

von Rechtsanwalt **Phil Salewski**

# IT-Sicherheitsgesetz: SSL-Verschlüsselung und technischer Zugriffsschutz in Online-Shops jetzt Pflicht?

Die steigende Strukturvielfalt im Internet und der wachsende finanziellen Gegenwert personenbezogener Daten haben dazu geführt, dass bestehende Sicherheitslücken immer häufiger für Datendiebstähle missbraucht werden. Aus diesem Grunde ist jüngst das umstrittene IT-Sicherheitsgesetz in Kraft getreten, das vor allem für Netzpräsenzen von staatsdienlichen Institutionen erhöhte Sicherheitsanforderungen etabliert. Fast unbemerkt blieb dabei aber eine Änderung des Telemediengesetzes, die für sämtliche Diensteanbieter und so auch in Online-Shops - unter anderem - die Pflicht zur Einführung einer SSL-Verschlüsselung nach sich ziehen könnte. Folgender Beitrag setzt sich kritisch mit dem Inhalt der Änderung und den Konsequenzen für den Online-Handel auseinander.

## I. IT-Sicherheitsgesetz und TMG-Änderung

Nach einer fast sechsmonatigen Phase parlamentarischer Beratung und einer öffentlichkeitswirksamen Debatte um die Grenzen staatlicher Eingriffsermächtigungen ist am 24.07.2015 das IT-Sicherheitsgesetz in seiner endgültigen Fassung im Bundesgesetzblatt veröffentlicht worden und mit Wirkung zum 25.07.2015 in Kraft getreten.

Primär zielt das neue Regelwerk darauf ab, kritische Infrastrukturen, also solche mit essentieller Bedeutung für das staatliche Gemeinwohl, zur Einführung eines einheitlichen und hohen Schutzniveaus für ihre informationstechnologischen Systeme zu verpflichten und so der wachsenden Bedrohung von Cyber-Angriffen vorzubeugen. Dies soll längerfristig die Sicherheit derartiger Netzstrukturen verbessern und insbesondere rechtswidrige Zugriffe auf sensible Daten unterbinden.

Allerdings geht das Gesetz, das keinen eigenen Vorschriftenkatalog enthält, sondern nur bestehende Rechtsakte abändert, in seiner Reichweite über den augenscheinlich eng gefassten Adressatenkreis hinaus und erstreckt in einer bisher wenig beachteten Änderung des Telemediengesetzes das Pflichtenprogramm – unter der zusätzlichen Zielsetzung des verbesserten Schutzes personenbezogener Verbraucherdaten – auf sämtliche Diensteanbieter.

In dem durch das IT-Sicherheitsgesetz modifizierten §13 TMG heißt es in einem neu eingefügten Abs. 7 ab sofort:

„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.“

In Zusammenhang mit dem neuartigen Schutzpflichtprogramm wurde auch der Bußgeldkatalog des §16 TMG erweitert. Die unzulängliche, fehlerhafte oder ausbleibende Einführung von geeigneten Maßnahmen nach §13 Abs. 7 Satz 1 Nr. 1 und Nr. 2 lit. a TMG kann nunmehr mit einem Bußgeld von bis zu 50.000€ geahndet werden.

Abzuwarten bleibt demgegenüber, ob die neuen Pflichten als Marktverhaltensregelungen im Sinne des §4 Nr. 11 UWG eingestuft werden und mithin wettbewerbsrechtliche Bedeutung erlangen.

## II. Neue Pflichten im Online-Handel?

Durch die Aufnahme einer Datensicherungspflicht und einer Vorgabe an den Zugriffsschutz in das Telemediengesetz wurden die – nach der Gesetzesbegründung primär nur für kritische Infrastruktureinrichtungen intendierten – hohen Sicherheitsanforderungen allen „Diensteanbietern“ auferlegt.

### 1.) Online-Händler als Diensteanbieter

Nach §2 Nr. 1 TMG unterfallen dem neuen Pflichtenprogramm so alle natürlichen oder juristischen Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln.

Zwar sollen – in Anlehnung an §5 TMG – nur solche Anbieter betroffen sein, die die Dienste im Rahmen einer nachhaltigen und mithin geschäftsmäßigen Tätigkeit vorhalten oder nutzen. Aufgrund der vorherrschenden weiten Auslegung der Geschäftsmäßigkeit werden von den neuen Pflichten aber nur solche Personen entbunden werden, die Inhalte zu rein privaten Zwecken bereitstellen.

Mithin ist jedenfalls festzustellen, dass die technischen Sicherungspflichten prinzipiell gegenüber dem gesamten Online-Gewerbe Geltung entfalten und so vor allem Betreiber eigener Shops zu wesentlichen Umstellungen zwingen werden.

## 2.) Härteklausel/Einschränkung

Allerdings ist zu beachten, dass die neuen Anforderungen nur dann gelten sollen, wenn deren Einhaltung die Grenzen der technischen Möglichkeiten und der wirtschaftlichen Zumutbarkeit nicht übersteigt. Insofern enthält der §13 Abs. 7 TMG augenscheinlich eine Privilegierung von allem von kleinen und mittleren Unternehmen, bei denen eine Umstellung auf hocheffiziente Sicherheitsstandards nicht nur die organisatorischen und informationstechnologischen Kapazitäten übersteigen, sondern zudem zu nicht hinnehmbaren finanziellen Belastungen führen würde.

## III. Weitgehende Unbestimmtheit der Anforderungen

Durch die Änderung sind geschäftsmäßige Teledienstanbieter – allen voran Shopbetreiber – fortan zur Einführung und Umsetzung verschiedenartiger informationstechnologischer Sicherheitsmaßnahmen gehalten. Allerdings wird ihnen das Einleiten geeigneter Schritte erheblich dadurch erschwert, dass der §13 Abs. 7 TMG die neuartigen Pflichten weitestgehend generalisiert und insbesondere keine technischen Standards nennt, welche den Anforderungen gerecht werden könnten. Auch die zur Abschwächung eingeführte Möglichkeits- und Zumutbarkeitsgrenze entbehrt aber einer notwendigen Konkretisierung und führt so in Ermangelung verbindlicher Beurteilungswerte dazu, dass gerade die Betroffenen die Ausnahmevoraussetzungen nicht einschätzen können.

### 1.) Fehlende Konkretisierung der technischen Sicherungspflichten

Grundsätzlich sieht der neu eingeführte §13 Abs. 7 TMG drei Pflichten mit verschiedenartigen Zielrichtungen vor, die zum einem dem Systemschutz und der Integrität des Telemediums selbst ins Auge fassen, zum anderen aber die Sicherung von personenbezogenen Nutzerdaten betreffen.

So sollen geschäftsmäßige Anbieter von Telediensten durch entsprechende Vorkehrungen ab sofort dafür Sorge tragen, dass

- unerlaubte Zugriffe auf die für die Telemedien genutzten Einrichtungen verhindert werden
- die Telemedien Verletzungen des Schutzes personenbezogener Daten unterbinden und mithin zu deren Sicherheit beitragen
- die Telemedien vor – ggf. äußeren – Störungen geschützt werden

Problematisch ist, dass die Diensteanbieter ob der genauen Anforderungen an die zu treffenden Sicherheitsmaßnahmen weitestgehend im Dunkeln gelassen werden. Zwar macht Satz 2 deutlich, dass diese den Stand der Technik berücksichtigen müssen und insbesondere in Form eines anerkannten Verschlüsselungsverfahrens ergehen können.

Außer Acht gelassen wurde allerdings, dass informationstechnologische Sicherheitsvorkehrungen nicht generell gegen sämtliche Arten von Zugriffen schützen können, sondern für ihre Wirksamkeit stets auf bestimmte Angriffsziele und -strategien ausgerichtet werden müssen. Welche rechtswidrigen Praktiken die neu eingeführten Pflichten spezifisch unterbinden und welche Datensätze oder

Einrichtungsstrukturen insofern geschützt werden sollen, entbehrt allerdings jeglicher Erläuterung. Gerade eine solche wäre für die ordnungsgemäße Umsetzung der Pflichten jedoch essentiell.

In der Gesetzesbegründung zum IT-Sicherheitsgesetz (BT-Drucks. 18/4096, S. 34) werden insofern nur lückenhaft verschiedene Arten von Cyberpiratie-Angriffen genannt, deren Vorbeugung und Unterbindung die neuen Maßnahmen dienlich sein sollen.

So werden als unerlaubte Zugriffe im Sinne von §13 Abs. 7 Satz 1 Nr. 1 TMG insbesondere Praktiken genannt, mittels derer Angreifer anvisierte Webseiten präparieren und Codes einbetten, die das automatische Herunterladen von Malware oder Phishing-Programmen bei bloßen Aufrufen oder Benutzen der Website ermöglichen (Drive-by-Downloads).

Welche inneren oder gegebenenfalls äußeren Störungen im Sinne von §13 Abs. 7 Satz 1 Nr. 2 lit. b TMG durch technische Maßnahmen verhindert werden sollen, geht demgegenüber aus der Gesetzesbegründung nicht hervor. In Fachkreisen wird – angesichts der zunehmenden Relevanz – spekuliert, dass die Regelung insbesondere das systematische und gezielte Lahmlegen von Servern (sog. „Distributed Denial of Service“) erfassen und dieser Praktik entgegenwirken sollte.

## 2.) Fehlender Auslegungsmaßstab für die Härteklausel

Gleichermaßen gravierend erscheint es, dass der neue §13 Abs. 7 unter bestimmten Voraussetzungen zwar von der Pflicht zur Umsetzung der neuen Sicherungspflichten entbindet, diese Voraussetzungen aber in keiner Weise einer tatsächlichen Anwendung zugänglich sein können, sofern die Begriffe der „technischen Unmöglichkeit“ und „wirtschaftlichen Unzumutbarkeit“ nicht mit plastischen Richtwerten ausgestattet werden, die Diensteanbietern eine Orientierung ermöglichen

Insofern verbleibt bis auf Weiteres die Frage, ob ein Diensteanbieter aufgrund der Größe seines Gewerbes, der Reichweite seiner Internetpräsenz und deren informationstechnologischer Gestaltung von dem umfangreichen und unkonkreten Pflichtenprogramm befreit ist, im jeweiligen eigenen Ermessen.

Die gewählten Formulierungen bewirken somit im Ergebnis einen völligen Wegfall der Rechtssicherheit und werden zur Folge haben, dass sich auch kleine Anbieter – weil sie das Vorliegen der Befreiungsvoraussetzungen nicht beurteilen können – zur Umstellung verpflichtet sehen, um dem Damoklesschwert der hohen Bußgelder zu entgehen

## IV. SSL-Verschlüsselung zum Schutz personenbezogener Daten erforderlich?

Für viel Aufsehen sorgte in den letzten Wochen die Behauptung, sämtliche Internetpräsenzen müssten nach Inkrafttreten des IT-Sicherheitsgesetzes zukünftig durch SSL-Zertifikate verschlüsselt werden. Ob diese Pflicht nach der Änderung des §13 TMG tatsächlich besteht, soll nach einem kurzen Überblick über die Funktionsweise der Technologie erörtert werden.

## 1.) Überblick: SSL-Verschlüsselung

Das SSL (kurz für: „Secure Sockets Layer“) ist ein hybrides Verschlüsselungsprotokoll, mittels dessen personenbezogene Daten durch die Einbindung von Zertifikaten in Domains kodifiziert und so vor Drittzugriffen bei der Eingabe und im Transferprozess geschützt werden. Die Technologie ist in den letzten Jahren zum weltweiten Verschlüsselungsstandard aufgestiegen und zeichnet sich vor allem dadurch aus, dass sie eine wenig zeit- und kostenintensive Einbettung ermöglicht und die eingegebenen Daten mit einem Verfahren verschlüsselt, das – theoretisch – einzig den bestimmungsgemäßen Empfänger zur Dekodierung befähigt. Ihr Einsatz ist für den Nutzer dadurch erkennbar, dass beim Aufrufen der jeweiligen URL das normale Übertragungsprotokoll „http“ um ein „s“ (für das englische „secure“ = sicher) erweitert ist. Auf dem Markt kursieren derzeit verschiedene Zertifikate der SSL-Technologie, deren Vorzugswürdigkeit sich vor allem nach der Struktur der jeweiligen Internetpräsenz bemisst. Werden viele Subdomains verwendet, eignet sich so zum Beispiel insbesondere das sog. „Wildcard-Zertifikat“.

## 2.) Pflicht zum Schutz personenbezogener Daten nach §13 Abs. 7 Satz 1 Nr. 2 lit.a TMG

Der neue §13 Abs. 7 TMG zwingt Diensteanbieter – so auch Online-Händler – nach Nr. 2 lit.a dazu, geeignete Vorkehrungen zu treffen, um ihre Präsenzen vor verboteneren Zugriffen auf personenbezogene Daten zu schützen.

Nach Satz 3 können hierfür insbesondere als sicher anerkannte Verschlüsselungsverfahren verwendet werden.

### a) SSL noch als sicher anerkannt?

Zwar gelten nach der offiziellen Gesetzesbegründung solche Verfahren als „sicher“, die den aktuellen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) entsprechen. Die empfohlenen Verfahren sind allerdings teilweise so streng, dass ihre Einbettung mit einem Aufwand einhergehen dürfte, der das Maß der Zumutbarkeit regelmäßig übersteigt. Gerade ein solcher ist von §13 Abs. 7 TMG in Anlehnung an die Härteklausel aber nicht intendiert.

Ob SSL-Zertifikate also genügen, kann mangels einer eigentlich erforderlichen konkreten Stellungnahme nicht abschließend gesagt werden. Zu beachten ist in diesem Zusammenhang jedenfalls, dass viele SSL-Zertifikate inzwischen veraltet sind und Sicherheitslücken aufweisen können, für deren Missbrauch der jeweilige Händler mit einem entsprechenden Bußgeld haftbar gemacht werden könnte. Insofern ist darauf hinzuweisen, dass das ursprüngliche SSL-Protokoll inzwischen unter dem Namen „TSL“ (kurz für „Transport Layer Security“) weiterentwickelt wird und seinerseits den bisherigen Sicherheitsstandard aufwertet.

## b) keine ausdrückliche Verschlüsselungspflicht

Besteht schon ob der anzuwendenden Verschlüsselungsverfahren keine hinreichende Rechtssicherheit, so wird diese noch erheblich dadurch verstärkt, dass keinesfalls eine ausdrückliche Verpflichtung zum Einsatz von Verschlüsselungsverfahren vorgesehen ist. Vielmehr zwingt das Gesetz insofern nur – in wenig eindeutiger Weise – zum Ergreifen geeigneter Schutzmaßnahmen, die Zugriffe aus personenbezogene Daten verhindern. Diensteanbietern ist es insofern selbst überlassen, ob sie für die notwendige Sicherung auf andere Verfahren zurückgreifen wollen. Allerdings riskieren sie dann die Gefahr einer unzureichenden Pflichtumsetzung.

## c) Ausschluss durch Härteklausele

Wiederum zu berücksichtigen ist in diesem Zusammenhang aber, dass derjenige Diensteanbieter, der sich um eine ordnungsgemäße Erfüllung der neuartigen Pflichten bemüht, nach – nicht abschließend deutbarer – gesetzgeberischer Intention möglicherweise wegen eines unverhältnismäßigen Aufwandes von der Umsetzung befreit ist.

## d) Ergebnis

Zwar sieht der neue §13 Abs. 7 TMG keine ausdrückliche Verpflichtung zur Verwendung von Verschlüsselungsverfahren vor, sondern gestattet – zumindest theoretisch – auch alternative Maßnahmen, die verbotene Zugriffe aus personenbezogene Daten verhindern. Weil die SSL-Verschlüsselung derzeit (noch) als sichere Methode gilt und ob ihrer Einbettung zwar eine Umstellung, aber im Vergleich zu anderen Verfahren einen nur relativen Aufwand erfordert, ist jedem Shopbetreiber zu empfehlen, derartige Zertifikate zukünftig zu verwenden.

Aufgrund fehlender geeigneter Auslegungsmaßstäbe und mangelnder handfester Anhaltspunkte für ihr Eingreifen sollte eine Berufung auf die Ausschlussklausel des §13 Abs. 7 im Zweifel unterlassen werden.

## 3.) Unklares Verhältnis zum §13 Abs. 4 Nr. 3 TMG

Müssen personenbezogene Daten mithin nunmehr durch geeignete technische Maßnahmen, etwa durch SSL-Verschlüsselung, innerhalb der angebotenen Teledienste vor Drittzugriffen geschützt werden, so stellt sich die Frage, wie diese Pflicht vor dem Hintergrund des §14 Abs. 4 Nr. 3 TMG zu verstehen bzw. von genannter Vorschrift abzugrenzen ist.

Nach §14 Abs. 4 Nr. 3 TMG waren Diensteanbieter nämlich schon vor Inkrafttreten des IT-Sicherheitsgesetzes gehalten, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Nutzer Telemedien gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.

Teilweise wird insofern argumentiert, dass die Pflicht zum Schutz personenbezogener Daten durch Verschlüsselungsmethoden oder andere Sicherheitsmaßnahmen bereits vor Einführung des neuen Abs. 7 bestand. Wieder andere sahen in der älteren Regelung nur eine Pflicht, Zugänge zu bestimmten Bereichen des Online-Angebots mittels PINs oder Passwörter gegen Drittzugriffe zu schützen und

wollten dem Wortlaut keinesfalls die Vorgabe entnehmen, sämtliche personenbezogene Nutzerdaten der angriffsbedingten Preisgabe zu entziehen.

Das neue IT-Sicherheitsgesetz enthält keine Hinweise darauf, wie die beiden Vorschriften in Wechselwirkung zu verstehen sind.

Realistisch scheint es jedoch mit Blick auf die gesetzgeberische Intention mit der zweiten Ansicht davon auszugehen, dass §13 Abs. 4 Nr. 3 TMG (nur) auf einen gesicherten Zugang zu bestimmten Bereichen der Telemedien abzielte. Ließe sich nämlich bereits hier eine Pflicht zum vollumfänglichen Schutz personenbezogener Daten ableiten, wäre die Neufassung des §13 Abs. 7 Satz 1 Nr. 2 lit. a TMG dem Gegenstand nach überflüssig.

## V. Fazit

Mit Inkrafttreten des IT-Sicherheitsgesetzes zum 25.07.2015 wurde der §13 TMG um ein zusätzliches Pflichtenprogramm für alle geschäftsmäßigen Diensteanbieter und mithin auch für sämtliche Online-Händler erweitert, das die Absicherung der Medienauftritte durch Sicherungsmaßnahmen vorsieht und zur Umsetzung von neuen Datenschutzvorgaben aufruft.

Während Händler, die ausschließlich auf Plattformen wie eBay oder amazon verkaufen und insofern nur auf die von den Betreibern zur Verfügung gestellten informationstechnologischen Lösungen zurückgreifen, von den Auswirkungen weitestgehend befreit bleiben, ergeben sich für Shopbetreiber mit eigenen Präsenzen einschneidende Konsequenzen.

Insofern nämlich entbehren die neuen Vorschriften auf allen Ebenen der Bestimmtheit, die für eine ordnungsgemäße Umsetzung erforderlich wäre. Weder werden so die Drittzugriffe, denen es vorzubeugen gilt, präzisiert, noch nennt das Gesetz die Maßnahmen, derer sich die Diensteanbieter in Zukunft bedienen sollen. Fehlen jedoch zuverlässige Leitlinien für die Umsetzung der technischen Sicherungspflichten, so wird eine Rechtsunsicherheit geschaffen, die sich im Zweifel zulasten derer auswirkt, die um eine ordnungsgemäße Erfüllung bemüht sind und dennoch riskieren, mit hohen Bußgeldern belastet zu werden.

Gesagtes gilt auch für den Ausnahmetatbestand der technischen Unmöglichkeit und wirtschaftlichen Unzumutbarkeit, der eigentlich von den Pflichten befreien soll, aber keine hinreichende Bewertungsgrundlage schafft.

Die mangelnde Regelungskompetenz des Gesetzgebers wird hier längerfristig durch die Rechtsprechung auszugleichen sein, führt aber dazu, dass eine Berufung auf die Härteklausele derzeit nicht zu empfehlen ist.

Allen Online-Händlern mit eigenen Web-Präsenzen ist daher bis auf Weiteres zu raten, die neuen Verpflichtungen ernst zu nehmen und insbesondere geeignete Maßnahmen zu treffen, die von ihnen erhobenen personenbezogenen Daten gegen Drittzugriffe zu sichern. Dies kann, muss aber nicht, mittels eines Verschlüsselungsverfahrens wie den SSL-Zertifikaten geschehen.

Über neue Entwicklungen zur Gesetzesänderung hält die IT-Recht Kanzlei Sie selbstverständlich auf

dem Laufenden und steht Ihnen in der Zwischenzeit für etwaige Rückfragen gerne persönlich zur Verfügung.

Autor:

**RA Phil Salewski**

Rechtsanwalt