Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

Das Gesetz sieht Regelungen zum Schutz der Bundesverwaltung, der Kritischen Infrastrukturen und weiterer Unternehmen im besonderen öffentlichen Interesse sowie zum Verbraucherschutz vor.

Kernpunkte des Gesetzesvorhabens

Stärkung des BSI

Das BSI wird befugt, Kontroll- und Prüfbefugnisse gegenüber der Bundesverwaltung auszuüben. Bei wesentlichen Digitalisierungsvorhaben des Bundes soll das BSI frühzeitig beteiligt werden. Zudem wird die mögliche Dauer zur Speicherung von Protokolldaten zum Zwecke der Abwehr von Gefahren für die Kommunikationstechnik des Bundes auf 12 Monate verlängert. Protokollierungsdaten werden neu in das BSI-Gesetz aufgenommen und das BSI wird befugt, diese Daten zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes zu verarbeiten.

Das BSI wird befugt, Sicherheitslücken an den Schnittstellen bestimmter informationstechnischer Systeme zu öffentlichen Telekommunikations-Netzen zu detektieren (Portscans) sowie Systeme und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden einzusetzen (Honeypots). Das BSI kann zudem Maßnahmen gegenüber Telekommunikations- und Telemedienunternehmen bei bestimmten Gefahren für die Informationssicherheit anordnen.

Auswirkung auf die Krankenhäuser:

Der Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse wird dringlich notwendig, da im Gesundheitswesen die Patientendaten den höchsten Schutzbedarf haben. Es werden dafür entsprechende Ressourcen (Zeit, Personal, Wissen, Technik etc.) benötigt. Aus Sicht des Verbandes lässt sich das nur sinnvoll durch Providerservicemodelle lösen. Die kritischen Netze z.B. Haustechniknetze oder Medizintechniknetze sollten selbstständig und mit Vorankündigung getestet werden. Den Behörden sollte wegen der Patientensicherheit der Zugang verwehrt, jedoch das Ergebnis in geeigneter Form zur Verfügung gestellt werden.

Stärkung des Verbraucherschutzes

Der Verbraucherschutz wird in den Aufgabenkatalog des BSI aufgenommen. Die Grundlage für ein einheitliches IT-Sicherheitskennzeichen wird eingeführt, das die IT-Sicherheitsfunktionen insbesondere von Produkten im Verbrauchersegment erstmals für Bürgerinnen und Bürger sichtbar und nachvollziehbar macht. Zum Schutz von Betroffenen und zum Zweck ihrer Benachrichtigung wird das BSI befugt, bei Anbietern von Telekommunikationsdiensten Bestandsdatenauskünfte zu verlangen. Die Befugnis des BSI zur Untersuchung von IT-Produkten wird neu gefasst. Hersteller werden bei Untersuchungen von informationstechnischen Produkten und Systemen zur notwendigen Auskunft über ihre Produkte verpflichtet.

Auswirkung auf die Krankenhäuser:

Im Kern werden IT-Systeme und IT-Software beim Thema Informationssicherheit besser. Das BSI wird bei der Normung, Regulierung und Prüfung mehr mitwirken. Dadurch werden die informationstechnischen Umsetzungen weniger am Anwendernutzen ausgelegt und sicherlich an Ergonomie verlieren. Die Herausforderung liegt hierbei darin, den Anwendern die Regelungen zu

erklären, begreiflich und nachvollziehbar zu machen, damit die Anwender am Ende das Bewusstsein für Informationssicherheit erhalten. Die Einführung von Identity Access Management (IAM) -Systemen könnte das Bewusstsein und den Mehrwert von Informationssicherheit erhöhen. Die Anwender können sich in verschiedenen Anwendungen einfach anmelden, wobei das System die Passwörter automatisch wechselt. Ebenso lassen sich schützenswerte Dienste durch einen zweiten Faktor (z.B. App auf dem Smartphone, RFID-Chip) schützen.

Stärkung der unternehmerischen Vorsorgepflichten

Betreiber Kritischer Infrastrukturen werden verpflichtet, Systeme zur Angriffserkennung einzusetzen. Über eine Änderung im Gesetz über die Elektrizitäts- und Gasversorgung gilt diese Pflicht auch für Betreiber von Energieversorgungsnetzen und Energieanlagen.

Die bereits für Betreiber Kritischer Infrastrukturen geltenden Meldepflichten gelten künftig auch für Unternehmen, die von besonderem öffentlichen Interesse sind wie Unternehmen der Rüstungsindustrie und Verschlusssachen-IT, Unternehmen, die wegen ihrer hohen Wertschöpfung eine besondere volkswirtschaftliche Bedeutung haben sowie Unternehmen, die der Regulierung durch die Störfallverordnung unterliegen.

Auswirkung auf die Krankenhäuser:

Das Gesundheitswesen ist sicherlich von besonderem Interesse. Daher wird das Meldewesen entsprechende Ressourcen (Zeit, Personal, Wissen, Technik etc.) benötigen. Aus Sicht des Verbandes benötigt ein gutes Meldewesen als Grundlage gutes Servicemanagement, z.B. nach ITIL oder ISO 270XX, welches alle Informationen sammelt und nach entsprechenden Regeln notwendige Entscheidungen ableitet oder empfiehlt.

Stärkung der staatlichen Schutzfunktion

Das Gesetz enthält eine Regelung zur Untersagung des Einsatzes kritischer Komponenten, für die eine Zertifizierungspflicht besteht. Zudem werden die Bußgeldvorschriften neu gefasst. Im Telekommunikationsgesetz wird erstmals eine Zertifizierungspflicht für kritische Komponenten in Telekommunikationsnetzen eingefügt.

Die Änderung der Außenwirtschaftsverordnung trägt der Einführung der kritischen Komponenten im BSI-Gesetz Rechnung.

Auswirkung auf die Krankenhäuser.

Das Bußgeld orientiert sich in Zukunft an europäischen Rahmenbedingungen. Damit ändert sich das Strafmaß von heute 100 T€ auf mehrere Millionen €, wie bei der DSGVO.

Weiterhin kann das BSI bestimmen, dass der Einsatz bestimmter Hersteller als kritisch gesehen wird. In diesen Fall muss die Auswirkung auf die kritische Dienstleistung der medizinischen Versorgung betrachtet werden. Sicherlich empfiehlt sich in solchen Fällen ein Wechsel des Herstellers, was im Falle eines KIS erhebliche Ressourcen benötigen dürfte.

Quelle: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html

Autoren: Horst-Dieter Beha, Reimar Engelhardt, Lars Forchheim, Helmut Schlegel