Prof. Dr. Viola Schmid, LL.M. (Harvard)

Fachgebiet Öffentliches Recht

Datum	Titel
04.06.2007	**CyLaw-Quiz: Das kleine 1x1 des IT-Sicherheitsrechts**

I. Was sind die sechs Ziele der IT-Sicherheit?

1. **Verfügbarkeit:** Der Berechtigte muss die IT nutzen können. Dem Entzug, dem Verlust und der Zerstörung von Informationen muss vorgebeugt werden.
2. **Unversehrtheit (Integrität)**: Die IT muss vor unautorisierten Veränderungen geschützt werden. Unautorisierte Veränderungen müssen wenigstens bemerkt werden.
3. **Authentizität**: Nutzer der IT müssen eindeutig identifiziert und ihre Identität muss verifiziert sein (Beispiel: elektronische Signaturen).
4. **Vertraulichkeit**: Die IT muss vor der Einsicht durch Unberechtigte geschützt werden.
5. **Verbindlichkeit**: Informationstechnologische Handlungen sollen beweisbar sein (Beispiel: Zugang elektronischer Willenserklärungen).
6. Nach Auffassung des Fachgebiets Öffentliches Recht an der Technischen Universität Darmstadt: **Recht auf informationelle Selbstbestimmung** (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz) muss geschützt werden.

Art. 1 GG [Schutz der Menschenwürde]
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. 3In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

II. Wo ist IT-Sicherheit gesetzlich definiert?

In § 2 Absatz 2 des Gesetzes zur Errichtung des Bundesamts für Sicherheit in der Informationstechnik (BSIG).

§ 2 BSIG [Begriffsbestimmungen]
(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
1. in informationstechnischen Systemen oder Komponenten oder
2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.

III. Was ist auf Bundesebene die „Magna Charta" des deutschen IT-Sicherheitsrechts?

§ 9 Bundesdatenschutzgesetz mit Anlage

§ 9 BDSG [Technische und organisatorische Maßnahmen]
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage (zu § 9 Satz 1)
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

IV. Ist IT-Sicherheit in der deutschen Verfassung – im Grundgesetz – verankert?

In wörtlicher Auslegung gibt es kein Recht auf Datenschutz im Grundgesetz von 1949. Dieses Recht auf Datenschutz musste vom Bundesverfassungsgericht 1983 in seiner bahnbrechenden „Volkszählungsentscheidung“ (BVerfGE 65, 1) aus Artikel 2 Absatz 1 und Artikel 1 Absatz 1 Grundgesetz entwickelt werden.

Art. 1 GG [Schutz der Menschenwürde]
(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]
(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. 3In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Das Recht auf Datenschutz trägt seit dieser Rechtsprechung den Namen „Recht auf Informationelle Selbstbestimmung“. Weil folgendes Motto gilt: „Kein Datenschutz ohne IT-Sicherheit“ ist auch der Anspruch auf IT-Sicherheit vom Recht auf informationelle Selbstbestimmung umfasst (teleologische Auslegung). Die Verpflichtung zur IT-Sicherheit zum Schutz **personenbezogener Daten** ergibt sich deshalb aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz. Darüber hinaus ist das Recht auf IT-Sicherheit dann verfassungsrechtlich geschützt, wenn IT-Sicherheit Voraussatzung für den Schutz der Gesundheit ist (Artikel 2 Absatz 2 Grundgesetz) – also etwa in der Medizintechnik.

Art. 2 GG [Freie Entfaltung der Persönlichkeit, Recht auf Leben, körperliche Unversehrtheit, Freiheit der Person]
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. 3In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

V. Welche deutschen und europäischen Behörden gibt es, die sich mit IT-Sicherheit im Speziellen befassen?

IT-Sicherheit ist eine Querschnittsmaterie, die alle staatlichen Akteure beschäftigen muss. Es gibt aber folgende Behörden, die sich fokussiert mit IT-Sicherheit befassen.

1. Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Das BSI forscht im Bereich der Informationssicherheit, prüft IT-Produkte und berät Hersteller, Vertreiber und Nutzer von Informationstechnik. Insbesondere versucht das BSI hierbei auf drohende Gefährdungen hinzuweisen und durch Sicherheitskonzepte IT-Sicherheit handhabbar zu machen. Hierzu stellt es ein Grundschutzhandbuch zur Verfügung. Seit 2001 übernimmt das BSI im Rahmen des CERT-Bund ("Computer Emergency Response Team für Bundesbehörden") die Aufgabe einer Expertenkommission zur Prävention zum Management akuter Krisenfälle im IT-Netz des Bundes.

§ 3 BSIG [Aufgaben des Bundesamtes]
(1) Das Bundesamt hat zur Förderung der Sicherheit in der Informationstechnik folgende Aufgaben:
1. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik, soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist,
2. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten,
3. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten,
4. Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlußsachen) im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen, sowie die Herstellung von Schlüsseldaten, die für den Betrieb zugelassener Verschlüsselungsgeräte benötigt werden,
5. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht,
6. Unterstützung
a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,
b) der Verfassungsschutzbehörden bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder anfallen.
Die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen. 3Die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen,

7. Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen.
(2) Im Falle des Absatzes 1 Nr. 2 werden Entscheidungen über Kriterien und Verfahren, die als Grundlage für die Erteilung von Sicherheitszertifikaten nach § 4 dienen, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie getroffen.

2. Bundesnetzagentur

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen entspricht der früheren Regulierungsbehörde für Gas, Elektrizität, Telekommunikation und Post (RegTP) und hat mit Wirkung vom 13.07.2005 deren Aufgaben übernommen.

§ 2 BEGTPG [Tätigkeiten, Aufgabendurchführung]
(1) Die Bundesnetzagentur ist auf den Gebieten
1. des Rechts der leitungsgebundenen Versorgung mit Elektrizität und Gas, einschließlich des Rechts der erneuerbaren Energien im Strombereich,
2. des Telekommunikationsrechts,
3. des Postrechts sowie
4. des Rechts des Zuganges zur Eisenbahninfrastruktur nach Maßgabe des Bundeseisenbahnverkehrsverwaltungsgesetzes
tätig.
(2) Die Bundesnetzagentur nimmt im Rahmen der ihr nach Absatz 1 zugewiesenen Tätigkeiten die Verwaltungsaufgaben des Bundes wahr, die ihr durch Gesetz oder auf Grund eines Gesetzes zugewiesen sind.

Die Bundesnetzagentur verfügt sowohl im Telekommunikations- (§ 115 Telekommunikationsgesetz) als auch im Signaturrecht (§ 19 Signaturgesetz) über Aufsichts- und Kontrollbefugnisse.

3. Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Die ENISA berät und unterstützt die Kommission und die Mitgliedstaaten bei der Verbesserung der Informationssicherheit, etwa durch Risikoanalysen, Entwicklung von Standards oder Förderung des Dialogs mit der Industrie.

Artikel 3 Verordnung 460/2004/EG zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit [Aufgaben]
Um zu gewährleisten, dass dem Zuständigkeitsbereich und den Zielen gemäß den Artikeln 1 und 2 entsprochen wird, nimmt die Agentur folgende Aufgaben wahr:
a) Erhebung geeigneter Informationen zur Analyse der derzeitigen und absehbaren Risiken sowie — insbesondere auf europäischer Ebene — der Risiken, die sich auf die Belastbarkeit und die Verfügbarkeit elektronischer Kommunikationsnetze und auf die Authentizität, Integrität und Vertraulichkeit der auf diesem Weg abgerufenen und übertragenen Informationen auswirken könnten, sowie Bereitstellung der Analyseergebnisse für die Mitgliedstaaten und die Kommission;

b) im Rahmen ihrer Ziele Beratung und — auf Verlangen — Unterstützung des Europäischen Parlaments, der Kommission, europäischer Stellen und Einrichtungen oder der von den Mitgliedstaaten benannten zuständigen Stellen;
c) Förderung der Zusammenarbeit zwischen verschiedenen Akteuren im Bereich der Netz- und Informationssicherheit, unter anderem durch regelmäßige Anhörung der Industrie, der Hochschulen sowie anderer betroffener Sektoren und durch den Aufbau von Kontaktnetzen für gemeinschaftliche Stellen sowie für die von den Mitgliedstaaten benannten öffentlichen Stellen und für Organisationen des Privatsektors und Verbraucherorganisationen;
d) Erleichterung der Zusammenarbeit zwischen der Kommission und den Mitgliedstaaten bei der Entwicklung gemeinsamer Methoden zur Verhütung, Bewältigung und Behebung von Problemen im Bereich der Netz- und Informationssicherheit;
e) Beitrag zur Sensibilisierung und zur frühzeitigen, objektiven und umfassenden Informationsvermittlung in Fragen der Netz- und Informationssicherheit für alle Nutzer, unter anderem durch Förderung des Austauschs der jeweils besten Verfahren, einschließlich der Verfahren zur Warnung der Nutzer, sowie durch Nutzung der Synergieeffekte zwischen Initiativen des öffentlichen und des privaten Sektors;
f) Unterstützung der Kommission und der Mitgliedstaaten in ihrem Dialog mit der Industrie, um sicherheitsrelevante Probleme bei Hardware- und Softwareprodukten anzugehen;
g) Verfolgen der Entwicklung von Standards für Produkte und Dienstleistungen im Bereich der Netz- und Informationssicherheit;
h) Beratung der Kommission in Bezug auf Forschungsarbeiten im Bereich der Netz- und Informationssicherheit sowie hinsichtlich des effizienten Einsatzes von Technologien zur Risikovermeidung;
i) Förderung von Risikobewertungsmaßnahmen und interoperablen Lösungen für das Risikomanagement sowie von Studien über Lösungen für das Präventionsmanagement innerhalb von Organisationen des öffentlichen und des privaten Sektors;
j) Beitrag zu den Bemühungen der Gemeinschaft um eine Zusammenarbeit mit Drittländern und gegebenenfalls mit internationalen Organisationen zur Förderung eines gemeinsamen Gesamtkonzepts für Fragen der Netz- und Informationssicherheit, wodurch zur Entwicklung einer Kultur der Netz- und Informationssicherheit beigetragen wird;
k) unabhängige Formulierung eigener Schlussfolgerungen, Leitlinien und Ratschläge zu Fragen innerhalb ihrer Zuständigkeiten und Ziele.

VI. Nach welchem Gesetz wird für Schäden infolge der Verletzung von IT-Sicherheitspflichten gehaftet?

Es gibt noch keine Gerichtsurteile, aber §§ 7 und 8 Bundesdatenschutzgesetz (BDSG) sehen Schadensersatzpflichten vor, wenn IT-Sicherheitspflichten nicht erfüllt werden („unrichtige Erhebung, Verarbeitung und Nutzung von Daten“).

§ 7 BDSG [Schadensersatz]
Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 BDSG [Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen]
(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.
(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.
(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130.000 Euro begrenzt. Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130.000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.
(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.
(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.
(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

Darüber hinaus kann die Nichterfüllung von IT-Sicherheitspflichten vertragliche Ansprüche begründen, etwa wenn Software verkauft wird, die „IT-unsicher“ ist.

VII. Müssen Computer mit Passwörtern geschützt werden?

Immer dann, wenn personenbezogene Daten nicht nur für persönliche und familiäre Tätigkeiten erhoben, genutzt oder verarbeitet werden; ja.

Anlage (zu § 9 Satz 1)
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
(…)
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
(…)

VIII. Müssen WLANs mit Passwort geschützt werden?

Wenn man eine unterinstanzliche Entscheidung des Landgerichts Hamburg (Urteil vom 26.07.2006, Aktenzeichen 308 O 407/06) verallgemeinern würde: ja.

IX. Ist ein Provider (IT-Infrastruktur) zur IT-Sicherheit verpflichtet?

Ja, nach § 109 des Telekommunikationsgesetzes.

§ 109 TKG [Technische Schutzmaßnahmen]
(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze
1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe
zu treffen.
(2) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Dabei sind der Stand der technischen Entwicklung sowie die räumliche Unterbringung eigener Netzelemente oder mitbenutzter Netzteile anderer Netzbetreiber zu berücksichtigen. Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Betreiber der Anlagen die Verpflichtungen nach Absatz 1 und Satz 1 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Betreiber zugeordnet werden können. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.
(3) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat einen Sicherheitsbeauftragten oder eine Sicherheitsbeauftragte zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,
1. welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden,
2. von welchen Gefährdungen auszugehen ist und
3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.
Das Sicherheitskonzept ist der Bundesnetzagentur unverzüglich nach Aufnahme der Telekommunikationsdienste vom Betreiber vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Bundesnetzagentur unter Hinweis auf die Änderungen erneut vorzulegen. Die Sätze 1 bis 4 gelten nicht für Betreiber von Telekommunikationsanlagen, die ausschließlich dem Empfang oder der Verteilung von Rundfunksignalen dienen. Für Sicherheitskonzepte, die der Bundesnetzagentur auf der Grundlage des § 87 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120) vorgelegt wurden, gilt die Verpflichtung nach Satz 2 als erfüllt.

X. Muss ein Unternehmen bei IT-Sicherheitslücken (öffentlich) warnen?

Eine ganz grundsätzliche Frage, die bisher von einer verbreiteten Meinung in der rechtswissenschaftlichen Literatur noch nicht beantwortet worden ist. Es gibt politische Bestrebungen, eine solche Warnpflicht spezialgesetzlich zu fixieren (Antrag „Informationspflichten für Unternehmen bei Datenschutzpannen einführen“, BT-Drs 16/1887).