IT-Sicherheitsgesetz:

Derzeit nicht viel mehr als eine Sammlung von Gummiparagraphen.

Seit Ende Juli ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in Kraft getreten, kurz „IT-Sicherheitsgesetz“. Damit sind zahlreiche Diskussionen einhergegangen, die den Sinn oder Unsinn dieses Gesetzes betreffen. Für betroffene Unternehmen sind aber die größtenteils noch zu klärenden Details zur Umsetzung und Ausführung unter Umständen noch von beträchtlicher Sprengkraft.

Das IT-Sicherheitsgesetz betrifft zunächst vor allem sogenannte kritische Infrastrukturen. Darunter fallen nach der Definition des federführenden Bundesministeriums des Innern (BMI) sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI)und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) alle Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Im Einzelnen sind das Energieversorger, Einrichtungen des Gesundheitswesens, des Finanzwesens, staatliche Einrichtungen, kulturelle Werte usw. (siehe Kasten). Genaueres muss jedoch erst noch im Rahmen von Rechtsverordnungen gemäß § 10 Absatz 1, BSI-Gesetz, bestimmt werden. Sicher ist aber, dass auf alle betroffenen Unternehmen erhebliche Aufwände und bisher völlig unklare Folgen zukommen.

Zwar ist das Gesetz entgegen ursprünglicher Referentenentwürfe schon deutlich entschärft worden, aber immer bleiben zahlreiche Fragen offen. So war ursprünglich definiert, dass jeder Angriff auf kritische Infrastrukturen dokumentiert

Das Bundesministerium des Inneren gliedert kritische Infrastrukturen in neun Sektoren:

1. Energie: Elektrizität, Gas, Mineralöl
2. Informationstechnik und Telekommunikation: Telekommunikation, Informationstechnik
3. Transport und Verkehr: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
4. Gesundheit: Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
5. Wasser: Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung
6. Ernährung: Ernährungswirtschaft, Lebensmittelhandel
7. Finanz- und Versicherungswesen: Banken, Börsen, Versicherungen, Finanzdienstleister
8. Staat und Verwaltung: Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich Katastrophenschutz
9. Medien und Kultur: Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke

und an das BSI gemeldet werden müsse – unabhängig vom Erfolg oder Misserfolg des Angriffs. Damit hätte ein für Hacker mittelmäßig interessantes Unternehmen aber locker einige Hundert, wenn nicht gar tausend Angriffe pro Tag, ja vielleicht sogar in einer Minute melden müssen. Denn ein „Angriff" besteht ja beispielsweise schon aus dem automatisiert erfolgenden Abfragen von offenen Ports, von empfangsbereiten Mail-Servern, dem Versenden von Pishing-Mails oder Spam.

Nun ist das schon deutlich genauer definiert und hinsichtlich des resultierenden Aufwands entschärft worden. Es heißt nämlich in §8b, Absatz 4, BSI-Gesetz „Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. führen können oder

2. geführt haben,

über die Kontaktstelle unverzüglich an das Bundesamt zu melden."

Auch diese Formulierung lässt natürlich noch hinreichend Spielraum für Interpretationen, aber zumindest ist mit dem Wort „wesentlich" prinzipiell schon eine dramatische Reduzierung des entstehenden Aufwands zu erwarten. Dennoch müsste dann beispielsweise auch der Ausfall einer Klimaanlage, ein herannahendes Gewitter oder eine Häufung von Grippefällen in der Urlaubszeit gemeldet werden, denn damit könnte die Verfügbarkeit von Infrastrukturen zweifelsohne beeinträchtigt werden. Darüber hinaus fußt das Kriterium für eine Meldepflicht vor allem auf der Größenordnung des Schadens, der hätte auftreten können, also dem potenziellen Schaden. Damit lässt sich ebenfalls wieder eine Reihe von Beispielen finden, die aus forensischer Sicht völlig irrelevant sind, aber aufgrund ihres fiktiven Schadens dennoch gemeldet werden müssen.

Das Gesetz erwartet aber glücklicherweise auch Vorschläge von den Betreibern Kritischer Infrastrukturen und deren Branchenverbänden, wie Sicherheitsstandards einzuhalten sind. Damit ist sicherlich die Hoffnung verbunden, auf Arbeitsebene geeignete Verfahren zu entwickeln, die hier zu einer sinnvollen Struktur führen und nicht zu einer übermäßigen Verwaltungsschlacht. Zudem sind kleinere oder mittlere Betriebe ausgenommen, deren Größe in keinem Verhältnis zum Aufwand steht. Für große Unternehmen wird die Herausforderung aber bleiben, den bisher auf Gefahrenabwehr liegenden Fokus ein wenig mehr in Richtung Gefahrenanalyse zu bewegen. Denn erfahrungsgemäß sind erfolgreich abgewehrt Angriffe von außen und insbesondere deren Dokumentation oder gar forensischen Analyse kaum im Interesse (bzw. im Budget) der Security-Officer. Insofern ist hier indirekt eine gesetzliche Anforderung geschaffen worden, die bisher z.B. nur bei Zertifizierungen nach ISO 27001 zwingend erforderlich war: Ein Chief Information Security Officer, der Informationen über sicherheitsrelevante Vorfälle im Unternehmen sammelt, bewertet und ggf. auch untersucht.

Voraussetzung für diesen gesetzlichen Druck ist aber die Einstufung eines Unternehmens bzw. deren Infrastruktur in die Gruppe der KRITIS-Betreiber. Darüber entscheiden diverse Bundesministerien einvernehmlich. Wissenschaft, betroffenen Firmen oder deren Verbandsvertreter werden hingegen nur noch „angehört". Insofern bestehen für die Unternehmen nur noch wenige Einflussmöglichkeiten bei der Frage, ob sie überhaupt zum erlauchten Kreis der KRITIS-Betreiber gehören. Zwar sind ein großer Kreis und damit auch ein hohes Maß an Gefahrenmeldungen hinsichtlich einer erfolgreichen

Analyse sicherlich von Vorteil. Auf der anderen Seite muss man sich aber die Frage stellen, wie das BSI die bei einem großflächigen Angriff die dann resultierende Flut von Meldungen noch sinnvoll bearbeiten können will. Aber das ist dann ein anderes Problem.

Formlos, Fristlos, Fruchtlos

Selbstverständlich haben sich die Autoren des IT-Sicherheitsgesetztes bereits Gedanken darüber macht, welche Druckmittel zur Verfügung stehen, um die Betreiber kritischer Infrastrukturen zu einer fruchtbaren Zusammenarbeit zu bewegen. Dabei ist sicherlich deutlich geworden, wie schwer eine Strafbewehrung im Zusammenhang mit IT-Sicherheit generell ist. Gleichzeitig bestehen hinsichtlich verpflichtender Meldungen von Sicherheitsvorfällen natürlich auch immer Datenschutz-relevante Bedenken. Und bei diesem Spagat zwischen Zwang, Aufwand und Sinn einer Vorschrift ist dann möglicherweise auch dieses Gesetz noch nicht ganz ausgegoren. So dürfen beispielsweise geringfügige Störungen anonym gemeldet werden. Fraglich nur, wie dann noch ermittelt werden soll, wer seiner Meldepflicht überhaupt nachgekommen ist.

Aus technischer Sicht zeugen die Formulierungen des Gesetzes offenbar eher von dem Gedanken, dass ein großangelegter Cyber-Angriff auf breiter Front oder einzelne Großrechner erfolgt. Dann wären statistische Werte und eine große Datenbasis zur Analyse vielleicht von Vorteil, aber was passiert dann? Verfügt das BSI wie einst große Armeen im kalten Krieg über Reservisten, die im Ernstfall dann in kürzester Zeit aktiviert und in die Abwehrschlacht geworfen werden könnten? Wohl kaum. Es bleibt also zu befürchten, dass die im IT-Sicherheitsgesetz verankerten Meldepflichten zu einem gewaltigen bürokratischen Moloch führen, im Ernstfall aber keine wirkliche Hilfestellung für Unternehmen bieten – schon gar nicht kurzfristig und wirkungsvoll.

Hinzu kommt, dass professionelle Angriffsszenarien - derzeit jedenfalls - eben nicht den Horror-Szenarien eines klassischen Angriffskriegs auf breiter Front folgen, sondern eher still und leise vorgehen. Das höchste Gut ist, möglichst lange unerkannt zu bleiben und vielfältig redundant vorzugehen. Diese Taktik richtet viel größeren Schaden an, sofern das im unmittelbaren Interesse des Initiators steht. Beispiele dafür sind Schadprogramme, die erst zu einem bestimmten Zeitpunkt, also beispielsweise Freitag, den 13. zuschlagen oder auf einen Schlag zig Millionen Online-Zahlungen auf ein anderes Konto umleiten, bis überhaupt jemand in der Lage ist, alles abzuschalten.

Auch Nachrichtendienste sind vor allem daran interessiert, diese Taktik möglichst erfolgreich umzusetzen, da sie auf diese Weise vielleicht nicht auf breiter Front, dafür aber kontinuierlich Daten absaugen können, ohne dass dieser Abfluss überhaupt bemerkt wird. Selbst wenn er dann bemerkt wird, dauert es nicht selten Wochen und Monate, bis alle Ursachen beseitig sind, da es längst eine epidemische Verbreitung der Schadsoftware gegeben hat, wie einmal mehr das Beispiel des infizierten Bundestags zeigt.

Bis also Schäden gemeldet, Statistiken ausgewertet, Gegenmaßnahmen gefunden und erfolgreich eingeleitet worden sind, ist es längst zu spät. Zudem verfügt das BSI nicht über Mittel und Wege, ähnlich wie die Polizei bei Gefahr im Verzug zu handeln, jedenfalls nicht außerhalb von Bundesbehörden. Schwer vorstellbar, was daraufhin passieren müsste, wenn Gefahrensituationen vielleicht noch rechtzeitig erkannt werden und vielleicht sogar Gegenmaßnahmen zur Verfügung stehen, aber die wirtschaftlichen Interessen eines Multi-Nationalen-Konzerns den eilig

ausgesprochenen Empfehlungen einer deutschen Behörde wie dem BSI völlig konträr gegenüber stehen.

Insofern ist das IT-Sicherheitsgesetz eher auf Dinosaurier ausgerichtet als auf moderne Methoden professioneller Cyber-Kriminalität mit ausgefeilten Verschleierungsmethoden und Tarntechnologien. Für Unternehmen müssen daher weiterhin eigene, effektive Schutzmaßnahmen im Fokus stehen, während der aufgrund des IT-Sicherheitsgesetztes zu erwartende Verwaltungsaufwand für die KRITIS-Betreiber auf das tatsächlich unvermeidbare Mindestmaß reduziert werden sollte.

Technische Sicherheitsmaßnahmen effektiv verbessern

Aller Erfahrung nach sind die technischen Sicherheitsmaßnahmen auch von Betreibern kritischer Infrastrukturen nur selten auf dem aktuellen Stand der Technik. Viel zu sehr steht hier noch die Abwehr von Gefahren an der Schnittstelle zwischen öffentlichen und eigenen Netzen im Vordergrund. Das kann aber aufgrund der heutigen Bedrohungslage auch nur noch Gefahren abwehren, die ins Reich der Dinosaurier gehören. Denn die Bedrohungslage hat sich längst insofern geändert, dass vom Vorhandensein einer Bedrohung im eigenen Netz grundsätzlich ausgegangen werden muss.

Für viele Sicherheitsexperten ist das zweifelsohne keine neue Erkenntnis, aber wie sehr die Erkennung von Anomalien und deren Beseitigung hinter dem Stand der Technik zurück sind, zeigt einmal mehr das Beispiel des Bundestags. Dabei sind leistungsfähige Systeme zur Anomalie-Erkennung seit Jahren auf dem Markt. Hier erheben aber nicht selten Datenschützer Einsprüche, da die Grenze zur Überwachung sehr schnell erreicht wird. Im Fall des Bundestags mag das ein Grund für die späte Entdeckung und die verheerenden Folgen gewesen sein.

Aber auch ohne eine ausgefeilte Anomalie-Erkennung bieten u.a. Zoning-Konzepte, Data Loss Prevention etc. zusätzliche Sicherheit. Leider sind solche Lösungen und Systeme aber auch mit erheblichem Pflegeaufwand verbunden und nicht selten gehen damit Einschränkungen der Nutzer oder des Nutzungskomforts einher. Dementsprechend muss hier regelmäßig zwischen Sicherheit, Kosten und Nutzbarkeit abgewogen werden. Beispiele, wo diese Abwägung nicht selten schief zu laufen scheint, gibt es viele. So ist unter anderem der vergleichsweise sorglose Umgang mit immer leistungsfähigeren Smartphones, Tablets und sonstigen zumeist mobilen Geräten im Firmennetz erstaunlich oft anzutreffen. Selbstverständlich soll der Nutzer damit möglichst komfortabel auf Ressourcen des Unternehmens überall und jederzeit zugreifen können, aber in aller Regel tut er das so dermaßen ungeschützt, dass es fast überall an grobe Fahrlässig grenzt. Dabei sind hier effektive Schutzmaßnahmen längst günstig zu bekommen.

Fragwürdig, warum hier nicht schon sehr mehr Haftungsprozesse gegen allzu sorglose IT-Leiter, CIO oder Vorstände laufen, die solche Dinge seit Jahren ignoriert und erhebliche Schäden durch Unterlassung verursacht haben. Das IT-Sicherheitsgesetz könnte hier indirekt für mehr Sensibilität sorgen, weil sich glimpflich verlaufene Sicherheitslücken etwas weniger gut verschweigen lassen als bisher. Ob das aber wirklich zu einem Umdenken führt muss sich erst noch zeigen.

Ohne organisatorische Maßnahmen geht es nicht

Ein anderes, auf den ersten Blick nicht so sehr technisches Beispiel für dringend erforderliche Sicherheitsmaßnahmen in Unternehmen ist die Einführung eines Information Security Management

System (ISMS) oder „Managementsysteme für Informationssicherheit“ wie es u.a. beim BSI heißt, also eine Sammlung von Prozessen und Regeln, die Informationssicherheit nachhaltig definieren, steuern, kontrollieren, aufrechtzuerhalten und kontinuierlich verbessern. Diese Maßnahmen sind seit Jahren zumindest generisch bei ISO 27001 definiert. Das BSI hat sich ebenfalls vor Jahren bereits technische Umsetzungsaspekte definiert und immer wieder überarbeitet. Aber weder das IT-Sicherheitsgesetz noch eine andere Rechtsgrundlage zwingt die Unternehmen bisher, eine solche Lösung generell einzuführen.

Eine Ausnahme bildet da die Bundesnetzagentur (BNetzA). Sie hat im August 2015 einen für Energieversorger verbindlichen Sicherheitskatalog veröffentlicht. Dieser Katalog enthält Mindeststandards zum Schutz gegen Bedrohungen der für einen sicheren Energienetzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme. Die Unternehmen müssen dazu z.T. erhebliche Melde- und Kontrollpflichten einhalten, ihren Schutzbedarf ermitteln, einen Sicherheitsbeauftragten benennen und vor allem ein Informationssicherheits-Management-System (ISMS) nach ISO 27001 unter Berücksichtigung der branchenspezifischen Ergänzung durch die ISO 27019 einführen. Allein die einmaligen Projektkosten für die Implementierung eines ISMS belaufen sich für kleinere Unternehmen nach Schätzungen aber auf mindestens 500.000 Euro. Betriebs- und Verwaltungskosten, z.B. aufgrund von erweiterten Meldepflichten sind dabei noch nicht berücksichtigt.

Gemäß EnWG §11 Absatz 1a ist dieser Katalog verbindlich. Weitere Sicherheitsvorgaben wie ein IT-Sicherheitskatalog für Energieanlagenbetreiber (§11 Abs. 1b EnWG) werden folgen. Von den Vorschriften sind alle Energienetz- und -anlagenbetreiber betroffen. Lediglich Anlagenbetreiber mit weniger als zehn Mitarbeitern und weniger als zwei Millionen Euro Jahresumsatz können hoffen, nicht als Betreiber kritischer Infrastruktur betrachtet zu werden, so dass bis zu 15.000 Unternehmen allein im Energie-Sektor betroffen sind. Nur die wenigsten Unternehmen verfügen heute aber schon über ein zertifiziertes ISMS. So gab es 2013 lt. einer ISO-Umfrage in Deutschland lediglich 581 ISO 27001 zertifizierte Unternehmen über alle Branchen hinweg.

Selbst Unternehmen mit Zertifikat müssen jedoch erheblichen Aufwand in Kauf nehmen, da 2013 die bisherige ISO 27001:2005 durch ISO 27001:2013 ersetzt wurde. Dabei haben sich zahlreiche Änderungen ergeben, die im Vergleich zu einer regulären Re-Zertifizierung eine wesentlich umfangreichere Prüfung nach sich ziehen. Das führt erfahrungsgemäß zu Einführungs- und Umstellungszeiten von bis zu 18 Monaten und mehr. Hinzu kommt, dass ISMS mindestens sechs Monate betrieben worden sein muss, um für eine mögliche Zertifizierungsprüfung ausreichende Nachweise der Effektivität und Wirksamkeit erbringen zu können. Grundsätzlich sollte deshalb mit mindestens anderthalb Jahren für die Einführung eines ISMS gerechnet werden. Für Energieversorger ist die Deadline jedoch bereits auf den 31.01.2018 festgelegt. Bis dahin muss gegenüber der BNetzA eine entsprechende Umsetzung nachgewiesen sein.

Die Einführung eines ISMS bedeutet für die allermeisten Energieversorger jedoch eine erhebliche Investition. Zunächst gehören dazu Maßnahmen wie die Einführung eines IT-Sicherheitsbeauftragten, der unter anderem auch Kontaktpunkt bei der Meldung von Sicherheitsvorfällen gemäß IT-Sicherheitsgesetz ist. Diese Maßnahme ist vielleicht noch relativ schnell mit einer personellen Ressource und einigen Schulungen erledigt. Als nächstes stellt sich dann aber die Frage nach dem Geltungsbereich eines ISMS, denn die Energieversorger bestehen in der Regel aus mehreren Gesellschaften mit unterschiedlichen Regularien. Erbringt beispielsweise die Holding IT-

Dienstleistungen für den Energieversorger als Tochterunternehmen, muss die Holding in den Geltungsbereich einbezogen werden. Darüber hinaus sind dann bestehende IT-Security-Maßnahmen auf ihre Eignung hin zu validieren, ggf. Anpassungen vorzunehmen und vieles andere mehr. Im Extremfall muss dazu jede einzelne Komponente des Energieversorgungsnetzes einbezogen werden, also beispielsweise auch die einzelne Trafostation auf dem Lande. Letzten Endes müssen diese Betrachtung in steter Regelmäßigkeit immer wieder durchgeführt und alle zwei Jahre zertifiziert werden.

Hinsichtlich des IT-Sicherheitsgesetztes bleiben aber noch weitere Risiken, auch für die Energieversorger. So ist beispielsweise noch nicht geklärt, wie und in welcher Form die Meldungen an das BSI erfolgen müssen. Auch hier sind konkrete Regelungen noch offen. Dennoch könnte der Katalog der BNetzA auch als Grundlage für die neben den Energieversorgern existierenden acht anderen Sektoren (siehe Kasten) mit kritischen Infrastrukturen herangezogen werden. Damit ergäben sich sehr schnell für mehr als die hier und da kolportierten maximal 2.000 Unternehmen der KRITIS-Kategorie auch noch für andere Unternehmen erhebliche Anforderungen an die IT-Sicherheit.

Fazit

Grundsätzlich stellt das IT-Sicherheitsgesetz zum zur Stunde nur eine ziemlich unkonkrete Rahmengesetzgebung für IT-Sicherheitsmaßnahmen in Unternehmen dar. Die Sprengkraft liegt aber in der Ausgestaltung einzelner Vorschriften und Verfahren. Diese Ausgestaltung ist weit unterhalb von Gesetzeskraft, daher aber auch nicht langwierigen, öffentlichen und kontroversen Diskussion ausgesetzt, sondern sehr viel schneller eingeführt als manches Mal befürchtet. Es gibt zahlreiche Beispiele dafür, wie eine solche Ausgestaltung zu erheblichen Betriebs- und Verwaltungsaufwänden führt. Eines davon sind die nach die zahlreichen Vorschriften und Maßnahmen, die im Bankensektor schon weit vor der Lehman-Pleite eingeführt und regelmäßig massiven Verschärfungen unterworfen worden sind. Insofern ist vor der - auf den ersten Blick vielleicht naheliegenden - Fehleinschätzung des IT-Sicherheitsgesetztes zu warnen, dass es sich hierbei nur um ein paar Gummiparagrafen handelt.

Das Beispiel der BNetzA zeigt zudem, dass auch mit sehr kurzen Fristen zur Einführung neuer Sicherheitsstandards bzw. deren Zertifizierung zu rechnen ist. Es ist daher dringend eine frühzeitige und umfassende Betrachtung entsprechender Maßnahmen zu empfehlen. Insbesondere ist – sofern noch nicht etabliert - die Einführung eines IT-Sicherheitsverantwortlichen zu empfehlen, der diese Aufgabe gesamtverantwortlich und an hervorgehobener Stelle übernimmt. Im nächsten Schritt sind dann alle organisatorischen Maßnahmen und Prozesse auf ihre Sicherheitsrelevanz hin zu untersuchen und ggf. anzupassen. Aus technischer Sicht kommen weitere Maßnahmen hinzu, die erst zusammen mit den organisatorischen Maßnahmen zu einem Gesamtpaket werden, das die IT-Sicherheit eines Unternehmens nachhaltig nach vorne bringt. Billig wird das nicht. Für kein Unternehmen. Umso wichtiger ist hier eine strukturierte und zielgerichtete Herangehensweise anstelle von Schnellschüssen, Insellösungen oder Provisorien. Nur so werden die aus dem IT-Sicherheitsgesetz resultierenden Anforderungen - ganz nebenbei - größtenteils und dauerhaft erfüllt.