Prof. Dr. Viola Schmid, LL.M.

Fachgebiet Öffentliches Recht

Informations- und Datenschutzrecht

Modul 6

A. Begriff der IT-Sicherheit

B. Szenario

C. Recht

*FÖR- Fachgebiet Öffentliches Recht cyberlaw@jus.tu-darmstadt.de

Art. 9 Internationaler Pakt über bürgerliche und politische Rechte

(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. (…)

Artikel 29 EU

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.

Art. 5 EMRK

(1) Jedermann hat das Recht auf Freiheit und Sicherheit. (…)

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. (…)

§ 1 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) [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. (…)

Artikel I- 42 EuV [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**

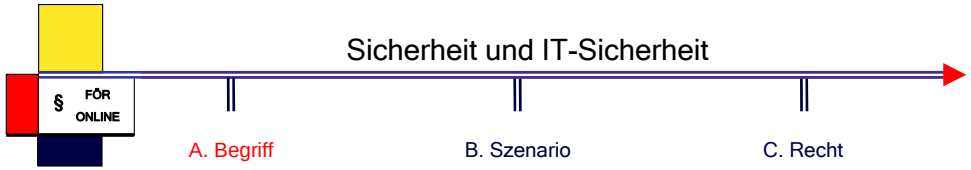
a) durch den Erlass von Europäischen Gesetzen und Rahmengesetzen, mit denen, soweit erforderlich,die Rechtsvorschriften der Mitgliedstaaten in den in Teil III genannten Bereichen einander angeglichen werden sollen;

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 derpolizeilichen und justiziellen Zusammenarbeit in Strafsachen.

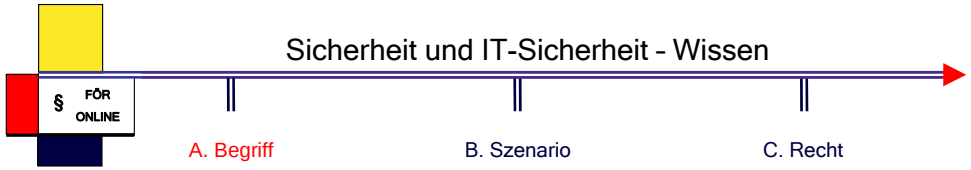


Der Beitrag von IT-Systemen zur Schaffung eines „Raums der Sicherheit“ wird vorausgesetzt:

Artikel I- 42 EuV [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**

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.**



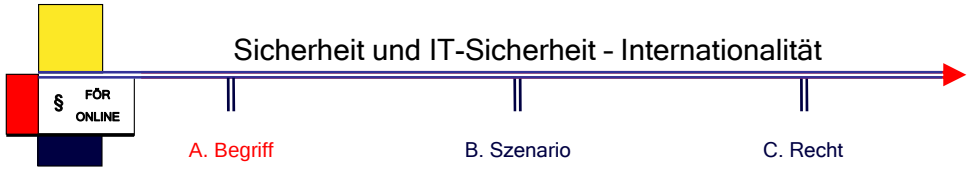
Sicherheit als Prävention und Sanktion von Verbrechen setzt Wissen voraus.

- Wissensvermehrung

→ Aufbau von europäischen Behörden und Daten„organisations“systemen (etwa Europol)

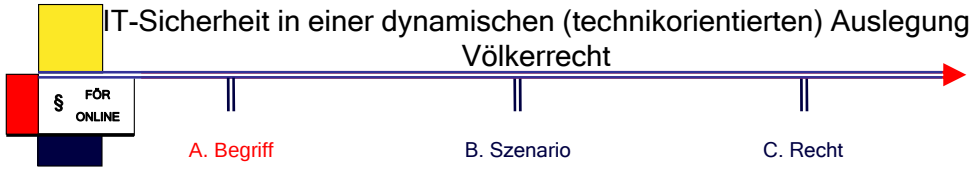
- Wissensverteilung

→ Förderung der Interoperabilität von mitgliedstaatlichen Behörden und Daten“organisations“systemen untereinander



Internationalität der IT-Systeme (Beispiel: „Fluggastdatenaffäre“) verlangt nach IT-Sicherheit. IT-Systeme müssen selbst sicher (und selbstsicher) sein.

→ Sicherheit durch IT-Systeme; aber keine Sicherheit ohne IT-Sicherheit.



OECD Guidelines for the Security of Information Systems and Networks

(...)

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.

Art. 4 Verordnung zur Gründung einer Agentur für Netz- und Informationssicherheit [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.

§ 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.

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**),

(…)

Anlage zu § 9 BDSG

(…)

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.

§ 2 Abs. 2 BSIG

(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.

§ 109 Telekommunikationsgesetz [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.

(...)

§ 109 Telekommunikationsgesetz [Technische Schutzmaßnahmen]

(...)

(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 Gesetzesentwurf zur Änderung der VwGO nach dem Justizkommunikationsgesetz 9/2004

(1) Die Beteiligten können dem Gericht elektronische Dokumente übermitteln, soweit dies für den jeweiligen Zuständigkeitsbereich durch Rechtsverordnung der Bundesregierung oder der Landesregierung 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. (...)

Richtlinie zur Gewährleistung der notwendigen Sicherheit beim IT-Einsatz in der Berliner Verwaltung (IT-Sicherheitslinie), Berlin

A Grundsätze der Sicherheitspolitik

(…)

Berücksichtigung von IT-Sicherheit beim IT-Einsatz

(3) Die Gewährleistung von Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Nachweisbarkeit im jeweils erforderlichen Maße ist unabdingbare Voraussetzung und Bestandteil jedes IT-Einsatzes und für den gesamten Einsatzzeitraum auf der Basis von Sicherheitskonzepten sicherzustellen.

Beispiel Signaturrecht: (Modul 5, Folie 17)

Elektronische Dokumente und Signaturen müssen „sicher“ sein; und hier lassen sich folgende Aspekte unterscheiden.

- kein Unbefugter Kenntnis des Dokuments erhält („Vertraulichkeit“ oder „Intimität“; *C. Eckert, S. 8: „Informationsvertraulichkeit“, „confidentiality“*)
- ein Dritter das elektronische Dokument nicht verändern kann („Integrität“, *C.Eckert, S. 7: „Datenintegrität“, integrity“*)
- die Signatur von der Person stammt, die signaturberechtigt ist („Identität“ (keine Entsprechung in der Informatik mehr …)).
- der Signierende unter seinem eigenen Namen agiert („Authentizität“; *C.Eckert: S. 6 f: „authenticity“, “authentication“*)

FÖR-TUD-“Formel”: I³A

So soll erreicht werden, dass Systeme Verfügbarkeit (availability) und Verbindlichkeit (non repudiation) gewährleisten.

Sicherheit in der Informationstechnologie (IT-Sicherheit)

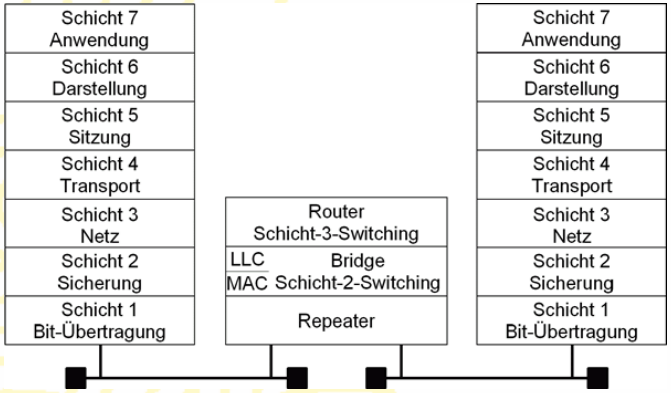
- **„Safety“ als Funktionssicherheit**
- **„Security“ als Informationssicherheit**
- **„Protection“ als Datensicherheit**

- IT-Sicherheit (im Kontext von Sicherheitspolitik) setzt „Safety“ und „Security“ voraus

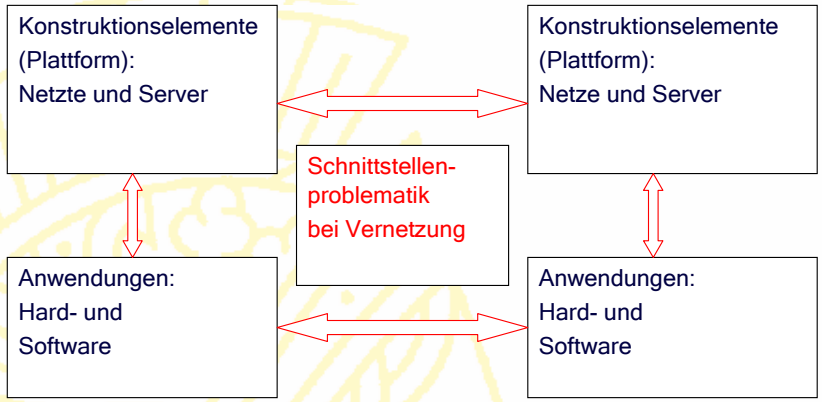
  →Sicherheitsrelevante Daten müssen nicht nur effektiv und effizient organisiert werden, sondern gegenüber Angriffen wehrfähig („resistent“) sein.

- Sicherheit und (IT-)Sicherheit gilt es zu optimieren – und nicht „nur“ zu definieren.

ISO (International Organization for Standardization)/
OSI-Modell (Open Systems Interconnection Reference Model



Quelle: IT-Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb/deutsch/m/m05013.html.



Gefahren für IT-Systeme können

- interne [personale und technische (etwa Mitarbeiter und/oder fehlende Safety)] und
- externe Ursachen [personale und technische (etwa Hacker und/oder fehlende Security)]

haben.

Personale „Ursachen“

- Vorsätzliche Angriffe
  → „Vorsatz ist Wissen und Wollen der Tatbestandsverwirklichung.“
  → Ausreichend bedingter Vorsatz (Der Handelnde ist mit dem Eintreten des für möglich gehaltenen Erfolges in dem Sinne einverstanden, dass er ihn billigend in Kauf nimmt.)
- andere Angriffe

Gefahrenlage – Mittelbare Täterschaft

A. Begriff | B. Szenario | C. Recht

Auch mittelbare Täter („durch einen anderen“) werden strafrechtlich als Vorsatztäter verfolgt.

§ 25 StGB [Täterschaft]
(1) Als Täter wird bestraft, wer die Straftat selbst oder **durch einen anderen** begeht. (...)

Gefahrenlage – Beispiele (1)

A. Begriff | B. Szenario | C. Recht

- **Hacken:**
  Bei von Hackern (bzw. Crackern, Cyberpunks, Computerspionen) begangenen Angriffen wird unbefugt in fremden Datensystemen operiert. Der Zugang hierzu kann auf verschiedene Weise erfolgen. Durch das Ausspähen von Daten oder Manipulationen von Daten oder Programmen können enorme wirtschaftliche Schäden aber auch Gefahren für Leib und Leben (etwa bei medizinischen Einrichtungen) entstehen.

- **Viren:**
  Viren sind zur Reproduktion fähige, nicht selbständig ablaufende Programme, die ein Wirtsprogramm zur Ausführung benötigt. Durch Viren können einzelne Daten manipuliert oder gelöscht werden. Sie können auch den gesamten Rechner und das BIOS schädigen.

Gefahrenlage – Beispiele (2)

A. Begriff | B. Szenario | C. Recht

- **Würmer:**
  Bei Würmern handelt es sich um sich selbst reproduzierende Programme, die nicht auf ein Wirtsprogramm angewiesen sind. Sie können zu einer Rechner/- Netzüberlastung führen.

- **DoS-Angriff:**
  Bei einem DoS-Angriff (Denial-of-Service-Angriff) wird ein Rechner, ein Netz oder ein Server gezielt mit Anfragen so überhäuft, dass es wegen Überlastung zum Systemausfall kommt.

Gefahrenlage – Beispiele (3)

A. Begriff | B. Szenario | C. Recht

- **Trojanische Pferde:**
  Trojanische Pferde sind Programme, die vortäuschen, ein reguläres Programm- oder Programmteil zu sein, dieses aber ersetzen, um Daten auszuspähen oder zu löschen.

- **Dialer:**
  Dialer sind Programme, die auf einem Rechner installiert werden und Verbindungen zu einer Mehrwertdienstrufnummer (0190er/ 0900er Nummer) aufbauen, die i.d.R. zu deutlich erhöhten Verbindungskosten führen. Die Installation und Verbindungsanwahl kann bei manipulativen Dialern erfolgen, ohne dass der Nutzer davon Kenntnis hat.

Gefahrenlage - Andere Angriffe

- **Fahrlässige Angriffe:**
  Fahrlässige Angriffe resultieren etwa aus menschlichem Fehlverhalten, wenn zwar ein Bewusstsein für eine Gefahrenlage vorhanden ist, allerdings darauf vertraut wird, dass „alles gut geht“.

- **Technisches Versagen**:
  Technisches Versagen wird zu einem „Angriff“ auf IT-Systeme, wenn etwa die Software unausgereift oder fehlerhaft, und oder kein Sicherheitsnetz für den Ausfall einer Komponente implementiert ist.

- **Höhere Gewalt:**
  Methodisch ist die höhere Gewalt ein unbestimmter Rechtsbegriff, dessen Inhalt kontextabhängig zu bestimmen ist. Dem Gefährdungskatalog des IT-Grundschutzhandbuches ist zu entnehmen, dass höhere Gewalt Gefährdungen durch Blitz, Wasser, Sturm, Feuer oder Personalausfall infolge Krankheit oder Streik umfasst. Die Abgrenzung zu technischem Versagen scheint nicht immer trennscharf.

Pro-Akteure - OECD (1)

Die OECD (Organization for Ecoconomical Co-Operation and Development) ist eine ursprünglich europäische, jetzt global offene, internationale Organisation (= auf völkerrechtlichem Vertrag beruhender, mitgliedschaftlicher Zusammenschluss von Völkerrechtssubjekten), welche die Interessen marktwirtschaftlicher Staaten vertritt.

→ „soft law“ (Empfehlungen und Stellungnahmen)

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. (...)

Pro-Akteure - OECD (2)

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; (...)

Pro-Akteure - ENISA (1)

Gründung (1.1.2004)

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.

(...)

Pro-Akteure - ENISA (2)

Ziele

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.

Pro-Akteure - BSI

BSI (Bundesamt für Sicherheit in der Informationstechnik)

§ 1 BSIG

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

- forscht im Bereich der Informationssicherheit,
- prüft IT-Produkte
- berät Hersteller, Vertreiber und Anwender von Informationstechnik
- weist auf drohende Gefährdungen hin
- informiert über aktuelle Viren
- stellt ein Grundschutzhandbuch für Unternehmen zur Verfügung
- übernimmt 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
- berät Bund beim Projekt BundOnline 2005 („E-Government“).

Pro-Akteure - RegTP (1)

RegTP (Regulierungsbehörde für Gas, Elektrizität, Telekommunikation und Post)

[„Gas und Elektrizität“ nach Verabschiedung des Energiewirtschaftgesetzes]

§ 116 TKG [Sitz und Rechtsstellung]

(1) Die Regulierungsbehörde für Telekommunikation und Post nimmt die ihr nach diesem oder anderen Gesetzen zugewiesenen Aufgaben und Befugnisse wahr. Die Regulierungsbehörde ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums für Wirtschaft und Arbeit mit Sitz in Bonn.

§ 3 SigG [Zuständige Behörde]

Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 obliegen der Behörde nach § 66* des Telekommunikationsgesetzes.

*Verweis bezieht sich auf das TKG a.F. (vor Novelle 2004)

Pro-Akteure - RegTP (2)

§ 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:

(…)

Pro-Akteure - RegTP (3)

A. Begriff | B. Szenario | C. Recht

§ 115 TKG [Kontrolle und Durchsetzung von Verpflichtungen]

(…)

(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 (…). 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.

Pro-Akteure - Landesrecht

A. Begriff | B. Szenario | C. Recht

Richtlinie (Entwurf zur Neufassung Stand: 21.11.01)
für die Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren
- IT-Sicherheitsrichtlinie-, Saarland

2.1 Ein IT-Sicherheitsmanagement soll jeweils dafür Sorge tragen, dass die Aspekte der **Datensicherheit und des Datenschutzes** berücksichtigt werden. Das IT-Sicherheitsmanagement ist auch zuständig für die Entwicklung einer IT-Sicher-heitsstrategie, die Begleitung der Projektarbeit und die Realisierung und Fortentwicklung der Maßnahmen für Datensicherheit und Datenschutz im laufenden Betrieb.

Verwaltungsinnenrecht

→ i.d.R. keine Rechte und Pflichten für Bürger (keine Außenwirkung)

Contra-Akteure

A. Begriff | B. Szenario | C. Recht

Als „Contra-Akteure“ werden diejenigen Beteiligten bezeichnet, die IT Sicherheit „durchbrechen“. Mit der Bezeichnung „Contra-Akteur soll keine Bewertung verbunden werden: So können Contra-Akteure, die die IT-Sicherheit gefährden durchaus zu Pro-Akteuren der Sicherheit in der Realworld werden (Prüfung des Verhältnismäßigkeitsgrundsatzes). 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.

Contra-Akteure

A. Begriff | B. Szenario | C. Recht

Als „Contra-Akteure“ werden diejenigen Beteiligten bezeichnet, die IT Sicherheit „durchbrechen“. Mit der Bezeichnung „Contra-Akteur soll keine Bewertung verbunden werden: So können Contra-Akteure, die die IT-Sicherheit gefährden durchaus zu Pro-Akteuren der Sicherheit in der Realworld werden (Prüfung des Verhältnismäßigkeitsgrundsatzes). 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.

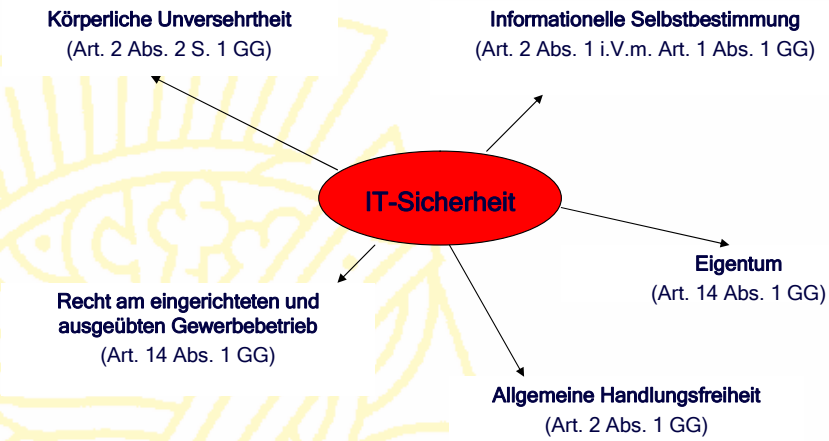
User

A. Begriff B. Szenario C. Recht

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“exemplifiziert die in der Vorlesung vorgestellte Ambivalenzthese.

Grundrechtliche Gefährdungslage

A. Begriff B. Szenario C. Recht



Grundrechtliche Gefährdungslage

A. Begriff B. Szenario C. Recht

➢Die körperliche Unversehrtheit kann beeinträchtigt werden, wenn etwa ein DoS-Angriff die Geräte eines Krankenhauses lahm legt.

➢Die informationelle Selbstbestimmung kann durch den unbefugten Zugang zu gespeicherten Daten beeinträchtigt werden, etwa durch das Einloggen auf den geschützten Bereich einer Homepage.

➢Das Eigentum kann durch Viren durch die Beschädigung der Hardware beeinträchtigt werden, wenn etwa bei Befall des BIOS der Lüfter abgeschaltet wird und der Rechner überhitzt.

➢Das Recht am eingerichteten und ausgeübten Gewerbebetrieb kann ebenfalls infolge der Schäden durch Virenbefall beeinträchtigt werden.

➢Die allgemeine Handlungsfreiheit kann durch einen DoS -Angriff beeinträchtigt werden, wenn etwa durch einen DoS-Angriff das IT-System eines Unternehmens kurzzeitig funktionsunfähig (ohne diesen in seiner Substanz zu beschädigen) gemacht wird.

Präventive Strategien

A. Begriff B. Szenario C. Recht

➢ **Institutionelle Optionen**

→ ENISA , BSI, RegTP; Sicherheitsbeauftragter

➢ **Kommunikationspolitische Strategien:** Information, Werbung und Public Relations)

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

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

→Common Criteria, ISO 17799, BS 7799, IT-Grundschutzhandbuch des BSI

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

Prozessuale Strategien - Telekommunikation

A. Begriff | B. Szenario | C. Recht

§ 109 Abs. 3 Telekommunikationsgesetz [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. (…)

Repressive Optionen – ex post: Szenario 1

A. Begriff | B. Szenario | C. Recht

„Clear Case“

Szenario 1

Der User X, der informationstechnisch sehr versiert ist, bastelt in seiner Freizeit ein Programm, das sich auf fremden PCs unbemerkt installiert. Bei der Verbindung ins Internet wird (unbemerkt von dem jeweiligen Nutzer) anstelle der normalen Verbindung eine kostenintensive Mehrwertdienstverbindung aufgebaut. Diese Mail verschickt er getarnt als Tipp, „Schnelles, günstiges und sicheres Surfen“. Danach sitzt er sicher in seinem Sessel und wartet auf die ersten Einnahmen.

Repressive Optionen – ex post: Szenario 2

A. Begriff | B. Szenario | C. Recht

„Hard Case“

Szenario 2

User Y findet in seiner Eingangspost eine Mail mit Tipps, „Schnelles, günstiges und sicheres Surfen“. User Y fühlt sich von dem schnellen, günstigen und sicheren Surfen angesprochen, und will dieses enorme Schnäppchen an seinen Bekanntenkreis weiterleiten. Unbewusst wird User Y zum Mittel, um einen Dialer zu verbreiten, der sich sofort und unbemerkt auf den jeweiligen Festplatten installiert.

→ **Kein Vorsatz!**

Repressive Optionen – Strafrechtliche Sanktionen (1)

A. Begriff | B. Szenario | C. Recht

Article 8 CCC [Computer-related fraud]

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Repressive Optionen – Strafrechtliche Sanktionen (2)

A. Begriff | B. Szenario | C. Recht

Art. 4 des Vorschlags für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme

Die Mitgliedstaaten stellen sicher, dass die nachstehenden vorsätzlichen oder unrechtmäßigen Handlungen unter Strafe gestellt werden:

(…)

(b) Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten eines Informationssystems, sofern dies in der Absicht geschieht, einer natürlichen oder einer juristischen Person Schaden zuzufügen.

Repressive Optionen – Strafrechtliche Sanktionen (3)

A. Begriff | B. Szenario | C. Recht

§ 263a StGB [Computerbetrug]

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Repressive Optionen – Zivilrechtliche Kompensation (1)

A. Begriff | B. Szenario | C. Recht

§ 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.

(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.

Repressive Optionen – Zivilrechtliche Kompensation (2)

A. Begriff | B. Szenario | C. Recht

Fahrlässigkeit

→ Außerachtlassen der im Verkehr üblichen Sorgfalt

§ 276 BGB [Verantwortlichkeit des Schuldners]

(…)

(2) Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt.

(…)

- *Buggisch, Walter*, Dialer-Programme, strafrechtliche Bewertung eines aktuellen Problems, NStZ 2002, 178.
- *Ernst, Stefan,* Hacker, Cracker und Computerviren, 2004.
- *Ernst, Stefan*, Hacker und Computerviren im Strafrecht, NJW 2003, 3234.
- *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,* IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer, NJW 2004, 3154.

Informations- und Datenschutzrecht

Modul 6

A. Begriff der IT-Sicherheit

B. Szenario

C. Recht