Linklaters

April 2016

IT-Sicherheitsgesetz: Welche neuen Pflichten gelten für Unternehmen?

Am 25. Juli 2015 ist das sog. IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – „IT-SiG“) in Kraft getreten. Das Gesetz bringt neue Pflichten für Betreiber sog. „Kritischer Infrastrukturen“, aber z.B. auch für Webseiten-Betreiber oder Telekommunikationsunternehmen. Das Bundeskabinett hat nun auch den Erlass einer Rechtsverordnung beschlossen, die Anfang Mai 2016 in Kraft treten soll.

Mit dem IT-SiG verfolgt der Gesetzgeber das Ziel, eine „signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland“ zu erreichen. Insbesondere Betreiber Kritischer Infrastrukturen (**„KRITIS“**) sollen verpflichtet werden, ein Mindestniveau an IT-Sicherheit einzuhalten. Dazu gehören die Bereiche Energieversorgung, Verkehr, Gesundheitswesen sowie Banken und Versicherungen. Eingeführt wurden ein Meldewesen und Pflichten zur Überprüfung durch die zuständigen Behörden, vor allem dem Bundesamt für die Sicherheit in der Informationstechnik (BSI). Ausfüllungsbedürftig bleibt der Begriff des „Standes der Technik“, den die Unternehmen künftig erreichen sollen.

Durch das IT-SiG wurden insgesamt acht Gesetze geändert und ergänzt, darunter u.a. das BSI-Gesetz (BSIG), das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG). Eine in Vorbereitung befindliche Rechtsverordnung soll festlegen, welche Kriterien für die Einstufung als KRITIS gelten sollen.

Hintergrund: Europäischer Rechtsrahmen

Auf europäischer Ebene haben sich Parlament, Rat und Kommission im Dezember 2015 im sog. Trilog-Verfahren auf eine europäische Richtlinie zur Netz- und Informationssicherheit geeinigt, die von den Mitgliedstaaten binnen 21 Monaten nach Inkrafttreten umzusetzen ist. Diese geht insofern über den Rahmen des IT-SiG hinaus, als dass sie auch bestimmte Anbieter digitaler Dienstleistungen erfasst (Online-Marktplätze, Suchmaschinen, Cloud Computing-Anbieter), die ebenfalls Maßnahmen anhand des Standes der Technik vorzuhalten und Sicherheitsvorfälle mit erheblichen Auswirkungen zu melden haben.

Der deutsche Gesetzgeber wird vermutlich das IT-SiG in naher Zukunft anpassen, um diese Richtlinie umzusetzen. Auch die Europäische Kommission hat sich bestimmte Rechtsetzungsbefugnisse vorbehalten.

Inhalt

Wer ist vom IT-SiG betroffen, und welche Pflichten gelten?

1. Betreiber von KRITIS

Betroffen sind zunächst Betreiber von KRITIS. KRITIS sind Einrichtungen, Anlagen oder Teile davon aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“ (§ 2 Abs. 10 BSI-Gesetz n.F.). Diese gelten nur dann als KRITIS, wenn sie bestimmte Schwellenwerte überschreiten, die per Rechtsverordnung festgelegt werden.

Beispiele: Betreiber von großen Stromversorgungs-, Abwasserbeseitigungs- und Lebensmittellageranlagen, Rechenzentrumsanbieter mit einer bestimmten Leistung, Hosting-Provider mit bestimmten Kapazitäten.

Wie werden KRITIS bestimmt?

Durch eine nunmehr beschlossene Rechtsverordnung wird festgelegt, welche Unternehmen zu den Betreibern von KRITIS zählen. Die Rechtsverordnung definiert KRITIS durch bestimmte Anlagen, die für festgelegte Dienstleistungen aus den einzelnen Sektoren benötigt werden und die als kritisch gelten, wenn sie bestimmte Schwellenwerte überschreiten.

Beispiel: Im Sektor Energie wird als eine KRITIS festgelegt z. B. eine „Speicheranlage“, die für die kritische Dienstleistung gung“ genutzt wird und den Schwellenwert einer installierten Leistung von 420 MW überschreitet.

Die Rechtsverordnung wird in zwei Abschnitten veröffentlicht. Der erste, nun beschlossene Teil der Rechtsverordnung beschränkt sich auf die Sektoren Energie, Wasser, Ernährung und Informationstechnik/Telekommunikation. Für das dritte Quartal 2016 wird der „zweite Korb“ der Rechtsverordnung erwartet, der dann die Sektoren Transport und Verkehr, Gesundheit und Finanz- und Versicherungswesen betreffen wird.

KRITIS-Betreiber haben im Wesentlichen folgende Pflichten:

- **Benennung einer jederzeit erreichbaren Kontaktstelle** gegenüber dem BSI binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung (d.h. für die Sektoren Energie, Wasser, Ernährung und Informationstechnik/Telekommunikation voraussichtlich bis Ende 3. Quartal 2016, für die anderen Sektoren voraussichtlich bis Ende 2016).
- **Unverzügliche Meldung von „erheblichen“ IT-Sicherheitsvorfällen** an das BSI, d.h. von Störungen, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der KRITIS führen können oder geführt haben.

- **Umsetzung des „Standes der Technik“** binnen zwei Jahren ab Inkrafttreten der Rechtsverordnung durch angemessene Sicherheitsmaßnahmen. Dieser Begriff nimmt eine zentrale Rolle ein.

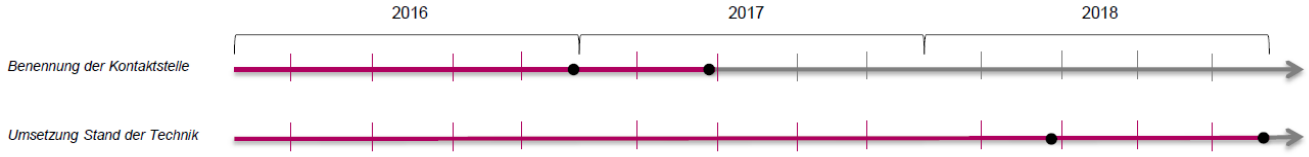
- **Nachweis der Einhaltung des Standes der Technik** alle zwei Jahre. Dies können die Verpflichteten durch Sicherheitsaudits, Prüfungen oder Zertifizierungen, etwa durch eine TÜV-Prüfung, tun.

Was ist der „Stand der Technik“?

Der Stand der Technik wird zwar in § 8a BSIG abstrakt definiert, seine genauen Parameter sind jedoch nicht gesetzlich oder per Rechtsverordnung festgelegt und auch nicht abschließend ermittelbar, sondern vielmehr dem technischen Wandel ausgesetzt. Was Stand der Technik ist, lässt sich zum Beispiel an nationalen oder internationalen Standards ablesen, wie etwa DIN oder ISO.

KRITIS-Betreiber können dem BSI branchenspezifische Sicherheitsstandards („B3S“) zur Festlegung des Standes der Technik in ihrem Bereich vorschlagen. Als Richtschnur hat das BSI eine Orientierungshilfe veröffentlicht. Dieser Orientierungshilfe lässt sich bereits entnehmen, welche Inhalte das BSI erwartet – z.B. eine Reihe von zu adressierenden Themen wie etwa Asset Management oder branchenspezifische Technik und eine Detailtiefe der Beschreibungen, die mindestens ISO/IEC 27002 entspricht.

Die folgende Abbildung zeigt die Zeitpunkte, zu denen die entsprechenden Pflichten aus dem IT-SiG umzusetzen sind. Wegen der unterschiedlichen Zeitpunkte des Inkrafttretens der zugehörigen Rechtsverordnung fallen diese jeweilige für die unterschiedlichen KRITIS-Betreiber auseinander.



2. Telemedienanbieter

Auch Telemedienanbieter, etwa von Webseiten oder Apps, treffen neue Pflichten. Sie müssen – soweit dies technisch möglich und zumutbar ist – durch technische und organisatorische Vorkehrungen den unerlaubten Zugriff auf die technischen Einrichtungen ihres Telemedienangebots verhindern und diese Einrichtungen gegen Verletzungen des Schutzes personenbezogener Daten und gegen Störungen sichern (§ 13 Abs. 7 TMG). Auch hierfür gilt der jeweilige „Stand der Technik“, womit der Gesetzgeber eine größere Rechtssicherheit und Verbindlichkeit erreichen möchte. Bestimmte Verstöße können mit Bußgeldern bis zu 50.000 Euro geahndet werden.

Welche Maßnahmen sollten Telemedienanbieter treffen?

Empfehlenswert ist es für Telemedienanbieter, wie folgt vorzugehen:

- Ermittlung vorhandener technischer und organisatorischer Einrichtungen;
- Ermittlung typischerweise eingesetzter technischer und organisatorischer Sicherheitsmaßnahmen. Hierfür können Leitfäden oder Veröffentlichungen des BSI aber auch von Verbänden dienen.
- Gap-Analyse zwischen vorhandenen technischen und organisatorischen Einrichtungen und typischerweise eingesetzten technischen und organisatorischen Einrichtungen. Vorhandene Einrichtungen sind sodann ggf. auch das Niveau typischerweise eingesetzter Einrichtungen anzuheben.

Beispiele für technische Sicherheitsmaßnahmen: Sicherheitssoftware, Firewalls, Virenerkennungsprogramme, Penetration Tests.

Beispiele für organisatorische Sicherheitsmaßnahmen: Entwicklung eines IT-Sicherheitskonzepts, Bestellung eines IT-Sicherheitsbeauftragten, Qualifikation des eingesetzten Personals.

3. Telekommunikations- und Energieversorgungsunternehmen sowie Genehmigungsinhaber nach dem Atomgesetz

Für Telekommunikations- und Energieversorgungsunternehmen sowie für Genehmigungsinhaber nach §§ 6, 7 oder 9 Atomgesetz (z.B. Kernkraftwerke, atomare Lager) gelten ähnliche Anforderungen wie für KRITIS-Betreiber: Sie müssen insbesondere die von ihnen eingesetzten Systeme und Komponenten gemäß des Stands der Technik sichern, sie unterliegen Melde- und Prüfpflichten. Allerdings gelten diese Pflichten für sie – im Unterschied zu anderen KRITIS-Betreibern – sofort. Das IT-SiG hat ihre Pflichten – etwa zur Meldung von Störungen an ihre Nutzer und zum Aufzeigen möglicher Wege zur Störungsbeseitigung – noch einmal erweitert.

Was sollten betroffene Unternehmen bereits jetzt tun?

Für Unternehmen sind folgende Schritte sinnvoll, um mögliche Pflichten aus dem IT-SiG frühzeitig zu adressieren:

- Unternehmen sollten bestimmen, ob ihr Unternehmen vom IT-SiG (möglicherweise) betroffen ist. Wenn es nicht naheliegt, dass das Unternehmen ein KRITIS-Betreiber ist, kann es z.B. neue Pflichten als Telemedienanbieter haben, weil es etwa eine Webseite betreibt.
- Unternehmen sollten ihre bisher eingesetzten IT-Sicherheitsmaßnahmen erfassen.
- Unternehmen sollten sich informieren, ob notwendige Anpassungen des IT-Sicherheitsstandards im Unternehmen notwendig sind. Dazu empfiehlt es sich beispielsweise, die Verlautbarungen des BSI zum „Stand der Technik“ in den unterschiedlichen Bereichen zu verfolgen oder sich entsprechend rechtlich beraten zu lassen. Zu beachten ist, dass bisher eingesetzte Standards wie ISO 27001 nicht zwingend auch unter dem IT-SiG als ausreichend angesehen werden.

Autoren: Dr. Daniel Pauly, Dr. Ingemar Kartheuser

Ansprechpartner

Für weitere Informationen kontaktieren Sie bitte:

Dr. Daniel Pauly
Partner, Head of TMT Practice Germany

(+49) 69 71003 570

daniel.pauly@linklaters.com

Dr. Ingemar Kartheuser
Managing Associate

(+49) 69 71003 542

ingemar.kartheuser@linklaters.com

Mainzer Landstraße 16
60325 Frankfurt am Main
Postfach 17 01 11
60075 Frankfurt am Main

Telefon (+49) 69 71003-0
Telefax (+49) 69 71003-333

Linklaters.com

Linklaters.de