von **Anna Bosch**

Neu: Online-Händler zu umfassenden IT-Sicherheitsmaßnahmen verpflichtet

Nicht nur in den Medien wurde u.a. nach Bekanntwerden von Cyber-Angriffen auf den deutschen Bundestag das Thema IT-Sicherheit heiß diskutiert. Auch der Gesetzgeber wurde tätig, mit der Folge, dass das IT-Sicherheitsgesetz am 25.7.2015 in Kraft trat. Eine der Neuregelungen im Bereich des Telemediengesetzes (TMG) hat unmittelbare Breitenwirkung u.a. für Online-Händler: der neue § 13 Abs. 7 TMG verpflichtet diese nunmehr zur Umsetzung von technischen Sicherheitsmaßnahmen. Wen die Neuregelung konkret betrifft und welche technischen und organisatorischen Pflichten einzuhalten sind, erfahren Sie im folgenden Beitrag.

1. Überblick

Der neu gefasste Gesetzestext sieht insbesondere für die Betreiber kritischer Infrastrukturen – also Unternehmen beispielsweise aus den Sektoren Energie, Verkehr, Telekommunikation (kurz KRITIS-Gruppe) - die Pflicht zur Einhaltung eines Mindestmaßes an IT-Sicherheit vor, wenn deren Funktionieren für das Gemeinwesen von zentraler Bedeutung ist. Neben technisch zu treffenden Vorkehrungen, besteht für diese zudem die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Das IT-Sicherheitsgesetz bringt jedoch nicht nur für die Betreiber kritischer Infrastrukturen Veränderungen mit sich, sondern formuliert weitere Pflichten für ganz „normale“ Webseiten-Betreiber – zum Beispiel also für Online-Händler.

Der neue § 13 Abs. 7 TMG lautet nun:

> „Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass
>
> 1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
> 2. diese
>
> a) gegen Verletzungen des Schutzes personenbezogener Daten und
> b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind.
>
> Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.“
>
> §

2. Welche Ziele verfolgt der Gesetzgeber mit dem IT-Sicherheitsgesetz?

Vordergründiges Ziel der Neuerungen ist es, das Netz insgesamt und die digitalen Infrastrukturen Deutschlands sicherer zu machen. Das heißt, dass beispielsweise das unbemerkte Herunterladen von Schadsoftware allein durch das Aufrufen bzw. Nutzen einer dafür von Hackern präparierten Webseite (sog. Drive-by-Downloads) vermieden werden soll, um sensible Daten vor Missbrauch zu schützen. „Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA)“, heißt es in der amtlichen Begründung (BT-Drs. 643/14).

3. Wer ist neben Online-Händlern noch von der Neuregelung betroffen?

Nicht nur Webseiten-Betreiber aus dem Bereich „kritischer Infrastrukturen“ sind betroffen. § 13 Abs. 7 TMG betrifft in seiner Neufassung alle geschäftsmäßig angebotenen Telemediendienste, also im Prinzip jede kommerziellen Interessen dienenden Website. Die Websites von Online-Shops sind daher ebenso betroffen, wie die von Freiberuflern. Ausdrücklich ausgenommen sind lediglich rein private Seiten (z.B. Blogs mit Urlaubsfotos) oder von Vereinen betriebene Angebote ohne kommerzielles Interesse. Vorsicht ist aber auch z.B. bei Mode- oder Urlaubs-Blogs geboten, wenn mit diesen ein ernstzunehmender Gewinn durch Werbeanzeigen erwirtschaftet wird.

4. Welche technischen und organisatorischen Vorkehrungen müssen getroffen werden?

Webseiten-Betreiber müssen grundsätzlich den unerlaubten Zugriff auf ihre Webseiten – etwa durch Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens wie „Gpg4win“ - unterbinden und ihre Plattformen gegen Cyber-Angriffe sichern. Dies liegt nicht mehr nur im eigenen bzw. Kunden-Interesse, sondern es besteht mittlerweile eine gesetzliche Pflicht zum Schutz von personenbezogenen Daten und zur Absicherung gegen Störungen. Dies kann auch bedeuten, dass Webseiten-Betreiber u.a. Sicherheits-Updates etwa für das CMS schnell einspielen oder eine regelmäßige Aktualisierung der verwendeten Software (Einspielen von Sicherheitspatches) vornehmen sollten. Auch bei der Wahl des Authentifizierungsverfahrens ist bei personalisierten Telemedien Vorsicht geboten. Aufschluss über geeignete Authentifikationsmechanismen geben die Richtlinien des BSI.

Zwar ist in der Neuregelung vorgesehen, dass Webseiten-Betreiber (nur) „Maßnahmen nach dem Stand der Technik“ zu ergreifen haben, was auf den ersten Blick einigermaßen anbieterfreundlich erscheinen

mag. Jedoch ist damit gleichzeitig eine ernstzunehmende Aktualisierungspflicht verbunden. Immerhin dürfen die Maßnahmen aber nicht wirtschaftlich unzumutbar sein. Wann diese Schwelle konkret erreicht ist, wird sich jedoch erst noch herausstellen müssen.

Organisatorische Maßnahmen sind schließlich zum Beispiel bezüglich auf der Webseite eingebundenen Werbebannern zu treffen, auf die der Diensteanbieter keinen unmittelbaren Einfluss hat.

Praxistipp: Werbedienstleister, denen Werbefläche eingeräumt wird, können vertraglich zu notwendigen Schutzmaßnahmen verpflichtet werden. Die IT-Recht-Kanzlei berät Sie dazu gerne!

5. Was droht bei Verstößen?

Bei Verstößen können - je nach (künftiger) gerichtlicher Bewertung des § 13 Abs. 7 TMG als potenzieller Marktverhaltensregel - nicht nur kostenpflichtige Abmahnungen durch Mitbewerber drohen. Auch ein mit einem Bußgeld von bis zu 50 000.- Euro verbundenes Ordnungswidrigkeitsverfahren droht Webseiten-Betreibern, wenn sie die Anforderungen des Telemediengesetzes und die Einhaltung verschärfter IT-Sicherheitsstandards nicht erfüllen.

6. Fazit

Das IT-Sicherheitsgesetz bringt nicht nur Neuerungen für Anbieter in den Bereichen „kritischer Infrastruktur“ mit sich. Die Breitenwirkung der Gesetzesänderung ist immens: Zahlreiche Webseiten-Betreiber, die bisher technische Updates höchstens im eigenen Interesse aufspielten, sind nun u.a. gehalten diese konsequent aufzuspielen und fortwährend zu aktualisieren.

Autor:
Anna Bosch
(freie jur. Mitarbeiterin der IT-Recht Kanzlei)