Bundesministerium
des Innern

Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)

www.bmi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Deutschlands Informationsinfrastrukturen

Deutschland hat auf dem Weg in das Informationszeitalter schon eine beachtliche Strecke zurückgelegt. Staat, Wirtschaft und Gesellschaft nutzen intensiv moderne Informationstechnik (IT). Informationsinfrastrukturen gehören heute neben Straßen, Wasser- und Stromleitungen zu den nationalen Infrastrukturen, ohne die das private wie das berufliche Leben zum Stillstand käme.

Informationsinfrastrukturen sind das Nervensystem unseres Landes

Unsere von Informationstechnik geprägte Gesellschaft ist neuartigen Gefahren ausgesetzt. IT-Sicherheitsvorfälle können angesichts globaler Vernetzung zu Störungen oder Ausfällen in deutschen Informationsinfrastrukturen führen, auch wenn sie ihren Ursprung nicht in unserem Land haben. Immer häufiger versuchen auch Kriminelle und Terroristen, die komplexen technischen Systeme durch gezielte Angriffe zu schädigen. Es ist nicht auszuschließen, dass auch lebenswichtige Informationsinfrastrukturen in Deutschland Gegenstand gezielter Anschläge werden.

Die Innere Sicherheit unseres Staates ist deshalb heute untrennbar mit sicheren Informationsinfrastrukturen verbunden, ihr Schutz ist für unsere nationale Sicherheitspolitik von herausragender Bedeutung. Unter Federführung des Bundesministeriums des Innern (BMI) wurde daher der vorliegende „Nationale Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) erstellt, dessen Umsetzung eine Stärkung des Schutzes der Informationstechnik in Deutschland gegen weltweite Bedrohungen bewirken wird.

1.2 Bedrohungen und Gefährdungen unserer Informationsinfrastrukturen

Häufige Ursachen für Störungen und Ausfälle von Systemen sind technische Defekte, menschliches Versagen oder mutwillige Beschädigungen und Zerstörungen, die sich durch die Vernetzung der Informationsinfrastrukturen untereinander unmittelbar auch auf andere Bereiche auswirken. Kettenreaktionen können dabei Auswirkungen auf weitere Bereiche der Wirtschaft und der Gesellschaft haben.

Neue Bedrohungen

IT-Systeme sind, egal ob es sich um die privater Anwenderinnen und Anwender oder ein ganzes Firmennetz handelt, Hackerangriffen und Bedrohungen durch Computerviren und -würmer ausgesetzt. Viele der schädlichen Programme und gezielten Angriffe gehen zunehmend auf das Konto organisierter Kriminalität und terroristischer Angreifer. Das Hauptmotiv ist nicht mehr wie bei den so genannten Script-Kiddies der Wunsch, an Bekanntheit zu gewinnen, sondern es geht darum, aus den Angriffen finanziellen Nutzen zu ziehen oder volkswirtschaftlichen Schaden anzurichten.

Neben privat genutzten Computern, in die Kriminelle eindringen, um beispielsweise Zugangsdaten für das Onlinebanking zu stehlen oder massenhaft Computerviren und Spam zu versenden, gehören zu den primären Zielen dieser Angriffe große Unternehmen, Banken und staatliche Einrichtungen.

Die Methoden der Angreifer sind vielfältig und werden hier nur beispielhaft benannt:

- massenhafte, gleichzeitige Zugriffsversuche über „gehackte“ Rechner von Bürgerinnen und Bürgern, um Systeme zu überlasten und deren Verfügbarkeit einzuschränken
- Angriffe über Spionagesoftware
- Angriffe zum Abhören oder Manipulieren von Datenströmen
- Ausnutzen von Schwachstellen oder Angriffe über Schadsoftware wie Computerviren oder -würmer

Die starke Verbreitung von Standardsoftware, die von einfachen Internetanwendungen bis hin zu komplexen Verwaltungssystemen reicht, erleichtert es, mögliche Angriffspunkte in einem System zu finden. Automatisierte Angriffe, die auf Sicherheitslücken in diesen Programmen zielen, richten gleichzeitig in vielen Systemen enormen Schaden an, bevor Gegenmaßnahmen ergriffen und die Fehler behoben werden können.

Nicht mehr einzelne PCs, sondern zunehmend Router, Firewalls und andere Sicherheitseinrichtungen, die in Unternehmen oder Verwaltungen Systeme schützen sollen, geraten ins Visier der organisierten Kriminalität. Solche Angriffe sind von einer neuen Qualität, da sie nicht mehr nur vereinzelte, sondern unter Umständen Tausende PCs des dahinterliegenden Netzwerks betreffen. Manipulationen zentraler Systeme von Informationsinfrastrukturen können im Extremfall zum Ausfall einer kompletten Informationsinfrastruktur führen. Hoher wirtschaftlicher Schaden ist die Folge.

1.3 Strategische Ziele

Um einen umfassenden Schutz der Informationsinfrastrukturen in Deutschland sicherzustellen, gibt die Bundesregierung mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ drei strategische Ziele vor:

- Prävention: Informationsinfrastrukturen angemessen schützen
- Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
- Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

Diese Ziele ergänzen die IT-Strategie des Bundes. Die Erreichung der Ziele wird durch einen Umsetzungsplan für die Bundesverwaltung, einen Umsetzungsplan für die Kritischen Infrastrukturen und gegebenenfalls weitere Umsetzungspläne sichergestellt.

Um den Schutz der Informationsinfrastrukturen in Deutschland nachhaltig zu gewährleisten, überprüft die Bundesregierung den Nationalen Plan und dessen Umsetzung regelmäßig und passt ihn gegebenenfalls an die aktuellen Erfordernisse an.

1.4 Verantwortlichkeiten beim Schutz von Informationsinfrastrukturen

Die zunehmende Bedeutung der Informationsinfrastrukturen für unser Land erfordert ein gemeinsames Vorgehen von Staat, Wirtschaft und Gesellschaft. Mit dem vorliegenden Nationalen Plan stellt die Bundesregierung sicher, dass diese Aufgaben erfüllt werden.

IT-Sicherheit in der Bundesverwaltung

Die Bundesverwaltung betreibt selbst einen Teil der nationalen Informationsinfrastrukturen. Mit der Umsetzung des vorliegenden Nationalen Plans wird IT-Sicherheit mittel- und langfristig auf hohem Niveau in der gesamten Bundesverwaltung gewährleistet. Daher legt die Bundesregierung genaue Richtlinien für den Schutz der Informationsinfrastrukturen in der Bundesverwaltung in einem Umsetzungsplan Bund fest.

Dieser soll gemeinsame, einvernehmlich erarbeitete technische, organisatorische und prozessuale Standards für die Bundesverwaltung festschreiben, die von den Ressorts eigenverantwortlich in ihrem jeweiligen Geschäftsbereich umgesetzt werden.

Damit setzt die Bundesregierung ein Zeichen: Der Schutz der eigenen Informationsinfrastrukturen ist die Grundlage für den Schutz und die Verlässlichkeit der Informationsinfrastrukturen in Deutschland. Die Umsetzung dieses Nationalen Plans stärkt damit auch den Wirtschaftsstandort Deutschland.

Das BSI ist als nationale IT-Sicherheitsbehörde und zentraler IT-Sicherheitsdienstleister des Bundes koordinierend für die Umsetzung des Nationalen Plans zuständig. Es wird hierzu deutlich gestärkt und mit einer aktiveren Rolle als IT-Sicherheitsberater neu positioniert.

Kooperation zwischen Bund und Wirtschaft

Die meisten Informationsinfrastrukturen unseres Landes sind in privatwirtschaftlicher Verantwortung. Der Schutz dieser Informationsinfrastrukturen ist zuallererst Aufgabe der Betreiber und Dienstleistungsanbieter. Bei möglichen schwerwiegenden Folgen für Staat, Wirtschaft oder große Teile der Bevölkerung reicht in vielen Fällen eine isolierte Eigenverantwortung der einzelnen Betreiber nicht aus. Das gilt auch für die Kritischen Infrastrukturen in Deutschland.

Die Bundesregierung definiert die erforderlichen Anforderungen zum Schutz der Informationsinfrastrukturen, kann sie aber nicht komplett selbst umsetzen. Sie wird daher mit den privaten Betreibern klare Vereinbarungen darüber treffen, wie die notwendigen Aufgaben bewältigt werden können und effektives gemeinsames Handeln bei IT-Sicherheitsvorfällen sichergestellt werden kann.

Die Partner in der Wirtschaft sind daher aufgefordert, gemeinsam mit der Bundesregierung bei der Umsetzung des Nationalen Plans – insbesondere in den Kritischen Infrastrukturen – mitzuwirken. Ziel muss sein, dass die Umsetzung dieser Schutzmaßnahmen nicht nur die eigenen Geschäftsprozesse sichert, sondern auch den Wirtschaftsstandort Deutschland und die internationale Wettbewerbsfähigkeit unseres Landes fördert.

Die Bundesregierung erstellt daher mit Beteiligung der Betreiber Kritischer Infrastrukturen einen „Umsetzungsplan KRITIS“. Hier werden Maßnahmen zu einer deutlichen Verbesserung des IT-Sicherheitsniveaus festgeschrieben. Das BSI sowie andere in Teilbereichen Verantwortung tragende Behörden werden die Betreiber Kritischer Infrastrukturen bei der Umsetzung der Maßnahmen des Umsetzungsplans KRITIS durch fachkompetente Beratung unterstützen.

Bürger und Gesellschaft

Für einen umfassenden Schutz der Informationsinfrastrukturen in Deutschland sorgen nicht allein Spezialisten. Hierzu ist die Mitwirkung aller gefordert – der Hersteller von IT-Produkten und IT-Dienstleistungen, der Beschäftigten und vor allem der Verantwortlichen in Behörden und Unternehmen sowie auch derjenigen, die diese Strukturen nutzen.

Bürgerinnen und Bürger nutzen auch in ihrer Rolle als Verbraucher Informationsinfrastrukturen immer intensiver. Dabei sind sich informierte Verbraucherinnen und Verbraucher der Sicherheitsproblematik bewusst. Vertrauenswürdige Produkte und Verfahren finden bei ihnen daher eher Akzeptanz. Ein hoher Sicherheitsstandard ist somit auch für Anbieter von IT-Produkten und IT-Dienstleistungen ein wirtschaftlicher Faktor – er bietet die Grundlage für einen funktionierenden Markt und für Innovationsmodelle.

Ziel der Bundesregierung ist es, dass die bereits bestehenden und mit Umsetzung dieses Nationalen Plans bereitgestellten Informationsangebote verstärkt genutzt werden. Durch die Berücksichtigung der Empfehlungen tragen einerseits Bürgerinnen und Bürger aktiv zur IT-Sicherheit in Deutschland bei, andererseits werden Hersteller und Verkäufer von IT-Produkten und IT-Dienstleistungen aufgefordert, der Sicherheit ihrer Produkte bei Entwicklung und Produktion sowie Implementierung höchste Priorität einzuräumen und ihre Kunden angemessen auf IT-Risiken hinzuweisen und über Schutzmöglichkeiten umfassend aufzuklären.

Internationale Zusammenarbeit beim Schutz von Informationsinfrastrukturen

Ein Eckpfeiler des vorliegenden Nationalen Plans ist neben der Zusammenarbeit mit den Unternehmen auch das aktive Einbringen deutscher Interessen in die politische Willensbildung auf internationaler Ebene.

Verbindliche Standards für die Prüfung und Bewertung von Sicherheitseigenschaften bei IT-Produkten sind die Voraussetzung für sichere Informationsinfrastrukturen. Deshalb forciert die Bundesregierung die Schaffung geeigneter internationaler Normen und Standards.

2 Prävention: Informationsinfrastrukturen angemessen schützen

Sicherheitsrisiken beim Einsatz von Informationstechnik werden reduziert, indem Wissen über Bedrohungen und Schutzmöglichkeiten vermittelt, Sicherheitsverantwortlichkeiten geregelt, Sicherheitsmaßnahmen umgesetzt und vertrauenswürdige Produkte und Verfahren eingesetzt werden.

Ziel 1: Bewusstsein schärfen über Risiken der IT-Nutzung

Die Bundesregierung wird weiterhin auf die Sensibilisierung für und die Aufklärung über IT-Risiken in allen Bereichen von Wirtschaft und Gesellschaft setzen. Hierzu werden über Initiativen und Maßnahmen Menschen auf allen Ebenen angesprochen, vom Management eines Unternehmens über die Führung einer Behörde bis hin zu Mitarbeiterinnen und Mitarbeitern sowie Bürgerinnen und Bürgern als private PC-Nutzer.

Ziel 2: Einsatz sicherer IT-Produkte und -Systeme

Die Bundesregierung stärkt den Einsatz von verlässlichen IT-Produkten und -Systemen sowie vertrauenswürdigen IT-Sicherheitsprodukten in Deutschland und insbesondere in der Bundesverwaltung. Das BSI wird seine Zertifizierungsleistungen ausbauen, um IT-Produkte und -Systeme schneller und umfangreicher auf ihre Sicherheitseigenschaften prüfen zu können. Es gibt Produktempfehlungen sowie technische Richtlinien zum Einsatz dieser Produkte heraus und veröffentlicht regelmäßig Listen über Produkte mit deutschen Sicherheitszertifikaten. Die Bundesregierung unterstützt die Entwicklung nationaler IT-Sicherheitsprodukte und neuer Informationstechnologien.

Ziel 3: Vertraulichkeit wahren

Ungeschützte digitale Kommunikation ist breitflächig angreifbar, abhörbar und manipulierbar. Deshalb ist es für die Sicherheit der deutschen Informationsgesellschaft und für den Industriestandort Deutschland unabdingbar, dass zur Gewährleistung vertraulicher Kommunikation innovative, vertrauenswürdige Kryptoprodukte verfügbar sind. Die Bundesregierung wird die Entwicklung und die deutschen Hersteller entsprechender Produkte nach Maßgabe des Kryptoeckwerte-Beschlusses aus dem Jahre 1999 fördern sowie die eigene Kommunikation umfassend verschlüsseln und sichern.

Bei der Vergabe von Aufträgen im Bereich IT/IT-Sicherheit werden Bundesbehörden verstärkt die nationalen Sicherheitsinteressen und die Vertrauenswürdigkeit der Anbieter berücksichtigen.

Die Wirtschaft wird gezielt auf die Risken durch Informationsabfluss (z. B. durch Wirtschaftsspionage) aufmerksam gemacht. Die Vorteile des Einsatzes vertrauenswürdiger deutscher Kryptoprodukte werden dabei herausgestellt.

Ziel 4: Gewährleisten umfassender Schutzvorkehrungen

Es sind in allen Bereichen aufeinander abgestimmte technische, bauliche, organisatorische und strukturelle Schutzvorkehrungen zu treffen. Verantwortlichkeiten für alle Aufgaben beim Schutz der Informationstechnik sind klar zu regeln. Für die Bundesverwaltung werden in allen Behörden angemessene IT-Sicherheitsmaßnahmen

realisiert. Die Aktualität und die wirksame Umsetzung der IT-Sicherheitskonzepte der Bundesbehörden werden durch die zuständigen Ressorts sichergestellt. Die Bundesregierung verstärkt die Koordination im Bereich IT-Sicherheitsmanagement der Bundesverwaltung mit dem Ziel, einheitliche bzw. grundsätzlich vergleichbare, effiziente und transparente Abläufe von der Ebene der Ressorts bis hinunter in jede Geschäftsbereichsbehörde sicherzustellen.

Unternehmen und Organisationen sind nachdrücklich aufgefordert, auch für ihre Informationstechnik einen umfassenden Schutz sicherzustellen.

Ziel 5: Vorgabe von Rahmenbedingungen und Richtlinien

Die Bundesregierung wird Rahmenbedingungen und Richtlinien unter Berücksichtigung internationaler Vorgaben so gestalten, dass ein umfassender Schutz in allen sicherheitsrelevanten Bereichen sichergestellt wird.

Jedes Ressort der Bundesverwaltung stellt für sich und die Behörden seines Geschäftsbereichs die Umsetzung der Standards und der Richtlinien gemäß Umsetzungsplan Bund u. a. durch eine IT-Sicherheitsorganisation (z. B. IT-Sicherheitsbeauftragte, Berichtswesen, Leitungsverantwortung) sicher.

Für Bereiche der Wirtschaft mit Anforderungen an ein besonderes Sicherheitsniveau werden entsprechende Leitlinien veröffentlicht. Allen weiteren gesellschaftlichen Bereichen werden Empfehlungen und Leitfäden zur IT-Sicherheit zur Verfügung gestellt.

Ziel 6: Abgestimmte Sicherheitsstrategien

Sicherheitssysteme sind immer nur so stark wie das schwächste Glied in der Kette. Daher kommt der Abstimmung von sicherheitsrelevanten Verfahren und Prozessen eine besondere Bedeutung zu. Aus diesem Grund fördert die Bundesregierung u. a. die Definition gemeinsamer Standards und abgestimmter Nutzungskonzepte, um sicherheitstechnisch, wirtschaftlich und datenschutztechnisch optimierte Systeme zu realisieren, die einen ganzheitlichen Ansatz verfolgen.

Ziel 7: Nationale und internationale Gestaltung politischer Willensbildung

Die Bundesregierung wird die aktive Gestaltung der politischen Willensbildung bei bestehenden und neuen Kooperationen zum Schutz der Informationsinfrastrukturen intensivieren. Die Zusammenarbeit auf nationaler und internationaler Ebene wird verstärkt, um in Richtlinien und Gesetze deutsche Sicherheitsinteressen einzubringen. Um auf Bedrohungen vor dem Hintergrund globaler Netze umfassend reagieren zu können, wird die Zusammenarbeit von Bundesministerien und Bundesbehörden mit den entsprechenden Einrichtungen anderer Staaten verstärkt. Zudem wird die Bundesregierung gemeinsam mit ihren Partnern, z. B. in der EU (hier insbesondere zusammen mit der europäischen IT-Sicherheitsbehörde ENISA), der NATO, der OECD, den UN, den G8 und auf internationaler Ebene, das Bewusstsein über die Verwundbarkeit von Informationsinfrastrukturen schärfen und sich für die Bereitstellung technischer Lösungen einsetzen.

3 Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln

Störungen in Informationsinfrastrukturen erfordern schnelle und wirksame Reaktionen. Dazu gehören neben dem Sammeln und Analysieren von Informationen insbesondere die Alarmierung von Betroffenen und das Ergreifen von Maßnahmen zur Schadensminimierung. Die Bundesregierung etabliert dazu ein nationales IT-Krisenmanagement.

Ziel 8: Erkennen, Erfassen und Bewerten von Vorfällen

Mit dem Krisenreaktionszentrum IT des Bundes im BSI wird ein nationales Lage- und Analysezentrum aufgebaut, das jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland verfügt und mit den etablierten Lage- und Krisenzentren anlassbezogen zusammenarbeitet. Hierzu wird durch das BSI ein Sensornetz für IT-Sicherheitsvorfälle eingerichtet. Weitere Informationsquellen zu IT-Vorfällen werden durch den Ausbau eines von der Bundesregierung mit initiierten internationalen „Watch-and-Warning“-Netzwerkes erschlossen. So wird die Voraussetzung dafür geschaffen, den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können.

Ziel 9: Informieren, Alarmieren und Warnen

Informationen zu aktuellen Bedrohungen und Risiken werden durch die zuständigen Bundesbehörden zielgruppengerecht bereitgestellt. Alle Verantwortlichen für IT-Systeme und Informationsinfrastrukturen werden Zugriff auf geeignete Informationsangebote haben, von der Privatperson bis zum Verantwortlichen für die IT in Unternehmen, Behörden oder anderen Organisationen.

Mit dem nationalen IT-Krisenmanagement des Bundes wird auch ein Alarmierungs- und Warnsystem eingerichtet, mit dem bei akuten Angriffen auf oder schwerwiegenden Störungen in Informationsinfrastrukturen alle potenziell Betroffenen schnell und umfassend informiert werden können. So werden rechtzeitige Gegenmaßnahmen ermöglicht und Schäden in größerem Ausmaß vermieden.

Ziel 10: Reagieren bei IT-Sicherheitsvorfällen

Die schnelle Reaktion auf schwerwiegende Vorfälle wird durch das Krisenreaktionszentrum IT des Bundes sichergestellt. Das Krisenreaktionszentrum IT gibt Analysen und Bewertungen zu Vorfällen an alle relevanten Stellen weiter und koordiniert die Zusammenarbeit mit lokalen und brancheninternen Krisenmanagementorganisationen. Falls Maßnahmen bei Krisen mit Auswirkungen auf größere Teile der Bundesverwaltung getroffen werden müssen, bei denen lokale Verantwortung nicht mehr ausreicht, werden diese Maßnahmen durch ein Koordinierungsgremium der Ressorts abgestimmt und durch das Krisenreaktionszentrum IT veranlasst.

Voraussetzung für effiziente Reaktionen sind vorbereitete Notfallpläne sowie klare Vorgehensweisen für die Bewältigung von IT-Sicherheitsvorfällen. Die Bundesregierung fordert, dass diese Notfallpläne neben Regelungen für das Krisen- und Notfallmanagement in Unternehmen und Behörden für den lokalen Umgang mit IT-Sicherheitsvorfällen auch geeignete Schnittstellen zum nationalen Krisenmanagement umfassen.

4 Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

Um die nationalen Informationsinfrastrukturen langfristig zu schützen, benötigt Deutschland neben dem politischen Willen und der Bereitschaft aller Verantwortlichen zur Stärkung der IT-Sicherheit Fachkompetenz sowie vertrauenswürdige IT-Dienstleistungen und IT-Sicherheitsprodukte.

Ziel 11: Fördern vertrauenswürdiger und verlässlicher Informationstechnik

Die Bundesregierung stärkt die Entwicklung verlässlicher deutscher IT-Produkte und IT-Dienstleistungen sowie vertrauenswürdiger Informationstechnik in Deutschland, insbesondere Industriezweige wie die Kryptoindustrie. Ziel ist hier die stärkere Durchdringung des Marktes und der breite Einsatz von verlässlichen IT-Produkten.

Ziel 12: Ausbau nationaler IT-Sicherheitskompetenz

Die Bundesregierung wird das Know-how der deutschen IT-Sicherheitsdienstleistungsunternehmen nutzen, zu seiner Stärkung beitragen und damit die nationale IT-Sicherheitskompetenz fördern. Bereits bestehende Kompetenzen und Aufgaben des BSI werden im Zuge der Umsetzung dieses Nationalen Plans deutlich erweitert und durch vorhandenes Know-how anderer Ressorts ergänzt. Das BSI wird als die nationale IT-Sicherheitsbehörde die IT-Sicherheit in der Bundesverwaltung, in Großvorhaben des Bundes und in Kritischen Infrastrukturen aktiv als IT-Sicherheitsberater mitgestalten und dabei mit anderen wichtigen staatlichen Aufsichtsorganen, wie der Regulierungsbehörde für Telekommunikation und Post (Reg TP), zusammenarbeiten.

Ziel 13: IT-Sicherheitskompetenz in Schule und Ausbildung

Die Bundesregierung bringt ihr Know-how auf dem Gebiet der IT-Sicherheit ein, um den Stellenwert der IT-Sicherheit in der schulischen und beruflichen Ausbildung auf breiter Basis zu erhöhen und bei der Entwicklung neuer Berufsbilder und neuer Ausbildungsgänge entsprechend zu berücksichtigen. Informationsangebote für Bürgerinnen und Bürger, Schulen und Hochschulen, Wirtschaft und Verwaltung sowie die Sensibilisierung aller gesellschaftlichen Gruppen für IT-Sicherheitsbelange werden ausgebaut.

Ziel 14: Fördern von Forschung und Entwicklung

Die Bundesregierung unterstützt die nationale Grundlagenforschung, die Beteiligung deutscher Unternehmen und die Zusammenarbeit im Rahmen internationaler Forschungs- und Technologieprogramme, insbesondere im Hinblick auf das 7. Europäische Forschungsrahmenprogramm. Durch die Entwicklung innovativer Produkte wird die Verlässlichkeit der deutschen Informationsinfrastrukturen langfristig gesichert. Die Zusammenarbeit zwischen Wirtschaft und dem Bereich „Forschung und Entwicklung“ der Universitäten wird intensiviert.

Ziel 15: International Kooperationen ausbauen und Standards setzen

Bei der Erarbeitung von internationalen Standards zum Schutz der Informationsinfrastrukturen wird die Bundesregierung aktiv nationale Sicherheitsinteressen einbringen. Dazu wird die nationale ressort- und fachübergreifende Zusammenarbeit zur Vorbereitung entsprechender Normen, Standards und Gesetze verstärkt.

Gemeinsam mit europäischen Partnern werden vertrauenswürdige IT-Sicherheitslösungen entwickelt. Deutsche IT-Sicherheitsprodukte und IT-Sicherheitslösungen finden dabei angemessen Berücksichtigung.

Abkürzungen

BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
ENISA	European Network and Information Security Agency
EU	Europäische Union
IT	Informationstechnik
ITSEC	Information Technology Security Evaluation Criteria
KRITIS	Kritische Infrastrukturen
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
PC	Personal Computer
PGP	Pretty Good Privacy
Reg TP	Regulierungsbehörde für Telekommunikation und Post
S/MIME	Secure Multipurpose Internet Mail Extension

Glossar

(Erläuterungen wesentlicher Begriffe für den Nationalen Plan zum Schutz der Informationsinfrastrukturen / Begriffsverständnis in diesem Dokument)

Informationsinfrastruktur

Die Gesamtheit der IT-Anteile einer Infrastruktur wird als Informationsinfrastruktur bezeichnet.

Interdependenzen

Eine Interdependenz ist die gegenseitige vollständige oder partielle Abhängigkeit mehrerer Güter oder Dienstleistungen.

IT-Sicherheit

IT-Sicherheit ist der Zustand, der die Verfügbarkeit, die Integrität, die Verbindlichkeit und die Vertraulichkeit von Informationen beim Einsatz von IT gewährleistet.

Dabei ist

- Verfügbarkeit der Zustand, der die erforderliche Nutzbarkeit von Informationen sowie IT-Systemen und -Komponenten sicherstellt;
- Integrität der Zustand, der unbefugte und unzulässige Veränderungen von Informationen und an IT-Systemen oder -Komponenten ausschließt;
- Verbindlichkeit der Zustand, in dem geforderte oder zugesicherte Eigenschaften oder Merkmale von Informationen und Übertragungsstrecken sowohl für die Nutzer verbindlich feststellbar als auch Dritten gegenüber beweisbar sind;
- Vertraulichkeit der Zustand, der unbefugte Informationsgewinnung und -beschaffung ausschließt.

IT-Sicherheitsprodukte

IT-Sicherheitsprodukte sind Produkte, die zur Erfüllung der Anforderungen von IT-Sicherheit eingesetzt werden. Beispiele sind Virenscanner, Firewalls, Public-Key-Infrastrukturen (PKI), Intrusion-Detection-Systeme (IDS), Plug-ins für die Datenverschlüsselung in E-Mail-Clients z. B. für PGP oder S/MIME. IT-Sicherheitsprodukte dienen dazu, Anwendungen, Prozesse, Systeme und/oder Daten besser abzusichern, als dies ohne Einsatz des IT-Sicherheitsprodukts der Fall wäre.

Kritische Infrastrukturen

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten.

Bei der Diskussion in Deutschland werden folgende Infrastrukturbereiche als Kritische Infrastrukturen betrachtet (siehe auch www.bsi.bund.de/fachthem/kritis):

- Transport und Verkehr
- Energie (Elektrizität, Öl und Gas)
- Gefahrenstoffe (Chemie- und Biostoffe, Gefahrguttransporte, Rüstungsindustrie)
- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen
- Versorgung (Gesundheits-, Notfall- und Rettungswesen, Katastrophenschutz, Lebensmittel- und Wasserversorgung, Entsorgung)
- Behörden, Verwaltung und Justiz (einschließlich Polizei, Zoll und Bundeswehr)
- Sonstiges (Medien, Großforschungseinrichtungen sowie herausragende oder symbolträchtige Bauwerke, Kulturgut)

Sichere IT-Produkte

Im Unterschied zu IT-Sicherheitsprodukten ist es ein Merkmal sicherer IT-Produkte, die IT-Sicherheit bereits in sich zu tragen. Die Sicherheit eines Produktes kann durch Evaluation nach IT-Sicherheitskriterien wie ITSEC oder Common Criteria nachgewiesen und mit einem IT-Sicherheitszertifikat zertifiziert werden. Zur Entwicklung sicherer IT-Produkte (Hardware und Software) werden besondere Entwicklungskonzepte verwendet, um die Komplexität und die Wahrscheinlichkeit von Schwachstellen möglichst gering zu halten.

Sichere IT-Systeme

IT-Systeme setzen sich aus IT-Produkten und -Komponenten zusammen und werden in konkreten baulichen Umgebungen mit definierten organisatorischen und personellen Rahmenbedingungen eingesetzt. Sichere IT-Systeme zeichnet aus, dass das Sicherheitsmanagement und die für die Sicherheit erforderlichen infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen umgesetzt, durch eine unabhängige Stelle geprüft und mittels eines Systemsicherheits-Zertifikats bestätigt sind.

Verlässlichkeit

Systeme, Anwendungen oder Dienstleistungen sind verlässlich, wenn sie ihre „Leistung" in der geforderten Art und Weise (z. B. Erfüllen von Quality-of-Service-Anforderungen) erbringen und nicht in (aus Sicht der Nutzung) unakzeptabler Weise vom erwarteten Verhalten abweichen. Verlässlichkeit wird dabei als Überbegriff verstanden, der (mindestens) folgende Begriffe umschließt:

- Verfügbarkeit oder Availability (d. h. ständige Nutzbarkeit)
- Zuverlässigkeit oder Reliability (d. h. Kontinuität der Funktion)
- Safety (d. h. Betriebs- und Anwendungssicherheit ohne nachhaltige oder gar katastrophale Auswirkungen auf Personen oder Umwelt)
- Vertraulichkeit oder Confidentiality (d. h. Ausschluss nichtautorisierter Weitergabe von Information)
- Integrität oder Integrity (d. h. Verhinderung nichtautorisierter Änderung oder Beseitigung von Daten)
- Wartbarkeit oder Maintainability (d. h. Gewährleistung der Aufrechterhaltung/Wiederherstellung durch Reparaturen/Möglichkeit zur Weiterentwicklung)

Nationaler Plan

zum Schutz der
Informationsinfrastrukturen

Herausgeber:

Bundesministerium des Innern

IT-Stab, Referat IT 3

Alt-Moabit 101D | 10559 Berlin

Redaktion:

Bundesministerium des Innern

IT-Stab, Referat IT 3

Gesamtgestaltung & Produktion:

Zucker.Kommunikation, Berlin

Druck:

Pinguin Druck, Berlin

Bilder:

Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Auflage:

1.000 Exemplare

Stand:

Juli 2005