

# **FDP-Bundestagsfraktion**

## **Positionspapier**

### **IT-Sicherheit**

Neue Medien und insbesondere das Internet eröffnen Chancen für den Einzelnen, die Wirtschaft und die Gesellschaft insgesamt. Technologische Entwicklung, moderne Kommunikationsformen und innovative Dienste bieten Möglichkeiten für wirtschaftliches Wachstum, technologische und soziale Innovation und nicht zuletzt für die Freiheit. Chancen im Internet bestehen nicht nur für Gesellschaft, Demokratie und Meinungsfreiheit, sondern auch für die Wirtschaft. Im Netz wird nicht nur „klassischer“ Handel getrieben, sondern es ermöglicht zahlreiche neue Geschäftsmodelle, die unsere Wirtschaft vorantreiben.

Dabei ist die Bedeutung unserer IT-Infrastrukturen für den Einzelnen, die Wirtschaft und die gesamte Gesellschaft offensichtlich. Computernetze sind das „Nervensystem“ privater und staatlicher Infrastrukturen. Das Zusammenwachsen von physischer Welt und IT-Welt hat zu komplexen und insbesondere voneinander abhängigen Systemen geführt. Wir hängen in allen Bereichen des gesellschaftlichen und wirtschaftlichen Lebens von ihrem reibungslosen Funktionieren ab. Seit der Digitalisierung und der weltweiten Vernetzung haben Daten als Wirtschaftsgut an Gewicht gewonnen. Daten sind für Prozesse in Gesellschaft, Staat, Forschung und Wirtschaft unverzichtbar. Zentral ist hierbei die Vertraulichkeit, Verfügbarkeit und Integrität der Daten und der Datenströme sowie deren Authentizität.

Die Abhängigkeit unserer gesamten Wirtschaft, des Staates und der Gesellschaft von digitalen Prozessen sowie die auch wirtschaftliche Bedeutung von Daten rücken IT-Systeme auch in den Fokus von Kriminellen. Es gibt kein „kriminelles Internet“, aber es gibt kriminelle Menschen, die im Internet agieren. Überall wo Menschen sind, gibt es leider auch Kriminalität. Notwendig ist daher, die IT-Sicherheit zu verbessern, um Daten zu sichern und Eingriffe in empfindliche Systeme zu verhindern.

IT-Angriffe gibt es, seit es Computer gibt, und es wird auch in der Zukunft immer Hacker<sup>i</sup> geben. 100%-ige Sicherheit kann es nie geben. Unsere IT-Sicherheit muss aber besser werden, als es jetzt der Fall ist. Wir müssen uns immer wieder neuen Herausforderungen stellen. IT-Infrastrukturen und insbesondere kritische Infrastrukturen<sup>ii</sup> möglichst sicher zu machen, ist eine gesamtgesellschaftliche Aufgabe: Sie betrifft alle und kann nur durch alle gemeinsam, das bedeutet Staat, Unternehmen und Bürger, verbessert werden. Und das nicht nur in Deutschland. Die Globalisierung und die damit einher gehende Internationalität von IT-Infrastrukturen hat internationale Kooperation unverzichtbar gemacht.

Bei Angriffen auf IT-Infrastrukturen werden Daten auf verschiedene Weisen manipuliert und landen dann nicht zum richtigen Zeitpunkt bei dem korrekten Empfänger. Es gibt eine sehr große Bandbreite an Angriffen mit unterschiedlichen Angreifern und Zielen. Angreifer können jugendliche Hacker, Terroristen, Unternehmen oder sogar Staaten<sup>1</sup> sein. Auch können Viren<sup>iii</sup> durch Unfälle verbreitet werden. Abhängig von Art, Angreifer, Ziel und Zweck können Angriffe sehr unterschiedlich bezeichnet werden: Als Internetkriminalität, terroristische Anschläge, Spionage oder selbst als Cyberkrieg<sup>iv</sup>. Gerade der Angreifer und das

---

<sup>1</sup> Angriffe auf Bundesbehörden mit nachrichtendienstlichem Hintergrund steigen ständig. Die meisten Angriffe auf die deutsche Wirtschaft und Behörden stammen aus China (Verfassungsschutzbericht 2010).

Ziel sind oft schwer festzustellen. Angriffe können mit begrenztem Aufwand, anonym und von jedem Ort aus erfolgen, dazu mit stetig besserer und zum Teil frei verfügbarer Technologie. Im Internet verfügbar sind Toolkits mit rund um die Uhr-Telefonsupport, so dass auch Personen ohne jedes Spezialwissen hacken können. Die Erhöhung des Vernetzungsgrads, immer neue Geräte mit Onlinezugang und immer wieder neue Bedrohungen sind eine Herausforderung. In diesem Umfeld sind Viren in der Regel heutzutage zielgerichtet, individualisiert und treten nur noch einmalig auf, weil sie automatisiert in Echtzeit generiert werden – das macht es wiederum schwieriger, sie zu identifizieren. IT ist gleichzeitig Tatwerkzeug und Angriffsziel. Angriffe können über Computer-Netzwerke (zum Beispiel das Internet) oder über Hardware- oder Softwarekomponenten erfolgen. Das Anbieten von Viren oder Hacking kann ein lohnendes Geschäftsmodell sein: Finanziell, da diejenigen, die den größten Schaden anrichten möchten, auch am meisten zu zahlen bereit sind; gleichzeitig ist das Risiko, entdeckt zu werden ziemlich gering.

Besonders gefährlich sind die sogenannten „Advanced Persistent Threats“, die von hoch qualifizierten Hackern insbesondere für Industrie- oder staatliche Spionage ausgeführt werden. Diese Angriffe können sehr großen Schaden verursachen und zum Beispiel das Verteidigungssystem ausschalten. Es handelt sich hierbei nur um einen kleinen Teil der Gesamtanzahl von Angriffen - viele werden nie bekannt, um Wirtschaft und Staaten zu schützen. Das führt zu einer falschen Problemwahrnehmung. Oft stehen Staaten hinter diesen Attacken, mit gefährlicher Intention, etwa militärischer oder Wirtschaftsspionage. Ein Beispiel hierfür ist der Computerwurm Stuxnet<sup>v</sup>, der weltweit industrielle Steuerungssysteme angegriffen hat. Laut Studien werden 80% der bekannt gewordenen Angriffe durch eigene Mitarbeiter von Unternehmen, Firmen und Behörden durchgeführt.<sup>2</sup> Dass auch Stuxnet durch einen USB-Stick eingeschleust wurde, hat die Wichtigkeit des „Faktors Mensch“ bzw. des Innetäters deutlich aufgezeigt.

Grundsätzlich werden klassische Angriffe inzwischen besser bekämpft. Zum Beispiel werden Spam<sup>vi</sup>-Mails ziemlich effizient durch sog. Greylisting<sup>vii</sup> bekämpft. Auch die Anti-Botnet Initiative des eco-Verbands ist erfolgreich.<sup>3</sup> Trotzdem gibt es weiterhin Bedrohungen: Botnetze sind teilweise politisch motiviert und Identitätsdiebstahl mit Hilfe trojanischer Pferde wird oft international organisiert. Schwachstellen in Betriebssystemen und insbesondere Sicherheitslücken in Anwendungsprogrammen und Softwarekomponenten von Drittanbietern werden vielfach ausgenutzt. Schädlicher Code<sup>viii</sup> ist heutzutage auch auf legitimen Webseiten oft zu finden.<sup>4</sup>

Insbesondere Angriffe auf Endgeräte bzw. Smartphones, die noch nicht adäquat gesichert sind, sind eine Herausforderung. Auch Entwicklungen wie zum Beispiel Smart Grids<sup>ix</sup>, Cloud Computing<sup>x</sup>, IPv6<sup>xi</sup> und die Verschmelzung von Medien sind besonders empfindlich. Hier ist zum Beispiel noch unklar, wie die Umstellung auf IPv6 auf Spam-Abwehr wirken wird, da der Adressraum zu groß für die Benutzung von schwarzen Listen ist. Das Filter-System auf

---

<sup>2</sup> „IT-Sicherheit: Konzepte - Verfahren – Protokolle“, Claudia Eckert, 2009

<sup>3</sup> <http://www.heise.de/newsticker/meldung/PC-Entseucher-verzeichnen-Erfolge-in-Deutschland-1342128.html>

<sup>4</sup> „Die Lage der IT-Sicherheit in Deutschland 2011, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Mail-Servern wird dann überlastet.<sup>5</sup> Soziale Netzwerke, in denen Angriffe großenteils über verkürzte Links verbreitet werden<sup>6</sup>, sind besonders gefährdet.

Aus diesen Gründen spricht sich die FDP-Fraktion im Deutschen Bundestag für folgende Ansätze bei der Verbesserung von IT-Sicherheit aus:

- Stärkere Konzentration auf **Prävention**. Das bedeutet

#### „Faktor Mensch“

- an erster Stelle die Kompetenz („Faktor Mensch“) in Gesellschaft, Wirtschaft und Staat zu verbessern.
  - Gesellschaft:
    - Bund und Länder sollen, ggf. gemeinsam mit der Wirtschaft, mehr und besser ausgestattete interdisziplinäre Lehrstühle für IT-Sicherheit an deutschen Universitäten schaffen,
    - IT-Sicherheit soll bei Schaffung und Ausgestaltung neuer und bestehender Berufsbilder in entsprechenden Berufsfeldern stärker beachtet werden,
    - Bürgerinnen und Bürger jeden Alters müssen aufgeklärt werden. Der mündige und kompetente Bürger kann durch mehr Selbstschutz sehr viel Schaden verhindern. Bürger sind Mitgestalter der IT-Sicherheit. Hier leisten das BSI mit seiner Website „BSI für Bürger“ und die Verbraucherzentralen bereits gute Beiträge. Zu verstärken ist die Zusammenarbeit mit der Wirtschaft, um möglichst alle Kunden zu erreichen und anwenderfreundliche Möglichkeiten zu implementieren, die auch ohne detaillierte IT-Kenntnisse vom Anwender umgesetzt werden können.
    - Notwendig ist auch die Stärkung der Sensibilität für den Datenschutz. Unter der Prämisse der Datensparsamkeit sollten persönliche Daten erst gar nicht an Dritte, insbesondere im Internet, weitergegeben werden, sodass sie nicht kompromittiert oder missbraucht werden können. Die von der Bundesregierung auf Initiative der FDP-Bundestagsfraktion geplante Stiftung Datenschutz kann durch Aufklärung der Bürgerinnen und Bürger und durch die Vergabe von Gütesiegeln an Unternehmen einen wesentlichen Beitrag zu mehr Datenschutz und damit auch zu mehr Datensicherheit leisten.
  - Wirtschaft:

---

<sup>5</sup> „Unter Dauerfeuer“, Holger Bleich, CT 29.08.2011

<sup>6</sup> Symantec Sicherheitsbericht 2011

- IT-Sicherheitsfirmen sollen unter besseren Bedingungen arbeiten können. Mit der Wirtschaft soll ein Dialog stattfinden, inwiefern der sog. „Hacker Paragraph“<sup>xiii</sup> für die weitere Entwicklung von Sicherheitssystemen hinderlich ist,
  - die Bedeutung von IT-Sicherheits-Schulung für Mitarbeiter bei der Risikominimierung gerade im Bereich von KMU muss besonders herausgestellt werden. Solche Investitionen in die Mitarbeiterkompetenz lohnen sich, weil dadurch schwere Schäden vermieden werden können. Auch eine wertorientierte Führung trägt dazu bei.
  - in Wirtschaft und Verwaltung sollen die Tarifpartner darauf hinwirken, ausgebildete IT-Administratoren als hoch spezialisierte Fachkräfte einzuordnen und adäquat zu bezahlen,
  - stärkerer Datenschutz führt zu mehr Datensicherheit. Für den Datenschutz unabdingbar und zwingend ist die Datensicherheit von Betriebs- und Geschäftsgeheimnissen sowie von personenbezogenen Daten der Mitarbeiter und Kunden. Hier kann die geplante Stiftung Datenschutz mit ihrer Aufgabe der Zertifizierung einen wesentlichen Beitrag leisten,
  - alle Unternehmen sollten IT-Sicherheitsverantwortliche benennen. Derzeit verfügt gerade bei den KMU nur jedes zweite Unternehmen über IT-Sicherheitsverantwortliche, die unternehmensinternen Abstimmungsabläufe und Verantwortlichkeiten sind noch verbesserungsfähig. Hier wäre Sensibilität dafür zu schaffen, dass in allen Unternehmen klare Verantwortlichkeiten und eindeutige Abstimmungsabläufe zwischen IT-Verantwortlichen und Geschäftsführung erforderlich sind. Die Beratung durch das BSI ist daher in diesem Bereich fortzuführen und in Zusammenarbeit z.B. mit den Kammern auszubauen.
  - Auch soll die Zusammenarbeit mit der Task Force IT-Sicherheit des BMWi als zentralem Ansprechpartner und Impulsgeber für den Mittelstand gestärkt werden. Die weiteren zahlreichen Initiativen und Programme des BMWi in diesem Bereich sind zu begrüßen.
- Staat:
- Behörden müssen ihre Systeme technisch nach dem Stand der Wissenschaft sichern und ihre Mitarbeiter angemessen schulen,
  - die IT-Kompetenz der Sicherheitsbehörden muss gestärkt werden, um geltendes Recht durchsetzen zu können,
  - Behörden müssen strikt die Vorgaben der Datensparsamkeit beachten, um sensible Daten von Bürgerinnen und Bürgern, Unternehmen oder von internen Entscheidungsprozessen sicher

aufzubewahren. Die zunehmende Vernetzung der Verwaltung führt dazu, dass ein Datenleck unabsehbare Folgen haben kann. Daher muss gerade im staatlichen Bereich dem Datenschutz besondere Priorität eingeräumt werden, um Datensicherheit zu gewährleisten.

### Höhere Standards

- die Gewährleistung eines grundsätzlichen höheren IT-Sicherheitsniveaus durch hohe Standards
  - auf System-/Architekturebene, damit zum Beispiel Isolierungen dafür sorgen können, dass Viren sich nicht überall ausbreiten,
  - gemeinsam mit Wirtschaft, Wissenschaft und öffentlicher Verwaltung in Gremien wie der Koordinierungsstelle IT-Sicherheit (KITS) des Deutschen Instituts für Normung e.V. (DIN) und möglichst international,
  - für Verfahren und Methoden, weil die Produktzyklen immer kürzer werden,
  - möglichst früh im Produktentwicklungsprozess implementiert,
  - insbesondere bei Cloud Computing, damit neben dem Endgerät auch die Daten in der Cloud sicher sind.
- auf die bestehende KRITIS-Strategie<sup>xiii</sup> zu bauen, um insbesondere kritische Infrastrukturen vor neuartigen IT-Angriffen besser zu schützen. Die KRITIS-Strategie sollte entsprechend der veränderten IT-Sicherheitslage angepasst werden. Falls die gemeinsame Diskussion mit der Wirtschaft zu dem Ergebnis gelangt, dass Instrumente auf freiwilliger Basis nicht ausreichen, dann könnte für besonders schutzbedürftige Bereiche eine gesetzliche Pflicht zur Zertifizierung - z. B. durch den TÜV – mit Überprüfung in regelmäßigen Zeitabständen zu einem höheren Standard führen.
- für Unternehmen und Behörden, dass IT-Sicherheit und Datenschutz eine Selbstverständlichkeit werden und gleichzeitig Priorität besitzen. Eine große Sensibilität für die eigenen Daten ist unerlässlich. Hierbei werden sich marktwirtschaftliche Lösungen entwickeln, da IT-Sicherheit ein immer wichtigerer Wirtschaftsfaktor ist. Der Kampf gegen Spam war gerade deshalb erfolgreich, weil Unternehmen viel Geld als Spam-Jäger verdienen konnten<sup>7</sup>.

### Forschung

- „Security made in Germany/Europe“: Wir müssen deutsche Kompetenzen in Forschung und Industrie nutzen und verbessern. Forschungsprojekte an Universitäten müssen verstärkt initiiert werden und deren Ergebnisse in Produkte einfließen. Das würde zu einer besseren Ausstattung der IT-Infrastrukturen in

---

<sup>7</sup> „Unter Dauerfeuer“, Holger Bleich, CT 29.08.2011

Deutschland und Europa führen. Das gilt für Hardware (z.B. eingebettete Chips) und Software (Betriebssysteme). Letztlich sollte die komplette Lieferkette sicher gestaltet werden. Dazu gehört auch die physische Infrastruktur. Insbesondere soll Innovation „von unten“, also von kleinen Unternehmen stimuliert werden.

- für IT-Sicherheitsforschungsprogramme, dass sichere Infrastruktur statt Überwachungstechnologie entwickelt wird. Bei der Finanzierung müssen die richtigen Prioritäten gesetzt werden.
- bessere Zusammenarbeit zwischen Herstellern, Providern, Sicherheitsexperten und Anwendern. Insbesondere eine enge Kooperation der Hersteller von mobilen Geräten, von Betriebssystemen und von Schutzsoftware ist dringend erforderlich. Dabei dürfen aber Verantwortlichkeiten und Haftungsfragen nicht verwischt oder unzulässig ausgeweitet werden.
- An zweiter Stelle **Reaktion**. Das bedeutet
  - eine nüchterne Analyse statt überhasteter Reaktionen. Zuerst muss die Gefährdungslage fundiert erfasst und bewertet werden, damit dann festgestellt werden kann, wer in der Abwehr bestimmte Funktionen wahrnehmen kann.
  - die Zusammenarbeit mit Cyber-Abwehrzentrum und Cyber-Sicherheitsrat, da ein besserer Informationsaustausch zwischen den verschiedenen Behörden und der Wirtschaft unverzichtbar ist. Wichtig ist uns dabei, dass das Cyberabwehrzentrum einen reinen Informationsaustausch anbietet, keine neuen Kompetenzen verteilt und das strikte Trennungsgebot eingehalten bleibt.
  - die Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) in seiner Rolle als zentrale und unabhängige Koordinierungsstelle für die IT-Sicherheit. Die Unabhängigkeit des BSI ist unverzichtbar und sollte gestärkt werden.
  - die Einführung von internationalen Regeln oder eines „Cyber-Kodex“ für das gute Verhalten vom Staaten im Netz in Form nicht rechtsverbindlicher Verhaltensnormen und vertrauensbildender Maßnahmen.
- Sicherheit kann nur durch abgestimmte Maßnahmen auf nationaler und internationaler Ebene erreicht werden. Zusätzlich zu Deutschlands aktuell schon sehr guter Unterstützung von ENISA, der Europäischen Agentur für Netz- und Informationssicherheit, muss die Kommunikation zwischen ENISA und den zuständigen deutschen Behörden kontinuierlich weiter verbessert werden.. Die

internationale Zusammenarbeit auf allen Ebenen – Europäische Union, NATO, G20-Staaten, Internet Governance Forum (IGF), und Vereinte Nationen – ist unverzichtbar.

---

<sup>i</sup> Ein **Hacker** zeichnet sich primär dadurch aus, dass er sich nicht fragt "Was ist das?", wenn man ihm ein unbekanntes Gerät in die Hand gibt, sondern: "Was kann ich mit diesem Gerät, außer dem Kernzweck, noch tun"? Hacker können aus allen Bereichen der Wissenschaft, Forschung und Technik kommen und besitzen meist auf ihrem Fachgebiet eine hohe Expertise. Es wird im Allgemeinen wenig Wert auf dokumentierte Bildungsabschlüsse gelegt. Die Mehrheit der Hacker ist in der Informationstechnologie beheimatet.

<sup>ii</sup> **Kritische Infrastrukturen** sind Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)). Das betrifft zum Beispiel die Energieversorgung, Trinkwasserversorgung oder die Telekommunikation.

<sup>iii</sup> Ein **Virus** ist eine Form der Schadsoftware. Viren verbreiten sich nicht von selbst weiter, sondern erfordern eine Aktion vom User, die dieser tätigt, ohne zu wissen, dass er dadurch gerade den Virus zur Ausführung bringt. Viren können jede Art von Schädigung auf einem Computer erzeugen.

<sup>iv</sup> Ein **Cyberkrieg** ist eine kriegerische Auseinandersetzung mit den Mitteln der Informationstechnik. Er ist theoretisch möglich geworden durch die Vernetzung der Welt. Ein Cyberkrieg könnte z. B. mit Viren oder andauernden Hackerangriffen auf die Infrastruktur ganzer Länder erfolgen. Die USA haben bereits angekündigt, auf Angriffe auf ihre IT-Infrastruktur auch mit konventionellen Waffen reagieren zu wollen. Es gibt bisher allerdings keine offizielle oder eindeutige Definition, welche Art oder welcher Umfang von Angriffen einen Cyberkrieg ausmachen.

<sup>v</sup> **Stuxnet** ist ein Computervirus, das sich online verbreitet und vorrangig Urananreicherungsanlagen infiziert. Dieser Virus wurde speziell entwickelt, um Maschinensteuerungen der Firma Siemens zu infizieren. Dieser Virus verbreitet sich über USB-Sticks von Servicetechnikern. Stuxnet fiel jahrelang niemandem auf, da Stuxnet, bevor er aktiv wird, die stattfindende Kommunikation belauscht und später nachempfendet. Stuxnet sucht sich, sobald installiert, einen Weg, um Daten ins Internet übertragen zu können.

<sup>vi</sup> **Spam** ist ein Begriff für unerwünschte E-Mail-Werbung. Er wird inzwischen für jegliche Art von unerwünschter Werbepost verwendet. Geschätzte 90% des weltweiten E-Mail-Aufkommens ist SPAM. Der Vorgang wird als "Spamming" bezeichnet. Die Ausführenden sind "Spammer".

<sup>vii</sup> Als **Greylisting** wird eine Form der [Spam](#)-Bekämpfung bei [E-Mails](#) bezeichnet, bei der die erste E-Mail eines unbekanntenen Absenders zunächst abgewiesen und erst nach einem weiteren Zustellversuch angenommen wird. Greylisting ist sowohl eine Methode, Spam zu erkennen, als auch eine Methode, den Absender aussortierter E-Mails zu benachrichtigen.

<sup>viii</sup> **Schadsoftware** ist der Oberbegriff für jegliche unerwünschte Software, wie z. B. Viren, Trojaner oder Keylogger. Schadsoftware kann einen direkten Schaden auf dem Computer des Users anrichten, z. B. Dateien löschen oder aber auch nur Rechenleistung "stehlen" und einem Botnetz zur Verfügung stellen. Schadsoftware kann auch Hintertüren für andere Schadsoftware öffnen, sodass bei einer einfachen Infektion davon ausgegangen werden muss, dass sich weitere Viren eingenistet haben. **Schadcode** ist der Quelltext eines Programms, das nach dem Ausführen unter den Begriff der Schadsoftware fällt.

<sup>ix</sup> Als **Smart Grid** bezeichnet man die Vernetzung und das daraus folgende Energiemanagement von Stromnetzen unter Einbeziehung von Daten aller am Netz beteiligten Akteure wie etwa Stromerzeuger, Verbraucher, Stromleitungen und Stromspeicher. Smart Grid zielt auf eine effizientere Auslastung und Nutzung des Stromnetzes sowie der Stromspeicher und eine schnelle Fehlererkennung und -behebung bei Problemen eines Beteiligten. Smart Grids bergen bei Einbeziehung von Verbraucherdaten Risiken für den Datenschutz, da aufgrund des Stromverbrauchs umfassende Rückschlüsse auf Lebensgewohnheiten, etc. möglich sind. In

---

Deutschland gibt es nach dem Energiewirtschaftsgesetz Regelungen zur Erfassung von Verbraucherdaten über das Netz. Dabei sind natürlich bestimmte Datenschutzregeln zu beachten.

<sup>x</sup> **Cloud Computing** bezeichnet die Zurverfügungstellung von Speicher- und Rechnerkapazität oder anderen Diensten wie Anwendungen von einem oder mehreren Rechenzentren an Kunden, die online darauf zugreifen. Dabei befinden sich die Daten regelmäßig nicht an einem physisch bestimmten Ort, sondern in der „Cloud“ immer dort, wo gerade Kapazitäten verfügbar sind, oft über die ganze Welt verteilt.

<sup>xi</sup> **IPv6** ist ein neuartiger Typ von IP. Eine IPv6-Adresse besteht aus 8 Blöcken, die durch Doppelpunkte voneinander getrennt sind. Jeder Block besteht aus 6 hexadezimalen Ziffern. Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. IPv6 hat deutlich mehr Adressen zu vergeben als IPv4, weswegen Schritt für Schritt weltweit auf IPv6 umgestellt wird.

<sup>xii</sup> **§ 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)**

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

<sup>xiii</sup> <http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf>