VERBAND DER INTERNETWIRTSCHAFT E.V.

Leitlinien

Zur IT-Sicherheitspolitik in Deutschland

Berlin, 10. Oktober 2016

Der Themenkomplex der IT-Sicherheit wird mit dem Voranschreiten der Digitalisierung von Staat, Wirtschaft und Gesellschaft zunehmend als relevantes Handlungsfeld der Politik gesehen. Die Veröffentlichung der Cybersicherheitsstrategie von 2011, das IT-Sicherheitsgesetz von 2015 und die vom Bundesministerium für Verteidigung gestartete Initiative zum Cyber- und Informationsraum zeigen nur einige Ansätze dafür, wie die Bundesregierung mit diesen Bedrohungen umgeht. Mit einer neuen Cybersicherheitsstrategie, die für das Jahr 2016 vorgesehen ist, beabsichtigt die Bundesregierung unter Federführung des Bundesministeriums des Innern nun, auf die voranschreitende Digitalisierung zu reagieren.

Der Internetwirtschaft kommt im Rahmen dieser Überlegungen in mehrerlei Hinsicht wachsende Bedeutung zu. Zum einen bietet und liefert sie die Infrastrukturen und Dienste, die die digitale Welt ausmachen und ist damit Quelle der voranschreitenden Digitalisierung. Gleichzeitig kann sie Angriffsziel und Opfer von Angriffen werden. Ihr spielt damit eine Schlüsselrolle bei der Gestaltung von IT-Sicherheit in Deutschland.

Im Wechselspiel zwischen ökonomischen Notwendigkeiten, gesellschaftlichen Diskussionen und staatlichem Handeln sieht der eco die Notwendigkeit, Leitlinien für laufende und zukünftige Diskussionen zum Thema IT-Sicherheit und die Gestaltung der Politik rund um diesen Themenkomplex zu setzen.

- **Den Schutz kritischer Infrastrukturen (KRITIS) sinnvoll gestalten und weiterentwickeln**

Mit dem IT-Sicherheitsgesetz und der zugehörigen KRITIS-Verordnung wurden Infrastrukturen definiert, deren Schutz aus Sicht der Bundesregierung besondere Bedeutung genießt. Der Schutz dieser Infrastrukturen kann jedoch nicht nur durch Verordnungen und Vorgaben erfolgen, sondern er muss auch operativ so gestaltet werden, dass ein wirtschaftlicher Betrieb der Infrastrukturen weiter möglich ist. Deshalb sollte bei der Evaluierung der KRITIS-Verordnung und des IT-Sicherheitsgesetzes auch überprüft werden, ob bzw. inwieweit Infrastrukturbereiche noch als kritisch einzustufen sind. In diesem Kontext sollten auch die in der NIS-Richtlinie entwickelten Kriterien herangezogen und auf eine weitgehende Harmonisierung dieser Maßstäbe geachtet werden. Unterschiedliche Meldeauflagen sorgen nicht nur für Rechtsunsicherheit, sondern auch für einen erheblichen Mehraufwand bei Unternehmen.

- **Die Organisation zum Schutz von KRITIS überdenken**

Vertrauen ist nicht nur für die Nutzerinnen und Nutzer von Diensten wichtig. Auch die Internetwirtschaft braucht Rechtssicherheit und muss sich darauf verlassen können, dass mit Schadensmeldungen und Hinweisen auf Sicherheitslecks in IT-Systemen vertrauenswürdig umgegangen wird. Daher sollte beim Schutz von KRITIS verstärkt auf Kooperation und Partnerschaften zwischen der öffentlichen Hand, privaten Diensteanbietern und Telekommunikationsunternehmen gesetzt werden. Ob in diesem Kontext die von der Europäischen Union initiierte European Cyber Security Association (ECSO) eine praxistaugliche Lösung für eine solche öffentlich-private Partnerschaft aufzeigt, bleibt abzuwarten. Die Sicherheitsherausforderungen der digitalen Welt brauchen schnelle Antworten. Die komplexen Strukturen der ECSO werden dem möglicherweise nicht gerecht, können aber einen Beitrag zur besseren strukturellen und institutionellen Zusammenarbeit liefern. Nur eine kooperative Lösung von Staat und Internetwirtschaft kann hier langfristig erfolgreich sein.

- **Haftung in der digitalen Welt**

Da auch in der digitalen Welt eine Schädigung Einzelner oder ganzer Personengruppen vorkommen kann, stellt sich häufiger neben der Frage nach der Verantwortung auch die Frage, wer dafür haftet. In Deutschland und in Europa ist der rechtliche Maßstab hierfür die e-Commerce Richtlinie, die ein ausgewogenes Haftungsgefüge für Internetanbieter bereitstellt. Dieses Gefüge sollte bewahrt werden. Provider sollen nicht für Rechtsbrüche Dritter in Anspruch genommen werden dürfen. Sämtliche Versuche, dieses Prinzip aufzuweichen oder zu unterlaufen, stehen im Widerspruch zu unserer Rechtsordnung.

Darüber hinaus sollte auch von weiteren Haftungspflichten für IT-Dienstleistungen und -Produkte abgesehen werden. Bereits jetzt bestehen im Bereich der Produkt und Produzentenhaftung für Anbieter hohe Hürden. Diese speziell für den IT-Sektor zu verschärfen, wäre nicht nachvollziehbar und würde der technischen Realität moderner vernetzter Systeme widersprechen.

- **Rechtsordnung bewahren – auch im Netz**

Das Rechtssystem basiert auf dem Grundprinzip von actio und reactio. In diesem System gibt es klar verteilte Rollen. Staatsanwaltschaften und Polizeibehörden ermitteln, Gerichte urteilen. Dieses rechtsstaatliche System gerät jedoch ins Wanken, wenn man dazu übergeht, Paralleljustizen zu etablieren oder Provider mit hoheitlichen Aufgaben zu belasten. Der Einsatz von Uploadfiltern, Internetfiltern oder die Verpflichtung, zum selbstständigen Vorgehen gegen rechtswidrige Inhalte oder Inhalte, die als rechtswidrig oder anstößig angesehen werden, höhlen das Rechtsstaatsprinzip aus. Auch

freiwillige Vereinbarungen zwischen Regierungen und Providern sind in diesem Kontext kritisch zu sehen.

- **IT-Sicherheit durch Innovationsfähigkeit erhalten – Verschlüsselung stärken**

Verschiedene IT-Sicherheitslösungen und komplexe Verschlüsselung sind zentrale Aspekte bei der Absicherung von IT-Systemen und digitalen Strukturen. Ihre Schwächung oder Aufweichung durch zentrales Key-Management, gezielt eingebaute zentrale Ausgabeschnittstellen oder Sicherheitslücken (Backdoors) schaden Wirtschaft und Gesellschaft gleichermaßen und untergraben das Vertrauen in digitale Technologien, in Internet-Dienste und in Regierungen. Auf eine gesetzliche Regelung oder eine Verordnung zum zentralen Key-Management oder zu „Behördenzugängen“ zu IT-Dienstleistungen sollte daher verzichtet werden. Bei der Ausgestaltung der neuen „Zentralen Stelle für Informationstechnik im Sicherheitsbereich“ (ZITIS) ist dringend darauf zu achten, dass diese nicht die systematische Schwächung von Verschlüsselungstechnologien betreibt. Allgemeine Erkenntnisse der ZITIS über Schwachstellen, Exploits und Backdoors müssen mit den betroffenen Unternehmen geteilt werden, damit diese umgehend reagieren und entsprechende Sicherheitslücken schließen können.

- **IT-Sicherheit als kollektive Herausforderung verstehen**

IT-Sicherheit betrifft staatliche Stellen, IT-Unternehmen und Internetnutzer gleichermaßen. Daher ist es nicht nur wichtig, dass KRITIS abgesichert und ihre Betreiber zur Einhaltung von Sicherheitsstandards verpflichtet werden. Vielmehr muss auch verstärktes Augenmerk auf die Verbreitung von Wissen über den richtigen Einsatz von IT-Sicherheit gelegt werden. Neben der informationstechnischen Bildung an Schulen und Universitäten sollten auch entsprechende Programme aufgesetzt werden, die nicht nur die Entwicklung neuer Verschlüsselungstechnologien und –verfahren fördern, sondern auch deren Implementierung bei Unternehmen und Privatpersonen vorantreiben. Dabei sollte speziell bei kleinen und mittelständischen Unternehmen auf einen Zugang ohne große Hürden Wert gelegt werden, so dass sie langsam an die Herausforderungen der IT-Sicherheit herangeführt werden. Jede Form einer gesetzlich auferlegten Lösung führt zur Bildung von separaten digitalen Ökosystemen, welchen kein flächendeckender Erfolg beschieden sein wird.

- **Staatlicher Überwachung klare Grenzen setzen**

Derzeit wird debattiert, ob Anbieter von Telemedien und OTT-Diensten strenger reguliert und zu einer schnelleren Herausgabe von Nutzerdaten verpflichtet werden können. Dies würde den Rechtsstaat aufweichen, ohne gleichzeitig für mehr Sicherheit im Netz zu sorgen. Die rechtsstaatlichen Prinzipien dürfen auch hier nicht durch Nebenabsprachen aufgeweicht

werden. Der Schutzstandard, den das Telemediengesetz bietet – insbesondere in Bezug auf die pseudonyme und anonyme Nutzung von Diensten – muss gewahrt werden. Dies sollte die Bundesregierung auch bei etwaigen Plänen zur Einführung eines einheitlichen Identitätsmanagements, wie das BMWi es im Grünbuch Digitale Plattformen anreißt, berücksichtigen. Eine Hochregulierung von Telemediendiensten in Telekommunikationsdienste hinein ist nicht zeitgemäß und würde die Markteintrittsbarriere für innovative Dienste erhöhen.

Darüber hinaus sollte auf pauschale und anlasslose staatliche Überwachungsmaßnahmen im Netz verzichtet werden. Sie greifen das Fernmeldegeheimnis unverhältnismäßig stark an und sorgen speziell bei Bürgerinnen und Bürgern für Misstrauen gegenüber digitalen Diensten.

Auch die Sperrung oder Filterung von Inhalten sollte nicht Teil von Strategien zur Bekämpfung von Kriminalität und Terrorismus sein. Das Prinzip „Notice and Take Down“ hat sich universell bewährt und sollte dementsprechend auch hier zur Anwendung kommen. Eine Verpflichtung zur Sperrung des Zugriffs auf bestimmte Inhalte im Netz kann durch Provider technisch nicht adäquat gewährleistet werden.

- **Geheimdienstbefugnisse beschränken**

Geheimdienste auf der ganzen Welt haben über Jahre hinweg Internetverkehr ausgeleitet, gespeichert und analysiert. Rechtsverstöße – wie bspw. Zugriffe des Bundesnachrichtendienstes auf die Kommunikation von Bundesbürgern – dürfen nicht fortgesetzt oder im Nachhinein legitimiert und mit einer gesetzlichen Grundlage versehen werden. Der Gesetzgeber muss grundrechtswidrige Praktiken, insbesondere bei der Fernmeldeaufklärung, einschränken, die Kompetenzen der Geheimdienste hier klar beschneiden und Rechtssicherheit für Telekommunikationsdiensteanbieter herstellen. Die durch die bekanntgewordenen Praktiken der Geheimdienste aufgeworfenen Probleme müssen grundgesetzkonform geregelt werden.

- **Kriminalität im Netz operativ bekämpfen**

Der Kriminalität im Netz muss adäquat begegnet werden. Dazu gehört eine angemessene und zeitgemäße Ausstattung von Strafverfolgungs- und Ermittlungsbehörden und die Führung von kompetentem, gut ausgebildetem Personal, das auf die digitale Welt vorbereitet ist und sich gesetzeskonform darin bewegen kann. Von der Schaffung neuer Straftatbestände speziell für Fälle im Internet ist grundsätzlich abzuraten, da diese den Blick auf die eigentlichen Probleme und die bestehenden Herausforderungen im deutschen Strafrecht verschleiern.

Leitlinien für eine zeitgemäße IT-Sicherheitspolitik

eco hält den Auf- und Ausbau der Resilienz gegenüber IT-Angriffen für unerlässlich. Er sieht dazu folgende Voraussetzungen als zwingend notwendig an:

- Gegenseitiges Vertrauen und Zusammenarbeit zwischen Staat und Internetwirtschaft: Staat und Wirtschaft sollten darauf vertrauen, dass beide Seiten verlässliche Partner bei der Realisierung von mehr IT-Sicherheit sind. Dies geschieht am ehesten durch gemeinsame Projekte und Partnerschaften.
- Sicherheitsstandards und Maßgaben so umsetzen, dass Internetnutzer „mitgenommen werden“. Der Schwerpunkt sollte dabei darauf gelegt werden, Unternehmen, Nutzerinnen und Nutzern mit sachgerechten Informationen für die Sicherheit ihrer IT-Systeme zu versorgen. Einfache Sicherheitschecks, Selbsttests und Cleaner Tools helfen mehr, als Warnhinweise oder Bekanntmachungen, die für Verunsicherung sorgen. Eingriffe in Netze, Dienste oder Haftungsregime sind keine Lösung bei der Durchsetzung von IT-Sicherheit.
- Man sollte nicht den Versuch unternehmen, IT-Sicherheit durch enge, rigide und pauschal hohe Auflagen zu erreichen. Stattdessen sollten mehr preiswerte, einfach bedienbare Sicherheitsprodukte mit einem hohen Schutzniveau dem Markt zur Verfügung gestellt und so ein Wettbewerb um starke IT-Sicherheit gefördert werden.
- Rechtsstaatsprinzip wahren – Vertrauen ins Netz erhalten: Keine Eingriffe in Netze oder Dienste ohne entsprechende richterliche Anordnung. Das Vertrauen der Nutzer in das Internet muss erhalten bleiben. Es darf nicht der Eindruck entstehen, man sei dort der Willkür von Providern oder Diensteanbietern ausgesetzt. Auch dürfen diese nicht für hoheitliche Aufgaben herangezogen werden.
- IT-Sicherheit als dynamisches Thema verstehen: Es muss ein grundsätzliches Verständnis für die Entwicklung von IT-Systemen bestehen, in dem allen Beteiligten klar ist, dass ein System nicht als „sicher“ definiert werden kann. Haftungsauflagen o.ä. sind hierfür ungeeignet. Sinnvoller ist es, gemeinsame Forschungsprojekte und Penetrationstests durchzuführen, um IT-Systeme gemeinsam besser absichern zu können.

Über eco

eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 900 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.