Innenausschuss
A-Drs. 16(4)570 A

Bundesamt
für Sicherheit in der
Informationstechnik

Stellungnahme für die Anhörung des Innenausschusses zum Gesetzesentwurf der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes

am 11. Mai 2009

Dr. Udo Helmbrecht

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Ausgangslage

Das BSI-Errichtungsgesetz stammt aus dem Jahr 1990. Die damalige Informationstechnik war von Großrechnern, kleinen lokalen Netzen und isolierten PCs geprägt. Diese Situation hat sich in den vergangenen rund 20 Jahren radikal geändert: das Internet hat inzwischen fast alle Arbeitsplätze der Wirtschaft und Verwaltung erobert. Im privaten Bereich ist die überwiegende Zahl der Haushalte durch Hochleistungs-Anschlüsse mit dem Internet verbunden. Eine kontinuierliche Zusammenarbeit der Wirtschaft, der Verwaltung und der Bürger findet seit E-Commerce und E-Government statt. Praktisch kann von einer total-vernetzten IT-Infrastruktur in Deutschland ausgegangen werden.

Mit diesem Technologieschub hat sich auch die Bedeutung der Informations- und Kommunikationstechnik (IKT) stark gewandelt. Sie ist gegenwärtig eine unabdingbare Voraussetzung für das Funktionieren des Gemeinwesens. Ohne funktionierende IKT-Strukturen ist die Versorgung mit Energie oder Wasser gefährdet, fallen wichtige Infrastrukturen (z.B. Verkehrsmittel, bargeldlose Zahlungswege, Produktionsbereiche der Wirtschaft) aus. Fehler in und Angriffe auf IKT-Infrastrukturen können unmittelbare Auswirkungen auf Leben und Gesundheit vieler Menschen haben.

Gefährdungslage

Die Informationstechnik ist in den vergangenen Jahren nicht sicherer geworden. Immer kürzere Entwicklungszeiten aufgrund des wirtschaftlichen Drucks (Time to Market) und immer komplexere Systeme verlangen ihren Tribut. Die Zahl entdeckter Fehler und Schwachstellen ist rasant gestiegen, so dass heute mehrere Dutzend neue Schwachstellen pro Tag publiziert werden. Die Möglichkeiten der Hersteller, dieser Flut Herr zu werden, sind jedoch nicht im gleichen Maße gestiegen. Und selbst wenn ein Hersteller ein Update innerhalb einer Woche bereitstellen kann, so dauert es oft Monate, bis die Endanwender dieses Update in der Fläche installiert haben.

War es 1991 noch so, dass Computerviren mittels Datenträger (Disketten) und vereinzelt über E-Mail verteilt wurden, so kann ein Angreifer heute Schadprogramme innerhalb von Sekunden an dutzende Millionen Rechner verteilen. Die Breite und die Schnelligkeit der Angriffe hat sich potenziert. Und auch die Angreiferfront hat sich verändert. Waren es in den 90er Jahren noch Hacker, die Schwächen in IT-Systemen pressewirksam aufzeigen wollten, sind es inzwischen Nachrichtendienste und die organisierte Kriminalität, die professionell IT-Angriffe vorbereiten und durchführen.

In den letzten Jahren überwogen ungezielte Massenangriffe mit Würmern, Computerviren und Phishing. In den letzten zwei Jahren ist eine neue Angriffsart verstärkt zu beobachten: gezielte Angriffe auf ausgesuchte IT-Systeme. Massenangriffe hatten paradoxerweise den Vorteil, dass die Hersteller von Antiviren-Software schnell Samples von Schadsoftware erhielten und nachrüsten konnten. Die heutigen gezielten Angriffe, die nur eine geringe Anzahl von Rechner betreffen, sind in der Lage, sämtliche Antiviren-Software und Firewalls zu umgehen. Diese Angriffe beruhen dabei auf der üblichen Internetnutzung der Endanwender: E-Mail und Surfen.

Die klassischen Schutzmaßnahmen der letzten 20 Jahre bilden heute nur noch einen Minimalschutz, der aber nicht gegen gezielte Angriffe ausreicht.

Dies haben die spektakulären Angriffe der letzten Jahre im Ausland und in Deutschland gezeigt.

Bezüglich Durchführung und Ziel der Angriffe ist zwischen informationstechnischer Sabotage und Spionage zu unterscheiden:
Für Sabotagezwecke werden überwiegend gekaperte private Rechner eingesetzt. Unzureichend geschützte Privatrechner werden im ersten Schritt mit einer Schadsoftware angegriffen, der Täter übernimmt die komplette Kontrolle, ohne dass dies dem Besitzer des Rechners bewusst ist. Im zweiten Schritt werden Millionen solcher gekaperter Rechner einer zentralen Kontrolle zugeführt (Botnetz), auf deren Kommando im nächsten Schritt Ziele über das Internet so massiv angegriffen

werden, dass diese Zielsysteme völlig überlastet werden. Leicht ist es möglich, Server, E-Commerce-Anbieter, kleinere Internetanbieter und sogar die Internetinfrastruktur kleinerer Staaten komplett für längere Zeit auszuschalten.

Für Spionagezwecke wird typischerweise zunächst ein Profil der Zielperson erstellt: Name, E-Mail-Adresse, Beruf, beruflich bedingte Interessen, etc. Anschließend wird der Zielperson eine auf sie zugeschnittene E-Mail zugesandt, die entweder einen vermeintlich interessanten Anhang besitzt oder auf eine vermeintlich interessante Webseite verweist. Sowohl Anhang als auch Webseite sind so manipuliert, dass neue Schwachstellen in Standardsoftware ausgenutzt werden, um den Rechner der Zielperson zu kapern. Einmal infiziert, können sämtliche Daten dieses Rechners und natürlich auch aller von diesem Rechner aus erreichbaren Systeme eines Unternehmens oder einer Behörde ausgeforscht und an den Angreifer übermittelt werden.

Beide Techniken gehören heute zum Standard-Repertoire der Nachrichtendienste und organisierten Kriminalität. Und beide Angriffstechniken finden täglich Verwendung:

Deutschland, sowohl Verwaltung als auch Wirtschaft, wird täglich gezielt über das Internet angegriffen.

Bezogen auf die Bundesverwaltung bedeutet dies, dass

- täglich Regierungsnetze angegriffen werden und damit die Regierungskommunikation und Handlungsfähigkeit bedroht ist,
- staatlich geheimzuhaltende Informationen täglich informationstechnischen Spionageangriffen ausgesetzt sind,
- die Informationen und Daten der Bundesbürger, die innerhalb der Bundesverwaltung verarbeitet werden, ebenso durch Spionage und Manipulation bedroht sind.

Ein ausreichender Schutz ist auch im Interesse des Bürgers bezüglich seiner personenbezogenen Daten und seiner Kommunikation mit Bundesbehörden

unabdingbar zu gewährleisten. Lediglich im Bundesamt für Sicherheit in der Informationstechnik sind Know-how und technische Fähigkeiten gebündelt vorhanden, um diesen Schutz aufzubauen. Das BSI besitzt aufgrund der bestehenden Gesetzeslage allerdings keinerlei diesbezügliche Befugnisse.

Handlungsbedarf

Die gegenwärtig vom BSI wahrzunehmenden Aufgaben und die hierfür erforderlichen Befugnisse sind im BSI-Errichtungsgesetz aus dem Jahr 1990 nicht verankert.

Um die dargelegten Bedrohungen zu bekämpfen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnologie in der heutigen Gesellschaft Rechnung zu tragen, müssen dem BSI weitreichendere Aufgaben und Befugnisse eingeräumt werden. So ist es zwingend erforderlich, dass das BSI Maßnahmen zur Erhöhung der IT-Sicherheit in der Bundesverwaltung und zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes ergreifen darf:

Zentrales Lagebild und Warnungen

Gemäß **§ 4** des Gesetzesentwurfs soll das BSI als zentrale Meldestelle für IT-Sicherheit Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik zentral sammeln sowie auswerten.

Die Bundesbehörden trifft ab dem 01. Januar 2010 die Pflicht, Erkenntnisse über neue Schadprogramme, Angriffsmuster oder IT-Sicherheitsvorfälle dem BSI zu melden. Durch die zentrale Sammlung und Auswertung der Informationen ist es dem BSI möglich, ein verlässliches Lagebild zu erstellen und Angriffe frühzeitig zu erkennen sowie Gegenmaßnahmen zu ergreifen. Im Gegenzug informiert das BSI die anderen Behörden, sofern es Erkenntnisse erhält, die zum Schutz der anderen Behörden beitragen.

Nach **§ 7 BSIG-E** kann das BSI Informationen und Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten sowie vor Schadprogrammen an

die betroffenen Stellen oder die Öffentlichkeit weitergeben. Hierbei besteht zunächst grundsätzlich die Pflicht, den Hersteller vorab zu informieren, sofern dies nicht den Zweck der Maßnahme gefährdet. Erst im Anschluss daran wendet sich das BSI an die Öffentlichkeit. Tatsachen die geeignet sind, Angriffe durch Dritte zu fördern, werden der Öffentlichkeit nicht bekannt gegeben. Dies ist beispielsweise der Fall, wenn Schwachstellen dem BSI bekannt geworden sind, gegen die noch keine Gegenmaßnahmen verfügbar sind. Eine Warnung wäre hier zu diesem Zeitpunkt kontraproduktiv, da potenzielle Täter auf die Schwachstellen hingewiesen werden, aber die betroffenen Stellen noch keine Möglichkeit zur Abwehr haben.

Abwehr konkreter informationstechnischer Angriffe

Das BSI benötigt zwingend die Befugnis, Protokolldaten (z. B. Logfiles von Servern, Firewalls, Kopfdaten der Kommunikationsprotokolle) sowie Daten, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallen (technische Telekommunikationsinhalte), zu erheben, auszuwerten, zu speichern, zu verwenden und zu verarbeiten **(§ 5 BSIG-E)**. Hierdurch erst können Anzeichen für bevorstehende oder laufende IT-Angriffe erkannt und diese nachhaltig bekämpft werden. Aufgrund dieser Befugnis wird es dem BSI unter anderem möglich, spezielle Malware-Scanner oder andere Detektionstools einzusetzen, was bislang nur nach ausdrücklicher Einwilligung der betroffenen Bundesbediensteten zulässig war.

Die genannten Befugnisse des § 5 BSIG-E beziehen sich lediglich auf Daten, die beim Betrieb der Kommunikationstechnik des Bundes anfallen. Die Vorschrift lässt somit nicht die Erhebung, Auswertung, Speicherung, Verwendung und Verarbeitung von Daten bei Dritten zu. Ebenfalls ausgeschlossen ist die Verwendung und Verarbeitung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Sofern das BSI im Rahmen der Ausübung seiner Befugnisse feststellt, dass derartige Daten betroffen sind, müssen diese unverzüglich gelöscht und die Tatsache ihrer Erlangung und Löschung aktenkundig gemacht werden.

Um dem Grundsatz der Verhältnismäßigkeit Rechnung zu tragen, untergliedert sich § 5 BSIG-E in vier Stufen. Je schwerwiegender der durch die Maßnahme

stattfindende Eingriff ist, umso höhere Anforderungen sind an die erforderliche Verdachtsstufe zu stellen:

§ 5 Abs. 1 BSIG-E gibt dem BSI die Befugnis, die entsprechenden Daten zu erheben und **automatisiert** auszuwerten, um Spuren von Schadprogrammen frühzeitig erkennen und Gefahren bekämpfen zu können (Stufe 1). Sofern nicht eine Weiterverarbeitung nach Absatz 2 oder 3 ausnahmsweise zulässig ist, sind die nach Absatz 1 erhobenen Daten nach der Auswertung unverzüglich und spurenlos zu löschen. Ein weiterer Zugriff auf die Daten ist somit ausgeschlossen. Insbesondere ist die personenbezogene Verwendung von Protokolldaten zu anderen Zwecken, wie z. B. zur Erstellung von Kommunikationsprofilen oder zur Verhaltens- und Leistungskontrolle der Mitarbeiter unzulässig.

Bestehen tatsächliche Anhaltspunkte, dass die Protokolldaten zur Abwehr von Gefahren, die von einem gefundenen Schadprogramm ausgehen oder zur Erkennung der Abwehr anderer Schadprogramme erforderlich sein können, dürfen die Protokolldaten gemäß § 5 Abs. 2 BSIG-E erhoben, automatisiert ausgewertet und für höchstens drei Monate gespeichert werden (Stufe 2). Eine ausreichende Frist vor einer endgültigen Löschung ist zwingend erforderlich, da Schadprogramme in der Regel erst mit einem zeitlichen Verzug von mehreren Tagen oder Wochen detektiert werden können. Wird ein neues Schadprogramm gefunden, besteht die Notwendigkeit, rückwirkend zu untersuchen, ob das Programm bereits zuvor innerhalb der Bundesverwaltung verbreitet wurde. Nur auf diese Weise können etwaige Schäden, die durch das Schadprogramm verursacht werden, vermieden oder begrenzt werden.

Besteht der konkrete Verdacht, dass ein Schadprogramm vorliegt, dürfen die Daten verarbeitet werden (Stufe 3, § 5 Abs. 3 BSIG-E). Wird der Verdacht widerlegt, sind die Betroffenen (Absender und Adressat) hiervon zu unterrichten und die Daten sind zu löschen.

Eine weitere Verarbeitung der Daten ist nur zulässig, wenn sich der Verdacht bestätigt und eine Verarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist (Stufe 4, § 5 Abs.

3 BSI G-E). In diesen Fällen wird der Empfänger der Nachricht gewarnt, die notwendigen Schutzmaßnahmen zu ergreifen.

Der Schutz der durch die Bundesverwaltung verarbeiteten Daten und Informationen, auch die der Bundesbürger, erfordert aufgrund der konkreten Gefährdungslage über die üblichen Sicherheitsmaßnahmen hinausgehende Abwehrstrategien. Die aufgrund des § 5 BSIG-E mögliche zentrale Abwehr durch das BSI ist dabei die effektivste und auch datenschutzrechtlich unbedenklichste Alternative. Andere Ansätze, bei denen die gleichen Maßnahmen dezentral in den jeweiligen Behörden umgesetzt würden, scheitern am fehlenden Know-how und sind in der Fläche weit weniger effektiv datenschutzrechtlich kontrollierbar.

Vorgabe von Sicherheitsstandards

Die Funktionsfähigkeit und Sicherheit der IT des Bundes hängt angesichts einer erheblich verschärften IT-Sicherheitslage von der Sicherheit und Vertrauenswürdigkeit einzelner IT-Komponenten ab. Erfahrungen zeigen, dass Angreifer die am schlechtesten geschützten Systeme innerhalb der Bundesverwaltung ausnutzen, um über diese in andere Bereiche vorzudringen. Hier gilt es zu verhindern, dass ungeeignete Produkte mit Schwachstellen oder manipulierte IT-Komponenten, die Möglichkeiten zur Spionage oder Sabotage eröffnen, in der Bundesverwaltung und in den Regierungsnetzen zum Einsatz kommen. Dieser Gefahr kann nur durch die Festlegung einheitlicher und strenger Sicherheitsstandards durch eine zentrale Stelle auf Bundesebene begegnet werden. Daher benötigt das BSI die Befugnis, einheitliche Sicherheitsstandards für die Bundesverwaltung zu definieren und bei Bedarf geeignete Produkte entwickeln zu lassen bzw. auszuschreiben und bereitzustellen, **§ 8 BSIG-E.**

Telekommunikationsgesetz und Telemediengesetz

Neben dem BSI müssen auch zentrale Träger der Informationsinfrastruktur in Deutschland, Telekommunikationsbetreiber und Telemediendiensteanbieter, verstärkt Sicherheitsmaßnahmen umsetzen, da auch sie Ziel von Angriffen sind, die

letztlich alle Wirtschaftsunternehmen, Behörden und Bürger betreffen. Auch diese Betreiber müssen befugt sein, die notwendigen Schutzmaßnahmen im Sinne ihrer Kunden umsetzen zu können. Umsetzungsdefizite müssen erkannt und ausgeräumt werden.

Deutschland steht an einem Wendepunkt.
Es ist zu entscheiden, ob Deutschland und die Bundesverwaltung ausreichende Mittel und Befugnisse erhalten, den Abwehrkampf ebenbürtig zu führen, oder ob Deutschland vor den technisch versierten IT-Angreifern kapituliert.