen der Digitalisierung angekommen ist. Die hohe Anzahl an Schwachstellen in IT-Systemen und Software, die breite Verfügbarkeit von geeigneten Angriffswerkzeugen sowie die zunehmende Nutzung mobiler Geräte und die oft unzureichende Absicherung industrieller Steuerungssysteme im Zuge der Entwicklung zur „Industrie 4.0" sind laut Bundesamt für Sicherheit in der Informationstechnik (BSI) die Haupteinfallstore für Cyber-Angreifer. Es ist also nur folgerichtig, dass auch auf politischer Ebene die Frage diskutiert wird „Welcher ist der richtige Weg zu mehr IT- und Cybersicherheit?"

Die Bundesregierung hat es sich im Koalitionsvertrag und zuletzt auch in der Digitalen Agenda 2014 - 2017 zum Ziel gesetzt, Deutschland zum führenden Standort im Bereich IT-Sicherheit zu machen.

Bundesinnenminister Thomas de Maizière hat dazu Ende vergangenen Jahres den Kabinettsentwurf für ein IT-Sicherheitsgesetz vorgestellt, der für die digitale Wirtschaft erhebliche neue rechtliche Anforderungen nach sich ziehen kann.

Der Entwurf sieht neue gesetzliche Regelungen, insbesondere im Hinblick auf die IT-Sicherheit sogenannter kritischer Infrastrukturen vor. Damit werden Einrichtungen erfasst, die für das Gemeinwesen von zentraler Bedeutung sind, zum Beispiel die Energieversorger. Diese sollen zukünftig einen Mindeststandard an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das BSI melden. Das BSI wiederum erhält den Auftrag, die zusammenlaufenden Informationen auszuwerten und den Betreibern kritischer Infrastrukturen zur Verfügung zu stellen.

Abseits kritischer Infrastrukturen ist aber auch geplant, die gesetzlichen Anforderungen an die IT-Sicherheit für Diensteanbieter im Telekommunikations- und Telemedienbereich zusätzlich zu den bereits bestehenden gesetzlichen Verpflichtungen weiter zu erhöhen.

Die deutsche Internetwirtschaft befürwortet zwar grundsätzlich die Pläne des Innenministers, Deutschland zum führenden Standort im Bereich IT-Sicherheit auszubauen. Dies kann Deutschland einen Standort- und Wettbewerbsvorteil im europäischen und internationalen Markt für innovative Sicherheitslösungen und Anwendungen bringen. Der Fokus der gesetzgeberischen Bestrebungen sollte dabei aber stärker als bisher auf die kritischen Infrastrukturen und deren Betreiber gelegt werden. Die Auferlegung zusätzlicher Verpflichtungen für bereits regulierte Telekommunikations- und Telemediendienstanbieter ist nicht notwendig und vor allem nicht gerechtfertigt. Dies bedeutet für die betroffenen Unternehmen, die ohnehin bereits seit Jahren gesetzliche und darüber hinausgehend auch freiwillige Sicherheitsverpflichtungen erfüllen, eine zusätzliche Belastung.

Die Digitalisierung durchdringt alle gesellschaftlichen Bereiche. IT-Sicherheit ist daher vor allem auch eine gesamtgesellschaftliche Aufgabe. Statt einzelne Branchen und Unternehmen als „Sündenböcke" herauszugreifen und allein in Verantwortung zu nehmen, sollte die Bundesregierung deswegen auch einen ganzheitlichen Ansatz verfolgen. Eine Verbesserung der IT-Sicherheit muss daher alle Bereiche berücksichtigen und einbeziehen, sei es Software oder Hardware. Vor allem aber muss auch das Bewusstsein der Anwender und Nutzer für IT-Sicherheit weiter sensibilisiert und gestärkt werden.

Angesichts des jetzt von der Bundesregierung beschlossenen Kabinettsentwurfs und im Hinblick auf die bisherigen Entwürfe des Bundesministeriums des Innern (BMI) vom 4. 11. 2014 und 18. 8. 2014 ist es zwar erfreulich, dass einige der wesentlichen Kritikpunkte der Internetwirtschaft Gehör gefunden haben und entsprechend berücksichtigt wurden. So ist beispielsweise die ursprünglich geplante Regelung von Speicherrechten für Telemediendienstanbieter zur Störungs- und Missbrauchsbekämpfung, die vor allem angesichts ihrer Unbestimmtheit sogar teilweise als neue Form der Vorratsdatenspeicherung bezeichnet wurde, weggefallen. Auch die unbestimmte Erweiterung der Sanktionsmöglichkeit der Bundesnetzagentur (BNetzA) gegenüber Telekommunikationsbetreibern ist erfreulicherweise gestrichen worden.

Offene Fragen bestehen jedoch nach wie vor im Zusammenhang mit dem europäischen Gesetzgebungsverfahren für eine Richtlinie zur Gewährleistung einer hohen gemeinsamen Netzwerk- und Informationssicherheit (NIS-Richtlinie), das parallel stattfindet und mit den gerade laufenden Trilog-Verhandlungen kurz vor dem Abschluss steht. Die Bundesregierung ist hier in der Pflicht Rechts- und Planungssicherheit für die Unternehmen zu gewährleisten und Widersprüche zwischen dem nationalen IT-Sicherheitsgesetz und den europäischen Vorgaben zu vermeiden. Ein nationales „Vorpreschen" ist weder in Deutschland noch in anderen Mitgliedstaaten zielführend. Damit droht ein Flickenteppich aus nationalen Regelungen, der Unternehmen schadet, Rechtsunsicherheiten befeuert und wenig zur Erhöhung der allgemeinen IT-Sicherheit in Europa beiträgt. Stattdessen müssen jetzt dringend europaweit einheitliche Regelungen und Standards geschaffen werden.