IM FOKUS

Das IT-Sicherheitsgesetz – lästig oder längst überfällig?

Im August dieses Jahres wurde der zweite Referentenentwurf des IT-Sicherheitsgesetzes (ITSiG) veröffentlicht. Nach jetzigem Planungsstand soll das Gesetz Mitte 2015 verabschiedet[1] werden. Während manche mit Sorge auf die zusätzliche Regulierung blicken, werden jene „Endlich!" sagen, die sich mit den vielfältigen Gefährdungen beim Einsatz von Informationstechnik auseinandersetzen.

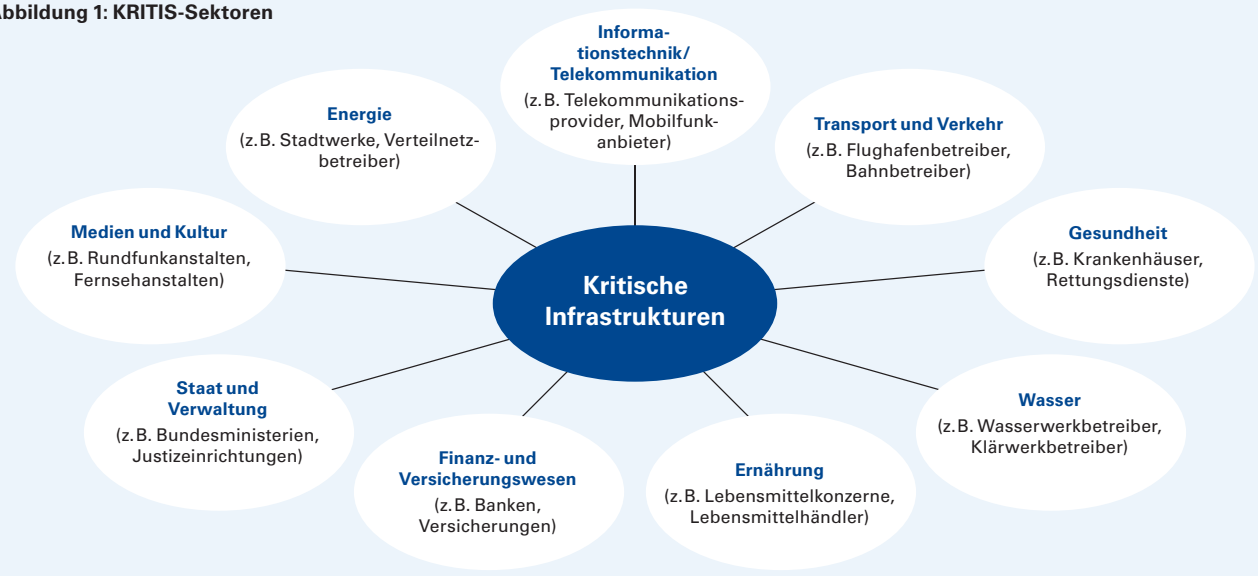
Im Grunde sind sich Wirtschaft, Verbände, Politik und öffentliche Hand einig: Eine verpflichtende Grundlage schafft in vielen Branchen die Notwendigkeit für die vielleicht längst überfälligen Detaildiskussionen zu mehr IT-Sicherheit, das heißt zum Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der datenverarbeitenden Systeme. Dass der IT-Sicherheit und deren Gefährdungen in Form von „Cyberangriffen" und Ähnlichem mehr Aufmerksamkeit geschenkt werden muss, ist unbestritten. In nahezu allen Unternehmen sowie der öffentlichen Verwaltung ist der Einsatz von IT-Komponenten nicht mehr wegzudenken. Mit der allseits diskutierten und rasant voranschreitenden Vernetzung der IT-Infrastrukturen und der Wirtschaftsakteure wird die Abhängigkeit von IT zudem weiter steigen. Es gilt also, sich besser früher als später Gedanken über die Absicherung der Verfügbarkeit der geschäftskritischen Prozesse zu machen.

Kritische Infrastrukturen im Fokus

Im Mittelpunkt stehen in diesem Kontext die Betreiber der sogenannten Kritischen Infrastrukturen (KRITIS). Der Entwurf des IT-Sicherheitsgesetzes löst jedoch noch nicht auf, wer zur Gruppe dieser „KRITIS-Betreiber" zählt. Bis zum Erlass der klärenden Rechtsverordnung zum ITSiG durch das Bundesministerium des Innern hilft deshalb nur die offizielle, aber wenig konkrete KRITIS-Definition: „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nach-

1 Der vorliegende Artikel basiert auf dem zweiten Referentenentwurf des ITSiG vom August 2014. Mit Stand November befindet sich ein dritter Entwurf in Abstimmung, der aber bis Redaktionsschluss noch nicht veröffentlicht wurde.

Abbildung 1: KRITIS-Sektoren



Quelle: KPMG AG Wirtschaftsprüfungsgesellschaft, Darstellung in Anlehnung an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

haltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."[2]

Zur besseren Ordnung werden KRITIS in Sektoren unterteilt (siehe Abbildung 1). Wie die Abbildung zeigt, betrifft der Schutz der KRITIS auch die öffentliche Verwaltung und öffentliche Unternehmen, wie beispielsweise Bundesministerien, Rundfunkanstalten und Stadtwerke.

Die bereits existierenden Aufgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) als nachgeordnete Behörde des Bundesministerium des Innern zur Unterstützung beim Schutz der Informationssysteme des Bundes werden im Entwurf des ITSiG noch einmal betont und erweitert. Die Verantwortung für die Sicherheit in den Organisationen der öffentlichen Verwaltung obliegt aber der jeweiligen Leitung.

Ein tiefer gehender Blick in die verschiedenen Branchen der KRITIS-Sektoren durch den damaligen Bundesinnenminister hat bereits 2012 gezeigt, dass der hohen Bedeutung der Infrastruktur mit sehr unterschiedlichen Niveaus der IT-Sicherheit begegnet wird. Sowohl innerhalb der einzelnen Sektoren als auch übergreifend fiel die Bilanz sehr durchwachsen aus.[3] Für die Politik ist die Konsequenz, dass es einer gemeinsamen Grundlinie und eines Bekenntnisses zur IT-Sicherheit – insbesondere zum Schutz der KRITIS – bedarf.

Was fordert der Entwurf des IT-Sicherheitsgesetzes? Auf das Wichtigste reduziert kommen drei Verpflichtungen auf Unternehmen und die öffentliche Hand[4] zu:

1. Eine Meldepflicht für Vorfälle und die Nennung von Warn- und Alarmierungskontakten an das BSI
2. Verpflichtende Mindestanforderungen an die IT-Sicherheit
3. Regelmäßige Sicherheitsüberprüfungen

Meldepflicht von IT-Sicherheitsvorfällen

Die Meldepflicht ist der erste zentrale Punkt des Gesetzentwurfs. Für deutsche Unternehmen, die Kritische Infrastrukturen betreiben oder zu deren Betrieb beitragen, hat die Meldepflicht zur Folge, dass sie alle IT-Sicherheitsvorfälle an das BSI melden müssen. KPMG hat diesen Punkt im Rahmen der Studie „IT-Sicherheit in Deutschland" analysiert[5]: Je nach Auslegung der Vorfallsdefinition kann demnach die Meldepflicht über alle Betreiber gesehen mehrere hunderttausend Meldungen im Jahr zur Folge haben. Auf Basis der vorgesehenen Meldepflichten im ersten Referentenentwurf des IT-Sicherheitsgesetzes schätzen die Studienautoren die Bürokratiekosten für die betroffenen Unternehmen auf bis zu 1,1 Milliarden Euro.

Der genaue Zeitpunkt, ab dem Unternehmen mit der Meldung beginnen sollen, ist noch nicht bekannt. Ebenso fehlt eine verlässliche Angabe, was als Vorfall gilt und gemeldet werden muss. Dies ist ein zentraler Kritikpunkt der KPMG-Studie und ein großer Unsicherheitsfaktor bei der Einschätzung der Aufwände.

Klar ist deshalb, dass dem Gesetzentwurf eine zügige Konkretisierung des „Sicherheitsvorfalls" folgen muss. Nur mit eindeutigen Kriterien zur Auswahl von Vorfällen ist es Betreibern möglich, ihr internes Monitoring und Berichtswesen so auszurichten, dass sie in wirtschaftlich angemessener Weise Meldungen vornehmen können. Aufgrund der hohen Kosten, die die Administration und das Melden von Vorfällen für die Unternehmen mit sich bringen, sollte die Meldepflicht auf bedeutende und vor allem tatsächlich durch das BSI verwertbare Vorfälle begrenzt sein.

Davon unberührt ist die Frage der Sensibilität der Sicherheitsvorfälle. Im Allgemeinen werden Sicherheitsprobleme ungern nach außen getragen. Als eine Empfehlung hat KPMG in der Studie die Einrichtung eines Treuhänders als zwischengeschaltete Instanz vorgeschlagen. Auf diesen Vorschlag geht der zweite Entwurf mit dem „gemeinsamen Ansprechpartner" ein. Er ermöglicht zumindest Unternehmen eines Sektors, weniger kritische Vorfälle anonym zu melden.

Dieser Punkt ist gerade im Hinblick auf das implizite Ziel des ITSiG wichtig: Das IT-Krisenmanagement des BSI soll mithilfe der gesammelten Informationen die zentrale Stelle zur Überwachung der Bedrohungslage und zur Unterstützung einer koordinierten Reaktion auf Vorfälle sein. Diese Aufgabe gelingt nur, wenn Betreiber Sicherheitsprobleme ohne Sorge vor Reputationsschäden melden können.

Benennung von Ansprechpartnern

Neben der Meldepflicht sind dem BSI innerhalb von sechs Monaten nach Inkrafttreten der Rechtsverordnung auch Melde- und Alarmierungskontakte mitzuteilen. Der Betreiber muss sicherstellen, dass in Fällen, in denen die Versorgungssicherheit gefährdet ist (Warnungen, Notfallsituationen), jederzeit ein qualifizierter Ansprechpartner für das BSI oder andere öffentliche Institutionen verfügbar ist. Die Benennung geeigneter Ansprechpartner wird den Betreibern unterschiedlich leicht- oder schwerfallen. Wer bereits heute formell den Austausch mit dem BSI sucht (beispielsweise im Rahmen der Allianz für Cyber-Sicherheit[6]), wird einen internen Ansprechpartner schon festgelegt haben. In der Regel sind dies der für IT-Sicherheit zuständige Mitarbeiter bzw. die für diesen Bereich zuständigen Mitarbeiter.

Verpflichtende Mindestanforderungen

Der zweite wesentliche Punkt des Gesetzentwurfs sind die verpflichtenden

2 Bundesamt für Sicherheit in der Informationstechnik

3 Rogall-Grothe, C. (2012): „Die Gewährleistung von IT-Sicherheit ist eine der zentralen Herausforderungen unserer Zeit". Unter: www.bmi.bund.de

4 Vom Gesetz grundsätzlich ausgenommen sind lediglich Kleinstunternehmen mit weniger als zehn Mitarbeitern. Darunter fallen gemäß der im Gesetzentwurf zitierten EG-Empfehlung (2003/361/EG) jedoch keine Unternehmen, die zu 25 Prozent oder mehr in öffentlicher Hand sind.

5 KPMG AG Wirtschaftsprüfungsgesellschaft (Hrsg.) (2014): IT-Sicherheit in Deutschland – Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes. Abrufbar unter http://www.kpmg.com/de/de/new/seiten/kpmg-it-sicherheit-in-deutschland.pdf

6 Die Allianz für Cyber-Sicherheit ist eine Initiative des BSI, die in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) zum Informations- und Erfahrungsaustausch über das Thema Cybersicherheit gegründet wurde.

Mindestanforderungen an die IT-Sicherheit der Unternehmen. Konkret soll ein Informationssicherheits-Managementsystem (ISMS) zur Vorgabe werden, das dafür sorgt, dass die für die Branche und die eingesetzten Technologien empfohlenen Sicherheitsmaßnahmen berücksichtigt werden. Zum ISMS sollen auch Maßnahmen zur Angriffsprävention und -erkennung sowie zum Notfallmanagement implementiert werden.

Nach jetzigem Stand muss nach unserer Interpretation binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung mindestens ein ISMS implementiert sein. Im Gesetzentwurf wird nicht festgelegt, ob der Aufbau des Managementsystems auf Basis des internationalen IT-Sicherheitsstandards ISO/IEC 27001 oder des nationalen Pendants, dem IT-Grundschutz des BSI, zu erfolgen hat. Während die Anforderungen der ISO-Norm eher abstrakter für unterschiedlichste Unternehmenstypen formuliert sind, geht „der Grundschutz" über konkrete Handlungsmaßnahmen mehr ins Detail. Eine verpflichtende Vorgabe wäre hier aber hinderlich, unter anderem, weil viele international aufgestellte Unternehmen bereits nach internationalem Standard arbeiten oder zertifiziert sind.

Der Gesetzentwurf legt Wert darauf, dass aus allgemein gehaltenen IT-Sicherheitsstandards branchenspezifische Ableitungen im Sinne eigener Mindeststandards entstehen. Damit soll den Besonderheiten einer jeden Branche mit praxistauglichen Maßnahmen Rechnung getragen werden. Ein Beispiel für einen branchenspezifischen Sicherheitsstandard ist die ISO/IEC TR 27019, die Leitlinien für ein ISMS für Prozessleitsysteme und Automatisierungstechnik in der Energieversorgung enthält.

Die Entwicklung der branchenspezifischen Sicherheitsstandards obliegt den Betreibern der KRITIS und ihren Branchenverbänden. Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), der Deutsche Verein des Gas- und Wasserfaches (DVGW) oder die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) haben bereits in der Vergangenheit zahlreiche Empfehlungen zur IT-Sicherheit erarbeitet. Es bietet sich an, die Kräfte und Kompetenzen zur Erstellung eines zentralen Sicherheitsstandards über die etablierten Arbeitskreise zu bündeln.

In Anbetracht einer voraussichtlichen Frist von zwei Jahren nach Verabschiedung der Rechtsverordnung ist bei der Umsetzung verbindlicher Mindeststandards Eile geboten. Die Entwicklung branchenspezifischer Sicherheitsstandards und deren Umsetzung sind durchaus herausfordernd und umfangreich.

Regelmäßige Sicherheitsüberprüfungen

Auf jede Vorgabe, in diesem Fall jene des Mindeststandards, muss eine Kontrolle der Umsetzung folgen. So schreibt der Gesetzentwurf als dritte wesentliche Verpflichtung vor, dass regelmäßig im Abstand von maximal zwei Jahren externe Audits zur Überprüfung der Sicherheitsstandards durchgeführt werden müssen. Die Ausgestaltung der Audit-Anforderungen wird bewusst nicht über das Gesetz vorgenommen, sondern soll sich an den branchenspezifischen Mindeststandards und bereits etablierten Auditierungs- und Zertifizierungssystemen ausrichten.

Letztlich müssen die Betreiber die Erfüllung der Anforderungen aus den noch zu erarbeitenden Mindeststandards gegenüber dem BSI nachweisen. Die Ergebnisse der durchgeführten Sicherheitsaudits, Prüfungen und Zertifizierungen mitsamt der dabei entdeckten Sicherheitsmängel sind dem BSI zur Einsicht auszuhändigen. Das BSI erhält mit dem Gesetz die Möglichkeit, auf Sicherheitsmängel mit weitergehenden Ermittlungen zu reagieren und die unverzügliche Beseitigung zu verlangen.

Herausforderung und Chance

Das ITSiG bringt also einige Herausforderungen für Unternehmen und die öffentliche Hand mit sich. Für alle betroffenen Organisationen wird die dem Gesetz noch folgende Rechtsverordnung Klarheit darüber bringen müssen, wie die Anforderungen konkret umgesetzt werden sollen. Auch wenn der zweite Entwurf des IT-Sicherheitsgesetzes der anfänglich harschen Kritik in einigen Punkten optimiert gegenübertritt, bleiben weiterhin Zweifel an der Effektivität und Effizienz des Gesetzes. Es gibt nach wie vor Stimmen, die behaupten, dass der Nutzen in keinem Verhältnis zu den tatsächlichen Aufwänden steht. Der Gesetzgeber bewertet die Aufwände zur Umsetzung des Gesetzes jedoch wie folgt: Angesichts der möglichen Schäden sei der Aufwand erträglich.[7] Je nachdem, welche IT-Sicherheitsphilosophie in der betroffenen Organisation herrscht, werden die Anforderungen aus unserer Sicht vielleicht schon heute zu großen Teilen erfüllt sein.

Um auf die Zweifler einzugehen und eine effektive Umsetzung der Vorgaben zu ermöglichen, sollten Politik und Verwaltung konstruktive Entwicklungen initiieren und fördern, statt durch Überregulierung Bürokratiekosten zu generieren und Innovationen zu bremsen. Ein regelmäßiger und tief greifender Austausch in den bereits vorhandenen öffentlich-privaten Kooperationsinitiativen, wie zum Beispiel dem UP KRITIS oder der Allianz für Cyber-Sicherheit, wird das Thema IT-Sicherheit in Deutschland weiter stärken.

Einen großen Verdienst hat das IT-Sicherheitsgesetz, trotz einiger Unklarheiten und Unsicherheiten, bereits jetzt erbracht. Seit über den Entwurf diskutiert wird, hat sich das Bewusstsein für IT-Sicherheit in Deutschland spürbar erhöht.

Die Diskussion um das IT-Sicherheitsgesetz ist keinesfalls eine lästige Debatte, sondern Teil einer längst überfälligen Initiative für mehr IT-Sicherheit in Deutschland.

Wilhelm Dolle, Torsten Redlich, Jan Tiedemann

7 Spiegel Online (2014): Cyberangriffe auf Unternehmen – De Maizière präsentiert Entwurf für IT-Sicherheitsgesetz, 19.8.2014. Unter www.spiegel.de