"Das ist die Schlüsselfrage der Gesellschaft" - Der Schutz von Computern und Netzwerken geht jeden an

Namensartikel von Bundesinnenminister Dr. Wolfgang Schäuble in "DER TAGESSPIEGEL" vom 06.02.2007

„Der Staat soll die Sicherheit zwischen den Bürgern gewährleisten und jene Einrichtungen schaffen, die nicht durch die Initiative des Einzelnen entstehen oder entstehen können." Der Wirtschaftsphilosoph Adam Smith hat schon im Jahr der amerikanischen Unabhängigkeitserklärung 1776 erkannt, dass staatlich organisierte Sicherheit notwendig ist, damit sich auch die persönliche Freiheit entfalten kann. Sicherheit ist ein Grundbedürfnis, und eine zentrale Aufgabe des Staates ist es, sie zu gewährleisten.

Mit der zunehmenden Nutzung von Information- und Kommunikationstechnik (IKT) in Wirtschaft, Verwaltung und im privaten Umfeld wird Sicherheit der IKT immer bedeutender. Je mehr Staat, Wirtschaft sowie Bürgerinnen und Bürger dabei zusammenwirken, desto besser können wir unsere Gesellschaft gegen Störungen der Informationsinfrastruktur schützen.

Die Bedrohungslage hat sich - was die Informationstechnik angeht - weltweit gewandelt. Der internationale Terrorismus und die organisierte Kriminalität nutzen das Internet zunehmend für ihre verbrecherischen Zwecke. Dabei werden die komplexen IKT-Systeme immer häufiger das Ziel von Kriminellen.

Besonderes Augenmerk muss auf die Sicherheit der IKT im Zusammenhang mit kritischen Infrastrukturen gelegt werden, also bei Einrichtungen, deren Ausfall zu nachhaltigen Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen kann. Dazu gehören das Transport- und Verkehrswesen, die Telekommunikationsbranche, die Energiebranche sowie der Finanz- und Geldsektor. Wegen ihrer besonderen Bedeutung für unsere Gesellschaft sind sie potenzielle Ziele des Terrorismus.

Die IT-Systeme sind besonders schutzbedürftig. Weil sie heute praktisch überall zum Einsatz kommen, sind sie für das Funktionieren fast aller herkömmlichen Infrastrukturbereiche Voraussetzung. Wir müssen heute nicht mehr nur gegen physische Bedrohung wie einen Sprengstoffanschlag auf einen Zug, sondern vor allem auch auf Gefährdungen der IKT, beispielsweise einen Angriff auf Stellwerksrechner der Bahn, gewappnet sein.

Sorge bereitet, dass nicht nur die Anzahl von Schadprogrammen und Hackerangriffen gegen Computer und Netzwerke steigt, sondern dass sich auch die Angreifer immer ausgefeilterer Techniken bedienen. Es sind nicht mehr vereinzelte Computerspezialisten, die durch das Eindringen in fremde IT-Systeme zweifelhaften Ruhm in der Szene erlangen wollen. Vielmehr begegnen wir immer mehr professionellen Hackern oder Crackern, die aus kriminellen Motiven handeln und dabei vielfach die Möglichkeiten des Internets nutzen.

Der Bogen der Straftaten reicht von Betrug und Erpressung über die Organisation terroristischer Verbrechen bis hin zu rechts- oder linksextremen Aktionen. Aber das Internet ist keineswegs nur Mittel zum Zweck: Auch Angriffe auf das Internetnetzwerk selbst nehmen zu. Wir können nicht mehr ausschließen, dass sich künftig Terroristen des Know-hows

krimineller Hacker bedienen, um die Information- und Kommunikationstechnik von Betreibern kritischer lnfrastrukturen gezielt anzugreifen. Verursacht ein solcher Angriff tatsächlich Schäden, kann es aufgrund der hohen Vernetzung zu Ausfällen der kritischen Infrastruktur, beispielsweise des Eisenbahnverkehrs, kommen, die eine Kette gravierender Folgeschäden in Wirtschaft und Gesellschaft nach sich ziehen würden.

Um auf die veränderte Bedrohungslage zu reagieren, hat der Bund mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen" eine umfassende IT-Sicherheitsstrategie mit den Ansätzen Prävention, Reaktion und Nachhaltigkeit erarbeitet. Mit dieser Strategie wollen wir die Informationsinfrastrukturen angemessen schützen, wirkungsvoll bei IT-Sicherheitsvorfällen handeln, die deutsche IT-Sicherheitskompetenz stärken und schließlich international Standards setzen.

Die Bundesregierung erstellt derzeit gemeinsam mit den überwiegend privatwirtschaftlichen Betreibern kritischer Infrastrukturen den „Umsetzungsplan Kritis", der die IT-Sicherheit und damit das Funktionieren der kritischen Informationsinfrastrukturen sicherstellen soll. Parallel arbeiten wir an einem „Umsetzungsplan Bund", um auch in der Bundesverwaltung ein angemessenes IT-Sicherheitsniveau zu gewährleisten.

Das Vertrauen der Verbraucher und der Wirtschaft in die sichere Abwicklung elektronischer Dienstleistungen, wie beispielsweise E-Commerce, E-Government oder Online-Banking, muss bewahrt werden. Täglich werden Bürger Opfer von heimtückischen Online-Betrügern. So versuchen Kriminelle beim sogenannten „Phishing" mit vermeintlich authentischen E-Mails, Internetnutzern Daten für sicherheitsrelevante Bereiche zu entlocken. Die erschlichenen Benutzerdaten - etwa für den Internetverkehr mit Kreditinstituten oder mit elektronischen Verkaufsplattformen - werden dann für betrügerische Zwecke eingesetzt. Die Strukturen des Phishings weisen alarmierende Parallelen zur organisierten Kriminalität auf. Dagegen hilft nur eine sichere Authentifizierung der Internetnutzer und der Diensteanbieter in der virtuellen Welt des Internets. Daher werden wir im Rahmen des Programms E-Government 2.0 zum Schutz vor Identitätsdiebstahl den elektronischen Personalausweis einführen und sichere, zertifizierte Bürgerportale fördern. Bürger und Organisationen sollen im Internet sicher, verbindlich und vertraulich kommunizieren können.

Während der deutschen EU-Ratspräsidentschaft im 1. Halbjahr 2007 wollen wir mit dem Projekt „check the web" die Zusammenarbeit beim Beobachten und Analysieren von Internetauftritten mit terroristischem Bezug vertiefen. Ein Mitgliedstaat allein kann das Internet nicht mehr beobachten. Daher wollen wir die besonderen Sprach- und Sachkompetenzen der Sicherheitsbehörden aller Mitgliedstaaten nutzen. Wir werden uns dafür einsetzen, dass ein Portal bei Europol eingerichtet wird, über das die Mitgliedstaaten einschlägige Informationen austauschen können.

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) im Geschäftsbereich des Bundesministeriums des Innern verfügt Deutschland über eine in der Welt führende spezialisierte Fachbehörde für alle Fragen rund um die IT-Sicherheit. Sie sensibilisiert seit Jahren erfolgreich mehr und mehr Bürger und macht sich um die Aufklärung vor Gefährdungen bei der Nutzung der IKT verdient. Das BSI bietet im Portal www.bsi-fuer-buerger.de auch für technische Laien leicht verständliche Informationen zu allen Themen rund um IT-Sicherheit.

Die Bedeutung der Sicherheit von IKT und des Internets hat die Bundeskanzlerin beim nationalen IT-Gipfel am 18. Dezember 2006 in Potsdam betont. Unter den Vertretern aus

Politik, Wirtschaft und Wissenschaft war man sich einig, dass ein stärkeres gesamtgesellschaftliches Engagement für die Sicherheit der IKT unerlässlich ist.

Denn viele Bürger und insbesondere kleinere Unternehmen gehen - aus Unkenntnis - zu sorglos mit dem Internet um. Nach einer Studie des BSI sind rund zehn Prozent der deutschen Internetnutzer ohne Virenschutz „unterwegs", mehr als ein Viertel trifft keine Vorkehrungen, um Sicherheitslücken in Softwareprogrammen zu schließen. Ungenügend gesicherte Rechner können aber ohne Wissen der Inhaber zur Verbreitung von Schadprogrammen missbraucht werden. Solche Nachlässigkeiten können nicht zuletzt in der Wirtschaft schwerwiegende Folgen haben - angefangen bei den Kosten für die Säuberung und Wiederherstellung der betroffenen IKT über die damit verbundenen Imageverluste bis hinzu Regressansprüchen geschädigter Dritter. Jeder einzelne Computernutzer trägt also eine Mitverantwortung für eine angemessene IT-Sicherheit in Deutschland.

Vor kurzem hat sich - vom Bundesministerium des Innern mit angestoßen - der Verein „Deutschland sicher im Netz e. V." gegründet. Der Verein möchte informieren und sensibilisieren sowie Abwehrstrategien gegen Internetangriffe stärken und empfehlen. Staat, Wirtschaft und gemeinnützige Organisationen arbeiten hier herstellerübergreifend und produktneutral partnerschaftlich zusammen. Die Vereinsstruktur gewährleistet eine Interessenvertretung aller Mitglieder und schließt eine Dominanz einzelner Beteiligter aus. Ich habe die Schirmherrschaft über den Verein übernommen, weil ich mir von ihm wertvolle Unterstützung bei der Umsetzung des „Nationalen Plans" erwarte.

Die gemeinsame Verantwortung von Wirtschaft und Staat für die Sicherheit der IKT und des Internets wird Schwerpunkt der europäischen IT-Sicherheitskonferenz im Juni 2007 sein, zu der ich während der deutschen EU-Präsidentschaft einlade. Gemeinsam mit der Europäischen Kommission möchten wir erreichen, dass in Europa Nutzer und Hersteller flächendeckend und rechtzeitig vor Computerviren oder anderen IT-Sicherheitsrisiken gewarnt werden.

Wir können „IT-Sicherheit" nachhaltig nur gemeinsam gewährleisten. Neben der Verantwortung des Staates und der Anwender sehe ich besonders die Hersteller von Hard- und Software in der Pflicht, sichere IT-Produkte herzustellen. Nur dann wird auch die Sensibilisierung und Aufklärung der IT-Nutzer etwa durch das BSI zu einem Mehr an IT-Sicherheit führen.

Die Sicherheit der privat wie beruflich genutzten Computer und Netzwerke entwickelt sich immer mehr zu der Schlüsselfrage unserer Informationsgesellschaft. Wir brauchen eine IT-Sicherheitskultur in Staat, Wirtschaft und Gesellschaft, die dem Stellenwert der lnformationstechnik für praktisch alle lebenswichtigen Strukturen unseres Gemeinwesens gerecht wird.