Verordnete Sicherheit

Neue gesetzliche Anforderungen an den Schutz kritischer Infrastrukturen

Nachdem Deutschland mit seinem IT-Sicherheitsgesetz im vergangenen Jahr vorausgegangen war, hat nun die EU eine Richtlinie zur Förderung der Cybersicherheit verabschiedet. Die neuen Regelungen stellen Betreiber von digitalen Diensten auch hierzulande vor erhebliche Herausforderungen.

Von Joerg Heidrich

Der Schutz von sogenannten kritischen Infrastrukturen steht derzeit ganz oben auf der Agenda sowohl der Bundesregierung als auch der Europäischen Union. Insbesondere geht es um die Herausforderung, Angriffen auf IT-Systeme wirksam zu begegnen. Um dieses Ziel zu erreichen, schaffen die Institutionen derzeit auf mehreren Ebenen gesetzliche Anforderungen für Unternehmen, deren reibungsloses Funktionieren als kritisch für das Gemeinwohl angesehen wird. Kommen diese Firmen den Vorgaben nicht nach, drohen hohe Strafen.

Nach dem bereits Mitte 2015 in Kraft getretenen deutschen IT-Sicherheitsgesetz gibt es solche Unternehmen und Anlagen in verschiedenen Branchen, etwa im Bankenwesen, in der Wasser- und Energieversorgung und auch im Medienbereich. Wer darunter fällt, muss regelmäßig etwa durch Zertifikate nachweisen, unternehmensrelevante Systeme und Prozesse besonders gesichert zu haben. Angriffe von außen muss er kategorisieren und melden. Herr des gesamten Verfahrens und zentrale Meldestelle für IT-Angriffe ist dabei das Bundesamt für Sicherheit in der Informationstechnik (BSI), dem der Staat dafür mehr als 200 neue Stellen spendiert hat.

Ob ein Unternehmen als kritische Infrastruktur (KRITIS) gilt, hängt von seiner Größe ab. Als Bemessungsgrundlage greift die Bundesregierung dabei auf eine 500.000er-Regel zurück: Sind jeweils 500.000 oder mehr Bürger von einer Versorgungsleistung abhängig, fällt die dazugehörige Anlage unter die Meldepflicht. Im Bereich der Informationstechnik gilt dies derzeit für rund 30 Rechenzentren, Server-Farmen und Trustcenter.

Strenge Pflichten

Kaum bekannt ist eine weitere erhebliche Änderung, die das IT-Sicherheitsgesetz mit sich gebracht hat. Sie betrifft alle Betreiber von Telemedien – und damit nahezu alle Anbieter von Websites in Deutschland. Nach dem neu geschaffenen Paragrafen 13 Absatz 7 des Telemediengesetzes (TMG) sind diese Anbieter gesetzlich dazu verpflichtet, dem Stand der Technik angemessene IT-Sicherheitsgrundlagen umzusetzen.

Alle Website-Betreiber müssen dem Gesetz zufolge also sicherstellen, dass „kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist“. Nach der Gesetzesbegründung soll „das unbemerkte Herunterladen allein durch das Aufrufen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads)“ verhindert werden. Schon das „Einspielen von Sicherheitspatches“ könne dies verhindern. In der Praxis konstruiert der Gesetzgeber hier wohl eine Pflicht zum Einspielen von Patches.

Technische Einrichtungen müssen außerdem gegen „Verletzungen des Schutzes personenbezogener Daten“ gesichert werden. Möglich sei dies durch Einsatz eines „als sicher anerkannten Verschlüsselungsverfahrens“. Darunter fallen solche Verfahren, die den aktuellen technischen Richtlinien des BSI entsprechen.

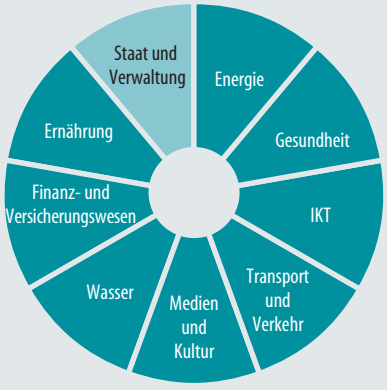
Wer gegen diese Pflichten verstößt, riskiert ein Bußgeld bis zu 50.000 Euro. Unangenehm könnte es für viele Unternehmen werden, wenn Gerichte in ihrer künftigen Rechtsprechung diese Vorschrift als sogenannte Marktverhaltensregel bewerten. Dann nämlich könnte jeder Mitbewerber mangelhafte Updates bei seinen Konkurrenten kostenpflichtig abmahnen, was zu einer erheblichen Rechtsunsicherheit führen würde.

EU-Regeln zur Cybersicherheit

Eine ähnliche Stoßrichtung wie das deutsche IT-Sicherheitsgesetz verfolgt die am 6. Juli 2016 vom Europäischen Parlament beschlossene „Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“, kurz NIS-Richtlinie. Im Rahmen einer

KRITIS

Das Bundesamt für Sicherheit in der Informationstechnik definiert 9 Sektoren, in denen kritische Infrastruktur (KRITIS) reguliert werden muss.



„Cybersicherheitsstrategie“ der EU sollen die neuen Regelungen helfen, die Widerstandsfähigkeit von IT-Systemen zu verbessern, Cyberkriminalität zu bekämpfen und die „Cyberverteidigung“ der EU zu stärken. Die NIS-Richtlinie ist am 8. August 2016 in Kraft getreten. Sie muss nun von allen europäischen Gesetzgebern bis zum Mai 2018 in nationales Recht umgesetzt sein.

Die Richtlinie verpflichtet alle EU-Mitgliedsstaaten, Meldestellen für die nationale „Netz- und Informationssicherheit“ (NIS) einzurichten. Bei der Umsetzung dieser Vorgabe muss eine enge Kooperation zwischen diesen Computer Security Incident Response Teams (CSIRTs), den nationalen Sicherheitsbehörden und den europäischen Koordinationsstellen sichergestellt werden. Und schließlich gilt es, Sicherheitsanforderungen und Meldeverpflichtungen für Betreiber „wesentlicher Dienste“ zu erarbeiten und durchzusetzen. Die im EU-Jargon so bezeichneten „wesentlichen Dienste“ entsprechen in etwa den kritischen Infrastrukturen im Sinne des IT-Sicherheitsgesetzes.

Bild: BSI

Im BSI-Lagezentrum sollen Pflichtmeldungen der KRITIS-Betreiber einlaufen.

Suchmaschinen, Clouds und Marktplätze

Im Unterschied zum IT-Sicherheitsgesetz regelt die NIS-Richtlinie allerdings auch „digitale Dienste“ (Digital Service Provider, DSP). Dies gilt explizit für Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze. Mit solchen Marktplätzen sind wohl keine Endkunden-Shops gemeint, denn der Richtlinientext spricht von Angeboten, die es Unternehmen erlauben, „Online-Shops im Rahmen von Marktplätzen einzurichten, um dort Produkte und Dienstleistungen anzubieten“. Neben Drittanbieter-offenen Shops wie Amazon und eBay könnten hierunter auch App-Anbieter und vergleichbare Einrichtungen fallen.

Einer Richtlinienbeschreibung der Europäischen Kommission zufolge haben diese DSP eine ganze Reihe von Pflichten: Risikovermeidung durch technische und organisatorische Vorbeugemaßnahmen, Durchsetzung von Maßnahmen zur Sicherung der Netzwerk- und Informationssysteme sowie Sicherheits- und Reaktionspläne, um in Notfällen auf akute Angriffe reagieren zu können. Zudem müssen auch diese Anbieter sicherheitsrelevante Angriffe auf die eigene IT künftig ans BSI melden.

Insgesamt ist die Kontrolle der DSPs weniger streng ausgestaltet als die der kritischen Infrastrukturen. Sie erfolgt überdies nur nachträglich, während KRITIS-Betreiber bereits im Vorhinein die Einhaltung der Vorgaben nachweisen müssen, etwa durch eine Zertifizierung. Gleichwohl gehen die Anforderungen an digitale Dienste deutlich über das IT-Sicherheitsgesetz hinaus. Von der Regulierung sind explizit nur Einzelunternehmer und kleinere Unternehmen ausgenommen.

Aus diesem Grund wird der deutsche Gesetzgeber die rechtlichen Regelungen an die neue Richtlinie anpassen müssen. Änderungen wird es vor allem im Telemediengesetz geben, das die Haftung und den Datenschutz im Internet regelt. Dort fehlt es bislang etwa an der Regelung von Meldepflichten für Bedrohungen der IT-Sicherheit.

Meer an Regelungen

Kritiker der neuen Richtlinie wie der ehemalige IT-Direktor im Bundesinnenministerium Martin Schallbruch befürchten die „Gefahr einer Zersplitterung der IT-Sicherheitsanforderungen für Dienste aus dem Bereich der Informationstechnik und Telekommunikation“. So seien etwa Telekommunikationsanbieter im Wesentlichen von den Neuregelungen ausgenommen. Andererseits würden einige wenige IT- und TK-Dienste als kritische Infrastrukturen definiert, während wieder andere unter die Regelungen der digitalen Dienste fallen. Auch die Abgrenzung zwischen den erfassten Online-Marktplätzen und den nach langem Ringen nicht regulierten Webshops ist alles andere als klar und eindeutig.

Schließlich ist bei den Neuregelungen auch noch die neue EU-Datenschutzgrundverordnung zu beachten, die zumindest hinsichtlich des Umgangs mit sensiblen persönlichen Daten Anforderungen an die Datensicherheit stellt. So müssen Behörden und Unternehmen „geeignete technische und organisatorische Maßnahmen“ ergreifen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass sie personenbezogene Daten in Übereinstimmung mit den neuen EU-Regelungen verarbeiten.

Es wird eine große Herausforderung für den deutschen Gesetzgeber sein, das IT-Sicherheitsgesetz und die NIS-Richtlinie miteinander sowie mit der EU-Datenschutzgrundverordnung in Einklang zu bringen, ohne dabei für massive Rechtsunsicherheit bei den betroffenen Unternehmen zu sorgen. Im Rahmen einer sogenannten Mindestharmonisierung gilt grundsätzlich, dass der nationale Gesetzgeber zwar eine schärfere Regulierung vornehmen darf, aber nicht hinter den europäischen Vorgaben zurückbleiben soll. Die Regelungen für die kritischen Infrastrukturen dürften daher nur in Details zu ändern sein. Aber bei der Regelung der digitalen Dienste besteht einiger Umsetzungsbedarf. *(hob@ct.de)* c't