WATSON FARLEY
&
WILLIAMS

BRIEFING

DAS NEUE IT-SICHERHEITSGESETZ

FEBRUAR 2016

- UNTERNEHMEN WERDEN ZUR VERBESSERUNG DER IT-SICHERHEIT VERPFLICHTET
- BEI VERSTÖßEN DROHEN BUßGELDER BIS ZU EUR 100.000

Selten hatte die Verabschiedung eines Gesetzes einen so aktuellen Bezug. Während die Gesetzesvorlage im Plenarsaal debattiert wurde, kämpften hinter den Kulissen die IT-Sicherheitsabteilung des Bundestages und das Bundesamt für Sicherheit in der Informationstechnik („**BSI**") nach einem Cyber-Angriff darum, die Kontrolle über das interne Netzwerk des Bundestages wiederzuerlangen.

Dem Bundestag ist damit genau das passiert, was das neue Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme („**IT-Sicherheitsgesetz**") verhindern will: Der Kontrollverlust über wichtige IT-Systeme.

"DEM BUNDESTAG IST GENAU DAS PASSIERT, WAS DAS NEUE IT-SICHERHEITSGESETZ VERHINDERN WILL: DER KONTROLLVERLUST ÜBER WICHTIGE IT-SYSTEME."

Insbesondere für Betreiber von Webseiten und andere Diensteanbieter, für Telekommunikationsunternehmen und für Betreiber Kritischer Infrastrukturen bringt das IT-Sicherheitsgesetz erhöhte Anforderungen mit sich.

WAS WILL DAS GESETZ ERREICHEN?

Zweck des bereits am 25. Juli 2015 in Kraft getretenen Gesetzes ist

- die signifikante **Verbesserung der IT-Sicherheit** in Deutschland im Hinblick auf deren Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität,
- die **Verbesserung der IT-Sicherheit von Unternehmen** und der verstärkte Schutz der Bürger im Internet, sowie
- der **Schutz Kritischer Infrastrukturen**, die für das Funktionieren des Gemeinwesens von zentraler Bedeutung sind.

FÜR WEN GILT DAS GESETZ?

Adressaten des neuen IT-Sicherheitsgesetzes sind insbesondere

- Betreiber von Webseiten und andere Diensteanbieter nach dem Telemediengesetz (siehe nachstehend jeweils zu A),
- Telekommunikationsunternehmen (siehe nachstehend jeweils zu B) sowie
- Betreiber Kritischer Infrastrukturen (siehe nachstehend jeweils zu C) in den Sektoren
  - Energie
  - Informationstechnik und Telekommunikation
  - Transport und Verkehr
  - Gesundheit
  - Ernährung
  - Finanz- und Versicherungswesen.

A. Betreiber von Webseiten und andere Diensteanbieter

Die durch das IT-Sicherheitsgesetz neu in das Telemediengesetz eingefügten Anforderungen gelten für alle Betreiber geschäftsmäßig angebotener Telemedien. Hierzu zählen auch alle Unternehmen, die eine eigene Webseite betreiben und zwar auch dann, wenn auf der Seite selbst keine Waren oder Dienstleistungen direkt angeboten werden, sondern auf diese nur hingewiesen wird.

B. Telekommunikationsunternehmen

Telekommunikationsunternehmen sind Anbieter die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken (zum Beispiel Internet Service Provider (ISPs) und andere Access Provider, etwa Betreiber von Fest- und Mobilfunknetzen).

"… DER AUSFALL ODER DIE BEEINTRÄCHTIGUNG KRITISCHER INFRASTRUKTUREN KANN ZU ERHEBLICHEN VERSORGUNGSENGPÄSSEN ODER GEFÄHRDUNGEN FÜR DIE ÖFFENTLICHE SICHERHEIT FÜHREN."

C. Betreiber Kritischer Infrastrukturen

Kritische Infrastrukturen im Sinne des Gesetzes sind solche, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder Gefährdungen für die öffentliche Sicherheit führen würde und die für das Funktionieren des Gemeinwesens daher von hoher Bedeutung sind.

Welche Unternehmen konkret als Betreiber Kritischer Infrastrukturen eingestuft werden, wird in einer noch zu erlassenden Rechtsverordnung im Einzelnen festgelegt. Diese Rechtsverordnung wird zurzeit im Bundesministerium des Innern vorbereitet und in zwei Teilen voraussichtlich wie folgt in Kraft treten:

- „Korb 1" für die Sektoren Energie, Informationstechnik und Telekommunikation, Ernährung und Wasser zum Ende des 1. Quartals 2016 und
- „Korb 2" für die Sektoren Finanz- und Versicherungswesen, Gesundheit, Transport und Verkehr zum Ende des Jahres 2016.

„WELCHE UNTERNEHMEN KONKRET ALS BETREIBER KRITISCHER INFRASTRUKTUREN EINGESTUFT WERDEN, SOLL IM LAUFE DIESES JAHRES IN EINER RECHTSVERORDNUNG FESTGELEGT WERDEN."

In dieser Rechtsverordnung wird das Bundesministerium des Innern anhand von branchenspezifischen Schwellenwerten den Versorgungsgrad für jede wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in dem jeweils betroffenen Sektor festlegen, zum Beispiel den zum Erreichen des Schwellenwertes erforderlichen Marktanteil an der Energie- oder Lebensmittelversorgung in einer bestimmten Region. Ein erster Referentenentwurf für die Sektoren des "Korb 1" wurde bereits an die Bundesländer und die maßgeblichen Branchenverbände zur Stellungnahme weitergeleitet.

Unternehmen, die die festgelegten Schwellenwerte erreichen, müssen dem Stand der Technik entsprechende Sicherheitsmaßnahmen treffen und unterliegen besonderen Meldepflichten gegenüber dem BSI. Die Gesetzesbegründung geht davon aus, dass etwa 2.000 Unternehmen als Betreiber Kritischer Infrastrukturen in den regulierten Sektoren von dem Gesetz betroffen sein werden.

WELCHER HANDLUNGSBEDARF BESTEHT FÜR DIE BETROFFENEN UNTERNEHMEN?

A. Betreiber von Webseiten und andere Diensteanbieter

Betreiber von Webseiten und andere Diensteanbieter müssen sicherstellen, dass kein unerlaubter Zugriff auf die von ihnen genutzten IT-Systeme möglich ist und ihre Systeme gegen den unbefugten Zugriff auf personenbezogene (Kunden-)Daten und Störungen durch äußere Angriffe gesichert sind. Zu diesem Zweck müssen Sie dem Stand der Technik entsprechende technische und organisatorische Maßnahmen vornehmen, wozu insbesondere auch die Verwendung sicherer Verschlüsselungsverfahren zählt.

Allerdings werden einem Diensteanbieter entsprechende Maßnahmen nur insoweit abverlangt, als ihm dies „*technisch möglich und zumutbar*" ist.

Die gesetzliche Regelung ist insoweit bewusst flexibel gestaltet, was es jedoch schwierig macht zu beurteilen, welche Maßnahmen von welchem Diensteanbieter konkret erwartet werden. So gibt es bereits erste Stimmen, die die Regelung wegen ihrer unbestimmten Verpflichtungen für verfassungswidrig halten. Hier gilt es, die weitere Entwicklung, insbesondere die Durchsetzungspraxis durch die zuständigen Landesb ehörden, im Auge zu behalten.

Ebenfalls noch nicht geklärt ist, ob es sich bei der neuen gesetzlichen Regelung um eine Marktverhaltensregelung handelt, also ob Gesetzesverstöße von Konkurrenten und/oder Verbraucherschutzverbänden abgemahnt werden können.

B. Telekommunikationsunternehmen

Telekommunikationsunternehmen haben neben der bereits bestehenden Pflicht, ihre Systeme und Anlagen ausreichend gegen Cyberangriffe abzusichern, jetzt insbesondere die Verpflichtung, ihre Kunden über Störungen und Missbräuche ihrer Anschlüsse sowie über geeignete und verfügbare Abwehrmaßnahmen zu informieren.

C. Betreiber Kritischer Infrastrukturen

Betreiber Kritischer Infrastrukturen werden durch das IT Sicherheitsgesetz nicht nur zum Schutz ihrer Webseiten, sondern auch zum Schutz ihrer sonstigen IT-Systeme verpflichtet. Sie sind danach verpflichtet, die für die Erbringung ihrer Dienste erforderliche IT spätestens **innerhalb von 2 Jahren nach Inkrafttreten der Rechtsverordnung nach dem Stand der Technik angemessen abzusichern** und diese Sicherheit mindestens alle 2 Jahre überprüfen zu lassen.

"BETREIBER KRITISCHER INFRASTRUKTUREN SIND VERPFLICHTET, DIE FÜR DIE ERBRINGUNG IHRER DIENSTE ERFORDERLICHE IT SPÄTESTENS INNERHALB VON 2 JAHREN NACH INKRAFTTRETEN DER RECHTSVERORDNUNG NACH DEM STAND DER TECHNIK ANGEMESSEN ABZUSICHERN UND DIESE SICHERHEIT MINDESTENS ALLE 2 JAHRE ÜBERPÜFEN ZU LASSEN..."

Was in welcher Branche konkret als Stand der Technik anzusehen ist, wird gesetzlich nicht definiert. Das BSI führt auf seiner Website zur Methodik aus:

„Was zu einem bestimmten Zeitpunkt Stand der Technik ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards wie DIN oder ISO-Standards oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln."

Die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen, die vom BSI auf Antrag als Stand der Technik in einem bestimmten Bereich anerkannt werden, wenn diese geeignet sind, Störungen zu vermeiden und die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der jeweils betroffenen Kritischen Infrastrukturen zu gewährleisten.

Allgemeine und branchenspezifische Best-Practice-Empfehlungen können bereits jetzt über die gemeinsame Internetplattform des BSI und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe („**BBK**)" abgerufen werden.

Für Energieversorgungsunternehmen mit eigenem Netzbetrieb hat die Bundesnetzagentur in Abstimmung mit dem BSI bereits im August 2015 einen IT-Sicherheitskatalog veröffentlicht, der konkrete Vorgaben zur Umsetzung von IT-Sicherheitsanforderungen aufstellt.

Darüber hinaus müssen die Betreiber Kritischer Infrastrukturen binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung eine interne Meldestruktur aufbauen, die es den Unternehmen ermöglicht, dem BSI IT-Sicherheitsvorfälle zu melden. Die aus diesen Meldungen, aber auch aus diversen weiteren Informationen gewonnenen Erkenntnisse stellt das BSI dann allen betroffenen Unternehmen zur Verfügung, damit diese ihre IT erforderlichenfalls laufend nachregeln können.

Aktuell gilt diese Meldepflicht bislang nur für die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen.

WELCHE KONSEQUENZEN DROHEN BEI VERSTÖSSEN?

Kontrollinstanz für die Betreiber von Webseiten und andere Diensteanbieter sind die jeweils zuständigen Aufsichtsbehörden der Länder. Telekommunikationsunternehmen unterliegen im Wesentlichen der Kontrolle der Bundesnetzagentur, die Betreiber Kritischer Infrastrukturen der Kontrolle des BSI.

A. Verstoßen Betreiber von Webseiten und andere Diensteanbieter gegen ihre Pflicht, dem Stand der Technik entsprechende technische und organisatorische Maßnahmen zum Schutz ihrer IT-Systeme und Kundendaten einzurichten, drohen **Bußgelder von bis zu EUR 50.000**.

B. Verstoßen Telekommunikationsunternehmen gegen die Hinweispflichten gegenüber ihren Kunden drohen ebenfalls **Bußgelder von bis zu EUR 50.000**.

C. Gegen Betreiber Kritischer Infrastrukturen, die IT-Sicherheitsvorfälle durch Versäumnisse bei der Umsetzung der IT-Sicherheitsmaßnahmen verursachen, können **Bußgelder von bis zu EUR 100.000** verhängt werden. Mit geringeren Bußgeldern werden Verletzungen der Meldepflichten sanktioniert.

"BEI VERSTÖßEN GEGEN DIE GESETZLICHEN PFLICHTEN DROHEN BUßGELDER VON BIS ZU EUR 100.000 ..."

Da den Betreibern Kritischer Infrastrukturen eine **Umsetzungsfrist von 2 Jahren** nach Inkrafttreten der Rechtsverordnung eingeräumt wird, müssen diese Unternehmer erst nach Ablauf dieser Frist mit Bußgeldern rechnen.

WAS IST AKTUELL ZU TUN?

A. Betreiber von Webseiten und andere Diensteanbieter

Die Betreiber von Webseiten und andere Diensteanbieter sollten, soweit sie die Server selbst betreiben (etwa in Form eines eigenen Rechenzentrums oder im Wege des Server Housing), insbesondere sicherstellen, dass bekannt werdende Sicherheitslücken und Schwachstellen durch das Einspielen von Updates und Patches umgehend geschlossen werden und die eingesetzte Software auf dem jeweils aktuellen Stand ist.

Unternehmen, die für den Betrieb ihrer Webseiten auf Host Provider zurückgreifen, sollten die zugrunde liegenden Verträge daraufhin überprüfen, ob die Host Provider zur Einhaltung des aktuellen Stands der Technik bezüglich der IT-Sicherheit verpflichtet sind und die Verträge erforderlichenfalls anpassen. Denn auch Unternehmen, die ihre Website technisch nicht selbst betreiben, bleiben gegenüber den Aufsichtsbehörden gleichwohl verantwortlich und bußgeldpflichtig.

B. Telekommunikationsunternehmen

Telekommunikationsunternehmen müssen durch ihre interne Prozessorganisation insbesondere sicherstellen, dass die durch das IT-Sicherheitsgesetz neu geschaffenen Melde- und Hinweispflichten gegenüber der Bundesnetzagentur und ihren Kunden eingehalten werden.

C. Betreiber Kritischer Infrastrukturen

Betreiber Kritischer Infrastrukturen wird die Schaffung der gesetzlich geforderten IT-Sicherheit sowie der Aufbau der Meldestrukturen vor nicht unerhebliche finanzielle und personelle Herausforderungen stellen.

Darüber hinaus ist der auf sechs Monate bzw. zwei Jahre angesetzte Zeitraum zum Aufbau der internen Meldestrukturen bzw. zur Umsetzung der neuen IT-Sicherheitsanforderungen knapp bemessen.

Hier gilt es, zügig Kontakt zu den jeweiligen Branchenverbänden aufzunehmen, den technischen Stand und die Sicherheit der IT-Systeme überprüfen zu lassen und damit zu beginnen, etwaige Defizite abzustellen. Ebenso zügig sollten leistungsfähige Strukturen aufgebaut werden, um rechtzeitig den gesetzlichen Meldepflichten nachkommen zu können.

KONTAKT

Sollten Sie Fragen zu diesem Briefing haben, können Sie sich gerne jederzeit an Axel Löhde, Dr. Torsten Rosenboom, Torge Rademacher, Sebastian Ens, Ursula Staab oder Ihre üblichen Ansprechpartner bei Watson Farley & Williams wenden.

AXEL LÖHDE
Partner
Hamburg
+49 40 800 084 314
aloehde@wfw.com

DR. TORSTEN ROSENBOOM
Partner
Frankfurt
+49 69 297 291 250
trosenboom@wfw.com

TORGE RADEMACHER
Senior Associate
Hamburg
+49 40 800 084 314
trademacher@wfw.com

SEBASTIAN ENS
Senior Associate
Frankfurt
+49 69 297 291 220
sens@wfw.com

URSULA STAAB
Associate
Hamburg
+49 40 800 084 449
ustaab@wfw.com