FRANZ
RECHTSANWÄLTE

AUGUST 2015

NEWSFLASH

IT-Sicherheit

» Neues IT-Sicherheitsgesetz ist am 25. Juli 2015 in Kraft getreten.

Schaffung von Mindeststandards und Einführung von Meldepflichten bei Cyber-Attacken für Unternehmen, die sogenannte „Kritische Infrastrukturen“ betreiben.

Erweiterung des Pflichtenkatalogs im Bereich der IT-Sicherheit für Unternehmen die kommerzielle Websites betreiben. «

FRANZ RECHTSANWÄLTE Partnerschaftsgesellschaft mbB | **Düsseldorf – Basel** | **www.franzlegal.com**
Kaistraße 16A | 40221 Düsseldorf | Deutschland | Tel +49 (0)211 157676-0 | Fax +49 (0)211 157676-76
Gerbergasse 1 | 4001 Basel | Schweiz | Tel +41 (0)61 26120-48 | Fax +41 (0)61 26120-49

Zusammenfassung

Angesichts der wachsenden Bedrohung durch Cyberattacken hat der Deutsche Bundestag ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das sogenannte **IT-Sicherheitsgesetz**, erlassen, welches **am 25. Juli 2015 in Kraft getreten** ist[1]. Im Zentrum der Diskussion des Gesetzentwurfes standen Pflichten für Unternehmen, die sogenannte „Kritische Infrastrukturen" betreiben. Allerdings verschärft das IT-Sicherheitsgesetz auch die Pflichten für sämtliche Anbieter kommerzieller Websites.

Betreiber von **Kernkraftwerken** und **Telekommunikationsanbieter** müssen bereits mit Inkrafttreten des IT-Sicherheitsgesetzes Cyber-Atacken melden. Beispielsweise müssen Telekommunikationsunternehmen Kunden darüber informieren, wenn von ihren datenverarbeitenden Systemen Verletzungen der IT-Sicherheit ausgehen. Betroffene sind auf Möglichkeiten hinzuweisen, wie diese Probleme behoben werden können. Für Betreiber sonstiger ***„Kritischer Infrastrukturen"*** gelten entsprechende Pflichten **erst nach Inkrafttreten** einer noch zu erlassenden **Rechtsverordnung**, die das Bundesministerium des Innern derzeit vorbereitet. Die betroffenen Unternehmen aus diesen Bereichen haben daher noch die Gelegenheit sich auf die Änderungen einzustellen und die Umstellung ihrer IT-Prozesse zu überprüfen.

Bereits jetzt bringt das IT-Sicherheitsgesetz **Änderungen** mit sich, die **für nahezu jeden Betreiber einer kommerziellen Website**, wie zum Beispiel Online-Shops oder Websites mit Benutzerkonten relevant sind. Es gelten ab sofort erhöhte Anforderungen zum Schutz von Kundendaten sowie der eigenen IT-Systeme. Diensteanbieter sind verpflichtet, technische und organisatorische Maßnahmen zum Schutz vor unerlaubten Zugriffen auf die personenbezogenen Daten und vor Störungen zu treffen. Dadurch sollen die Verbreitung von Schadsoftware über das Internet eingedämmt sowie Angriffe und Störungen durch Inhalte von Dritten verhindert werden. Diensteanbieter sollten daher den Stand der Technik ihrer Dienste aktualisieren. Die getroffenen Maßnahmen sollten dokumentiert und Vertragspartner zu entsprechenden Schutzmaßnahmen vertraglich verpflichtet werden.

I. Erweiterung der Pflichten für Betreiber „Kritischer Infrastrukturen"

Unternehmen aus systemkritischen Bereichen sind nun verpflichtet, ein Mindestniveau an IT-Sicherheit einzuhalten und Cyber-Atacken zu melden. Durch Änderungen des Telekommunikationsgesetztes sowie des Atomgesetzes gelten in diesen Bereichen bereits mit Inkrafttreten des IT-Sicherheitsgesetzes erhöhte Anforderungen. Für die Betreiber weiterer sogenannter ***„Kritischer Infrastrukturen"*** gelten **ähnliche Pflichten erst nach Erlass einer konkretisierenden Rechtsverordnung**. Relevant wird dies für Unternehmen aus bestimmten Sektoren, die für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung von hoher Bedeutung sind. Nach der Gesetzesbegründung gelten insbesondere Dienstleistungen in den Branchen **Strom-**, **Erdgas-** oder **Mineralölversorgung**, **Telekommunikation** und **Informationstechnik**, **Transportdienstleister im Bereich Luft-**, **Seeschiff-** und **Binnenschifffahrt**, **Schienen-** und **Straßenverkehr**, **medizinische Versorgung**, **Labore**, **Arzneimittel** und **Impfstoffe**, **öffentliche Wasser-** und **Abwasserversorgung**, **Ernährungswirtschaft** und **Lebensmittelhandel**, **Banken**, **Börsen**, **Versicherungen**, sowie **Finanz-** und **Zahlungsdienstleister als Kritische Infrastrukturen**. Der Begriff „Kritische Infrastrukturen" wird daher voraussichtlich weitgefasst werden.

Die Unternehmen, die Kritische Infrastrukturen betreiben, werden unter anderem dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zu treffen, zu denen auch infrastrukturelle und personelle Maßnahmen gehören können, um die Sicherheit ihrer IT-Systeme zu verbessern. Erfasst sind auch Maßnahmen zur Auffindung und Behebung von Störungen. Konkrete Sicherheitsstandards sollen in der Rechtsverordnung festgelegt werden, können aber auch von den betroffenen Unternehmen branchenspezifisch selbst vorgeschlagen werden.

Erhebliche Störungen von IT-Systemen, Komponenten oder Prozessen, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen können, müssen zukünftig der Kontaktstelle beim Bundesamt für Sicherheit in der Informationstechnologie gemeldet werden. Ist es tatsächlich zu einer Beeinträchtigung oder einem Ausfall gekommen, so muss auch der Name des betroffenen Unternehmens offengelegt werden.

Bei vorsätzlichen oder fahrlässigen Verstößen gegen die Vorgaben des IT-Sicherheitsgesetzes drohen den betroffenen Unternehmen Bußgelder in Höhe von bis zu 100.000 Euro.

II. Zusätzliche Pflichten für jeden Anbieter einer kommerziellen Website

Das IT-Sicherheitsgesetz führt zusätzliche Pflichten und Anforderungen für Betreiber geschäftsmäßig angebotener Websites durch Änderung des Telemediengesetzes

[1] http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1349.pdf

ein. Unter den weiten Anwendungsbereich fallen damit jedenfalls sämtliche kommerziellen Websites, Online-Shops sowie durch Werbung finanzierte Websites.

Verhindert werden sollen unerlaubte Zugriffe auf die für Telemedienangebote genutzten technischen Einrichtungen (u.a. Websites). Zudem sollen die kommerziellen Websites gegen unbefugten Zugriff auf personenbezogene Daten und Störungen, gerade auch soweit sie durch äußere Angriffe verursacht sind, besser gesichert werden. Die Unternehmen, die kommerzielle Websites betreiben, haben im Rahmen des ihnen jeweils technisch Möglichen und wirtschaftlich Zumutbaren technische und organisatorische Vorkehrungen zu treffen, um solche Zugriffe möglichst zu verhindern. Dabei gilt es auch Angriffe Dritter abzuwenden, auf die der Diensteanbieter möglicherweise keinen unmittelbaren technischen Einfluss hat, wie beispielsweise im Fall kompromittierter Werbebanner als „Einfallstor" für Schadsoftware.

Verstöße gegen diese Verpflichtungen können mit Bußgeldern in Höhe von bis zu 50.000 Euro geahndet werden.

Zwar führt die Gesetzesänderung unmittelbar keine neuen, zusätzlichen Schadensersatzansprüche ein. Jedoch ist nicht ausgeschlossen, dass durch die erhöhten Pflichten und Anforderungen allgemeine zivilrechtliche Ansprüche von Betroffenen nun einfacher durchgesetzt werden können. Die Gefahren, die durch die Verwendung zum Beispiel unverschlüsselter Websites drohen (zum Beispiel durch Phishing oder Infizierung mit Schadsoftware), können im Einzelfall eine Eigentumsverletzung oder eine Verletzung des allgemeinen Persönlichkeitsrechts darstellen. Für diese könnte der Anbieter der kommerziellen Website dann haften, wenn er es unterlassen hat, die ihm durch die Gesetzesänderung obliegenden Maßnahmen zu treffen und er dadurch möglicherweise Verkehrssicherungspflichten verletzt. Denkbar erscheint auch, dass die durch das IT-Sicherheitsgesetz geschaffenen Anforderungen als sogenanntes „Schutzgesetz" eingeordnet werden, dessen Verletzung den Betroffenen ebenfalls den direkten Weg zu einem allgemeinen, deliktischen Schadensersatzanspruch eröffnet.

Unternehmen, die kommerzielle Websites betreiben, sollten daher die **Sicherheit ihrer Websites prüfen und regelmäßig aktualisieren**. Als sicher anerkannte Verschlüsselungsverfahren sowie sichere und dem jeweiligen Schutzbedarf angemessene Authentifizierungsverfahren, insbesondere bei Verwendung von personenbezogenen Daten, sind zu verwenden. **Verträge mit Dienstleistern und Vertragspartnern**, denen der Anbieter beispielsweise Werbefläche auf einer Website zur Verfügung stellt, **sollten überprüft und bei Bedarf** so **geändert werden**, dass entsprechende Verpflichtungen sowie etwaige Schadenersatzansprüche an diese Vertragspartner weitergereicht werden können. Sämtliche Maßnahmen sollten rechtssicher dokumentiert werden, um etwaigen Vorwürfen mangelhafter Organisation im Ernstfall effektiv begegnen zu können.

Wir wollen, dass unsere Mandanten auch in rechtlicher Hinsicht mit dem technischen Fortschritt und den gesetzlichen Anforderungen Schritt halten. Hierzu beraten wir unsere Mandanten in sämtlichen Fragen, die sich ihnen in den Bereichen des IT-Rechts stellen. Wir vertreten in- und ausländische IT-Unternehmen, Softwareentwickler, aber auch Auftraggeber bei der Vorbereitung und Durchführung von IT- und EDV-Projekten, beraten IT-Unternehmen bei ihren M&A Projekten und betreuen unsere Mandanten bis hin zum Streitfall vor Gericht.

Ansprechpartner:

Axel Staudt, LL.M.
Rechtsanwalt und Partner
staudt@franzlegal.com
Praxisgruppe
Mergers & Acquisition

Karsten Korrat
Rechtsanwalt und Partner
korrat@franzlegal.com
Praxisgruppe
Operatives Geschäft