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

Fachgebiet Öffentliches Recht

Informations- und Datenschutzrecht I

DATUM	MODUL	TITEL
24.01.2006	**6**	**Sicherheitsrecht für IT-Systeme**

A. Begriff der IT-Sicherheit

I. Sicherheit im Recht?

Sicherheit ist im Völker-, Europa-, Bundes- und Landesrecht ein ebenso viel benutzter wie explizit grammatisch nicht definierter Begriff:

1. Völkerrecht

Art. 9 Internationaler Pakt über bürgerliche und politische Rechte[1]
(1) Jedermann hat ein Recht auf persönliche Freiheit und **Sicherheit**. Niemand darf willkürlich festgenommen oder in Haft gehalten werden. Niemand darf seine Freiheit entzogen werden, es sei denn aus gesetzlich bestimmten Gründen und unter Beachtung des im Gesetz vorgeschriebenen Verfahrens. (…)

2. Europarecht

Artikel 29 EU[2]
Unbeschadet der Befugnisse der Europäischen Gemeinschaft verfolgt die Union das Ziel, den Bürgern in einem **Raum der Freiheit, der Sicherheit und des Rechts** ein hohes Maß an Sicherheit zu bieten, indem sie ein gemeinsames Vorgehen der Mitgliedstaaten im Bereich der polizeilichen und justitiellen Zusammenarbeit in Strafsachen entwickelt sowie Rassismus und Fremdenfeindlichkeit verhütet und bekämpft.
Dieses Ziel wird erreicht durch die Verhütung und Bekämpfung der - organisierten oder nichtorganisierten - Kriminalität, insbesondere des Terrorismus, des Menschenhandels und der Straftaten gegenüber Kindern, des illegalen Drogen- und Waffenhandels, der Bestechung und Bestechlichkeit sowie des Betrugs im Wege einer
- engeren Zusammenarbeit der Polizei-, Zoll- und anderer zuständiger Behörden in den Mitgliedstaaten, sowohl unmittelbar als auch unter Einschaltung des Europäischen Polizeiamts (Europol), nach den Artikeln 30 und 32;
- engeren Zusammenarbeit der Justizbehörden sowie anderer zuständiger Behörden der Mitgliedstaaten, auch unter Einschaltung der Europäischen Stelle für justizielle Zusammenarbeit (Eurojust), nach den Artikeln 31 und 32;
- Annäherung der Strafvorschriften der Mitgliedstaaten nach Artikel 31 Buchstabe e, soweit dies erforderlich ist.

Die Bedeutung von Sicherheit in der Europäischen Union kann nur im Kontext der Trias von Freiheit, Sicherheit und Recht verstanden werden. In einem Aktionsplan[3] haben Kommission und Rat grundlegende Feststellungen dazu getroffen:

---

[1] Internationaler Pakt über bürgerliche und politische Rechte vom 19.12.1966.
[2] Vertrage über die Europäische Union (Konsolidierte Fassung) vom 24.12.2002, ABl C 325.
Der Vertrag wird hier mit „EU-Vertrag“ abgekürzt, soweit es sich um die bis zum 01.05.1999 geltende Fassung handelt, und mit „EU“, soweit es sich um die ab dem 01.05.1999 geltende Fassung handelt, so wie es auch der EuGH in seinen Hinweisen zur Zitierweise vorsieht und handhabt.
[3] Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts vom Rat vom 3.12.1998, ABl. 1999 C 19.

Aktionsplan, ABl. C 19, S. 1
„Diese drei Begriffe hängen eng zusammen. Die Freiheit verliert viel von ihrer Bedeutung, wenn sie nicht in einem sicheren Umfeld und mit der vollen Unterstützung eines Rechtssystems genossen werden kann, in das alle Bürger und Gebietsansässigen der Union Vertrauen haben können. Diese drei untrennbar miteinander verknüpften Konzepte haben einen gemeinsamen Nenner - die Menschen -, **und die volle Verwirklichung des einen setzt die Verwirklichung der beiden anderen voraus**. Zwischen ihnen ein ausgewogenes Verhältnis zu wahren, muss für das Vorgehen der Union Richtschnur sein."

Zum Begriff „Freiheit" heißt es im Aktionsplan zunächst:

Aktionsplan, ABl. C 19, S. 3
„Ein umfassender Freiheitsbegriff (…)
Freiheit im Sinne des freien Personenverkehrs innerhalb der Europäischen Union bleibt ein grundlegendes Ziel... zu dem die flankierenden Maßnahmen im Zusammenhang mit den Konzepten Sicherheit und Recht einen wesentlichen Beitrag leisten müssen."

Der Aktionsplan nimmt auch Stellung zur Bedeutung der Privatsphäre als Grundfreiheit und setzt diesen in Beziehung zu öffentlichen Sicherheitsinteressen.

Sicherheit wird als Grundvoraussetzung für ein Leben in einem Raum der Freiheit gesehen.

Aktionsplan, ABl. C 19, S. 3
„Ein Raum der Sicherheit (…)
Die Vorteile eines **Raums der Freiheit** können im vollen Umfang nur in einem Umfeld genossen werden, in dem sich Menschen völlig **sicher** fühlen (….)
Erklärtes Ziel ist die Verhütung der „organisierten oder nicht organisierten Kriminalität insbesondere des Terrorismus, des Menschenhandels und der Straftaten gegenüber Kindern, des illegalen Drogen- und Waffenhandels, der Bestechung und Bestechlichkeit sowie des Betrugs" auf der jeweils angemessenen Ebene."

Schließlich wird im Aktionsplan auch die Bedeutung des Rechts für die Wahrung von Freiheit und Sicherheit betont. Dabei wird jedoch darauf hingewiesen, dass in den einzelnen Mitgliedstaaten unterschiedliche rechtliche Traditionen vorhanden sind. Es soll eine gemeinsame Vorstellung von Recht in der EU entwickelt werden.

Aktionsplan, ABl. C 19, S. 4
„Ein Raum des **Rechts** (…)
wobei berücksichtigt werden muss, dass aus tief in der Geschichte und der Tradition verwurzelten Gründen die Rechtssysteme der Mitgliedstaaten große Unterschiede aufweisen. Ziel ist es, den Bürgern in der gesamten Union eine gemeinsame Vorstellung davon zu vermitteln, was **Recht** ist:
Es erleichtert das alltägliche Leben der Menschen und gewährleistet, daß jene, welche die **Freiheit und Sicherheit** des einzelnen und der Gesellschaft gefährden, zur Rechenschaft gezogen werden. Dies setzt den Zugang zum Recht und eine uneingeschränkte justitielle Zusammenarbeit zwischen den Mitgliedstaaten voraus."

Art. 5 EMRK[4]
(1) Jedermann hat das Recht auf **Freiheit** und **Sicherheit**. (…)

3. Bundesrecht

Art. 24 Abs. 2 GG
(2) Der Bund kann sich zur Wahrung des Friedens einem System gegenseitiger kollektiver **Sicherheit** einordnen; er wird hierbei in die Beschränkungen seiner Hoheitsrechte einwilligen, die eine friedliche und dauerhafte Ordnung in Europa und zwischen den Völkern der Welt herbeiführen und sichern. (…)

4. Landesrecht

§ 1 HSOG[5] **[Aufgaben der Gefahrenabwehr- und der Polizeibehörden]**
(1) Die Gefahrenabwehrbehörden (Verwaltungsbehörden, Ordnungsbehörden) und die Polizeibehörden haben die gemeinsame Aufgabe der Abwehr von **Gefahren für die öffentliche Sicherheit oder Ordnung (Gefahrenabwehr)**, soweit dieses Gesetz nichts anderes bestimmt. Sie haben im Rahmen dieser Aufgabe auch die erforderlichen Vorbereitungen für die Hilfeleistung in Gefahrenfällen zu treffen.
(2) Die **Gefahrenabwehr**- und die Polizeibehörden haben ferner die ihnen durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben zu erfüllen.
(3) Der Schutz privater Rechte obliegt den Gefahrenabwehr- und den Polizeibehörden nach diesem Gesetz nur dann, wenn gerichtlicher Schutz nicht rechtzeitig zu erlangen ist und wenn ohne gefahrenabwehrbehördliche oder polizeiliche Hilfe die Verwirklichung des Rechts vereitelt oder wesentlich erschwert werden würde.
(4) Die Polizeibehörden haben im Rahmen der Gefahrenabwehr auch zu erwartende Straftaten zu verhüten sowie für die Verfolgung künftiger Straftaten vorzusorgen (vorbeugende Bekämpfung von Straftaten).
(…)

§ 26 HSOG [Besondere Formen des Datenabgleichs]
(1) Die Polizeibehörden können von öffentlichen Stellen oder Stellen außerhalb des öffentlichen Bereichs zur Verhütung von Straftaten erheblicher Bedeutung
1. gegen den Bestand oder die **Sicherheit** des Bundes oder eines Landes oder
2. bei denen Schäden für Leben, Gesundheit oder Freiheit oder gleichgewichtige Schäden für die Umwelt zu erwarten sind,
die Übermittlung von personenbezogenen Daten bestimmter Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung dieser Straftaten erforderlich und dies auf andere Weise nicht möglich ist. Rechtsvorschriften über ein Berufs- oder besonderes Amtsgeheimnis bleiben unberührt.
(2) Das Übermittlungsersuchen ist auf Namen, Anschriften, Tag und Ort der Geburt sowie auf im einzelnen Falle festzulegende Merkmale zu beschränken. Werden wegen technischer Schwierigkeiten, die mit angemessenem Zeit- oder Kostenaufwand nicht beseitigt werden können, weitere Daten übermittelt, dürfen diese nicht verwertet werden.

[4] Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04.11.1950.
[5] Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i.d.F. vom 14.01.2005.

(3) Ist der Zweck der Maßnahme erreicht oder zeigt sich, daß er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind, unverzüglich zu vernichten. Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische und organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.
(4) Die Maßnahme nach Abs. 1 bedarf der schriftlich begründeten Anordnung durch die Behördenleitung und der Zustimmung des Landespolizeipräsidiums. Von der Maßnahme ist die oder der Hessische Datenschutzbeauftragte unverzüglich zu unterrichten.
(5) Personen, gegen die nach Abschluss einer Maßnahme nach Abs. 1 weitere Maßnahmen durchgeführt werden, sind hierüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zweckes der weiteren Datennutzung erfolgen kann. § 15 Abs. 7 HSOG gilt entsprechend.

II. Sicherheit und IT-Sicherheit

Das Verhältnis von Sicherheit zu IT-Sicherheit kann exemplarisch am Beispiel von Art. I-42 VEV[6] - ansatzweise vergleichbar mit Art. 29 EU - aufgezeigt werden.

Artikel I-42 VEV [Besondere Bestimmungen über den Raum der Freiheit, der Sicherheit und des Rechts]
(1) Die Union bildet einen **Raum der Freiheit, der Sicherheit und des Rechts**.
a) durch den Erlass von Europäischen Gesetzen und Rahmengesetzen, mit denen, soweit erforderlich, die Rechtsvorschriften der Mitgliedstaaten in den in Teil III genannten Bereichen einander angeglichen werden sollen;
b) durch Förderung des gegenseitigen Vertrauens zwischen den zuständigen Behörden der Mitgliedstaaten, insbesondere auf der Grundlage der gegenseitigen Anerkennung der gerichtlichen und außergerichtlichen Entscheidungen;
c) durch operative Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten einschließlich der Polizei, des Zolls und anderer auf die Verhütung und die Aufdeckung von Straftaten spezialisierter Behörden.
(2) Die nationalen Parlamente können sich im Rahmen des Raums der Freiheit, der Sicherheit und des Rechts an den Bewertungsmechanismen nach Artikel III-260 beteiligen. Sie werden in die politische Kontrolle von Europol und die Bewertung der Tätigkeit von Eurojust nach den Artikeln III-276 und III-273 einbezogen.
(3) Die Mitgliedstaaten verfügen nach Artikel III-264 über ein Initiativrecht im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.

Der Beitrag von IT-Systemen zur Schaffung dieses **„sicheren Raums“** wird in Art. I-42 Abs. 1 c VEV von den Verfassungsgebern vorausgesetzt.

[6] Vertrag über eine Verfassung für Europa vom 16.12.2004, ABl. C 310.

Sicherheit als Prävention und Sanktion von „Verbrechen“[7] setzt Wissen voraus. Die Europäische Union will ihr Wissen durch IT-Systeme vermehren beziehungsweise unter den Mitgliedsländern verteilen. Dabei werden zwei Strategien verfolgt: zum einen der Aufbau von europäischen Behörden und Daten„organisations“systemen[8] (etwa Europol) und zum anderen die Förderung der Interoperabilität von mitgliedstaatlichen Behörden und öffentlich-rechtlichen sowie privat-rechtlichen Datenorganisationssystemen untereinander. Bereits die Komplexität und Quantität dieser sicherheitsrechtlichen Zusammenarbeit verlangt nach IT-Sicherheit. Prozesse der Datenorganisation sind nicht auf einen Mitgliedstaat oder die Union beschränkbar – Datenorganisationen via Cyberspace sind international, wie etwa der Zugriff amerikanischer Zoll- und Grenzschutzbehörden[9] auf die Fluggastdaten von (europäischen) Fluggesellschaften zeigt. Diese Internationalität der IT-Systeme verlangt, dass sie, wenn sie sicherheitspolitisch eingesetzt werden, selbst sicher (und selbstsicher) sind. Andernfalls würde IT-Sicherheit zu einem zusätzlichen Risiko für die Sicherheit. Auch diese Gefahr lässt sich anhand des europäisch-amerikanischen Konflikts über die „Organisation“ von Fluggastdaten belegen. Sicherheitsrechtlich ist hier auch zu beachten, dass es Kriminellen nicht ermöglicht werden soll, die Angriffsziele zu ermitteln, indem sie die potentiellen Opfer zwischen den Fluggästen konkreter Routen informiert auswählen. Diese Gefahr ist nicht zu gering einzuschätzen, wenn man den Inhalt der Daten[10] in Betracht zieht.

Zusammengefasst: **Sicherheit durch IT-Systeme; aber keine Sicherheit ohne IT-Sicherheit.**

---

[7] FEX: Im (Neben-)Strafrecht werden Verbrechen, Vergehen, und Ordnungswidrigkeiten unterschieden. FÖR befasst sich im IT-Sicherheitskontext fokussiert mit Straftaten, die die juristische Bewertung als „Verbrechen“ bezeichnen würde:

§ 12 StGB [Verbrechen und Vergehen]
(1) Verbrechen sind rechtswidrige Taten, die im Mindestmaß mit Freiheitsstrafe von, einem Jahr oder darüber bedroht sind. (…)

[8] „Organisation“ wird hier als Oberbegriff für die Erhebung, Verarbeitung und Nutzung im Sinne von § 3 Abs. 3– 5 BDSG verwandt (siehe Modul 1, B III).

[9] Geregelt im Aviation and Transportation Security Act vom 19.11.2001. Den amerikanischen Behörden müssen nicht nur Daten übermittelt, es muss ihnen darüber hinaus der Zugriff auf die Fluggastdatenbank gewährt werden.

[10] So enthält etwa der PNR (Passenger Name Record) Fluggastdatensatz Informationen über Buchungsinformationen (Daten, Kreditkarteninformationen, etc.), Reisestrecke und Angaben zu Religion und Ethnie (Wahl des Menüs).

III. IT-Sicherheit in einer dynamischen (technikorientierten) Auslegung

Auch zur IT-Sicherheit gibt es keine normübergreifende Legaldefinition – IT-Sicherheit wird in unterschiedlichen Gesetzen aus unterschiedlichen Perspektiven verlangt bzw. vorausgesetzt. So definieren Gesetze und internationale Empfehlungen für den jeweiligen territorialen, personalen und objektiven Geltungsbereich (IT-)Sicherheit unterschiedlich.

1. Völkerrecht

OECD Guidelines for the Security of Information Systems and Networks[11]
PREFACE
(...) Today, participants are increasingly interconnected and the connections cross national borders. (...) The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially. As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security.

2. Europarecht

Art. 4 Verordnung zur Gründung einer Agentur für Netz- und Informationssicherheit[12] **[Begriffsbestimmungen]**
Im Sinne dieser Verordnung bezeichnet der Ausdruck
(…)
– *„Netz- und Informationssicherheit"*: die Fähigkeit eines Netzes oder Informationssystems, bei einem bestimmten Vertrauensniveau Störungen und rechtswidrige oder böswillige Angriffe abzuwehren, die die **Verfügbarkeit**, **Authentizität**, **Integrität** und **Vertraulichkeit** gespeicherter oder übermittelter Daten und entsprechender Dienste beeinträchtigen, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind.

3. Bundesrecht

§ 9 Bundesdatenschutzgesetz (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.

[11] OECD Guidelines for the Security of Information Systems and Networks vom 25.07.2002.
[12] Verordnung zur Gründung einer Agentur für Netz- und Informationssicherheit vom 10.3.2004, ABl. L 77/1.

Anlage zu § 9 BDSG
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.

Das BDSG enthält anders als das Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG)[13] keine Normierung bestimmter Sicherheitsschutzziele, sondern einen Katalog von Kontrollen, die bei der Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen einzuhalten sind.

§ 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.

Im Vergleich zu dem gemeinschaftsrechtlichen Definitionsvorschlag verzichtet das BSIG in grammatischer Auslegung auf die Authentizität.

[13] Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG) vom 17.12.1990, BGBL I, 2834.

§ 109 Telekommunikationsgesetz (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.**
(…)

§ 55a VwGO [Elektronische Dokumentenübermittlung]
(1) Die Beteiligten können dem Gericht elektronische Dokumente übermitteln, soweit dies für den jeweiligen Zuständigkeitsbereich durch Rechtsverordnung der Bundesregierung oder der Landesregierungen zugelassen worden ist. Die Rechtsverordnung bestimmt den Zeitpunkt, von dem an Dokumente an ein Gericht elektronisch übermittelt werden können, sowie die Art und Weise, in der elektronische Dokumente einzureichen sind. Für Dokumente, die einem schriftlich zu unterzeichnenden Schriftstück gleichstehen, ist eine qualifizierte elektronische Signatur nach § 2 Nr. 3 des Signaturgesetzes vorzuschreiben. **Neben der qualifizierten elektronischen Signatur kann auch ein anderes sicheres Verfahren zugelassen werden, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt.** Die Landesregierungen können die Ermächtigung auf die für die Verwaltungsgerichtsbarkeit zuständigen obersten Landesbehörden übertragen. Die Zulassung der elektronischen Übermittlung kann auf einzelne Gerichte oder Verfahren beschränkt werden. Die Rechtsverordnung der Bundesregierung bedarf nicht der Zustimmung des Bundesrates.
(2) Ein elektronisches Dokument ist dem Gericht zugegangen, wenn es in der von der Rechtsverordnung nach Absatz 1 Satz 1 und 2 bestimmten Art und Weise übermittelt worden ist und wenn die für den Empfang bestimmte Einrichtung es aufgezeichnet hat. Die Vorschriften dieses Gesetzes über die Beifügung von Abschriften für die übrigen Beteiligten finden keine Anwendung. Genügt das Dokument nicht den Anforderungen, ist dies dem Absender unter Angabe der für das Gericht geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.
(3) Soweit eine handschriftliche Unterzeichnung durch den Richter oder den Urkundsbeamten der Geschäftsstelle vorgeschrieben ist, genügt dieser Form die Aufzeichnung als elektronisches Dokument, wenn die verantwortenden Personen am Ende des Dokuments ihren Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 des Signaturgesetzes versehen.

4. Landesrecht

§ 10 HDSG[14] [Technische und organisatorische Maßnahmen]
(1) Die datenverarbeitende oder in ihrem Auftrag tätige Stelle hat die **technischen und organisatorischen Maßnahmen** zu treffen, die nach Abs. 2 und 3 erforderlich sind, um die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu gewährleisten. Erforderlich sind diese Maßnahmen, soweit der damit verbundene Aufwand unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Verarbeitung zum Schutz des in § 1 Abs. 1 Nr. 1 genannten Rechts angemessen ist.
(2) Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, daß
1. Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, erhalten (**Zutrittskontrolle**),
2. Unbefugte an der Benutzung von Datenverarbeitungsanlagen und -verfahren gehindert werden (**Benutzerkontrolle**),
3. die zur Benutzung eines Datenverarbeitungsverfahrens Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (**Zugriffskontrolle**),
4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (**Datenverarbeitungskontrolle**),
5. es möglich ist, festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (**Verantwortlichkeitskontrolle**),
6. personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. durch eine Dokumentation aller wesentlichen Verarbeitungsschritte die Überprüfbarkeit der Datenverarbeitungsanlage und des -verfahrens möglich ist (**Dokumentationskontrolle**),
8. die innerbehördliche oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird (**Organisationskontrolle**).
(3) Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Das Hessische Datenschutzgesetz formuliert ähnlich wie das BDSG verschiedene Kontrollen, welche bei der Verarbeitung personenbezogener Daten durch technische und organisatorische Maßnahmen einzuhalten sind. Anders als das HDSG nimmt die landesdatenschutzrechtliche Regelung in Nordrhein-Westfalen ausdrücklich Bezug auf die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Diese werden durch die Schutzziele Revisionsfähigkeit und Transparenz ergänzt.

[14] Hessisches Datenschutzgesetz vom 11.11.1986.

§ 10 DSG-NW[15] [Technische und organisatorische Maßnahmen]
(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen.
(2) Dabei sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass
1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (**Vertraulichkeit**),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (**Authentizität**),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).
(3) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzepts zu ermitteln, zu dessen Bestandteilen die Vorabkontrolle hinsichtlich möglicher Gefahren für das in § 1 geschützte Recht auf informationelle Selbstbestimmung gehört, die vor der Entscheidung über den Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens durchzuführen ist. Das Verfahren darf nur eingesetzt werden, wenn diese Gefahren nicht bestehen oder durch Maßnahmen nach den Absätzen 1 und 2 verhindert werden können. Das Ergebnis der Vorabkontrolle ist aufzuzeichnen. Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.
(4) Der Landesrechnungshof kann von der zu prüfenden Stelle verlangen, dass für ein konkretes Prüfungsverfahren die notwendigen Maßnahmen nach den Absätzen 1 bis 3 zeitnah geschaffen werden.

In Hessen erfolgt eine Bezugnahme auf Sicherheitsziele zwar nicht auf gesetzlicher Ebene. Allerdings finden die Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit bei der internen Organisation der IT in der Landesverwaltung durch eine IT-Sicherheitsleitlinie[16] Beachtung.

IT-Sicherheitsleitlinie für die Hessische Landesverwaltung
3. Ziele
3.1 Alle Beschäftigten gewährleisten die IT-Sicherheit durch ihr verantwortliches Handeln und halten die für die IT-Sicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.
3.2 Für den IT-Einsatz sind die **Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit** im jeweils erforderlichen Maße zu erreichen. Die daraus abgeleiteten Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die IT-Nutzung ergeben.

[15] Datenschutzgesetz Nordrhein-Westfalen 09.06.2000.
[16] IT-Sicherheitsleitlinie für die Hessische Landesverwaltung. FEX: Bei der IT-Sicherheitsleitlinie handelt es sich um bloßes Verwaltungsinnenrecht ohne Bindungswirkung nach außen.

3.3 Die Sicherheit der IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.

Aus rechtswissenschaftlicher Sicht ist festzuhalten, dass eine Definition der IT-Sicherheit normspezifisch ermittelt werden muss. Darüber hinaus wird auch deutlich, dass das Recht grundsätzlich nicht bestimmt, **welche IT-Sicherheit wie im Detail verlangt wird**. Eine dynamische und technikorientierte Auslegung verlangt deshalb die Integration der technikwissenschaftlichen Perspektive. Nicht überraschend gilt dort: "Begriffsauffassungen zum Thema Sicherheit in der Informationstechnologie gibt es viele."[17] Denn einzelne Aspekte von IT-Sicherheit können nicht immer eindeutig und trennscharf von anderen Aspekten abgegrenzt werden.

Hier sollen folgende Sicherheitsaspekte unterschieden werden:

- **Intimität** oder **Vertraulichkeit** (*confidentiality*):
  Schutz vor unbefugter Kenntnisnahme[18]
- **Integrität** (*integrity*):
  Schutz vor Veränderung durch Dritte[19]
- **Identität**:[20]
  Gewährleistung der Herkunft vom Berechtigten
- **Authentizität** (*authenticity*):
  Gewährleistung von Echtheit und Glaubwürdigkeit[21]
- **Verfügbarkeit** (*availability*):
  Schutz vor unautorisierter (Funktions-)Beeinträchtigung des Systems[22]
- **Verbindlichkeit** (*non repudiation*):
  Gewährleistung der Zuordenbarkeit[23]

Da der Identität im Sinne von Identifikation bzw. Identifizierung (*identification*) in einzelnen Bereichen – etwa dem Signaturrecht – besondere Bedeutung zukommt, wird Identität hier noch einmal explizit als eigenständiger Sicherheitsaspekt genannt.

[17] Martin Raepple, Sicherheitskonzepte für das Internet, 2. Aufl., 2001, S.3.
[18] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 8.
[19] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 8.
[20] Die Gewährleistung der Identität wird oftmals als (Teil-)Aspekt des Sicherheitsziels Authentizität begriffen (BSI: E-Government-Handbuch, „Authentisierung im E-Government", S. 10).
[21] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 7.
[22] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 10.
[23] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 11.

Ein grundsätzliche Unterscheidung ist indes verbreitet: Für die **Sicherheit in der Informationstechnologie** (IT-Sicherheit) differenziert C. Eckert[24]

„Safety" als Funktions- und

„Security" als Informationssicherheit.

Unter **Funktionssicherheit** (*safety*) wird das Funktionieren eines Systems unter normalen Betriebsbedingungen verstanden; unter **Informationssicherheit** (*security*) die Eigenschaft eines funktionssicheren Systems, nur Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder –gewinnung führen. Beiden Begriffen entspricht im Deutschen – d.h. zumindest in der Gesetzessprache des deutschen Rechts - „Sicherheit". Daneben wird der Begriff **Datensicherheit** (*protection*) verstanden als die Systemeigenschaft, nur Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen.

Aus juristischer Sicht festzuhalten ist: Regelmäßig setzt IT-Sicherheit (im Kontext von Sicherheitspolitik) *safety* und *security* voraus: Sicherheitsrelevante Daten müssen nicht nur effektiv und effizient organisiert werden, sondern – wie beim Fluggastdatensachverhalt dargestellt - gegenüber Angriffen wehrfähig („resistent") sein. Darüber hinaus gilt: Sicherheit und (IT-)Sicherheit gilt es zu optimieren – und nicht „nur" zu definieren. In der Rechtsprechung ist bereits deutlich geworden, dass die IT-Sicherheit nicht einfach in der Werbung behauptet[25] sondern geleistet werden muss.

B. (IT-)Sicherheit als (relative) Freiheit von Gefahren

I. Relativität der Sicherheit

In einer technischen Perspektive wird Sicherheit als **„Freiheit von unvertretbaren Risiken"** definiert.[26] Nach hier vertretener Ansicht ist zwischen Gefahren und Risiko zu unterscheiden. Konkrete Gefahren sind auszuschließen. Die Hinnahme von (Rest)risiken ist in unserer Rechtsordnung unter bestimmten Voraussetzungen zumutbar, wie es das Bundesverfassungsgericht in seiner Kernenergierechtsprechung formuliert hat:

> „Will der Gesetzgeber die Möglichkeit künftiger Schäden durch die Errichtung oder den Betrieb einer Anlage oder durch ein technisches Verfahren abschätzen, ist er weitgehend auf Schlüsse aus der Beobachtung vergangener tatsächlicher Geschehnisse auf die relative Häufigkeit des Eintritts und den gleichartigen Verlauf gleichartiger Geschehnisse in der Zukunft

[24] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004 , S. 4 f.
[25] Nach dem Urteil des LG Hamburg v. 31.10.2002 (MMR 2003, 340) ist es irreführend (§ 3 des Gesetzes gegen den unlauteren Wettbewerb), wenn ein Provider damit wirbt, dass der Netzzugang „sicher" sei.
[26] DIN EN 61508-4: Definition 3.1.8.

angewiesen; fehlt eine hinreichende Erfahrungsgrundlage hierfür, muß er sich auf Schlüsse aus simulierten Verläufen beschränken. Erfahrungswissen dieser Art, selbst wenn es sich zur Form des naturwissenschaftlichen Gesetzes verdichtet hat, ist, solange menschliche Erfahrung nicht abgeschlossen ist, immer nur Annäherungswissen, das nicht volle Gewißheit vermittelt, sondern durch jede neue Erfahrung korrigierbar ist und sich insofern immer nur auf dem neuesten Stand unwiderlegten möglichen Irrtums befindet. Vom Gesetzgeber im Hinblick auf seine Schutzpflicht eine Regelung zu fordern, die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließt, die aus der Zulassung technischer Anlagen und ihrem Betrieb möglicherweise entstehen können, hieße die Grenzen menschlichen Erkenntnisvermögens verkennen und würde weithin jede staatliche Zulassung der Nutzung von Technik verbannen. Für die Gestaltung der Sozialordnung muß es insoweit bei Abschätzungen anhand praktischer Vernunft bewenden.
Was die Schäden an Leben, Gesundheit und Sachgütern anbetrifft, so hat der Gesetzgeber durch die in § 1 Nr. 2 und in § 7 Abs. 2 AtomG niedergelegten Grundsätze der bestmöglichen Gefahrenabwehr und Risikovorsorge einen Maßstab aufgerichtet, der Genehmigungen nur dann zuläßt, wenn es nach dem Stand von Wissenschaft und Technik praktisch ausgeschlossen erscheint, daß solche Schadensereignisse eintreten werden (vgl. dazu Breuer, DVBl. 1978, S. 829 ff.; 835 f.). Ungewißheiten jenseits dieser Schwelle praktischer Vernunft haben ihre Ursache in den Grenzen des menschlichen Erkenntnisvermögens; sie sind unentrinnbar und insofern als sozialadäquate Lasten von allen Bürgern zu tragen."[27]

Sicherheit ist demnach nicht definierbar, sondern nur optimierbar. Diese Vorstellung findet sich auch im IT-Sicherheitshandbuch wieder: (IT-)Sicherheit ist danach stets nur eine relative Sicherheit und keine absolute.[28] Die Relativität des Sicherheitsbegriffs setzt die Kenntnis der Sicherheitslage voraus, die wiederum durch die Schwachstellen der IT-Sicherheit charakterisiert wird. Nicht überraschend verlangen deswegen die so genannten Common Criteria (ein Zertifizierungskatalog), dass die Beseitigung, Minimierung und Überwachung von Schwachstellen erreicht wird.

Teil 3 der Common Criteria[29] [Bedeutung von Schwachstellen]
1.2.2.1 Das Brechen von IT-Sicherheit geschieht durch die absichtliche Ausnutzung oder unabsichtliche Auslösung von Schwachstellen bei der Anwendung von IT in Geschäftsabläufen. Es sollen Schritte zur Vermeidung der Entstehung von Schwachstellen in IT-Produkten und –Systemen ergriffen werden. Die Schwachstellen sollen soweit wie durchführbar:
a) beseitigt werden — d.h., es sollen aktive Schritte zur Aufdeckung sowie Entfernung oder Neutralisierung aller benutzbaren Schwachstellen unternommen werden;
b) minimiert werden — d.h., es sollen aktive Schritte zur Reduzierung der möglichen Auswirkungen der Benutzung jeglicher Schwachstelle auf ein akzeptables Restniveau unternommen werden;
c) überwacht werden — d.h., es sollen aktive Schritte unternommen werden, um sicherzustellen, daß jeder Versuch der Benutzung einer noch vorhandenen Schwachstelle aufgedeckt wird, so daß Maßnahmen zur Schadensbegrenzung ergriffen werden können.

[27] Kalkar I - BVerfGE 49, 89, Rn. 177f.
[28] BSI: IT-Sicherheitshandbuch, Kapitel 2.3.
[29] „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation" (Common Criteria – CC), Version 2.1, August 1999.

Sicherheit wird demzufolge vorrangig als Negativ-Definition durch das Fehlen spezifischer Risiken determiniert. Dafür, dass das Gefährdungs- und Risikopotential im IT-Bereich besonders hoch ist, sind nach dem IT-Grundschutzhandbuch folgende Faktoren ursächlich:[30]

- kurze Innovationszyklen der IT
- zunehmende Öffnung von IT-Systemen nach außen (Vernetzung, Internet…)
- stetig wachsende Verbreitung und damit auch Abhängigkeit von IT
- wachsende Angriffsflächen auf Grund steigender Funktionalität von (Anwendungs-)Software
- einzelne Verantwortliche für IT-Sicherheit stehen vielschichtigen Herausforderungen gegenüber[31]

II. IT-Sicherheitskonzept

Basis jedes IT-Sicherheitskonzepts ist eine Analyse des Schutzbedarfs des IT-Systems (Schutzbedarfsermittlung).[32] Dabei sind zunächst mögliche Schäden zu identifizieren (Bedrohungsanalyse). Im Anschluss wird eine Risikoabschätzung hinsichtlich der Wahrscheinlichkeit des Schadenseintritts und der Schwere der Folgen vorgenommen (Gefahren- und Risikoanalyse). Aus der Wahrscheinlichkeit eines bestimmten Schadenseintritts und aus den drohenden Folgen des Eintritts ergibt sich das anzustrebende Schutzniveau. Das IT-Sicherheitskonzept stellt die Gesamtheit der Maßnahmen dar, die den erforderlichen Soll-Zustand auf der Basis des festgestellten Ist-Zustandes implementieren.

1. Bedrohungsanalyse: Schwachstellen

Mögliche Schwachstellen und daraus resultierende Bedrohungen sind zu identifizieren. Hierfür kann eine Vielzahl von denkbaren Kategorisierungen herangezogen werden[33]. Hier sollen

---

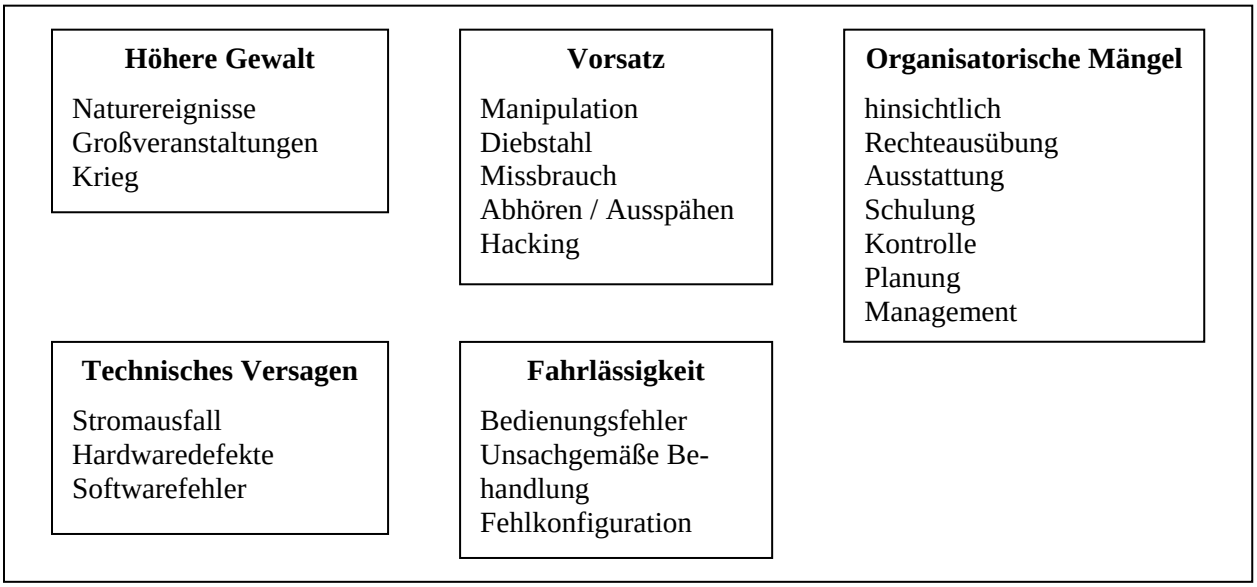
[30] BSI: IT-Grundschutzhandbuch, 2004, Einleitung, S. 11.

[31] Hierbei ist einerseits an strukturelle Defizite zu denken, die sich daraus ergeben, dass mehrere Einzelverantwortliche nebeneinander Maßnahmen treffen, die nicht auf einem (notwendigen) Gesamtkonzept beruhen. Andererseits ergibt sich eine Disproportionalität zwischen dem einzelnen Sicherheitsverantwortlichen und den unzähligen Sicherheitsproblemen.

[32] Dabei scheint in der Informatik keine Einigkeit zu herrschen, wie das Verfahren zur Erstellung eines IT-Sicherheitskonzepts im Einzelnen konkret ablaufen soll. Die Abweichungen zwischen den einzelnen Verfahrensweisen dürften zum einen in der Komplexität der Materie begründet sein. Zum anderen führen Unterschiede in der Aufgabenstellung (das IT-Grundschutzhandbuch etwa zielt auf die Gewährung von Grundschutz und sieht daher komplexere Analysen nur im Rahmen einer ergänzenden Sicherheitsanalyse bei besonders hohem Schutzbedarf vor), dem konkreten IT-System etc. zu abweichenden Lösungsansätzen. Hier soll lediglich ein Überblick gegeben werden.

[33] Etwa eine Bedrohungsmatrix (C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 162) oder ein Bedrohungsbaum (C. Eckert, a.a.O., S. 163); die Entscheidung für die eine oder die andere Vorgehensweise kann dabei in Anpassung an die konkrete Aufgabenstellung erfolgen.

folgende Gefährdungsfaktoren – in Anlehnung an das BSI-Grundschutzhandbuch - unterschieden werden:[34]



So klar diese Einteilung auf den ersten Blick erscheinen mag, ist dennoch eine eindeutige Zuordnung einer konkreten Bedrohung in diese Gefährdungskategorien oft nicht möglich. Ein fahrlässiger Bedienungsfehler eines Mitarbeiters kann etwa auf einem organisatorischen Mangel beruhen, nämlich unzureichender Schulung. Oder ein Softwarefehler wird eventuell erst durch eine Fehlkonfiguration (menschliche Fahrlässigkeit) oder durch mangelhaftes Sicherheitsmanagement (organisatorischer Mangel) zu einer Bedrohung.

In einer juristischen Perspektive sind insbesondere die Gefährdungsfaktoren interessant, die auf menschlichem Verhalten beruhen, da strafrechtliche oder zivilrechtliche Verantwortlichkeit regelmäßig an menschliches Verhalten anknüpft. Hier ist vor allem die Unterscheidung zwischen vorsätzlichen und fahrlässigen Angriffen relevant.

Vorsätzliche Angriffe können etwa sein:

- **Spoofing**

  Unter dem Begriff Spoofing werden Angriffe zusammengefasst, die auf die Vorspiegelung einer falschen Identität abzielen Beim E-Mail-Spoofing wird eine falsche Absenderadresse angegeben. Als IP-Spoofing bezeichnet man die Versendung von IP-Paketen mit gefälschter Sender-IP-Adresse. Dadurch kann sich ein externer Angreifer etwa als zu einem bestimmten internen Netzwerk gehörend darstellen und so Authentifizierungsmaßnahmen umgehen.

[34] BSI: IT-Grundschutzhandbuch 2004, Gefährdungskataloge G 1 – G 5, S. 288 ff. sowie C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 14.

- **Buffer-Overflow (Pufferüberlauf)**

  Buffer-Overflow-Angriffe nutzen durch nachlässige Programmierung auftretende Softwareschwachstellen aus. Zu große Datenmengen werden in zu kleine Speicherbereiche (Pufferbereiche) geschrieben, so dass dem Speicherbereich nachfolgende Informationen überschrieben werden (Bereichsüberschreitung).

- **Viren**

  Viren sind zur Reproduktion fähige, nicht selbständig ablaufende Programme, die ein Wirtsprogramm zur Ausführung benötigt. Die Daten in infizierten Dateien werden manipuliert und teilweise zerstört. Die Zerstörung von Hardware durch Viren kommt selten vor.

- **Würmer**

  Würmer sind ebenfalls zur Reproduktion fähige, aber selbständige Computerprogramme. Würmer können allein durch die Beanspruchung von Ressourcen zur aktiven Weiterverbreitung große (finanzielle) Schäden anrichten

- **Trojanisches Pferd**

  Ein Trojanisches Pferd ist ein Programm, das zusätzliche, verborgene Funktionen besitzt, die über die offen gelegte Funktionalität hinausgehen.

- **DoS-Angriff**

  Denial of Service Angriffe zielen darauf ab, die Verfügbarkeit von Systemkomponenten oder –diensten durch Überlastung infrage zu stellen. Geht der Angriff von mehreren Systemen aus, spricht man von Distributed Denial of Service (DDoS).

Typisch für Angriffe, die fahrlässiges Verhalten von Menschen ausnutzen, sind Angriffe im Wege von

- **Social Engineering / Social Hacking**

  Darunter werden alle Angriffe zusammengefasst, bei denen die Neugier, Unvorsichtigkeit, Unkenntnis etc. von Geheimnisträgern zur Erlangung vertraulicher Informationen genutzt wird. Dies kann etwa dadurch geschehen, dass sich ein Angreifer als Administrator ausgibt und Mitarbeiter um die Angabe ihres Passworts bittet. Auch Phishing setzt auf einer vergleichbaren Basis an. Viren oder Würmer, die sich per E-Mail verbreiten, setzten auch gezielt Betreffzeilen ein, die die Neugier der Empfänger wecken.

Ein Angriff auf ein IT-System stellt sich häufig als eine Kombination von verschiedenen Angriffen dar. Als Beispiel sei hier nur auf den Sobig-Virus/Wurm hingewiesen[35]:
Dieser Virus nutzte E-Mail-Attachments als Verbreitungsmedium. Wurde das Attachment vom Empfänger geöffnet, legte der Virus zunächst Einträge in der Windows-Registry ab, damit der Virus beim Booten automatisch gestartet wird. Anhand der Netzwerkfreigabe suchte der Virus aktiv nach möglichen Opfersystemen. Der Virus verschickte sich außerdem selbst per E-Mail an alle auf dem Rechner vorhandenen E-Mail-Adressen. Er versuchte weiter, ein Trojanisches Pferd aus dem Internet zu laden. Glückte dies, dann installierte der Trojaner unter anderem einen Key-Logger auf dem Rechner, um Passwort-Eingaben abzufangen. Das Trojaner-Programm spähte auch Registry-Einträge aus, um Informationen über die System-Konfiguration zu sammeln. In periodischen Abständen baute der Trojaner eine TCP-Verbindung auf, um die gesammelten Benutzerkennungen und Passworte an eine vom Angreifer bestimmte URL zu übergeben. Der Trojaner versuchte schließlich, Port 1180 für weitere Angriffe zu öffnen.

2. Risikoanalyse

Im Rahmen der Risikoanalyse werden die im Wege der Bedrohungsanalyse ermittelten potentiellen Gefährdungen bewertet, und zwar zum einen nach der Wahrscheinlichkeit einer Realisierung des Gefährdungspotentials und zum anderen nach den dadurch entstehenden Schäden. Dabei kommt es entscheidend auf den Angreifer-Typus an: seine Motive und Kenntnisse sowie der (voraussichtliche) Aufwand (finanziell, technisch, zeitlich…), mit dem der Angriff betrieben wird.[36] Außerdem sind die potentiellen Schäden zu ermitteln. Hierbei fließen in besonderem Maß die Gegebenheiten des Einzelfalls ein, da sich ein bestimmter Schaden für den einen als katastrophal und für einen anderen lediglich als unangenehm darstellen kann. Aus der Kombination von Eintrittswahrscheinlichkeit und drohendem Schaden ergibt sich die Bewertung der einzelnen identifizierten Bedrohungen als vertretbare oder unvertretbare Risiken. Das Risiko ist also eine Kombination von Werten für Schadenshöhe und Schadenswahrscheinlichkeit.[37]

---

[35] Beispiel nach C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 49 f., deren Terminologie hier gefolgt werden soll. Sobig wird von C. Eckert als Virus eingestuft, während er ansonsten teilweise auch als Wurm bezeichnet wurde (etwa vom BSI).
[36] Daraus ergibt sich, dass die Risikoanalyse sehr stark von subjektiven Einschätzungen geprägt ist. Grundlagen für verlässliche Schätzungen existieren nicht. Daher wird teilweise auf eine explizite Abschätzung der Eintrittswahrscheinlichkeit verzichtet (BSI: Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Februar 2004, S. 3).
[37] BSI: IT-Sicherheitshandbuch, Kapitel 5.1.

3. Bedrohungsanalyse: Folgenermittlung

Für jede IT-Anwendung innerhalb des IT-Systems ist der Schutzbedarf zu ermitteln. Dazu kann eine Unterteilung in folgende **Schadensszenarien** vorgenommen werden:[38]

- **Verstoß gegen Gesetze/Vorschriften/Verträge**
- **Beeinträchtigung des Rechts auf informationelle Selbstbestimmung**
- **Beeinträchtigung der persönlichen Unversehrtheit**
- **Beeinträchtigung der Aufgabenerfüllung**
- **negative Außenwirkungen**
- **finanzielle Auswirkungen**

Dabei kann ein möglicher Schaden in mehrere Schadensszenarien zugleich fallen. Für jedes Schadensszenario ist eine Schutzbedarfskategorie zu bestimmen:[39]

Schutzbedarfkategorien	
„niedrig bis mittel“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Soweit es um die Sicherheit von IT-Systemen geht, sind bei der Schutzbedarfsermittlung außerdem die folgenden Überlegungen zu beachten:[40]

- **Maximum-Prinzip:**

  Mögliche Schäden für ein IT-System sind in ihrer Gesamtheit zu betrachten, da der größte Schaden in der Regel das Sicherheitsniveau bestimmt.

- **Beachtung von Abhängigkeiten:**

  Besonderes Augenmerk ist auf Abhängigkeiten zwischen einzelnen IT-Anwendungen zu richten. Eine an sich unbedeutende Anwendung kann etwa Ausgangsdaten für eine IT-Anwendung mit hohem Schutzbedarf liefern. Dadurch erhöht sich auch der Schutzbedarf der an sich weniger bedeutsamen Anwendung.

- **Kumulationseffekt:**

  Mehrere Einzelschäden, die an sich als gering anzusehen wären, können in ihrer Gesamtheit einen über ihre Summe hinausgehenden Schaden hervorrufen.

---

[38] BSI: IT-Grundschutzhandbuch, S. 44 ff.
[39] Übersicht nach IT-Grundschutzhandbuch, S. 44.
[40] BSI: IT-Grundschutzhandbuch, S. 54.

- **Verteilungseffekt:**

  Umgekehrt kann ein IT-System einen nur geringen Schutzbedarf haben, obwohl Teilbereiche einer IT-Anwendung mit hohem Schutzbedarf auf dem System ablaufen, denn nicht alle Teilbereiche sind in gleichem Maße wesentlich.

4. IT-Sicherheitsstrategie

Der ermittelte Schutzbedarf beschreibt den Soll-Zustand des IT-Systems, die Bedrohungs- und Risikoanalyse beschreiben den Ist-Zustand. Aus dem Abgleich von Ist- und Soll-Zustand lassen sich die erforderlichen IT-Sicherheitsmaßnahmen ermitteln und in einer IT-Sicherheitskonzept zusammenfassen.

III. Sicherheitsrelevante Akteure

Akteure der IT-Sicherheit gibt es auf der Seite derjenigen, die zum Schutz und/oder um Verbesserung der IT-Sicherheit bemüht sind („Pro-Akteure"), und auf Seite derjenigen, die die IT-Sicherheit gefährden oder verletzen („Contra-Akteure").

1. „Pro-Akteure"

a. Völkerrecht

Die **OECD**[41] ist eine ursprünglich europäische, jetzt global offene, internationale Organisation (d.h. ein auf völkerrechtlichem Vertrag beruhender, mitgliedschaftlicher Zusammenschluss von Völkerrechtssubjekten), welche die Interessen marktwirtschaftlicher Staaten vertritt. Mitglieder sind unter anderem Deutschland, Frankreich, die USA und Japan. Die OECD handelt gegenüber ihren Mitgliedern vor allem in Form von Stellungnahmen und Empfehlungen. Diese sind nicht bindend und enthalten insbesondere keine Sanktionsmöglichkeiten. Sie werden daher als **„soft law"** bezeichnet.

Die OECD hat im Jahr 2002 Empfehlungen zur IT-Sicherheit abgegeben. Dabei formuliert sie das Ziel einer **„Culture of Security"**.

OECD Guidelines for the Security of Information Systems and Networks
II. Aims
These Guidelines aim to
-Promote a **culture of security** among all participants as a means of protecting information systems and networks. (...)

[41] Organisation for Economic Co-operation and Development (OECD).

Zum Bereich Kryptographie hat die OECD bereits im Jahr 1997 Empfehlungen abgegeben.

OECD Guidelines for Cryptography Policy
I. Aims
These Guidelines are intended
to promote the use of cryptography;
to foster confidence in information and communication infrastructure, networks and systems and the manner in which they are used;
to help ensure the **security of data**, and to protect privacy, in national and global information and communicaton infrastructures, networks and systems; (...)

b. Europarecht

Auf europäischer Ebene hat 2004 die **ENISA** (Europäische Agentur für Netz- und Informationssicherheit) ihre Arbeit aufgenommen. Ihre Einrichtung beruht auf der „Verordnung zur Gründung der Europäischen Agentur für Netz- und Informationssicherheit“[42].

Artikel 1 Verordnung zur Gründung der Europäischen Agentur für Netz- und Informationssicherheit [Zuständigkeitsbereich]
(1) Zur Gewährleistung einer hohen und effektiven Netz- und Informationssicherheit innerhalb der Gemeinschaft und der Entwicklung einer Kultur der Netz- und Informationssicherheit, die den Bürgern, Verbrauchern, Unternehmen und Organisationen des öffentlichen Sektors der Europäischen Union Nutzen bringt und damit zum reibungslosen Funktionieren des Binnenmarkts beiträgt, wird eine **Europäische Agentur für Netz- und Informationssicherheit**, nachstehend "Agentur" genannt, errichtet.
(…)

In der Art. 2 der Verordnung werden die Ziele der ENISA benannt.

Artikel 2 Verordnung zur Gründung der Europäischen Agentur für Netz- und Informationssicherheit [Ziele]
(1) Die Agentur verbessert die Fähigkeit der Gemeinschaft und der Mitgliedstaaten und folglich der Wirtschaft, Probleme im Bereich der Netz- und Informationssicherheit zu verhüten, zu bewältigen und zu beheben.
(2) Die Agentur unterstützt und berät die Kommission und die Mitgliedstaaten in Fragen der Netz- und Informationssicherheit, die gemäß dieser Verordnung in ihre Zuständigkeit fallen.
(3) Aufbauend auf einzelstaatlichen und gemeinschaftlichen Anstrengungen arbeitet die Agentur auf ein hohes Niveau fachlicher Kompetenz hin. Die Agentur nutzt diese Fachkompetenz, um Anstöße zu einer umfassenden Zusammenarbeit zwischen den Akteuren des öffentlichen und des privaten Sektors zu geben.
(4) Auf Aufforderung unterstützt die Agentur die Kommission bei den technischen Vorarbeiten für die Aktualisierung und Weiterentwicklung der gemeinschaftlichen Rechtsvorschriften im Bereich der Netz- und Informationssicherheit.

Die ENISA hat mittlerweile ihre praktische Arbeit aufgenommen.[43]

[42] Verordnung zur Gründung einer Agentur für Netz- und Informationssicherheit vom 10.3.2004, ABl. L 77/1.
[43] So sieht es zumindest das Arbeitsprogramm der ENISA für 2005 vor.

c. Bundesrecht

➢ **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Zum Schutz vor Gefährdungen für die Informationstechnik wurde 1991 das BSI gegründet.

§ 1 BSIG
Der Bund errichtet das Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesminister des Innern. (…)

Das BSI forscht im Bereich der Informationssicherheit, prüft IT-Produkte und berät Hersteller, Vertreiber und Anwender von Informationstechnik. Insbesondere versucht das BSI hierbei auf drohende Gefährdungen hinzuweisen und durch Sicherheitskonzepte IT-Sicherheit handhabbar zu machen. Es informiert z.B. über aktuelle Viren und stellt ein Grundschutzhandbuch[44] für Unternehmen zur Verfügung. Seit 2001 übernimmt das BSI im Rahmen des CERT-Bund ("Computer Emergency Response Team für Bundesbehörden") die Aufgabe einer Expertenkommission für Prävention und akute Krisenfälle beim IT-Netz des Bundes.

➢ **Bundesnetzagentur**

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen entspricht der früheren Regulierungsbehörde für Gas, Elektrizität, Telekommunikation und Post (RegTP). Die RegTP wurde mit dem Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BEGTPG)[45], das am 13.07.2005 in Kraft getreten ist, in Bundesnetzagentur umbenannt.

§ 1 BEGTPG [Rechtsform, Name]
Die auf der Grundlage des Zehnten Teils des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120), das zuletzt durch Artikel 4 Abs. 73 des Gesetzes vom 5. Mai 2004 (BGBl. I S. 718) geändert worden ist, errichtete "Regulierungsbehörde für Telekommunikation und Post" wird in "Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen" (Bundesnetzagentur) umbenannt. Sie ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Arbeit mit Sitz in Bonn.

---

[44] BSI: IT-Grundschutzhandbuch. Das Grundschutzhandbuch ist eine Weiterentwicklung des IT-Sicherheitshandbuchs des BSI aus dem Jahr 1992: Während im Sicherheitshandbuch bei der Sicherheits- und Risikoanalyse noch Eintrittswahrscheinlichkeiten betrachtet wurden, verzichtet das Grundschutzhandbuch – wegen der tatsächlichen Schwierigkeit verlässlicher Schätzungen – darauf, die Eintrittswahrscheinlichkeiten explizit in einem eigenen Prüfungspunkt abzuschätzen.

[45] Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BEGTPG) vom 07.07.2005, BGBl I 2009 (Art. 2 des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsrechts).

Die Bundesnetzagentur übernimmt die Aufgaben der RegTP.

§ 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.

Ab dem 01.01.2006 wird die Bundesnetzagentur zusätzlich auch für den Eisenbahninfrastrukturmarkt zuständig sein.[46] Die Bundesnetzagentur verfügt sowohl im Telekommunikations- als auch im Signaturrecht über Kontrollbefugnisse. Im Telekommunikationsbereich kann die Bundesnetzagentur Maßnahmen zur Gewährleistung der Sicherungspflichten treffen (§ 115 Abs. 1 TKG).

§ 115 TKG [Kontrolle und Durchsetzung von Verpflichtungen]
(1) Die Regulierungsbehörde kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. Der Verpflichtete muss auf Anforderung der Regulierungsbehörde die hierzu erforderlichen Auskünfte erteilen. Die Regulierungsbehörde ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.
(2) Die Regulierungsbehörde kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder wie folgt festsetzen: (…)
(3) Darüber hinaus kann die Regulierungsbehörde bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.
(4) Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, tritt bei den Unternehmen an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend den §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes. Der Bundesbeauftragte für den Datenschutz richtet seine Beanstandungen an die Regulierungsbehörde und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.
(5) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit dies die Kontrollen nach Absatz 1 oder 4 erfordern.

[46] § 4 Abs. 1 Bundeseisenbahnverkehrsverwaltungsgesetz (BEVVG) vom 27.12.1993.

Zu diesen Eigensicherungspflichten der Telekommunikationsdiensteanbieter zählt neben der Erstellung eines Sicherheitskonzeptes auch die Einsetzung eines betrieblichen Sicherheitsbeauftragten (§ 109 Abs. 3 TKG).

§ 109 TKG [Technische Schutzmaßnahmen]
(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 Regulierungsbehörde 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 Regulierungsbehörde 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 Regulierungsbehörde 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 Regulierungsbehörde 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.

Diese Maßnahmen der Eigensicherung werden hoheitlich überwacht, weil die Telekommunikationsdienstleistungen für die Allgemeinheit erbracht werden und der Staat so seiner Schutzaufgabe nachkommt. Wenn die Anforderungen aus § 109 TKG nicht erfüllt werden, kann die Bundesnetzagentur als ultima ratio den Weiterbetrieb ganz oder teilweise untersagen (§ 109 Abs. 3 TKG).

Im Bereich des Signaturrechts ist die Bundesnetzagentur Aufsichtsbehörde.[47]

§ 19 SigG [Aufsichtsmaßnahmen]
(1) Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.
(2) Die zuständige Behörde kann gegenüber Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 treffen.
(3) Die zuständige Behörde hat einem Zertifizierungsdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, dass er
1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,
2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,
3. nicht über die erforderliche Deckungsvorsorge verfügt,

[47] § 3 des SigG wurde durch Art. 3 Nr. 9 des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsrechts vom 07.07.2005 (BGBl I 1970) entsprechend geändert.

4. ungeeignete Produkte für qualifizierte elektronische Signaturen verwendet oder
5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt
und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.
(4) Die zuständige Behörde kann eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen.
(5) Die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate bleibt von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt.
(6) Die zuständige Behörde hat die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit nach § 13 eingestellt haben oder deren Betrieb nach § 19 Abs. 3 untersagt wurde, für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

d. Landesrecht

In der landesrechtlichen Verwaltung wird zunehmend die IT-Sicherheit etwa durch IT-Sicherheitsrichtlinien berücksichtigt.

IT-Sicherheitsleitlinie für die Hessische Landesverwaltung[48]
5. Verantwortlichkeiten
5.1 Die Dienststellenleitung trägt in dem Bereich, den sie beeinflussen kann, die Verantwortung für eine angemessene IT-Sicherheit.
5.2 Ein Sicherheitsmanagement besteht aus dem bzw. der IT-Sicherheitsbeauftragten, den Zuständigen für die Fachanwendungen, für den IT-Service und für den IT-Betrieb. Es ist damit zu betrauen, gemäß den Sicherheitsvorgaben die Sicherheit im Umgang mit der IT und den Schutz der Daten und Informationen zu gewährleisten. Ebenso gehört es zu seinen Aufgaben, das IT-Sicherheitskonzept fortzuschreiben und Maßnahmen umzusetzen, die ein angemessenes und dem Stand der Technik entsprechendes IT-Sicherheitsniveau sicherstellen. Der behördliche Datenschutzbeauftragte unterstützt den Dienststellenleiter bei der Umsetzung der IT-Sicherheit. Ihm ist deshalb die Teilnahme an den Beratungen des IT-Sicherheitsmanagements zu ermöglichen, soweit er dies wünscht.
5.3 Die Mitarbeiter sind dafür verantwortlich, dass die Sicherheitsmaßnahmen in ihrem Bereich umgesetzt werden. Unterstützt durch sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten Sicherheitsvorfälle von innen und außen vermeiden. Sicherheitsrelevante Ereignisse sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.
5.4 Die jeweils Zuständigen für Daten, Informationen und Verfahren sowie für unterstützende Systeme, Netze und Infrastruktur entscheiden, wer in welchem Umfang Zugriff auf das jeweilige System hat. Wenn sie Vorgaben zur Sicherheit formulieren, haben sie auch die angemessene Sicherheitsstufe, Finanzierbarkeit bzw. Wirtschaftlichkeit abzuwägen.
5.5 Ein Auftragnehmer (vgl. § 4 HDSG), der für die Verwaltung Leistungen erbringt, hat Vorgaben des Auftraggebers zur Einhaltung der IT-Sicherheitsziele (Wahrung der Vertrau-

[48] IT-Sicherheitsleitlinie für die Hessische Landesverwaltung.

lichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) gemäß dieser IT-Sicherheitsleitlinie einzuhalten. Der Auftraggeber hat Sicherheitsanforderungen vertraglich festzulegen und deren Einhaltung zu kontrollieren. Der Auftraggeber hat den Auftragnehmer zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren.
5.6 Die Einhaltung der IT-Sicherheit bei der Verarbeitung, Nutzung und Kontrolle von Daten und Informationen ist zu überprüfen. Art und Umfang der Kontrolle sind von der Dienststellenleitung auf der Grundlage des jeweiligen Sicherheitskonzeptes festzulegen. Eine Kontrolle kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass keine unzulässige Kenntnisnahme von Daten und Informationen damit verbunden ist.

Solche Verwaltungsrichtlinien sind lediglich Verwaltungsinnenrecht ohne Außenwirkung, d.h. sie enthalten i.d.R. keine Rechte oder Pflichten für Bürger. Bei Behörden soll dadurch ein effektives und effizientes IT-Sicherheitsmanagement eingeführt werden. Zu diesem Zweck wird ein IT-Sicherheitsbeauftragter bestellt. Dieser ist in Zusammenarbeit mit den jeweils für die Fachanwendungen, den IT-Betrieb und den IT-Service Zuständigen für das Sicherheitsmanagement verantwortlich.

2. „Contra-Akteure“

Als „Contra-Akteure“ werden diejenigen Beteiligten bezeichnet, die IT-Sicherheit „durchbrechen“. Auch hier kann zwischen den einzelnen Rechtsebenen (Völkerrecht, Europarecht, Bundesrecht, Landesrecht) unterschieden werden. Eine detaillierte Darstellung wird einem späteren Modul vorbehalten. Bereits hier kann darauf hingewiesen werden, dass Contra-Akteure nicht immer Private (User) sein müssen. So wird etwa in der Presse berichtet, dass unter Federführung der USA und Großbritanniens und Beteiligung weiterer Staaten, auch Deutschlands, seit Jahrzehnten im so genannten Echelon-Projekt internationale Kommunikation in hohem Umfang abgehört, automatisch verarbeitet und nachrichtendienstlich verwertet werde.

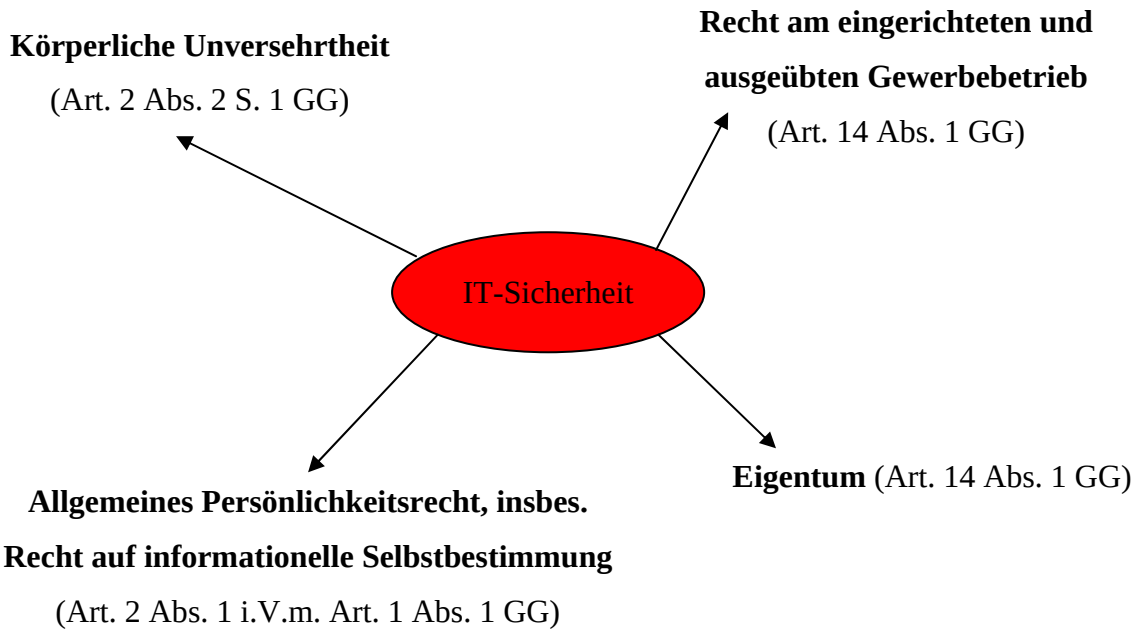
3. User

Als User werden hier natürliche und juristische Personen verstanden, welche die Informationstechnologie nutzen. Man kann für die IT-Sicherheit die These aufstellen, dass der Mensch sowohl das größte Risiko (Contra-Akteur) als auch die größte Chance (Pro-Akteur beim Einsatz von IT-Sicherheits-Tools) ist. Die Positionierung der „User“ müsste deshalb zu 1 und/oder 2 erfolgen und exemplifiziert die in der Vorlesung vorgestellte Ambivalenzthese.

C. Beitrag des Rechts zur (Verbesserung der) IT-Sicherheit?

I. Rechtliche Optionen

1. Grundrechtliche Gefährdungslage



- Die körperliche Unversehrtheit kann durch technische Fehlfunktionen etwa von medizinischen Diagnosegeräten, Flugkontroll- oder Verkehrsleitsystemen beeinträchtigt werden.
- Die informationelle Selbstbestimmung kann durch den unbefugten Zugang zu gespeicherten personenbezogenen Daten beeinträchtigt werden.
- Das Eigentum kann durch eine Funktionsbeeinträchtigung beeinträchtigt werden, etwa wenn durch einen DoS-Angriff der eigene Server lahmgelegt wird.
- Das Recht am eingerichteten und ausgeübten Gewerbebetrieb kann ebenfalls durch einen solchen DoS-Angriff beeinträchtigt werden.

Diesen Gefahren kann das Recht präventiv oder repressiv begegnen.

2. Präventive Optionen (ex ante)

- **Institutionelle Optionen**

  ENISA , BSI, Bundesnetzagentur; IT-Sicherheitsbeauftragter

- **Kommunikationspolitische Strategien: Information, Werbung und Public Relations**

  Aufklärung der IT-Nutzer, z.B. Grundschutzhandbuch des BSI

- **Produkt- und prozessorientierte Strategien: IT-Sicherheitskriterien**

  Im Bereich der IT-Sicherheit sind durch Normierungsorganisationen technische Anforderungen an IT-Sicherheit entwickelt worden, die die sicherheitstechnische Überprüfung und Standardisierung ermöglichen sollen. Zunächst wurden nationale Kriterienkataloge[49], dann auch europäische, wie die Information Technology Security Evaluation Criteria (ITSEC), entwickelt. Die International Standardization Organization (ISO) und die International Electrotechnical Commission (IEC), bestehend aus Teilnehmern aus Wissenschaft, Wirtschaft und Behörden, haben schließlich 1999 den internationalen Standard ISO 15408 für die Sicherheit von IT-Produkten entwickelt. In Zusammenarbeit von deutschen und US-amerikanischen Behörden wurden 1998 die Common Criteria für IT-Sicherheit[50] entwickelt, deren Standard seit 1999 in seiner aktuellen Version CC 2.1 der ISO 15408 entspricht. ISO und IEC haben zudem den Standard ISO/IEC 17799[51] für den Bereich des IT-Sicherheitsmanagements entwickelt. Ziel dieses Standards ist es, eine einheitliche Basis für Unternehmen und sonstige datenverarbeitende Organisationen zu schaffen, die eine effektive Sicherheitsorganisation entwickeln, implementieren und überprüfen wollen.

- **Prozessuale Strategie: Anzeige- und Vorsorgepflichten, Organisationspflichten**

  Als Beispiel für Organisationspflichten sei hier die Pflicht zur Benennung eines Sicherheitsbeauftragten/einer Sicherheitsbeauftragten und die Erstellung eines Sicherheitskonzeptes im Telekommunikationsgesetz genannt.

§ 109 TKG [Technische Schutzmaßnahmen]
(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 Regulierungsbehörde 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 Regulierungsbehörde im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren un-

[49] Trusted Cmputer Security Evaluation Criteria (TCSEC) in den USA, Security Criteria der Zentralstelle für Sicherheit in der Informationstechnik (ZSISC) in Deutschland
[50] „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik / Common Criteria for Information Technology Security Evaluation“ (Common Criteria – CC), Version 2.1, August 1999.
[51] vgl. Karl L. Lincke/Jesús Sánchez Echeverría, Die neue ISO/IEC 17799 – Sicherheitsverwaltung von Informationen, exolex 2003, 382-385.

verzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Regulierungsbehörde 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 Regulierungsbehörde 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.

- **Selbstregulierung**

  Zertifikate, etwa durch das BSI für anhand der Sicherheitskriterien geprüfte Produkte.

3. Repressive Optionen (ex post)

Als repressive Option kommt zunächst strafrechtliche Sanktionierung in Betracht. Überschreitet ein Verhalten die Schwelle zur Strafbarkeit nicht, können sich eventuell Rechtsfolgen aus dem Ordnungswidrigkeitenrecht ergeben.[52] Selbständig neben möglichen strafrechtlichen Sanktionen steht die Frage nach der zivilrechtlichen Verantwortlichkeit. Dabei steht nicht die Bestrafung des Täters durch den Staat für begangenes Unrecht im Vordergrund, sondern die Kompensation der von den Geschädigten erlittenen Einbußen.

II. Strafbarkeit bei vorsätzlicher Verbreitung von Viren - „Clear Case“[53]

Der User X, der informationstechnisch sehr versiert ist, hat in seiner Freizeit einen Internetwurm programmiert und in Umlauf gebracht. Der Wurm verbreitet sich nicht über E-Mail-Attachments, sondern nutzt eine Sicherheitslücke in bestimmten Betriebssystemen zu seiner Verbreitung - wenn diese nicht durch ein entsprechendes Patch geschlossen wurde.
Sobald ein Rechner Verbindung zum Internet hat, kann er über diese Schwachstelle angegriffen und infiziert werden. Dabei schleust der Wurm im Wege eines Pufferüberlaufs Fremdcode ein, wodurch dann der eigentliche Wurm heruntergeladen wird. Nach erfolgreichem Download versucht der Wurm sogleich, andere Rechner anzugreifen und zu infizieren. Eine darüber hinausgehende Schadensroutine weist er nicht auf.
Der Befall eines Rechners macht sich durch eine erhebliche Verlangsamung und zum Teil durch wiederholtes Herunterfahren des Rechners bemerkbar.

[52] Ordnungsrechtliche Normen und Rechtsfolgen werden in diesem Modul nicht näher beleuchtet.
[53] Der Sachverhalt entspricht dem so genannten „Sasser-Wurm-Fall“.

1. Datenveränderung (§ 303a StGB)

X könnte sich dadurch, dass er den Wurm in Umlauf gebracht hat, wegen Datenveränderung strafbar gemacht haben. Eine Strafbarkeit des X allein wegen des Programmierens des Wurms kommt dagegen nicht in Betracht, da dadurch (noch) keine Daten verändert werden.[54]

§ 303a StGB [Datenveränderung]
(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

a. Objektiver Tatbestand

- **Fremdheit der Daten**

Auf den befallenen Rechnern sind Daten vorhanden. Die Norm des § 303a StGB wird dahingehend einschränkend ausgelegt, dass nur die Löschung, Unterdrückung, Unbrauchbarmachung und Veränderung fremder Daten strafbar sein soll.[55] Die Daten stellen sich für X als fremd dar. Es ist kein Grund ersichtlich, der X dazu berechtigen könnte, die Daten auf den angegriffenen Rechnern zu verarbeiten oder zu nutzen etc. Das Merkmal der Fremdheit ist bei dem Angriff des X durch einen Wurm zu bejahen.

- **Tathandlung**

Durch den Wurm müssten Daten gelöscht, unterdrückt, unbrauchbar gemacht oder verändert worden sein. Dies ist insoweit fraglich, als der Wurm keine Schadensroutine im eigentlichen Sinn aufweist. Umfasst ein Wurm oder Virus etc. eine solche Schadensroutine, dann liegt klar eine Datenveränderung vor. Aus der konkreten Wirkungsweise der Schadsoftware ergibt sich, welche Tatbestandalternativen verwirklicht werden.

- **Löschen** bedeutet vollständige, unwiederbringliche Unkenntlichmachung der konkreten Speicherung.[56] Hier könnte ein Löschen von Daten im Rahmen des Pufferüberlauf-Angriffs in Betracht kommen. Dabei wird ausführbarer Fremdcode eingeschleust. Dieser überschreibt zwangsläufig andere Daten. Dies könnte dann als „Löschen“ im Sinne der Norm angesehen werde, wenn eine Rekonstruktion der Daten aufgrund der Aufhebung der physischen Verkörperung unmöglich wäre.[57] Dies wäre durch Sachverständigengutachten zu klären.

[54] Eichelberger, MMR 2004, 594 (597).
[55] Tröndle/Fischer, § 303a Rn. 4; unter Verweis auf das Merkmal „rechtswidrig“ im Ergebnis auch Lackner/Kühl § 303a, Rn. 4.
[56] Lackner/Kühl, § 303a, Rn. 3; Tröndle/Fischer, § 303a, Rn. 9.
[57] Tröndle/Fischer, § 303a Rn. 9.

- Ein **Unterdrücken** liegt vor, wenn die Daten dem Berechtigten vorübergehend oder auf Dauer entzogen werden.[58] Eine Datenunterdrückung könnte in der Verlangsamung und dem wiederholten Herunterfahren der Rechner gesehen werden. Die dadurch eintretende Verzögerung der Nutzung der auf dem Rechner gespeicherten Daten dürfte aber so geringfügig sein, dass noch nicht von einem vorübergehenden Entzug der Daten gesprochen werden kann.[59]
- Die Alternative des **Unbrauchbarmachens** ist verwirklicht bei Aufhebung der bestimmungsgemäßen Verwendbarkeit der Daten.[60] Durch das Einschleusen von ausführbarem Fremdcode wird das Programm umgestaltet. Mit der Ausführung dieses Codes arbeitet das Betriebssystem nicht mehr ordnungsgemäß. Die Daten können nicht mehr bestimmungsgemäß verwendet werden. Damit dürfte ein Unbrauchbarmachen zu bejahen sein.
- Das **Verändern** von Daten umfasst alle Formen inhaltlicher Umgestaltung gespeicherter Daten.[61] Allerdings bewirkt das reine Hinzufügen von Daten noch keine inhaltliche Umgestaltung der zuvor schon vorhandenen Daten – jedenfalls wenn vorher nicht belegter Speicherplatz verwendet wird.[62] Erst wenn durch die Hinzufügung neuer Daten der Bedeutungsgehalt vorhandener Daten verändert wird liegt ein „Verändern“ im Rechtssinne vor.[63] Durch den eingeschleusten Fremdcode werden hier Daten umgestaltet.[64]

b. Subjektiver Tatbestand

X müsste **Vorsatz** bezüglich der Datenveränderung gehabt haben. Es kann davon ausgegangen werden, dass der informationstechnisch versierte X wusste, dass durch das Einschleusen von Fremdcode ein vorhandenes Programm derart manipuliert wird, dass seine Funktionalität vermindert oder aufgehoben wird. Auf dieser Idee basierte ja gerade der von ihm programmierte Wurm. Bei In-Umlauf-Bringen des Wurms wusste X mithin, welche Folgen sich daraus ergeben werden.

c. Ergebnis

X hat sich mit dem In-Umlauf-Bringen des Wurms wegen Datenveränderung strafbar gemacht. Gründe, die die Tat rechtfertigen könnten oder die Schuld des X bezüglich der Tat

---

[58] Lackner/Kühl, § 303a, Rn. 3; Tröndle/Fischer, § 303a, Rn. 10.
[59] Eichelberger, MMR 2004, 594 (595).
[60] Lackner/Kühl, § 303a, Rn. 3; Tröndle/Fischer, § 303a, Rn. 11.
[61] Lackner/Kühl, § 303a, Rn. 3; Tröndle/Fischer, § 303a, Rn. 12.
[62] Tröndle/Fischer, § 303a, Rn. 12.
[63] Ernst, NJW 2003, 3233 (3238).
[64] Selbst wenn man eine Aufhebung oder Minderung der Gebrauchstauglichkeit als Voraussetzung für eine Datenveränderung annehmen möchte (was nach Ernst: Hacker, Cracker und Computerviren, Rn. 278 teilweise der Fall zu sein scheint), dürfte eine Datenveränderung vorliegen (Eichelberger, MMR 2004, 594 (595)).

ausschließen könnten, sind nicht ersichtlich. Dabei dürfte X sowohl die Tathandlungen des Unbrauchbarmachens wie auch des Veränderns verwirklicht haben. Dies dürfte als eine Tat zu bewerten sein (Tateinheit), da mittels derselben Handlung beide Tatbestandsalternativen verwirklicht wurden.

2. Computersabotage (§ 303b StGB)

X könnte sich durch das In-Umlauf-Bringen des Wurms außerdem wegen Computersabotage strafbar gemacht haben.

§ 303b StGB [Computersabotage]
(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, daß er
1. eine Tat nach § 303a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

a. Objektiver Tatbestand

In Betracht kommt hier nur eine Strafbarkeit nach § 303b Abs. 1 Nr. 1 StGB, da Nr. 2 nur Einwirkungen auf die Hardware umfasst.[65] Eine Hardwareschädigung scheidet im vorliegenden Fall aus.

X müsste durch die Datenveränderung nach § 303a Abs. 1, 4. Alt. StGB eine Datenverarbeitung, die für ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, stören. Vom Begriff der „**Datenverarbeitung**“ dürfte der Gesamtbereich eines Daten verarbeitenden Systems umfasst sein.[66] **Wesentliche Bedeutung** hat die Datenverarbeitung, wenn die Funktionsfähigkeit der Einrichtung nach der jeweiligen Organisationsstruktur und Aufgabenstellung ganz oder jedenfalls überwiegend von ihr abhängig ist.[67] Eine **Störung** liegt vor, wenn der reibungslose Ablauf der Datenverarbeitung nicht unerheblich beeinträchtigt ist.[68] Vertretbar scheint, dass durch die reine Verlangsamung der Arbeitsgeschwindigkeit der Rechner und teilweise wiederholtes Herunterfahren eine erhebliche Störung nicht hervorgerufen wird.[69]

[65] Tröndle/Fischer, § 303b, Rn. 14.
[66] Lackner/Kühl, § 303b, Rn. 2; Tröndle/Fischer, § 303b, Rn. 4.
[67] Tröndle/Fischer, § 303b, Rn. 10.
[68] Eichelberger, MMR 2004, 594 (596).
[69] Eichelberger, MMR 2004, 594 (596).

b. Ergebnis

Eine Strafbarkeit des X wegen Computersabotage scheidet danach aus.

3. Ausspähen von Daten (§ 202a StGB)

X könnte sich durch das In-Umlauf-Bringen des Wurms wegen Ausspähens von Daten strafbar gemacht haben.

§ 202a StGB [Ausspähen von Daten]
(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

a. Objektiver Tatbestand

Tathandlung des § 202a StGB ist das **Verschaffen,** das durch die Herrschaft des Täters selbst oder eines Dritten über die Daten gekennzeichnet ist.[70] Beim im Sachverhalt beschriebenen Wurm[71] liegt keine Verschaffung von Daten vor.

b. Ergebnis

Eine Strafbarkeit wegen Ausspähens von Daten ist nicht gegeben.

4. Gesamtergebnis

X hat sich damit wegen Datenveränderung strafbar gemacht.[72]

III. Zivilrechtliche Haftung für die vorsätzliche Verbreitung von Viren – „Clear Case“

Da zwischen Täter und Opfer regelmäßig keine besonderen (Vertrags-)Beziehungen bestanden haben, kommen deliktsrechtliche Ansprüche in Betracht.

---

[70] Lackner/Kühl, § 202a, Rn. 5.
[71] Bei einem Wurm, der über E-Mail-Adressen verbreitet wird, könnte man die mittelbare Verschaffung der E-Mail-Adressen durch den Täter bejahen (Eichelberger, MMR 2004, 594 (597)).
[72] Im „Sasser-Wurm-Prozess“ wurde der Angeklagte dagegen sowohl wegen Datenveränderung als auch wegen Computersabotage schuldig gesprochen. Da das Urteil, soweit ersichtlich, nicht veröffentlicht wurde, kann der genaue Tathergang, der dem Urteil zugrunde lag, nicht nachvollzogen werden. In verschiedenen Einzelfällen scheint es durch das Herunterfahren der Rechner doch (im Gegensatz zu der hier zu Grunde gelegten Konstellation) zu massiven Beeinträchtigungen gekommen zu sein. Es kommt insoweit entscheidend auf die tatsächlichen Feststellungen an.

1. Schadensersatzanspruch (§ 823 Abs. 1 BGB)

Die Geschädigten könnten einen Schadensersatzanspruch gegen X auf Ersatz ihrer Schäden haben (§823 Abs. 1 BGB).

§ 823 BGB [Schadensersatzpflicht]
(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet. (…)

a. Rechtsgutverletzung

X müsste eines der genannten Schutzgüter verletzt haben.

- **Eigentum**

Hier könnte eine Eigentumsverletzung in Betracht kommen.[73] Eigentum besteht nur an Sachen (§ 903 S. 1 BGB).

§ 903 BGB [Befugnisse des Eigentümers]
Der Eigentümer einer Sache kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. (…)

Fraglich ist, ob Daten als **Sachen** anzusehen sind. Sachen sind körperliche Gegenstände (§ 90 BGB).

§ 90 BGB [Begriff der Sache]
Sachen im Sinne des Gesetzes sind nur körperliche Gegenstände.

Teilweise wurde darauf hingewiesen, dass Daten nur aus elektrischen Spannungen bestünden und daher keine körperlichen Gegenstände seien.[74] Jedenfalls für den Fall einer Verkörperung auf einem Datenträger wurde ein Programm vom BGH als Sache angesehen.[75] Daher wird zunehmend auf den Datenträger, auf dem die Daten verkörpert sind, abgestellt. Man könnte somit argumentieren, dass hier das Eigentum an der Festplatte durch den Wurm verletzt werde. Das Eigentum kann nicht nur durch Beschädigung oder Zerstörung verletzt werden, sondern auch durch die nicht nur kurzfristige Beeinträchtigung des bestimmungsgemäßen Gebrauchs.[76] Durch den eingeschleusten ausführbaren Fremdcode wurde der Programmablauf manipuliert, so dass dieses nicht mehr wie vorgesehen und von den Eigentümern der Rechner

[73] Eine Eigentumsverletzung wäre dagegen ohne weiteres zu bejahen, wenn durch einen Wurm oder Virus Hardwareschäden verursacht worden sind.
[74] LG Konstanz, Urteil vom 10.05.1996, Az.: 1 S 292/95; NJW 1996, 2662.
[75] BGH, Urteil vom 04.11.1987, Az.: VIII ZR 314/86; NJW 1988, 406 (408).
[76] Palandt-Sprau, BGB, 65. Auflage 2006, § 823, Rn. 7.

gewollt, ausgeführt wurde. Diese Beeinträchtigung war auch nicht nur kurzfristig. Dieser Ansicht[77] ist im Ergebnis zuzustimmen.[78]

➢ **Recht am eingerichteten und ausgeübten Gewerbebetrieb**

In Betracht kommt außerdem – soweit es sich bei den Geschädigten um Unternehmen handelt – eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb. Erforderlich ist ein betriebsbezogener Eingriff. Ein solcher liegt vor, wenn der Gewerbebetrieb als solcher unmittelbar beeinträchtigt wird. Der Eingriff muss sich spezifisch gegen den betrieblichen Organismus oder die unternehmerische Freiheit richten - und nicht nur gegen vom Betrieb ohne weiteres ablösbare Rechte oder Rechtsgüter.[79] Wenn es durch den Wurm zu einer Betriebsstörung kommt, die nicht nur unerheblich ist, dann dürfte in der vorliegenden Fallkonstellation eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetriebs vorliegen, da der X den Wurm vorsätzlich in den Verkehr gebracht hat.[80]

b. Rechtswidrigkeit

X müsste dabei rechtswidrig gehandelt haben. Da weder Rechtfertigungsgründe zu Gunsten des X noch Duldungspflichten der Geschädigten ersichtlich sind, ist von der Rechtswidrigkeit auszugehen.

c. Verschulden

➢ **Verschulden des X**

X müsste ein Verschulden treffen. Im Zivilrecht umfasst Verschulden Vorsatz und Fahrlässigkeit (§ 276 Abs. 1 BGB).

§ 276 BGB [Verantwortlichkeit des Schuldners]
(1) Der Schuldner hat Vorsatz und Fahrlässigkeit zu vertreten, wenn eine strengere oder mildere Haftung weder bestimmt noch aus dem sonstigen Inhalt des Schuldverhältnisses, insbesondere aus der Übernahme einer Garantie oder eines Beschaffungsrisikos, zu entnehmen ist. Die Vorschriften der §§ 827 und 828 finden entsprechende Anwendung. (…)

Da X den Wurm vorsätzlich in Umlauf gebracht hat, liegt ein Verschulden des X vor.

[77] Koch, NJW 2004, 801 (802); Libertus, MMR 2005, 507 (508); Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 440; OLG Karlsruhe, Urteil vom 07.11.1995, Az.: 3 U 15/95, NJW 1996, 200.
[78] Die ebenfalls in der Literatur vertretene Ansicht, die – in Parallele zum grundrechtlichen Recht auf informationelle Selbstbestimmung - ein Recht am eigenen Datenbestand anerkennen möchte, konnte sich, soweit ersichtlich, bisher in der Rechtsprechung nicht durchsetzen (Vergleiche die Nachweise bei Libertus, MMR 2005, 507 (508) und Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 440).
[79] Palandt-Sprau, § 823, Rn. 128.
[80] Koch, NJW 2004, 801 (803); Meier/Wehlau, NJW 1998, 1585 (1589).

➢ **Mitverschulden der Geschädigten**

Fraglich ist aber, ob den Geschädigten eventuell ein Mitverschulden entgegengehalten werden kann (§ 254 Abs. 1 BGB).

> **§ 254 BGB [Mitverschulden]**
> (1) Hat bei der Entstehung des Schadens ein Verschulden des Beschädigten mitgewirkt, so hängt die Verpflichtung zum Ersatz sowie der Umfang des zu leistenden Ersatzes von den Umständen, insbesondere davon ab, inwieweit der Schaden vorwiegend von dem einen oder dem anderen Teil verursacht worden ist.
> (…)

Das Mitverschulden der Geschädigten könnte darin gesehen werden, dass diese bei Bekanntwerden der Sicherheitslücke nicht das von der Softwarefirma angebotene Patch heruntergeladen und so die Lücke geschlossen haben.

Der Vorschrift des § 254 BGB liegt der Gedanke zugrunde, dass der Geschädigte nicht für einen Schaden Ersatz verlangen können soll, den er durch vernünftige Vorsorgemaßnahmen hätte verhindern können und der ihm billigerweise aufgrund seines eigenen Fehlverhaltens zuzurechnen ist.[81] Dies zeigt, dass die Frage des Mitverschuldens in besonders starkem Maß von Wertungen abhängt: Was sind vernünftige Vorsorgemaßnahmen? Wann ist dem Geschädigten billigerweise ein Fehlverhalten zuzurechnen? Die Beantwortung dieser Fragen hängt zum einen von der Verkehrsanschauung und von den besonderen Umständen im Einzelfall ab. Rechtsprechung zu diesen Fragen gibt es derzeit – soweit ersichtlich – noch nicht. Der BGH hat in seiner so genannten „Dialer-Entscheidung“[82] vom 04.03.2004 zu den Pflichten der User, sich selbst vor Dialern zu schützen, Stellung genommen (siehe unten unter IV 2 b).Zu prüfen ist, inwieweit die Geschädigten nach den Grundsätzen der Dialer-Entscheidung des BGH eine Verkehrssicherungspflicht dergestalt haben, dass sie etwa mit Firewalls oder Virenscannern Vorkehrungen zum Schutz ihrer Computer treffen müssen.

Vielleicht könnte man nach der Verkehrsauffassung von einem „Durchschnittsuser“ nicht erwarten, dass er sich (täglich) über Sicherheitslücken seines Betriebssystems informiert.[83] Andererseits darf sich auch ein technisch wenig versierter User nicht stets seiner Eigenverantwortung entledigen können. Man könnte etwa für den Fall, dass es bereits eine breite mediale Berichterstattung über eine Sicherheitslücke und deren Ausnutzung durch Schadsoftware gegeben hat und dabei auch auf ein existierendes Sicherheitspatch hingewiesen wurde,

[81] Meier/Wehlau, NJW 1998, 1585 (1590)
[82] Urteil des BGH vom 04.03.2004, Az.: III ZR 96/03.
[83] Vergleiche die parallele Argumentation von Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 531 für veröffentlichte Passwörter.

durchaus ein Mitverschulden des Geschädigten annehmen, wenn dieser die Sicherheitslücke nicht beseitigt hat.
Andererseits könnte man auch vertreten, dass angesichts der vorsätzlichen Schädigung durch X ein nur fahrlässiges Mitverschulden der Geschädigten nicht ins Gewicht fallen könne.[84]

d. Schaden

Durch die Rechtsgutsverletzung müsste adäquat-kausal ein Schaden entstanden sein. Da der Wurm hier keine eigentliche Schadenroutine aufwies, kommen als Schaden nur die Kosten in Betracht, die die Betroffenen aufwenden mussten, um den Wurm wieder von ihren Rechnern zu entfernen. Dazu war das Schließen der Sicherheitslücke durch das Patch und die Entfernung des Wurms mit einem speziellen Entfernungs-Tool, das zum Download zur Verfügung stand, erforderlich.[85] Die Kosten hierfür sind grundsätzlich– auch soweit es sich um die selbst aufgewendete Arbeitskraft handelt – Kosten der Schadensbeseitigung[86] und daher ersatzfähig.[87]

e. Ergebnis

X hat sich durch das In-Umlauf-Bringen des Wurms wegen einer Eigentumsverletzung schadensersatzpflichtig gemacht. Daneben kommt – soweit Unternehmen betroffen sind – auch eine Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb in Betracht. Der Anspruch besteht – je nachdem, welcher Auffassung man hier folgt – in voller Höhe oder nur gekürzt um den individuellen Mitverschuldensanteil.

2. Schadensersatzanspruch (§ 823 Abs. 2 BGB i.V.m. § 303a StGB)

Die Geschädigten haben außerdem einen Schadensersatzanspruch aus § 823 Abs. 2 i.V.m. § 303a StGB gegen X.

---

[84] Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 513.
[85] Vergleiche die Kurzbeschreibung des BSI.
[86] Meier/Wehlau, NJW 1998, 1585 (1589); BGH, Urteil vom 02.07.1996, Az.: X VR 64/94, NJW 1996, 2924 (2925).
[87] FEX: Diskutieren könnte man allenfalls darüber, ob auch die durch das Schließen der Sicherheitslücke entstehenden Kosten ersatzfähig sind. Schließlich hätte der Geschädigte diese Kosten sowieso tragen müssen – aus eigenem Interesse und um sich nicht einem Mitverschuldensvorwurf auszusetzen. Diese Kosten könnte der Geschädigte aber eventuell vom Verkäufer des Betriebssystems erstattet bekommen. Ein Betriebssystem mit einer Sicherheitslücke ist eine mangelhafte Ware. Der Verkäufer muss den Mangel grundsätzlich beseitigen. Bietet der Hersteller seinen Kunden insoweit ein Patch an, dass diese selbst herunterladen müssen, könnte der Verkäufer die Kosten hierfür erstatten müssen.

§ 823 BGB [Schadensersatzpflicht]
(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

§ 303a StGB bezweckt den Schutz der Berechtigten über die in Datenspeichern enthaltenen Informationen[88] und ist deswegen Schutzgesetz im Sinne des § 823 Abs. 2 BGB.[89] Hinsichtlich der weiteren Voraussetzungen ergeben sich keine Abweichungen zu dem soeben zu § 823 Abs. 1 BGB Dargelegten.

3. Schadensersatzanspruch (§ 826 BGB)

Daneben liegt ein Schadensersatzanspruch wegen vorsätzlicher sittenwidriger Schädigung vor (§ 826 BGB).[90]

§ 826 BGB [Sittenwidrige vorsätzliche Schädigung]
Wer in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt, ist dem anderen zum Ersatz des Schadens verpflichtet.

Vorteilhaft für den Geschädigten ist dabei, dass ein Mitverschulden des fahrlässig handelnden Geschädigten bei der Verursachung des Schadens gegenüber dem vorsätzlichen, sittenwidrigen Verhalten in der Regel nicht zu einer Minderung des Ersatzanspruchs führt.[91] Außerdem ist der Schadensersatzanspruch aus § 826 BGB nicht an die Verletzung eines bestimmten Rechtsguts gebunden, so dass, wenn vorsätzliches In-Umlauf-Bringen gegeben ist, in der Regel ein Schadensersatzanspruch in voller Höhe wegen vorsätzlicher sittenwidriger Schädigung besteht.

4. Ergebnis

X ist den Betroffenen zum Ersatz ihrer Schäden verpflichtet (§§ 823 Abs. 1; 826; 823 Abs. 2 BGB i.V.m. § 303a StGB). Dabei kommt es nicht darauf an, ob der Rechner des Betroffenen direkt vom Rechner des X aus infiziert wurde, oder ob dies im Wege der Weiterverbreitung über arglose Dritte geschehen ist. Auch diese Schäden sind vom Vorsatz des X umfasst.[92]

---

[88] Tröndle/Fischer, § 303a, R. 2.
[89] Eine Norm ist als Schutzgesetz anzusehen, wenn sie zumindest auch dazu dienen soll, den Einzelnen oder einzelne Personenkreise gegen die Verletzung eines bestimmten Rechtsguts zu schützen (Palandt, § 823, Rn. 57).
[90] Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 500 f.
[91] Palandt-Sprau, § 826, Rn. 16.
[92] Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 512, 516.

IV. Verantwortlichkeit bei fahrlässiger Weiterverbreitung von Viren („Hard Case“)

User Y verwendet auf seinem Rechner ein Betriebssystem der Softwarefirma S. Das Betriebssystem weist eine Sicherheitslücke auf, die der Wurm des X nutzt, um den Rechner des Y unbemerkt anzugreifen und zu infizieren. Y wundert sich zwar, dass sein Rechner langsamer arbeitet als gewohnt und in einem Fall auch selbsttätig herunterfährt. Er unternimmt aber nichts. Vom Rechner des Y aus wird in der Folgezeit der Rechner des Users Z angegriffen und infiziert. Z möchte deswegen gegen Y vorgehen. Y ist der Ansicht, ihn treffe überhaupt keine Schuld und will sich seinerseits an die Herstellerfirma S halten, die ihm das Betriebssystem auch verkauft hat.

1. Strafbarkeit des Y wegen Datenveränderung (§ 303 a StGB)

Y könnte sich dadurch, dass von seinem Rechner aus der Rechner des Z mit dem Wurm infiziert wurde, wegen Datenveränderung strafbar gemacht haben.

a. Objektiver Tatbestand

Der Wurm macht fremde Daten unbrauchbar und verändert Daten (siehe oben unter C II 1).

b. Subjektiver Tatbestand

Das Verhalten des Y müsste vorsätzlich erfolgt sein.. Anhaltspunkte dafür, dass Y die Gefahr, von seinem Rechner aus könnte sich ein Wurm weiterverbreiten und andere User schädigen, erkannt hat und diese Folgen billigend in Kauf genommen hat – was Vorsatz darstellen würde – sind nicht ersichtlich. Datenveränderung ist aber nur bei vorsätzlichem Handeln strafbar, da § 303a StGB nicht explizit auch die fahrlässige Begehung unter Strafe stellt.

§ 15 StGB [Vorsätzliches und fahrlässiges Handeln]
Strafbar ist nur vorsätzliches Handeln, wenn nicht das Gesetz fahrlässiges Handeln ausdrücklich mit Strafe bedroht.

c. Ergebnis

Y hat sich nicht strafbar gemacht.

2. Zivilrechtliche Haftung des Y

Da mangels Vorsatzes des Y Schadensersatzansprüche aus § 823 Abs. 2 i.V.m. § 303a StGB und aus § 826 BGB ausscheiden, kommt als Anspruchgrundlage allein ein **Schadensersatzanspruch aus § 823 Abs. 1 BGB** in Betracht.

a. Rechtsgutverletzung

Wiederum müsste eines der von § 823 Abs. 1 BGB geschützten Rechtsgüter verletzt sein. In Betracht kommt eine **Eigentumsverletzung**, die hier zu bejahen sein dürfte (siehe oben unter C III 1 a).

b. Zurechenbare Verletzungshandlung

- Es müsste eine **zurechenbare Verletzungshandlung** des Y vorliegen. Y hat aber gerade nicht gehandelt, sondern unternahm überhaupt nichts. Ein Unterlassen ist nur dann als Verletzungshandlung im Sinne der Norm anzusehen, wenn eine Pflicht zur Verhütung der Rechtsgutsverletzung bestanden hat, bei deren Beachtung die Verletzung verhindert worden wäre.[93]
- Eine derartige **Verkehrssicherungspflicht** kann sich im Wesentlichen aus folgenden Aspekten ergeben:[94] Beherrschung einer Gefahrenquelle, Schaffung einer besonderen Gefahrenlage, Aufgabenübernahme.
- In Betracht kommt hier vor allem die **Beherrschung einer Gefahrenquelle**, denn Y hat weder eine besondere Aufgabe übernommen noch durch vorangegangenes Tun eine besondere Gefahrenlage geschaffen. Als Inhaber der Sachherrschaft über einen infizierten Computer muss Y grundsätzlich die von diesem ausgehenden Gefahren kontrollieren und Schädigungen fremder Rechtsgüter verhindern.[95] Andererseits könnte man auch argumentieren, dass - angesichts der starken Verbreitung von Viren und Würmern - eine Infektion des eigenen Rechners unter das allgemeine Lebensrisiko falle.[96]
- Fraglich sind der genaue **Inhalt** und der **Umfang** dieser **Verkehrssicherungspflicht**. Dabei sind insbesondere die Sicherungserwartungen der betroffenen Verkehrskreise zu berücksichtigen. Nach der Aufsatzliteratur ist eine **Interessenabwägung** erforderlich, die folgenden Gesichtspunkten Rechnung trägt: [97]

---

[93] Palandt-Sprau, § 823, Rn. 2.
[94] Koch, NJW 2004, 801 (803).
[95] Koch, NJW 2004, 801 (803).
[96] Libertus, MMR 2005, 507 (509).
[97] Koch, NJW 2004, 801 (804).

- Ausmaß der drohenden Gefahr
- Möglichkeit und Zumutbarkeit der Gefahrvermeidung
- Möglichkeit und Zumutbarkeit des Selbstschutzes
- Vertrauensschutzgedanke
- Aspekte der Vorteilsziehung und Risikotragung

Das **Ausmaß der drohenden Gefahr** ist nicht besonders hoch, da der Wurm keine Schadensroutine aufweist und über die Einschleusung von Fremdcode hinaus keine Daten löscht oder verändert. Andererseits können für den einzelnen Betroffenen durchaus erhebliche Schäden entstehen, insbesondere wenn der Betriebsablauf von Unternehmen gestört wird.

Die **Gefahrvermeidung** war für Y durch das rechtzeitige Aufspielen des Patches möglich und zumutbar. Darüber hinaus hätte er nach der Infektion seines Rechners durch das selbsttätige Herunterfahren und das verlangsamtem Arbeiten auf den Wurm aufmerksam werden können und dann eine Weiterverbreitung verhindern können.

Als **Selbstschutz** war es Z möglich und zumutbar, sich selbst durch das Aufspielen des Patches zu schützen.

Unter dem Gesichtspunkt des **Vertrauensschutzes** sind Y und Z beide als im gleichen Maße schützenswert anzusehen, da es sich bei beiden um normale User handelt.

Auch aus den **Aspekten von Vorteilsziehung und Risikotragung** ergibt sich nichts anderes. Davon ausgehend, dass beide ihre Rechner für den privaten Gebrauch benutzen, sind Y und Z auch in dieser Hinsicht gleich zu beurteilen.

- Hinweise auf die (Verkehrssicherungs-)Pflichten eines privaten Users könnten sich aus der **„Dialer-Entscheidung“ des BGH** ergeben:

Exkurs: „Dialer-Entscheidung“ des BGH vom 04.03.2004[98]

In dieser Entscheidung ging es unter anderem um die Frage, welche Vorkehrungen ein durchschnittlicher Endnutzer treffen muss, um sich vor Dialern zu schützen.

Der BGH führt dazu in seiner Entscheidung aus:[99]

- Der durchschnittliche Nutzer muss nicht damit rechnen, dass sich in harmlos erscheinenden Dateien illegale Dialer verstecken, die nicht durch bloßes Löschen unschädlich gemacht werden können.

[98] Urteil des BGH vom 04.03.2004, Az.: III ZR 96/03.
[99] BGH, Urteil vom 04.03.2004, Az.: III ZR 96/03, S. 15 f.

- Ohne besondere Verdachtsmomente gibt es **keine Pflicht der Nutzer**
  - ihren Computer auf Dialer zu überprüfen
  - den Verbindungsaufbau ins Internet zu überwachen oder nur ausdrücklich freizugeben
  - Dialerschutzprogramme zu installieren
  - vorsorglich Mehrwertdienstenummern sperren zu lassen

- In Parallele zur Dialer-Entscheidung des BGH könnte man vertreten, dass Y keine Verpflichtung traf, ein **Virenschutzprogramm/Firewall** zu installieren. Dann könnte er erst recht nicht verpflichtet sein, selbst mit Hilfe eines Patch Sicherheitslücken zu schließen. Andererseits dürften Virenschutzprogramme stärker verbreitet sein als Dialerschutzprogramme, so dass die Installation eines Virenscanners eher als zumutbar und angemessen anzusehen sein könnte.[100] Rechtsprechung zu diesem Themenkomplex existiert bisher noch nicht. In der Literatur wird vertreten, dass die Installation eines Virenschutzprogramms zumutbar sei.[101]
- Ist ein Virus oder Wurm so neuartig, dass er von gängiger Schutzsoftware noch nicht erfasst ist, dann wäre das Versäumnis, Virenschutzsoftware zu installieren und regelmäßig zu aktualisieren, nicht ursächlich für einen durch die Verbreitung dieser neuartigen Viren oder Würmer verursachten Schaden. Weitere Vorsorgemaßnahmen wie etwa das vorbeugende Installieren von **Sicherheitspatches** dürfte für einen durchschnittlichen Nutzer wohl nicht zumutbar sein – anders könnte dies aber bei Unternehmen aussehen.[102]
- Allerdings gilt dies auch nach der Dialer-Entscheidung des BGH nur, solange sich keine besonderen **Verdachtsmomente** ergeben. Derartige Verdachtsmomente könnten hier in dem langsameren Arbeiten des Rechners und dem einmaligen selbsttätigen Herunterfahren gesehen werden. Y könnte daher verpflichtet gewesen sein, sein System auf Virenbefall zu prüfen.

c. Rechtswidrigkeit

Da Rechtfertigungsgründe oder Duldungspflichten nicht ersichtlich sind, kann von der Rechtswidrigkeit ausgegangen werden.

[100] Libertus, MMR 2005, 507 (509).
[101] Koch, NJW 2004, 801 (804); Libertus, MMR 2005, 507 (510); Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 516; Spindler, CR 2005, 741 (744).
[102] Libertus, MMR 2005, 507 (509 f.).

d. Verschulden

➢ **Verschulden des Y**

Y müsste ein Verschulden treffen. Vorliegend kommt nur Fahrlässigkeit in Betracht. Fahrlässigkeit liegt vor, wenn die im Verkehr erforderliche Sorgfalt außer Acht gelassen wird (§ 276 Abs. 2 BGB).

> **§ 276 BGB [Verantwortlichkeit des Schuldners]**
> (2) Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt.
> (…)

Fahrlässigkeit setzt **Vorhersehbarkeit** und **Vermeidbarkeit** des pflichtwidrigen Erfolges voraus.[103] Vorhersehbar ist ein schädigendes Ereignis schon dann, wenn die nicht ganz fern liegende Möglichkeit einer Schädigung besteht.[104] Heute dürfte davon ausgegangen werden können, dass es sich bei der Gefahr einer Infektion des Computers mit Schadsoftware um eine vorhersehbare Gefahr handelt. In den letzten Jahren wurde eine Vielzahl von Viren, Würmer etc. in Umlauf gebracht. Angesichts der teilweise gewaltigen Schäden, die dadurch verursacht wurden, gab es eine breite mediale Berichterstattung zu diesem Thema. Daher ist auch bekannt, dass Auffälligkeiten bei der Nutzung des Computers Hinweise auf einen Befall mit Viren oder Würmern sein können. Dabei kommt es auch nicht darauf an, ob diese Gefahr vom einzelnen User tatsächlich erkannt wurde. Im Zivilrecht gilt ein objektiv-abstrakter Sorgfaltsmaßstab.[105] Schließlich ist auch allgemein bekannt, dass sich Viren und Würmer ohne (bewusstes) Zutun des Nutzers weiterverbreiten und damit bei Befall des eigenen Rechners immer die Gefahr der Weiterverbreitung besteht. Die Weiterverbreitung des Wurms dürfte auch als vermeidbar anzusehen sein. Y hätte die Auffälligkeiten bei der Nutzung seines Computers bemerken und diesen überprüfen können.

➢ **Mitverschulden des Z**

Z könnte aber ein **Mitverschulden** treffen (§ 254 Abs. 1 BGB). Sieht man in der Installation einer Virenschutzsoftware eine zumutbare Vorsorgemaßnahme, dann hätte sich Z hierdurch selbst schützen können und müssen. War ein Schutz durch Virenschutzsoftware im Einzelfall nicht zu erreichen, dürfte ein Mitverschulden des Z ausscheiden.

e. Ergebnis

Je nachdem, welche Schutzmaßnahmen man auch von privaten Durchschnittsnutzern verlangen möchte, ist ein Schadensersatzanspruch wegen fahrlässiger Weiterverbreitung von Viren

[103] Palandt-Heinrichs, § 276, Rn. 12.
[104] Palandt-Heinrichs, § 276, Rn. 20.
[105] Palandt-Heinrichs, § 276, Rn. 15.

oder Würmer gegeben oder eben nicht. Auch in Ermangelung von Rechtsprechung dürfte derzeit eine Haftung für die fahrlässige Weiterverbreitung (noch?) bei nicht gewerblichen Nutzern ausscheiden.

3. Zivilrechtliche Verantwortlichkeit der Softwarefirma S

Fraglich ist, welche Verpflichtungen die Herstellerfirma S treffen im Hinblick darauf, dass der Wurm für seinen Angriff eine Sicherheitslücke in dem von S hergestellten Betriebssystem ausgenutzt hat.

a. Produkthaftungsgesetz

S könnte nach dem Produkthaftungsgesetz (ProdHaftG)[106] für Mängel seines Produktes haften und daher zum Ersatz der durch den Wurm verursachten Schäden verpflichtet sein (§ 1 ProdHaftG).

§ 1 ProdHaftG [Haftung]
(1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.
(2) Die Ersatzpflicht des Herstellers ist ausgeschlossen, wenn
1. er das Produkt nicht in den Verkehr gebracht hat,
2. nach den Umständen davon auszugehen ist, daß das Produkt den Fehler, der den Schaden verursacht hat, noch nicht hatte, als der Hersteller es in den Verkehr brachte,
3. er das Produkt weder für den Verkauf oder eine andere Form des Vertriebs mit wirtschaftlichem Zweck hergestellt noch im Rahmen seiner beruflichen Tätigkeit hergestellt oder vertrieben hat,
4. der Fehler darauf beruht, daß das Produkt in dem Zeitpunkt, in dem der Hersteller es in den Verkehr brachte, dazu zwingenden Rechtsvorschriften entsprochen hat, oder
5. der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte.
(3) Die Ersatzpflicht des Herstellers eines Teilprodukts ist ferner ausgeschlossen, wenn der Fehler durch die Konstruktion des Produkts, in welches das Teilprodukt eingearbeitet wurde, oder durch die Anleitungen des Herstellers des Produkts verursacht worden ist. Satz 1 ist auf den Hersteller eines Grundstoffs entsprechend anzuwenden.
(4) Für den Fehler, den Schaden und den ursächlichen Zusammenhang zwischen Fehler und Schaden trägt der Geschädigte die Beweislast. Ist streitig, ob die Ersatzpflicht gemäß Absatz 2 oder 3 ausgeschlossen ist, so trägt der Hersteller die Beweislast.

[106] Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG) vom 15.12.1989, BGBl I 2198.

- **Produkt**

Fraglich ist, ob auch Software ein Produkt in diesem Sinne darstellt (§ 2 ProdHaftG).

> **§ 2 ProdHaftG [Produkt]**
> Produkt im Sinne dieses Gesetzes ist jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität.

Im Hinblick auf die Sacheigenschaft von Software könnte wiederum auf die Verkörperung der geistigen Leistung abgestellt werden.[107] Schutzzweckerwägungen könnten für diese Einordnung sprechen. Das Produkthaftungsgesetz soll dem Schutz der Verbraucher vor durch fehlerhafte Produkte verursachten Schäden dienen. Es geht hauptsächlich um Konstruktions-, Fabrikations- und Instruktionsfehler des Herstellers. Unter anderem da der Geschädigte Schwierigkeiten haben wird, derartige Fehler nachzuweisen, ist die Produkthaftung als verschuldensunabhängige Garantiehaftung ausgestaltet. Standardsoftware wie ein Betriebssystem eines großen Herstellers ist heute ein ebensolches Massenprodukt wie die klassischen industriell hergestellten (Massen-)Waren. Im Ergebnis dürfte die Einbeziehung von Standardsoftware in den Anwendungsbereich des ProdHaftG sachgerecht sein – jedenfalls wenn man Literaturmeinungen folgt.[108]

- **Fehler**

Die Sicherheitslücke müsste einen Fehler der Software darstellen (§ 3 ProdHaftG).

> **§ 3 ProdHaftG [Fehler]**
> (1) Ein Produkt hat einen Fehler, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere
> a) seiner Darbietung,
> b) des Gebrauchs, mit dem billigerweise gerechnet werden kann,
> c) des Zeitpunkts, in dem es in den Verkehr gebracht wurde,
> berechtigterweise erwartet werden kann.
> (2) Ein Produkt hat nicht allein deshalb einen Fehler, weil später ein verbessertes Produkt in den Verkehr gebracht wurde.

Die Produktfehler werden in drei Kategorien eingeteilt: Fabrikations-, Konstruktions- und Instruktionsfehler.[109] Programmierungsfehler bei Software fallen immer in die Kategorie der Konstruktionsfehler, da die technische Konzeption des Produkts dann ungeeignet ist und dieser Fehler der gesamten Serie anhaftet.[110]

---

[107] Palandt-Sprau, BGB, 65. Auflage 2006, § 2 ProdHaftG, Rn. 1.
[108] Hohmann, NJW 1999, 521 (525), Mankowski, in: Ernst, „Hacker, Cracker und Computerviren“, Rz. 441; Meier/Wehlau, NJW 1998, 1585 (1589); Spindler, NJW 1999, 3737 (3742); derselbe, NJW 2004, 3145 (3149).
[109] Palandt-Sprau, § 3 ProdHaftG, Rn. 8 ff.
[110] Hohmann, NJW 1999, 521 (524); Palandt-Sprau, § 3 ProdHaftG, Rn. 8; Spindler, NJW 1999, 3737 (3738).

Der Maßstab, nach dem sich das Vorliegen eines Fehlers bestimmt, richtet sich nach den berechtigten Sicherheitserwartungen. Dabei sind alle Umstände des Einzelfalls zu berücksichtigen. Angesichts der teilweise behaupteten objektiven Unvermeidbarkeit von Programmierungsfehlern bei Software[111] kommt es in diesem Bereich entscheidend auf den Stand von Wissenschaft und Technik bei In-Verkehr-Bringen des Produktes an.[112] Wertet man Pufferüberlauf-Angriffe als bekannt, dann sind Programme vom Hersteller so zu programmieren, dass Pufferüberläufe vermieden werden.[113] Versäumt der Hersteller dies, liegt ein Fehler vor. Bewertet man die Sicherheitslücke als zum Zeitpunkt des In-Verkehr-Bringens nicht bekannt, scheidet eine Haftung nach dem ProdHaftG aus.

- **Ergebnis**

  S macht sich bei zum Zeitpunkt des In-Verkehr-Bringens fehlerhafter Software schadensersatzpflichtig.Ein Schadensersatzanspruch nach dem ProdHaftG kommt aber immer nur bei Körper- oder Gesundheitsverletzungen in Betracht oder bei Beschädigung von Sachen in privatem Gebrauch.[114]

b. Produktbeobachtungspflichten

S könnte sich des Weiteren schadensersatzpflichtig gemacht haben wegen Verletzung seiner Verkehrssicherungspflichten (§ 823 Abs. 1 BGB).

§ 823 BGB [Schadensersatzpflicht]
(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.
(…)

- **Zurechenbare Verletzungshandlung**

Der Hersteller eines Produkts haftet neben der speziellen Produkthaftung aus dem ProdHaftG auch nach allgemeinen deliktsrechtlichen Grundsätzen. Er ist verkehrssicherungspflichtig, da er ein gefährliches Produkt in den Verkehr gebracht und damit eine Gefahrenlage für Dritte geschaffen hat. Den Hersteller treffen daher Produktbeobachtungs-, Warn- und Rückrufpflichten. Auch wenn ein Programm bei In-Verkehr-Bringen nicht fehlerhaft war, kann sich der Hersteller schadensersatzpflichtig machen, wenn das Produkt später unsicher wird. Gerade im Hinblick auf die objektive Unvermeidbarkeit von Programmierungsfehlern trifft einen Soft-

[111] Spindler, CR 2005, 741 (741 f.).
[112] Palandt-Sprau, § 3 ProdHaftG, Rn. 2 ff.
[113] Vergleiche zu den Möglichkeiten „sicherer“ Programmierung C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 3. Auflage 2004, S. 41 ff.
[114] Palandt-Sprau, § 1 ProdHaftG, Rn. 6 f.

warehersteller die Pflicht zu besonders sorgfältiger Produktbeobachtung.[115] Ein Softwarehersteller muss daher beispielsweise Literatur und sonstige Erkenntnisse über mögliche Defekte seiner Software sammeln und auswerten.[116] Dazu gehört auch, die Produktentwicklung der wichtigsten Mitbewerber zu beobachten.[117]

S hat hier ein Sicherheitspatch veröffentlicht und ist damit seinen Pflichten nachgekommen.[118] Eine Pflichtverletzung liegt deswegen nicht vor.

- **Ergebnis**

S hat sich nicht wegen Verletzung von Verkehrssicherungspflichten schadensersatzpflichtig gemacht.

[115] Spindler, NJW 2004, 3145 (3147).
[116] Spindler, CR 2005, 741 (743).
[117] Palandt-Sprau, § 823, Rn. 172.
[118] Spindler, CR 2005, 741 (743).

D. Literaturhinweise

- *Buggisch, Walter*: Dialer-Programme, strafrechtliche Bewertung eines aktuellen Problems, NStZ 2002, 178.
- *Eichelberger, Jan*: Sasser, Blaster, Phatbot & Co. – alles halb so schlimm? – Ein Überblick über die strafrechtliche Bewertung von Computerschädlingen, MM 2004, 594.
- *Ernst, Stefan*: Hacker, Cracker und Computerviren, 2004.
- *Ernst, Stefan*: Hacker und Computerviren im Strafrecht, NJW 2003, 3233.
- *Hoeren, Thomas*: Virenscannng und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., NJW 2004, 3513.
- *Hohmann, Harald*: Haftung der Softwarehersteller für das „Jahr 2000"-Problem, NJW 1999, 521.
- *Koch, Robert*: Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801.
- *Libertus, Michael*: Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren. MMR 2005, 507.
- *Meier, Klaus / Wehlau, Andreas*: Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585.
- *Popp, Andreas*: Von „Datendieben" und „Betrügern" - Zur Strafbarkeit des so genannten „phishing", NJW 2004, 3517.
- *Rösler, Hannes*: Zur Zahlungspflicht für heimliche Dialereinwahlen, NJW 2004, 2566.
- *Spindler, Gerald*: Das Jahr 2000-Problem in der Produkthaftung: Pflichten der Hersteller und der Softwarenutzer, NJW 1999, 3737.
- *Spindler, Gerald*: IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3145.
- *Spindler, Gerald*: Haftung und Verantwortlichkeit im IT-Recht, Ein Rück- und Ausblick zu den Bewährungsproben der allgemeinen Grundsätze des Haftungsrechts, CR 2005, 741.