IT-Sicherheit lebt vom Verständnis dafür

Prof. Dr.-Ing. Ina Schieferdecker, Vizepräsidentin des ASQF und Institutsleiterin des Fraunhofer FOKUS zum neu beschlossenen IT-Sicherheitsgesetz der deutschen Bundesregierung:

Das Bundesministerium des Innern hat einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt, welcher von der Bundesregierung am 17. Dezember 2014 beschlossen wurde [1]. Der Entwurf entstand entlang der Vereinbarungen des Koalitionsvertrags zur Absicherung der für das Gemeinwesen zentralen Infrastrukturen, sogenannten kritischen Infrastrukturen wie den Energienetzen oder Telekommunikationsnetzen. Dabei geht es um die Erhöhung der Sicherheit informationstechnischer Systeme, die Verbesserung der IT-Sicherheit von Unternehmen und ebenso um einen verstärkten Schutz der Bürgerinnen und Bürger im Internet. So formuliert der Gesetzentwurf Mindeststandards an IT-Sicherheit für den Betrieb kritischer Infrastrukturen und eine Meldeplicht an das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei erheblichen IT-Sicherheitsvorfällen. Diensteanbieter im Telekommunikations- und Telemedienbereich sollen Sicherheit nach dem jeweiligen Stand der Technik bieten und zudem ihre Kunden warnen, wenn deren Anschluss für Angriffe missbraucht wird. Es fallen kommunale Unternehmen der Netz- und Energiewirtschaft, der Wasser- und Abwasserwirtschaft und der Telekommunikation in den Anwendungsbereich des Entwurfs.

Mit Hinblick auf die zunehmende Vernetzung der Infrastrukturen im öffentlichen Raum, in der Wirtschaft und Gesellschaft werden die Qualität, Sicherheit und Widerstandsfähigkeit von Informations- und Kommunikationsnetzen (IKT) selber und ihren Anwendungen in anderen Bereichen immer zentraler. Das Gemeinwesen und die öffentliche Sicherheit sind von IKT zunehmend abhängig. Der Gesetzentwurf stellt sich den damit verbundenen Herausforderungen. Der ASQF begrüßt diesen weiteren Schritt, die Widerstandsfähigkeit als auch Schutzmaßnahmen bei den Betreibern kritischer Infrastrukturen durch Kooperation und gesetzliche Vorgaben weiter zu verbessern. Jedoch muss das kommende IT-Sicherheitsgesetzt mit Leben gefüllt und operationalisiert werden: Verordnungen und Bestimmungen sollten die Mindestanforderungen, Meldepflichten, etc. detaillieren und zudem an EU-Richtlinien und laufende Aktivitäten auf europäischer und internationaler Ebene anpassen. Es ist Augenmaß bei den Auflagen an die Unternehmen zu wahren. Das spricht gleichsam eine noch unterbeleuchteten Aspekt an: den des konstruktiven Quality-Engineerings. Qualität, Widerstandsfähigkeit und Sicherheit der IKT-basierten Systeme und Infrastrukturen sollten proaktiv in Entwurf und Entwicklung umgesetzt werden, so dass sich die Aufwände in Auditierungs-, Zertifizierungs-, Melde- und Korrekturverfahren reduzieren. Der ASQF wird sich für entsprechende Angebote an die Wirtschaft stark machen.

Ein besonderes Augenmerk ist zudem auf die Stärkung des Verständnisses bei Unternehmen für IT-Sicherheit zu richten. Ohne das Bewusstmachen, Verstehen und Umsetzen hilft auch das beste Gesetz nicht. Heute sind Unternehmen noch viel zu zögerlich und warten (leider) ab, ob es sie denn überhaupt trifft. Bereits 2011 [7] sprachen Guus Dekkers, CIO von Airbus, und Dieter Schmidbaur, Cassidian, davon, dass IT-Sicherheit 2021 mehr als ein Viertel der gesamten Bundeswehr kosten könnte. Wenn man diese Schätzung mit den durchschnittlichen Kosten von Unternehmen für eine Cyber-Attacken vergleicht (Schätzungen zufolge [8] sind es durchschnittlich über 360.000 Euro Folgekosten für ein deutsches Großunternehmen), ist dies betriebswirtschaftlich mittlerweile nachvollziehbar.

Diese Folgekosten von vornherein durch hinreichende Qualitätsanforderungen an IKT-basierte Infrastrukturen, die betrieblichen Prozesse und agierende Personen wesentlich zu reduzieren, ist derzeit in der Wirtschaft, Gesellschaft und Politik noch nicht konsensfähig. Weitere Schritte zu widerstandsfähigen und sicheren Infrastrukturen sollte der ASQF kritisch und konstruktiv begleiten. ■

Referenzen: **[1]** Gesetzentwurf der Bundesregierung zum IT-Sicherheitsgesetz: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?__blob=publicationFile **[2]** Lagebericht zur IT-Sicherheit http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/bsi-lagebericht-it-sicherheit.pdf?__blob=publicationFile **[3]** BITKOM: Stellungnahme zum Entwurf des IT-Sicherheitsgesetzes http://www.bitkom.org/files/documents/Stellungnahme_BITKOM_ITSIG_final.pdf **[4]** GDD: Stellungnahme zum Entwurf des IT-Sicherheitsgesetzes https://www.gdd.de/downloads/aktuelles/stellungnahmen/GDD_Stellungnahme_IT-Sicherheitsgesetz_07.10.2014.pdf **[5]** Cyber-Sicherheitsrat: Stellungnahme zum Entwurf des IT-Sicherheitsgesetzes. http://www.cybersicherheitsrat.de/CyberSecurityCouncil//wp-content/uploads/ITSiG_Entwurf19112014_PM_CSRD_finalfinal.pdf **[6]** DIHK: Stellungnahme zum Entwurf des IT-Sicherheitsgesetzes http://www.dihk.de/themenfelder/recht-steuern/rechtspolitik/nationale-stellungnahmen/dihk-positionen-zu-nationalen-gesetzesvorhaben/dihk-stellungnahme-refentwurf-it-sicherheitsgesetz/at_download/file?mdate=1416383819168 **[7]** Lars Reppesgaard: IT-Security: Wie sich EADS schützt, Stuxnet war nur der Anfang. http://www.cio.de/a/stuxnet-war-nur-der-anfang,2272318 **[8]** Kaspersky Lab: Schäden durch Cyberangriffe gehen für deutsche Unternehmen in die Hunderttausende. http://www.kaspersky.com/de/about_kaspersky/news/business/2014/Schaden_durch_Cyberangriffe_gehen_fur_deutsche_Unternehmen_in_die_Hunderttausende