FIfF
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Fachhochschule Brandenburg
University of Applied Sciences

Ute Bernhardt, Ingo Ruhmann

IT-Sicherheit nach dem neuen IT-Sicherheitsgesetz

1. Ziele und Lösungsansatz
2. Probleme der rechtskonformen Umsetzung
3. Fragen für die Praxis

Ziele und Lösungsansatz

Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit

a) von **Unternehmen**,

„Betreiber Kritischer Infrastrukturen [werden verpflichtet], ein *Mindestniveau an IT-Sicherheit* einzuhalten und dem BSI *IT-Sicherheitsvorfälle* zu melden."

b) verstärkter Schutz der **Bürgerinnen und Bürger im Internet**

Dazu werden „Telekommunikationsanbieter verpflichtet,

- IT-Sicherheit [bezüglich der] *Verfügbarkeit* ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten.
- *IT-Sicherheitsvorfälle*, die zu einem unerlaubten *Zugriff auf die Systeme der Nutzerinnen und Nutzer* oder einer *Beeinträchtigung der Verfügbarkeit führen können*, an das BSI *melden* und betroffene *Nutzerinnen und Nutzer* über bekannte Störungen *informieren*, die durch *Schadprogramme auf den datenverarbeitenden Systemen* der *Nutzerinnen und Nutzer* hervorgerufen werden. "

c) Stärkung von **BSI und Bundeskriminalamt**

Durch mehr Personal und weitere Zuständigkeiten

a) IT-Sicherheit bei Unternehmen

Kritische Infrastrukturen

- Energie,
- IT und Telekommunikation,
- Transport und Verkehr
- Gesundheit,
- Wasser, Ernährung
- Finanz- und Versicherungswesen

„Mindestmaß an IT-Sicherheit" = „Stand der Technik"

Aber:

neue Sicherheitslücken bedeuten keinen neuen „Stand der Technik"

Bisheriges Verständnis der IT-Sicherheit nach BSI-Grundschutzhandbuch:

Risiko = Eintrittswahrscheinlichkeit * Schadenshöhe

- Kalkulierter vertretbarer Schaden versus Aufwand für IT-Sicherheit
- Dynamische Bewertung: Neue Sachlage erzwingt neue Bewertung (inklusive Abschalten)

IT-Sicherheit bei Unternehmen

Das Informationsmodell des ITSIG

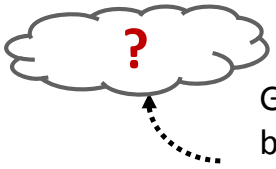
Melden

erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT die zu Ausfall oder Beeinträchtigung der Funktionsfähigkeit **führen können** oder geführt haben

KRITIS-Betreiber

nach Stand der Technik

BSI



Gem. §7 (1) BSIG „**kann**“ das BSI KRITIS-Betreiber bzw. die Öffentlichkeit über Gefährdungen informieren

IT-Sicherheit für die IT des Bundes

- BSI-Gesetzesnovelle 2007:
  Sonderrechte für BSI bei der Datenerhebung für Analysen

- IT-SiG 2015:
  BKA als Sonderermittler bei Angriffen auf die IT des Bundes
- Personalzuwachs (abgeleiteter Stellenbedarf) bei
  - BSI (115-216 Stellen),
  - BKA (48-78 Stellen), BfV (26-48 Stellen), BND (30 Stellen),
  - Bundes-Netzagentur (28 Stellen),
  - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (9-13 Stellen)
  - Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (4 Stellen),
  - BfDI (2-7 Stellen)

IT-Sicherheit für Bürgerinnen und Bürger

- IT-Sicherheit bei TK- und Internet-Providern nach dem „Stand der Technik“
- Idee der TK- / Internet-Provider als Service-„Virenscanner“ für Nutzer

Vergleich aus systematischer Sicht

- Keine Informationsrechte an Erkenntnissen des BSI zu Sicherheitsvorfällen
- Keine Informationsrechte und Hilfen (im Verhältnis zu Providern) bei „unerlaubtem Zugriff“ auf eigene Systeme
- Keine Hilfe bei Ermittlungen und rechtsförmiger Verfolgung von Sicherheitsvorfällen

2. Probleme der rechtskonformen Umsetzung

„De lege Germaniae, Internet divisa est in partes tres“

Für die IT-Sicherheit besteht das Internet im deutschem Recht aus drei verschiedenen Welten:

I. Telekommunikationsgesetz (TKG)

II. Telemediengesetz (TMG)

III. BSI-Gesetz (BSIG)

I. TKG

§100 TKG seit 1995

(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die **Bestandsdaten und Verkehrsdaten** der Teilnehmer und Nutzer **erheben und verwenden**.

(2) Zur Durchführung von Umschaltungen sowie zum Erkennen und Eingrenzen von Störungen im Netz ist dem Betreiber der Telekommunikationsanlage oder seinem Beauftragten das **Aufschalten auf bestehende Verbindungen** erlaubt, soweit dies betrieblich erforderlich ist.

- Umfassende Befugnis zur Datenerhebung bei der Störungsbeseitigung für analoge TK-Technik
- Verfassungsmäßigkeit bei IP-Netztechnik äußerst zweifelhaft

Neufassung §100 TKG im IT-Sicherheitsgesetz

Zulässig ist die Datenerhebung

„für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können".

Nutzer (nach §3 Nr. 14 TKG) = „natürliche oder juristische Personen, die einen öffentlich zugänglichen Telekommunikationsdienst für private oder geschäftliche Zwecke in Anspruch" nehmen

Neuer §109a TKG:

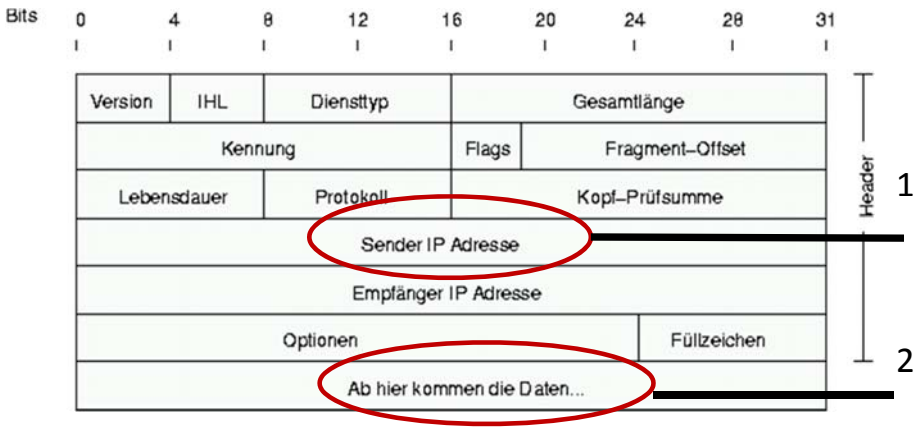
TK-Provider sollen bei „Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen", diese Nutzer (keine Kunden)

„soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können".

Neufassung von § 100 und 109a TKG

Wie sieht ein Provider durchlaufende „Nutzer“daten, die Schadcode enthalten (gem. §100 TKG)?

Datenpaket nach dem Internet-Protokoll (IP) V.4 gemäß RFC 791



1. IP-Nummer des Verursachers (Störers)
2. Schadcode-Inhalt nach „Deep Packet Inspection“

- Wie informiert ein Provider diese „Nutzer“ (gem. §109a TKG) – per Code-Injection wie die NSA?
- Welchen Aufwand muss der Provider treiben, um Nutzer zu ermitteln?

TK-Recht nach dem ITSIG

Das Fernmeldegeheimnis wurde zur Information von Störern über Mittel zur „Störungsbeseitigung“ eingeschränkt

Erlaubt ist ein nahezu unbegrenzter Eingriff in Art. 10 GG, ohne ausreichend konkreten

- **Anlass**: statt Gefährdung, nur „Störung“ oder „unerlaubter Zugriff“
- **Art und Umfang** der Datennutzung
- Angabe zu **Speicherfristen**
- Generell: **Normenklarheit**

mit dem Zweck der **Information** von beliebigen Nutzern, nicht Kunden

II. Telemedien-Gesetz – vom ITSIG unverändert

§12 TMG: klassische Verbotsnorm mit Erlaubnisvorbehalt

§13 TMG

(4) Der Diensteanbieter hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass

2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung **unmittelbar nach deren Beendigung gelöscht** oder in den Fällen des Satzes 2 gesperrt werden,

§14 **TMG**

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines **Vertragsverhältnisses** zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (**Bestandsdaten**).

§15 TMG

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die **Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen** (**Nutzungsdaten**). Nutzungsdaten sind insbesondere
   1. Merkmale zur Identifikation des Nutzers,
   2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
   3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

(3) Der Diensteanbieter darf für Zwecke **der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedie**n Nutzungsprofile bei Verwendung von **Pseudonymen** erstellen, sofern der Nutzer dem nicht widerspricht.

Beschluss des Ersten Senats BVerfG vom 24. Januar 2012 (- 1 BvR 1299/05 -)

> „In der Zuordnung von Telekommunikationsnummern zu ihren Anschlussinhabern liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung. Demgegenüber liegt in der Zuordnung von dynamischen IP-Adressen ein Eingriff in Art. 10 Abs. 1 GG.“

Zu statischen IP-Adressen im IPv6 formuliert das BVerfG die Gefahr beliebiger Speicherung:

> "Angesichts dieses erhöhten Informationspotenzials wäre die generelle Möglichkeit der Identifizierung von IP-Adressen nur unter engeren Grenzen verfassungsrechtlich zulässig„

Dem EUGH liegt immer noch ein Fall zu IP-Nummern zur Entscheidung vor.

Damit im TMG erlaubt

1) IDS-Systeme bei sofortiger Löschung der Daten nach Nutzungsende

2) Speicherung pseudonymisierter IP-Daten (durch Verkürzung oder Hashing)

3) Einwilligung des Angreifers zur Speicherung von Daten (mit Widerrufsmöglichkeit)

Durch TMG verboten

1) Protokolle mit IP-Daten über Angriffe erstellen für die Strafverfolgung (illegales Beweismittel)

2) Ermittlungen bei der IT-Strafverfolgung bei Telemedien durch andere als das BSI

III. BSIG

BSI-G (Fassung von 2009)

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können.

§ 5 BSI-Gesetz regelt die **Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes**

1) Das BSI ist weder TK-Provider noch Telemedienanbieter, sondern hat eine Sonderrolle
2) Die Verarbeitung von IP-Daten ist detailliert und einschränkend geregelt – ein Sonderweg im Vergleich zu TKG und TMG
3) Erlaubt und geregelt ist der Einsatz von IDS-Systemen und Virenscannern und deren automatisierte Datenanalyse, die nach §206 StGB nicht strafbar ist
4) Außer dem BSI ist auf Bundesseite keine Stelle zur Datenerhebung befugt
5) Behörden der Länder und Kommunen können weder auf BSI zurückgreifen noch sind sie zur Datenerhebung befugt

3. Fragen für die Praxis

Wie und für wen lässt sich IT-Sicherheit in Deutschland rechtskonform realisieren?

Allgemeinheit

- §100 TKG kaum verfassungskonform
- TMG verbietet diverse Werkzeuge

➢ **Rechtskonforme IT-Sicherheit für die Allgemeinheit ist weiterhin ein Hindernislauf**

IT des Bundes

- geschützt durch Sonderrechte des BSI
- Strafverfolger sind in der Fläche nicht den Aufgaben gewachsen (Aussage der Bundesregierung); BKA als Sonderkommissariat

➢ **Der Bund hat für die IT-Sicherheit die deutlich besseren Instrumente**

Fazit

- IT-Sicherheit mit Mitteln des Rechts zu stärken, ist positiv – bestehende Rechtsprobleme wurden aber nicht beseitigt, neue geschaffen.
- IT-Sicherheit erfordert schnelle Information und Reaktion. Das BSI ist als Informations-Sammelstelle konzipiert – ausbaufähig ist die Rolle als Informations-Vermittler und Berater.
- Bei IT-Sicherheit manifest ist das Misstrauen der Nutzer gegenüber IT-Systemen und der Wirtschaft gegenüber staatlichen Stellen – vertrauensbildende Maßnahmen sind nötig.

➢ **Das IT-Sicherheitsgesetz lässt noch Spielraum für Verbesserungen**