Positionspapier

10 Punkte für mehr IT-Sicherheit

Herausgeber: CSUnet

Franz Josef Strauß-Haus
Nymphenburger Straße 64
80335 München

Tel.: 0 89/12 43-251

csunet@csu-bayern.de
twitter.com/csu_net
facebook.com/csunet
www.csunet.de

A. Problem und Ziel

In einer immer digitaler werdenden Welt kommt der Sicherheit der Informations- und Kommunikationssysteme eine große Bedeutung zu. Dies gilt sowohl für die Kommunikation privater Anwender, aber insbesondere auch für den Informationsaustausch in Deutschland ansässiger Unternehmen. Während generell wünschenswert ist, dass als vertraulich versandte Informationen auch vertraulich bleiben, steht hier auch die Wettbewerbsfähigkeit der deutschen Wirtschaft und die Handlungsfähigkeit der Behörden auf dem Spiel. Das wiederum setzt auch die Verfügbarkeit und Integrität elektronischer Dokumente und IT-Systeme voraus, also ihren Schutz vor Hackerangriffen und Manipulationen durch Innentäter. Nicht zuletzt die Ereignisse der letzten Jahre haben uns gezeigt, welchen großen Handlungs- und Nachholbedarf wir dazu noch in unserem Land haben. Wir fordern daher die Umsetzung des nachfolgenden 10-Punkte Programms zur Förderung der IT-Sicherheit in Deutschland.

B. Forderungen

1. **Bessere personelle und finanzielle Ausstattung für das Bundesamt für Sicherheit in der Informationstechnik (BSI)**

   Das Bundesamt für Sicherheit in der Informationstechnik ist eine unabhängige und neutrale Stelle für die IT-Sicherheit betreffende Fragen, die organisatorisch dem Bundesministerium des Inneren angehört. Als spezifisch der IT-Sicherheit gewidmete und von Cyber-Sicherheits- und Kryptographieexperten besetzte Einrichtung ist eine angemessene, sowohl personelle als auch finanzielle Ausstattung für das BSI, das etwa auch für die Zertifizierung der Sicherheitsstandards digitaler Systeme verantwortlich ist, unerlässlich, wenn das gesamte **Sicherheitsniveau** in der digitalen Welt langfristig angehoben werden soll. Zwar sieht der von der Bundesregierung bereits beschlossene Gesetzesentwurf zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) erste Maßnahmen in dieser Richtung vor, jedoch zwingt die rapide voranschreitende Digitalisierung aller Lebensbereiche eben auch, darüber hinaus mit der Geschwindigkeit der Gesamtentwicklung schrittzuhalten. Eine unterfinanzierte und personell schlecht ausgestattete Behörde kann bundesweite **Informations- und Kommunikationssicherheit** nicht effektiv gewährleisten. Das BSI sollte darüber hinaus, wenn signifikante Datendiebstahlsfälle - besonders in Bezug auf E-Mail-Konten - bekannt werden, mit den Providern gemeinsam überprüfen, ob Kunden der jeweiligen Provider vom Datendiebstahl betroffen waren oder nicht. Eine solche Sicherheitsallianz vom BSI und Providern, die eine Stärkung des BSI voraussetzt, würde somit für jeden Bürger auch unmittelbar positive Effekte mit sich bringen. Den Regierungsstellen bekannt gewordene Sicherheitslücken sind durch das BSI den betroffenen Herstellern von Hard- und Software umgehend mitzuteilen und nach einer angemessenen Frist zu veröffentlichen. Bei öffentlichen Ausschreibungen ist der

Einblick in die Quellcodes/Schaltpläne zu von staatlicher Seite in Auftrag gegebener Hard-, Soft- und Firmware zu berücksichtigen.

2. Ende-zu-Ende Verschlüsselung von E-Mails

Bis zum heutigen Tag läuft ein Großteil der E-Mail-Kommunikation sowohl zwischen Privatleuten als auch in der freien Wirtschaft oder bei Behörden, auch in sensibleren Bereichen, unverschlüsselt und damit ungeschützt ab. Kriminellen ist es damit ein leichtes, die Kommunikation zumindest auf dem Versandweg abzufangen und mitzulesen – ohne dass der Geschädigte unmittelbar den Datendiebstahl bemerken würde. Selbst die kürzlich eingeführte DE-Mail kann einzig den Eindruck von Sicherheit vermitteln durch das Fehlen einer konsequenten Ende-zu-Ende-Verschlüsselung. Diese Sicherheitsprobleme könnten technisch gesehen jedoch mit Leichtigkeit bekämpft werden: Bereits jetzt stehen die technischen Möglichkeiten zur Verschlüsselung des E-Mail-Verkehrs zur Verfügung, diese sind aber für Privatleute ohne kryptografische oder informatische Hintergrundkenntnisse oft nur schwer benutzbar. Das Fraunhofer-Institut für sichere Informationstechnologie (SIT) etwa hat aber gezeigt, dass durch von einer öffentlichen Institution (etwa des BSI) entwickelte und gepflegte Apps Anwendern die Einrichtung der Verschlüsselung auf den Endgeräten abnehmen könnten. Würde eine solche Verschlüsselung genutzt, wären versandte E-Mails für alle „Zwischenstationen" wie Provider, etc. wertlos. Nur mit massivem, unverhältnismäßigem Aufwand könnte dann der Informationsaustausch zweier identifizierter Personen noch „abgehört" werden. Wir fordern weiterhin, dass das BSI digitale Zertifikate, die der Identifizierung von Anwendern in verschiedensten Dienstleistungen dienen, der Bevölkerung kostenlos zur Nutzung zur Verfügung stellt.

3. Verschlüsselung von Kundendaten bei Nutzung von Cloud-Diensten

Eine Vielzahl an Online-Dienstleistern, Betreibern von Online-Shops, etc. speichern Kundendaten auf ihren Servern, um die Abwicklung diverser Interaktionen zu erleichtern. Zu diesen sensiblen Daten zählen natürlich der Name des Kunden, dessen Adressdaten, andere Kontaktinformationen wie etwa Telefonnummern, aber auch Zahlungsinformationen u.ä. Es ist notwendigerweise sicherzustellen, dass diese Daten gerade in der Gesamtschau nicht in die Hände von Unternehmen oder Organisationen geraten, für die sie nicht bestimmt sind. Durch die gängige Praxis von Anbietern, Kundendaten in sogenannten Clouds zu speichern, wird genau dieses Ziel aber unterminiert. Häufig werden sensible Daten unverschlüsselt somit auf eigentlich fremden Servern abgelegt. Daher ist es notwendig, rechtliche Maßnahmen zu ergreifen und Anbieter dazu zu verpflichten, dass, wenn sie Cloud Computing zur Speicherung von Kun-

dendaten einsetzen, sensible Informationen nur in einer verschlüsselten und damit sicheren Form „ausgelagert" werden.

4. **Verpflichtende SSL-Verschlüsselung für Internetshops und Behörden**
   Seit dem 12.12.2014 ist mit Beschluss des IT-Rats der flächendeckende Einsatz von SSL-Sicherheitsprotokollen in Anwendungen des Bundes als Verwaltungsvorschrift verbindlich. Auch Onlineshops nutzen schon weitestgehend SSL-Sicherheitsprotokolle, die eventuellen Datendiebstahl bei der Kommunikation sensibler Daten zwischen Nutzer und Onlineshop oder Behörde massiv erschweren. Nichtsdestotrotz mangelt es bis dato an einem entsprechenden Gesetz, das die Betreiber datenschutzrechtlich relevanter Websites tatsächlich rechtlich dazu verpflichtet, Protokolle zur Sicherung des Informationsaustausches in beidseitigem Interesse zu nutzen. Besonders um den Endbenutzer zu schützen, dürfen in der Interaktion mit den Websites von Onlineshops oder Behörden und Organisationen die Daten nur verschlüsselt übertragen werden.

5. **Förderung der Weiterentwicklung von Sicherheits- und Verschlüsselungssoftware**
   Es ist bereits jetzt ein Aspekt der Arbeit des BSI, die Entwicklung und Aktualisierung von Open Source-basierter Sicherheits- und Verschlüsselungstechnologie zu fördern. Besonders in Anbetracht von Fragen der Zugänglichkeit solcher Technologien für Nutzer mit begrenzten finanziellen und materiellen Ressourcen ist aber eine **Intensivierung der Zusammenarbeit mit und Unterstützung von Open Source Projekten** erforderlich. Es ist eine Konsequenz der freien Verfügbarkeit von Software, dass sie auch breitere Verwendung findet, und gerade bei Sicherheitssoftware ist das Sammeln von Anwendungserfahrungen möglichst vieler Nutzer für eine möglichst zielgerichtete Weiterentwicklung der Software wünschenswert. Ein Beispiel für Open Source Technologien, die u. a. bei Universitäten und auch behördlichen Einrichtungen mittlerweile breite Verwendung finden und dort auch zu einer **Erhöhung des Sicherheitsstandards** beigetragen haben und dementsprechend gefördert worden wären, sind sogenannte **Single-Sign-On Verfahren** (wie bspw. Shibboleth), die die Authentifizierung eines Individuums bei Benutzung verschiedener, verbundener Webservices erleichtern. Der CSUnet lehnt jede Schwächung von Verschlüsselungen und IT Systemen und insbesondere den Einbau von sogenannten „Hintertüren" – egal von welcher Seite – entschieden ab. Ebenso sprechen wir uns gegen jedes Verbot, welches den Einsatz von Verschlüsselung verbieten oder auch nur einschränken soll, aus.

6. **Vermittlung von Kompetenzen in der IT-Sicherheit an Schulen**
   Eine frühe Auseinandersetzung mit dem Thema IT-Sicherheit ist gerade in Anbetracht der stetig fortschreitenden Digitalisierung unerlässlich. Es zeichnet sich ein Trend ab, dass Personen aufgrund der großen Chancen des Umgangs mit Computertechnologie immer früher mit den damit auch verbundenen Risiken in Kontakt kommen. Jugendliche können also bereits lange in der digitalen Welt aktiv sein, bis sie zum ersten Mal auf Fragen der IT-Sicherheit aufmerksam gemacht werden. Dies ist besonders signifikant, da auch zunehmend wichtige Aspekte des alltäglichen Lebens, etwa die Abwicklung von Bankgeschäften, ins Internet verlagert werden. Daher fordern wir, dass so schnell wie möglich flächendeckend an deutschen weiterführenden Schulen die bestehende Struktur genutzt (z.B. der Informatikunterricht) bzw. entsprechend als Übergangslösung erweitert wird, damit den Schülern von qualifiziertem Personal sowohl eine **Einführung in die möglichen Sicherheitsgefährdungen**, die bei virtueller Kommunikation und Interaktion anfallen können, als auch in die Möglichkeiten zur **individuellen Abwendung solcher Sicherheitsgefährdungen** in diversen Bereichen gegeben werden kann. Der CSUnet fordert zudem die Einführung eines eigenen Schulfaches „**Medienkunde**", das unabhängig von der Schulform unterrichtet wird. In diesem sollen perspektivisch auch Inhalte zum Themenbereich IT-Sicherheit vermittelt werden. Im Gegenzug zur Einführung des neuen Schulfachs sollen die Inhalte zur Medienbildung in den übrigen Fächern auf die Anwendung ausgerichtet werden. So kann das in der Medienkunde erlernte gleich in der Schule eingeübt werden. Die so freiwerdenden Unterrichtskapazitäten können dann für Medienkunde verwendet werden. Ein solches Fach sehen wir als die Basis für weiteres, internetbasiertes Lernen und Arbeiten. Ziel muss es sein, die **Medien- und Informationskompetenz** neben Lesen, Schreiben und Rechnen als die **vierte Grundkompetenz** zu vermitteln. Sie ist zudem verbindlich, fächerspezifisch und altersgerecht in den Bildungsplänen zu integrieren. Die erlernte Informationskompetenz unterstützt die Anwender auch, sich vor Social Engineering Angriffen zu schützen. Wie oben gezeigt, kann bereits die grundlegende Auseinandersetzung mit dem Thema IT-Sicherheit, beziehungsweise die Erkenntnis, dass die IT-Sicherheit und Datenschutz keine vernachlässigbaren Themen sind, dazu beitragen, dass insgesamt die Sicherheitsstandards im Datenverkehr nachhaltig erhöht werden können.

7. **Bessere Information der Bürger und der Unternehmen**
   Gemeinsam mit dem vorgeschlagenen verstärkten Fokus auf IT-Sicherheit in weiterführenden Schulen, fordern wir, dass im Allgemeinen die Bürger verstärkt auf die Thematik IT-Sicherheit aufmerksam gemacht werden. Bundesweite Kampagnen, die auf verschiedenste gesundheitliche Risiken hinweisen, hatten bereits Erfolg in der Sensibilisierung der Bevölkerung in Bezug auf der-

artige Themen. Es kann daher davon ausgegangen werden, dass eine **IT-Sicherheitskampagne** tatsächlich auch zu signifikanten Veränderungen der generell eingehaltenen Sicherheitsstandards führen würde. Das ist wiederum besonders der Fall, da Maßnahmen, die mit äußerst wenig Aufwand verbunden sind, bereits zu einer deutlichen und nutzbringenden Erhöhung der Kommunikationssicherheit führen können. Besonders in Bezug auf Unternehmen ist darauf hinzuweisen, dass IT-Sicherheit auch aus Eigeninteresse ein Thema ist: Nicht nur Kundendaten können gestohlen werden, sondern auch alle anderen Arten an unternehmensinternen Daten, die womöglich in den Händen von Konkurrenten zu einem Wettbewerbsnachteil gereichen könnten.

8. Einrichtung eines IT-Sicherheitsnotrufs für Bürger und Unternehmen

Damit Bürger und Unternehmen aber auch im Falle eines tatsächlichen Angriffs oder einer Verletzung der Vertraulichkeit versandter oder gespeicherter Daten nicht auf sich gestellt bleiben, fordern wir darüber hinaus die Einrichtung einer, möglicherweise an das BSI gekoppelten, Stelle, die Verdachtsfälle des Datendiebstahls und andere sicherheitsrelevante Probleme aufnehmen und behandeln kann. Während im Falle einer „gewöhnlichen" Rechtsverletzung die Polizei natürlich der erste Ansprechpartner sein würde, sind besonders kleinere Dienststellen auch aufgrund der höheren **Komplexität von Cyberkriminalität** überfordert. So macht es Sinn, gerade für derartige Verbrechen eine gesonderte, zentrale Einrichtung zu begründen, die auch erste Maßnahmen zur Gefahrenabwehr empfehlen kann. Darüber hinaus hat die zentrale Verwertung und Behandlung solcher Meldungen den signifikanten Vorteil, dass das BSI schnell und effizient einen Überblick sowohl qualitativer als auch quantitativer Natur über die Gesamtheit aller Vorfälle erhält und mit diesen gewonnenen Daten effektive Gegenmaßnahmen erarbeiten kann. Ein solcher „IT-Notruf" sollte Bürgern und Unternehmen rund um die Uhr zur Verfügung stehen und an entsprechende Stellen der Landes- oder Bundespolizei sowie weitere relevante Behörden und zertifizierte IT-Sicherheitsdienstleister, wie z.B. IT-Forensiker, vermitteln. Im Gegenzug müsste auch dafür Sorge getragen werden, dass lokale Polizeidienststellen über die Existenz einer solchen Einrichtung informiert werden. So könnte sie im Rahmen einer noch zu regelnden Zuständigkeitsordnung Bürger an den IT-Notruf weiter verweisen. Es sollte auch angemerkt werden, dass eine solche IT-Hotline besonders auch dann einen Nutzen hat, wenn bereits ein sicherheitsrelevantes Problem aufgetreten ist: Erfahrungsgemäß zeigt sich, dass Betroffenen die größten Schäden dadurch entstehen, dass nicht schnell genug auf Datendiebstahl oder andere Hackerangriffe reagiert wird. Darüber hinaus ist die Chance, den Urheber eines Cyber-Angriffes zu finden größer, wenn unmittelbar entsprechend qualifizierte Experten zu Rate gezogen werden.

9. **Rechtliche Grundlagen für die Öffentlichkeitsfahndung im Internet setzen**
   Es ist in Deutschland zulässig, dass die Polizei, Staatsanwaltschaften und Gerichte zur Aufklärung gewisser Straftaten das Mittel der Öffentlichkeitsfahndung verwenden. Konkret heißt das, dass die Öffentlichkeit an der Auffindung des Täters durch Bereitstellung gewisser Informationen durch die Polizei partizipiert. Die Infrastruktur des Internets, speziell die **hohe Interaktivität digitaler Kommunikation**, könnte das Mittel der Öffentlichkeitsfahndung noch effektiver machen. Die Nutzung sozialer Netzwerke privater Betreiber zur Öffentlichkeitsfahndung ist bisher aus datenschutzrechtlicher Sicht sehr problematisch. Nur unter engen Voraussetzungen ist eine solche Öffentlichkeitsfahndung durch Strafverfolgungsbehörden zulässig. Wir fordern daher, dass eine zur Ermöglichung einer effektiv einsetzbaren Öffentlichkeitsfahndung im Internet unter Berücksichtigung der Erfordernisse des Datenschutzes geeignete Rechtslage geschaffen wird.

10. **Regelmäßige Überprüfung und Aktualisierung der IT-Gesetzgebung**
    Schließlich fordern wir generell in Bezug auf alle Arten von IT-Gesetzgebung, und insbesondere in Bezug auf Gesetzgebung, die Fragen der IT-Sicherheit betrifft, dass entsprechende Gesetze bereits strukturell so angelegt sind, dass eine Anpassung und evtl. durch neue Entwicklungen notwendig gewordene Überarbeitung erleichtert wird. Typische Gesetzgebungsverfahren sind meist schlichtweg zu träge, um mit den rapiden, aber signifikanten, technologischen Fortschritten in IT und Kryptographie mitzuhalten. Die Folge ist, dass rechtliche Grauzonen entstehen oder bestehende Gesetze schwer auf modernere Technik anwendbar werden. Daher sollte ein rechtlicher Mechanismus eingeführt werden, der die Legislative und Fachministerien dazu verpflichtet, in festen Zeiträumen (alle 36 Monate) nach letzter Beschlussfassung durch das jeweilige Parlament als relevant gekennzeichnete Gesetze erneut zu bewerten, und nach Bedarf Fachterminologie sowie den Anwendungsbereich des Gesetzes modifizieren zu können. Darüber hinaus ist zu prüfen, inwieweit das Bundesministerium des Inneren ermächtigt werden kann, Rechtsverordnungen in diesem Bereich zu erlassen. Mit möglichst **technologieoffenen Regelungen in den Parlamentsgesetzen** und **konkreten Ausgestaltungen durch Verordnungen**, die das BSI ausarbeitet, kann schnell auf den technologischen Fortschritt und neue Gefahren reagiert werden. In den hierzu nötigen Rechtsgrundlagen hat der Gesetzgeber ein **hohes Schutzniveau und die Ziele der IT-Sicherheit** festzulegen; Inhalt, Zweck und Ausmaß sind im Gesetz hinreichend bestimmt zu regeln. Ebenso sind die verschiedenen möglichen Maßnahmen zu nennen. Somit kann das Ministerium das jeweilig passende Werkzeug wählen, um die auftretende Gefahr zu bekämpfen. Die Ausarbeitung der Normen durch das BSI in Zusammenarbeit mit dem Bundesinnenministerium sichert die Einbeziehung der gesamten Expertise des Bundes in diesem Gebiet; ebenso soll die

Expertise der Wirtschaft und weiterer Sachverständiger aus Wissenschaft, Verbänden und gesellschaftlichen Kreisen einbezogen werden. IT-Sicherheit kann nur kooperativ gewährleistet werden. Über diese Rechtsverordnungen ist sichergestellt, dass trotz der Verzögerungen im Gesetzgebungsverfahren ein möglichst effektiver Schutz auf aktuellem Niveau gewährleistet ist. Parallele Regelungen sind auf Landesebene zu prüfen und bei Bedarf einzuführen.

C. Fazit

Wie bereits in der Einleitung betont, schreitet die Digitalisierung unserer Lebenswelt unaufhaltsam voran. Immer mehr, für unseren alltäglichen Lebenswandel essentielle Aktivitäten werden ins Netz verlagert. Um auch in Zukunft der Bevölkerung sicheres Kommunizieren und Interagieren ermöglichen zu können, sollte die baldige Umsetzung von Maßnahmen wie den Vorgeschlagenen daher oberste Priorität sein.