Weckruf für deutsche Großunternehmen? – Der neue Entwurf des IT-Sicherheitsgesetz 2.0

RA Dr. Alexander Golland, Düsseldorf

Der erste Entwurf des IT-Sicherheitsgesetz 2.0 hatte vor allem deshalb für Aufregung gesorgt, weil es das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur „Hackerbehörde" machen sollte. Mit dem aktuellen, Mitte Mai bekanntgewordenen zweiten Entwurf ändert sich hieran wenig: Mehr Aufgaben und Befugnisse für das BSI. Neu ist insoweit vor allem, dass das BSI künftig als nationale Behörde für Cybersicherheitszertifizierungen tätig werden kann.

Aus Unternehmenssicht sind jedoch andere Aspekte von größerer Relevanz: Mit dem ersten IT-Sicherheitsgesetz wurden die Betreiber kritischer Infrastrukturen (KRITIS) eingeführt. Mit dem nun vorgelegten Entwurf wird der Adressatenkreis der Pflichten aus dem BSIG durch die hinzugekommenen „Unternehmen im besonderen öffentlichen Interesse" (UIBÖFI) voraussichtlich erheblich erweitert.

Nach § 2 Abs. 14 BSIG-E sollen dies Unternehmen sein, deren Geschäftstätigkeit unter § 60 Abs. 1 der Außenwirtschaftsverordnung fällt oder die aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer Wertschöpfung von besonderem öffentlichen Interesse sind oder die einer Regulierung zum Schutz vor Gefahrenstoffen unterliegen. UIBÖFI sollen, ähnlich wie KRITIS, in einer gesonderten Verordnung bestimmt werden. Die tautologisch anmutende zweite Variante hat potenziell große Reichweite: Es bleibt offen, was letztlich das „besondere öffentliche Interesse" darstellt. Der Wortlaut impliziert, dass es auf die ökonomische Bedeutung ankommt. Daher liegt nah, zur Bestimmung auf (zu definierende) wirtschaftliche Schwellenwerte abzustellen, d. h. bestimmte Bilanzsummen, Umsatzerlöse und/oder Mitarbeiterzahlen. Letztlich ist nicht ausgeschlossen, dass eine Vielzahl deutscher Großunternehmen unter die UIBÖFI-VO fallen werden.

UIBÖFI haben sich künftig beim BSI zu registrieren und eine Kontaktstelle zu benennen (§ 8 b Abs. 3 b BSIG-E). Nach § 8 b Abs. 4 a und 4 b BSIG-E müssen UIBÖFI Störungen unverzüglich an das BSI melden, sofern diese Störungen zu einem Ausfall oder einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung oder aber zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung bereits geführt haben oder führen können. Nach dem neu eingeführten § 8 f BSIG-E haben UIBÖFI dem BSI ein dezidiertes IT-Sicherheitskonzept vorzulegen, welches alle zwei Jahre erneut vorgelegt werden muss.

Abseits der Novellierung des BSI-Gesetzes soll die Behörde nach einem künftigen § 13 Abs. 7 a TMG ermächtigt werden, die Umsetzung von technischen und organisatorischen Vorkehrungen gegenüber bestimmten Anbietern von Telemediendiensten anordnen zu können. Ferner sollen sämtliche Diensteanbieter bereits bei Anhaltspunkten für eine unrechtmäßige Erlangung oder Verbreitung personenbezogener Daten nach dem neuen § 13 Abs. 9 TMG den Zugang sperren und die Nutzer informieren. Im Bereich der Telemedien geht der Gesetzgeber damit in zweifacher Hinsicht über die Vorgaben von Art. 34 DSGVO hinaus, wonach eine solche Benachrichtigung nur beim tatsächlichen Data Breach und auch nur beim Bestehen hoher Risiken für Betroffene erfolgen muss.

Überdies wird der Bußgeldrahmen in § 14 BSIG-E an die DSGVO angeglichen: Geldbußen von bis zu 4 % des Vorjahresumsatzes oder 20 Mio. Euro (je nachdem, welcher Betrag höher ist) sind möglich, wenn gegen behördliche Anordnungen verstoßen wird; bei anderen Verstößen gegen das BSIG soll es immerhin die Hälfte dieser Beträge sein. Ob hierbei die Umsätze der konkreten juristischen Person maßgeblich sind oder die „single economic entity doctrine" des Kartellrechts Anwendung finden soll, ist unklar.

Klar ist hingegen: Durch die Aufnahme der Unternehmen im besonderen öffentlichen Interesse und empfindliche Bußgelder werden zusätzliche wirtschaftliche Anreize für flächendeckende Cybersecurity gesetzt. Jährlich entstehen deutschen Unternehmen Schäden von über 100 Mrd. Euro durch Defizite bei der IT-Sicherheit. Dennoch scheuen selbst Konzerne zum Teil (noch) eine übergreifende IT-Sicherheitsstrategie und agieren erst, wenn es bereits zu spät ist.

Ob das IT-Sicherheitsgesetz 2.0 nicht nur das BSI zur aktiv agierenden Behörde macht, sondern auch Unternehmen aus der Opferrolle in den „driver's seat" zwingt, bleibt abzuwarten. Entscheidend für den Erfolg des Gesetzes in Bezug auf IT-Sicherheit in Unternehmen wird die ergänzende Verordnung sein. Kritisch sind jedoch die geplanten Änderungen im TMG zu werten: Vor dem Hintergrund des abschließenden Charakters der DSGVO zeichnet sich ein Konflikt der verschiedenen Regelungsregimes bereits ab.