Joerg Heidrich

Verordnete Sicherheit

Das neue IT-Sicherheitsgesetz ist heiß umstritten

Ende Juli ist das IT-Sicherheitsgesetz in Kraft getreten. Es wird nicht nur die Betreiber sogenannter kritischer Infrastrukturen teuer zu stehen kommen, sondern erlegt auch jedem Anbieter einer geschäftsmäßig betriebenen Website technische Pflichten auf. Außerdem könnte es eine neue Abmahnlawine lostreten.

Die digitale Infrastruktur Deutschlands zu der weltweit sichersten machen – diesen Anspruch stellt Innenminister Thomas de Mazière an sein neues „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme". Damit sei man „europaweit Vorreiter und Vorbild" und leiste einen Beitrag dazu, dass das Netz sicherer werde. Kritiker sehen das allerdings anders: Das Gesetz sei ein gigantischer Papiertiger und ermögliche zu allem Überfluss auch noch eine Vorratsdatenspeicherung.

Das IT-Sicherheitsgesetz verpflichtet die Betreiber kritischer Infrastrukturen (KRITIS), ein Mindestniveau an IT-Sicherheit einzuhalten und Sicherheitsvorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Begründet werden diese Forderungen mit den weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung der Angebote nach sich ziehen könnte, und einer „besonderen Verantwortung für das Gemeinwohl". Ausnahmen gelten lediglich für Firmen mit weniger als zehn Mitarbeitern.

Öffentliche Sicherheit

Zur KRITIS-Gruppe gehören Unternehmen, die zwei Voraussetzungen erfüllen. Erstens müssen sie in einem der folgenden neun Bereiche tätig sein: Energie, Informationstechnik, Telekommunikation, Transport, Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz- und Versicherungswesen. Zweitens müssen zumindest Teile ihre Einrichtungen und Anlagen „von hoher Bedeutung für das Funktionieren des Gemeinwesens" sein. Das bedeutet, dass ein Ausfall oder eine Beeinträchtigung zu erheblichen Versorgungsengpässen oder zur Gefährdung der öffentlichen Sicherheit führen würde.

Diese Definition ist recht schwammig. So ist das einzige Krankenhaus in einer Kleinstadt von zentraler Bedeutung für das dortige Gemeinwohl. Gilt dies aber auch auf landes- oder gar bundesweitem Niveau? Unzweifelhaft fällt die Zentrale einer großen Versicherung unter die Maßstäbe für kritische Infrastrukturen. Vermutlich gilt dies auch für die ausgelagerte IT. Aber was ist mit den vielen Computern in kleinen und mittleren Versicherungsbüros, ohne die das Gesamtunternehmen zwar nicht arbeiten könnte, die aber gleichwohl kaum systemrelevant sind.

Aufgrund dieser Unklarheiten sollte man die Schätzung des Gesetzgebers, wonach etwa 2000 Unternehmen von der neuen Regelung betroffen sind, mit Vorsicht genießen. Demnächst soll eine Verordnung mehr Klarheit bringen. Darin will der Gesetzgeber unter anderem „messbare Kriterien wie beispielsweise den Marktanteil an der Versorgung einer bestimmten Region" festlegen.

Wer dann zur KRITIS-Gruppe zählt, wird verpflichtet, seine IT „nach dem Stand der Technik angemessen abzusichern". Der Stand der Technik lasse sich etwa anhand existierender Standards nach DIN oder ISO ermitteln. Außerdem können Verbände branchenspezifische Sicherheitsstandards vorschlagen und vom BSI genehmigen lassen.

> ***„Mit diesem Gesetz sind wir europaweit Vorreiter und Vorbild. Es leistet seinen Beitrag dazu, dass das Netz sicherer wird und die digitalen Infrastrukturen Deutschlands künftig zu den sichersten weltweit gehören."***
>
> *Thomas de Maizière, Bundesminister des Inneren*

Eingebettet werden die neuen Vorschriften im BSI-Gesetz. Dort schreibt Paragraf 8a vor, dass „organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit" der Infrastruktur zu treffen sind.

Meldepflichten

Ein Betreiber muss mindestens alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen, dass er die Vorgaben einhält. Über diese Maßnahmen muss er das BSI informieren – und zwar „einschließlich der dabei aufgedeckten Sicherheitsmängel". Die Behörde prüft das Ergebnis und kann anordnen, dass Sicherheitsmängel beseitigt werden.

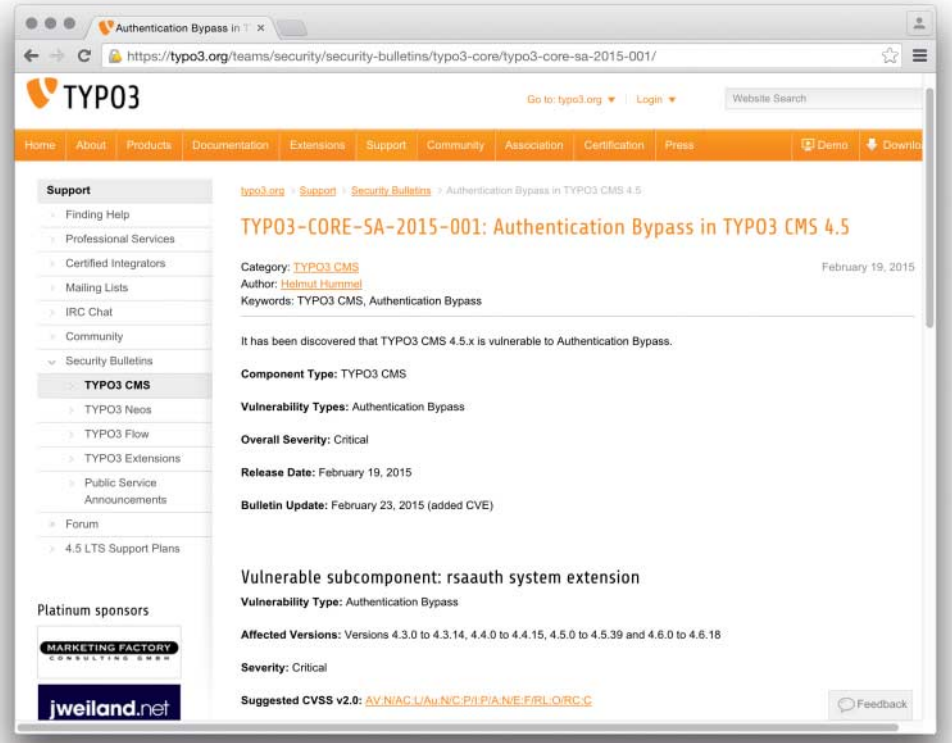
Die Meldepflichten an das Bundesamt gehen sogar noch weiter. Betreiber müssen über eine Kontaktstelle an das BSI melden, wenn erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer Beeinträchtigung ihrer Infrastrukturen geführt haben – auch nur führen können. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen enthalten.

Dabei muss der Betreiber aber nur dann genannt werden, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der IT geführt hat. Die meisten Meldungen dürften also anonym erfolgen. Die aus den Meldungen gewonnenen Erkenntnisse soll das BSI dann auch anderen KRITIS-Betreibern zur Verfügung stellen, damit diese ihre IT vor den bekannt gewordenen Bedrohungen schützen können.

Diese Regelung erweitert die Befugnisse und Kompetenzen des BSI erheblich. Außerdem sollen 294 Stellen neu geschaffen werden: 216 beim BSI und 78 beim Bundeskriminalamt. Die Machterweiterung des BSI gab während der Beratung des IT-Gesetzes Anlass für Kritik: Die Behörde sei zu eng mit den Geheimdiensten verwoben, als dass man sie mit der Speicherung und Auswertung hochsensibler Unternehmensdaten betrauen sollte.

Galgenfrist

Die meisten betroffenen Unternehmen haben zur Umsetzung der Pflichten noch etwas Zeit. Zunächst muss die noch ausstehende Verordnung erlassen werden, ohne die man den Kreis der Betroffenen nicht konkret ermitteln kann. Danach haben die Betroffenen noch zwei Jahre Zeit, bis sie die IT-



Website-Betreiber sollten künftig Sicherheits-Updates etwa für das CMS schnell einspielen, da ihnen sonst juristischer Ärger droht.

Sicherheitsstandards einhalten müssen. Wer nach dieser Frist noch gegen die Vorgaben des IT-Sicherheitsgesetzes verstößt, dem drohen Bußgelder bis zu 100 000 Euro – was angesichts der vom Branchenverband Bitkom geschätzten Investitionskosten von mehr als einer Milliarde Euro gar nicht so viel erscheint.

Keine Übergangsfrist gibt es allerdings für Energieversorger und Anbieter von Telekommunikations- und Telemediendiensten. TK-Unternehmen unterlagen schon vorher einer Meldepflicht gegenüber der Bundesnetzagentur. Künftig müssen sie zudem ihre Angebote nach dem „Stand der Technik" vor Cyberangriffen schützen. Provider sind außerdem verpflichtet, ihre Kunden zu warnen, wenn deren Zugang für IT-Angriffe missbraucht wird. Und sie sollen den Betroffenen Hilfe bei der Beseitigung des Malware-Befalls anbieten.

Vorratsdatenspeicherung

Datenschützern stößt ein weiterer Passus besonders auf, bei dem es um eine Änderung des Telekommunikationsgesetzes (TKG) geht. Dort sieht Paragraf 100 nun vor, dass Diensteanbieter die Bestands- und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden dürfen, um „Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen". Laut Gesetzesbegründung dürfen die Provider diese Daten nicht nur speichern, sondern darüber hinaus etwa für „Prüfungen des Netzwerkverkehrs und die Verwendung von sogenannten Honeypots (Fallen für Schadprogramme im Netz) oder Spamtraps (Blockieren der Versendung von Schadprogrammen)" verwenden.

Die Möglichkeit, Verkehrsdaten über einen längeren Zeitraum zu erheben und zu speichern, wurde in dem Gesetzgebungsverfahren heftig als weitreichende „Vorratsdatenspeicherung durch die Hintertür" kritisiert. Das Bundesverfassungsgericht und der Europäische Gerichtshof haben dem langfristigen Speichern von Nutzerdaten sehr enge Grenzen gesetzt. Die neue Vorschrift erlaubt hingegen eine anlasslose und uneingeschränkte Speicherung solcher Daten. Experten haben den Passus daher in der Anhörung zu dem Gesetz als unverhältnismäßig und damit möglicherweise verfassungswidrig bezeichnet.

Breitenwirkung

Bislang in der Öffentlichkeit kaum wahrgenommen wurde eine weitere Neuregelung, die das Telemediengesetz (TMG) und damit die allermeisten Betreiber von Internet-Angeboten betrifft. Auch für diese gelten ab sofort erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme. Das könnte erhebliche Folgen haben.

Der neu formulierten Paragraf 13 des TMG betrifft alle geschäftsmäßig angebotenen Telemedien. Diese Definition umfasst Online-Shops ebenso wie Websites von Freiberuflern oder werbefinanzierte Angebote. Ausdrücklich ausgeschlossen sind nur rein privat oder von Vereinen betriebene Angebote ohne kommerzielles Interesse. So fällt zum Beispiel die Website mit Bildern der eigenen Katze nicht unter Paragraf 13, wohl aber die eines Katzenzüchters. Wie schon bei der sehr ähnlichen Unterscheidung für die Impressumspflicht gelten die meisten Websites als geschäftsmäßige Angebote.

Ihre Betreiber müssen mit Inkrafttreten des IT-Sicherheitsgesetzes „technische und organisatorische Maßnahmen nach dem Stand der Technik" ergreifen, um unerlaubte Zugriffe auf ihre technischen Einrichtungen und gespeicherte personenbezogene Daten zu verhindern. Laut Gesetzesbegründung ist es ein wesentliches Ziel dieser Regelung, das „unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads)" zu verhindern. Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software, also das Einspielen von Sicherheits-Patches, könnten nach Ansicht des Gesetzgebers zahlreiche dieser Angriffe vermieden werden.

Die Website-Betreiber sollen auch organisatorische Maßnahmen ergreifen. Als Beispiel wird hier vorgeschlagen, Werbedienstleister vertraglich zu Schutzmaßnahmen zu verpflichten. Zum Schutz sensibler Daten sei es empfehlenswert, ein als sicher anerkanntes Verschlüsselungsverfahren einzusetzen. Und personalisierte Telemedien sollten bei der Anmeldung ein dem Schutzbedarf angemessenes Authentifizierungsverfahren verwenden.

Abmahngefahr

Im Endeffekt bedeutet diese neue Regelung nicht weniger als die Verpflichtung nahezu jedes Website-Betreibers, ab sofort und künftig dauerhaft aktuelle Updates zeitnah aufzuspielen. Zwar kann man diese Pflicht vertraglich an seinen Provider weitergeben, juristisch bleibt aber dennoch der Betreiber verantwortlich. Wer gegen die Vorgabe verstößt, begeht eine Ordnungswidrigkeit und riskiert ein Bußgeld von bis zu 50 000 Euro.

Eine solche Strafzahlung kommt bisher in der Praxis in vergleichbaren Fällen äußerst selten vor. Weitaus praxisrelevanter ist dagegen die Frage, ob die Gerichte die neue Regelung als sogenannte Marktverhaltensregel bewerten, die auch das Ziel verfolgt, die Grundsätze eines fairen Wettbewerbs zu schützen. Dann wäre für Mitbewerber der Weg eröffnet, missliebige Konkurrenz künftig auch für das Fehlen von Updates und Patches kostenpflichtig abzumahnen. Hier könnte ein neues Abmahn-Eldorado entstehen, bei dem es Jahre dauern kann, bis die Rechtslage gefestigt wird. (ad@ct.de)

Joerg Heidrich ist Justiziar und Datenschutzbeauftragter bei Heise Medien und als Rechts- und Fachanwalt für IT-Recht in Hannover tätig. c't