Bundesamt
für Sicherheit in der
Informationstechnik

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 D

Stellungnahme für die Anhörung des Innenausschusses
zum Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

am 20. April 2015

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

1. Ausgangslage und Herausforderungen

Die millionenfachen Identitätsdiebstähle von Bürgern, Meldungen zu Cyber-Angriffen auf Wirtschaftsunternehmen und nicht zuletzt die Snowden-Enthüllungen haben weit über die Expertenebene hinaus das Bewusstsein der Verletzbarkeit im Cyber-Raum deutlich gemacht. Insbesondere wird deutlich, dass alle Gesellschaftsgruppen hiervon betroffen sind.

Um zu verstehen, welchen Herausforderungen wir gegenüberstehen, ist es wichtig zu wissen, welche Rolle die Informationstechnik (IT) heutzutage spielt:

1. Während IT bis vor wenigen Jahren von den zur Produktion eingesetzten Maschinen klar abgrenzbar war, durchdringt sie heute alles. Sie findet sich gleichermaßen in allen möglichen Haushaltsgegenständen wie auch in industriellen Prozessen und Anlagen wieder - sie ist allgegenwärtig.
2. Daneben geht der Trend dahin, alle IT-Systeme zu vernetzen, um Komfort- oder Produktivitätsgewinne zu erzielen. Es wird das Ziel verfolgt, möglichst viele Informationen nutzbar zu machen. So werden beispielsweise die „digital-ertüchtigten“ Systeme eines Unternehmens wie etwa Maschinen, Sensoren und Feldgeräte in den Produktionsanlagen, aber auch Systeme in Marketing, Vertrieb oder Einkauf untereinander sowie nach innen und außen vernetzt.
3. Unter dem Stichwort Internet der Dinge sind bereits heute viele Hausgeräte, Gebäudesteuerungen, Gefahren- und Brandmeldeanlagen, Verkehrsleitsysteme und Automobile mit dem Internet verbunden.

   Die Vision ist im urbanen Bereich mit „Smart City“ und im häuslichen Bereich mit „Smart Home“ bereits gegenwärtig und greifbar. Die Digitalisierung von ursprünglich physischen Systemen führt zu einem Anstieg der Komplexität dieser Systeme und damit zugleich zu größeren Herausforderungen bei der Sicherheit. Während beispielsweise bisher im Bereich der Stromversorgung primär elektrotechnische Aspekte eine Rolle spielten, kommen bei intelligenten Energienetzen die Fragen

der Zuverlässigkeit von IT hinzu. Eine intelligente Netzsteuerung ist nicht nur auf die elektrische Funktionsfähigkeit der Netze angewiesen, sondern ebenso auf die Integrität und Verfügbarkeit der zur Netzsteuerung notwendigen Daten(verarbeitung).

2. Gefährdungslage

Neben dem Wissen über Technologie und Technologieentwicklung ist das Kennen der Gefährdungslage unerlässlich. Denn technologische Entwicklung und Gefährdungslage sind im Zusammenhang zu betrachten.

Das BSI hat im Dezember 2014 erstmals einen Bericht zur Lage der IT-Sicherheit in Deutschland[1] herausgegeben, der Auskunft über die Ursachen von Cyber-Angriffen, über Angriffsmittel und -methoden gibt. Eine wesentliche Schlussfolgerung ist: Das Internet ist als Plattform für Angreifer sehr attraktiv, denn der Aufwand für einen Angriff ist gering. Es reichen ein Laptop und ein Internetanschluss. Zudem existiert ein florierender globaler Markt mit „Trojanerkoffern“ und Maleware-as-a-Service-Angeboten. Das Entdeckungsrisiko ist gering, da das dezentral und offen gestaltete Internet für den Angreifer vielfältige Tarnmöglichkeiten bietet. Außerdem erweitert sich die Zahl der möglichen Angriffsziele mit der fortlaufenden technologischen Weiterentwicklung. Ein weiterer Grund für die Attraktivität des Internets als Angriffsplattform ist die Tatsache, dass Schwachstellen in komplexer Software systemimmanent sind. Sie sind der häufigste Ausgangspunkt für die Entwicklung von Cyber-Angriffsmitteln in Form von Schadprogrammen.

Die wesentlichen Fakten der Bedrohungslage im Jahr 2014 stellen sich wie folgt dar:

Schadprogramme

Die Gesamtzahl der detektierten PC-basierten Schwachstellen liegt bei mehr als 250 Millionen und steigt täglich um ca. 300.000. Sie betreffen primär das führende Desktop-Betriebssystem. Dieses wird jedoch nicht nur auf Arbeitsplatzsystemen eingesetzt, sondern ebenso auf Serversystemen und in industriellen Steuerungsanlagen –

1 Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014.

teilweise noch mit einem seit Jahren veralteten Softwarestand, dessen Schwachstellen durch Updates nicht mehr beseitigt werden.

Die Anzahl der Schadprogramme für Smartphones und Tablets liegt bei mindestens drei Millionen, hiervon sind ca. 98 Prozent dem führenden Betriebssystem zuzuordnen.

Botnetze

In Deutschland sind mehr als eine Millionen Internetrechner Teil von Botnetzen. Die Nachlässigkeit der Nutzer beim Einspielen von Patches gegen Schwachstellen begünstigt die Chancen der Angreifer, die Rechner entsprechend zu übernehmen.

DDoS

In 2014 gab es allein in Deutschland über 32.000 DDoS-Angriffe. Zu ca. einem Drittel waren die Web-Seiten von Unternehmen Ziel der DDoS-Angriffe. Zu ca. einem Viertel war mit gravierender Wirkung die Netzinfrastruktur von DDoS-Angriffen betroffen. Zur Durchführung der Angriffe missbrauchten die Täter auch viele falsch konfigurierte Serversysteme unwissender Anwender.

APT

Neben den bekannten und weit verbreiteten Angriffsmethoden wie beispielsweise Spam, Schadsoftware oder Drive-by-Exploits, sind die sogenannten Advanced Persistent Threats (APT) von besonderer Bedeutung. Sie sind die hochwertigen komplexen Angriffe, die schwer detektierbar sind und möglichst dauerhaft Wirkung entfalten sollen. APT-Angriffe zeichnen sich durch sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus. Problematisch ist, dass klassische Antivirenprogramme eine immer geringer werdende Erkennungsrate insbesondere bei hochwertigen Angriffen haben.

3. Handlungsbedarf

Die technologische Entwicklungen und die damit einhergehenden Risiken sind inzwischen nicht nur eine technologische und organisatorische, sondern auch eine

gesellschaftspolitische Herausforderung. Für die Bundesverwaltung hat der Gesetzgeber bereits 2009 wichtige Voraussetzungen geschaffen, um den Bedrohungen für die Bundesverwaltung adäquat zu begegnen und der zunehmenden Bedeutung der Informations- und Kommunikationstechnik in der Verwaltung Rechnung zu tragen. Die Meldepflicht der Behörden gegenüber dem BSI sowie die auf der Grundlage von § 5 BSIG vorgenommenen Maßnahmen zur Erkennung und Abwehr von Gefahren für die Kommunikationstechnik des Bundes haben bereits zu einer signifikanten Steigerung der IT-Sicherheit in der Bundesverwaltung beigetragen.

Die steigende Abhängigkeit der Wirtschaft von IT-Prozessen verlangt auch ihr Maßnahmen ab. Bereits heute bestehen vielfältige Kooperationen zwischen Unternehmen und Staat, um die IT-Sicherheit zu fördern. So sind z.B. die Allianz für Cyber-Sicherheit und der Umsetzungsplan KRITIS (UP KRITIS) Plattformen der Zusammenarbeit, in denen auf freiwilliger Basis relevante Informationen, Erfahrungen und Know-How zwischen Staat und Wirtschaft ausgetauscht werden.

Die technologischen Entwicklungen einerseits und die damit einhergehende, weitreichende Bedrohungslage andererseits zeigen jedoch, dass ein regulativer Rahmen für die Zusammenarbeit erforderlich ist. Dies gilt insbesondere für die Wirtschaftsakteure, die wegen der möglichen weitreichenden gesellschaftlichen Folgen eines Ausfalls oder einer Beeinträchtigung der von ihnen angebotenen Leistungen eine besondere Verantwortung für das Gemeinwohl tragen. Dieses Erfordernis wird in § 8a bis § 8d des Gesetzentwurfs aufgegriffen. Betreiber Kritischer Infrastrukturen werden nach § 8a verpflichtet, ein Mindestniveau an IT-Sicherheit für die Systeme, Komponenten und Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Durch die Berücksichtigung des Standes der Technik ist sichergestellt, dass zum einen die zu ergreifenden Maßnahmen für die Betreiber verhältnismäßig bleiben, zum anderen aber auch der Einsatz von hinreichend aktuellen Systemen vorgeschrieben wird. Die Branchen haben die Möglichkeit, durch branchenspezifische Sicherheitsstandards den Stand der Technik zu konkretisieren.

Dadurch kann zum einen das branchenspezifische Know-How der Betreiber einbezogen werden; nur diese kennen die zur Erbringung der Dienstleistungen eingesetzten Techniken und Prozesse im Detail. Zum anderen wird den Betreibern die alle zwei Jahre erforderliche Nachweisführung, dass der Stand der Technik eingehalten ist, durch einen anerkannten Branchenstandard vereinfacht.

Daneben ermöglicht die in § 8b verankerte Meldepflicht für Betreiber Kritischer Infrastrukturen dem BSI nicht nur die Erstellung verlässlicher Lagebilder. Insbesondere erwarte ich, dass das BSI durch die Meldepflicht auch Angriffe frühzeitig erkennen, präventive Schutzmaßnahmen ermitteln und diese Erkenntnisse anderen Betreibern aber auch anderen Anwendern von IT rechtzeitig zur Verfügung stellen kann. Durch dieses „Geben und Nehmen“ zwischen den Akteuren wird es leichter werden, neuen Gefährdungen rechtzeitig entgegenzutreten.

Das BSI wird gemäß Gesetz den vertraulichen Umgang mit den Daten der Betreiber Kritischer Infrastrukturen sicherstellen. Aus der langjährigen Zusammenarbeit mit Unternehmen weiß das BSI um den Stellenwert von Vertrauen, wenn es um IT-Sicherheit geht.

Die in § 7 BSIG des Gesetzentwurfes vorgesehene Änderung stellt sicher, dass das BSI Dritte zur Durchführung der Warnung der Betroffenen einbeziehen und somit die Betroffenen selbst mit seiner Warnung erreichen kann. Eine unmittelbare Warnung ist oftmals nicht möglich, da dem BSI zwar die missbräuchlichen Daten (z.B. IP-Adressen oder Bankverbindungen) vorliegen, diese aber nicht zugeordnet werden können. Bei IP-Adressen können dies die Provider, bei Bankdaten die Banken sein.

Zur Erfüllung seiner präventiven Aufgaben benötigt das BSI die in § 7a des Gesetzentwurfes vorgesehene Befugnis, Produkte und Systeme unabhängig von der Zustimmung des Herstellers und unter Anwendung aller nach dem Stand der Technik notwendigen Untersuchungsmethoden auf ihre Sicherheit hin zu untersuchen, um

mögliche Sicherheitsrisiken bei kritischen Infrastrukturen und in der Bundesverwaltung beurteilen zu können. Bisher sind Produktanalysen aufgrund urheber-, wettbewerbs- oder strafrechtlicher Regelungen unzulässig, obwohl die Notwendigkeit, Produkte auf Sicherheitsrisiken zu untersuchen, größer ist als je zuvor.

Da die aus den Untersuchungen gewonnenen Ergebnisse den Markt beeinflussen können, wird vor deren Veröffentlichung stets abgewogen, ob der damit verbundene Eingriff in die Tätigkeit der Unternehmen gerechtfertigt ist. Schutzmaßnahmen zu Gunsten der Unternehmen, wie die Einbindung vor der Veröffentlichung und die Möglichkeit zur Stellungnahme, sieht das Gesetz vor. Es greift somit das mit der letzten Gesetzesänderung 2009 eingeführte und seit dem bewährte Verfahren zur Warnung auf.

Telemediengesetz

Als Präsident des BSI befürworte ich ausdrücklich, dass auch Telemediendiensteanbieter künftig einen Beitrag zur Schaffung von IT-Sicherheit leisten sollen. Ungesicherte Telemedienangebote sind oft der Grund dafür, dass z.B. ein Webserver als Angriffswerkzeug missbraucht werden kann oder Täter an die personenbezogenen Daten der Kunden eines Telemedienangebotes gelangen – etwa weil keine hinreichend sicheren Authentifizierungsmaßnahmen eingesetzt wurden.

Telekommunikationsgesetz

Die im TKG vorgesehene Pflicht der TK-Anbieter, ihre Nutzer auf Störungen auf deren Systemen hinzuweisen, ist aus Sicht des BSI neben gemeinsamen Initiativen mit der Wirtschaft eine wichtige und notwendige Maßnahme zur Förderung der IT-Sicherheit. Wenn TK-Anbieter z.B. weil sie sogenannte Honey-Pot-Systeme betreiben, wissen, dass ihre Kunden Teil eines Botnetzes sind, sollten sie ihrer Verantwortung nachkommen und diese oftmals ahnungslosen Nutzer auch informieren. Nur so kann verhindert werden, dass die Nutzer oder Dritte weitere Schäden erleiden, etwa durch den Abfluss von sensiblen personenbezogenen Daten oder die unbeabsichtigte Teilnahme an Angriffen.

Da die TK-Anbieter auch den direkten Kontakt zu ihren Kunden haben, sind sie näher am Nutzer. Daher hält das BSI die Pflicht der Anbieter, ihre Kunden auf Werkzeuge zur Erkennung und Beseitigung von Störungen hinweisen zu müssen, für zweckmäßig und notwendig. Solch zielgerichtete Hinweise sind effektiver und erreichen mehr Nutzer als allgemeine Informationen im Netz, die die Nutzer erst einmal suchen und finden müssen. Gerade technisch weniger versierten und damit leicht angreifbaren Nutzern von IT wird die Absicherung dadurch erleichtert. Insofern stellt die Regelung eine sinnvolle Ergänzung zu bestehenden Informationsangeboten wie z.B. BSI-für-Bürger oder botfrei.de dar.

4. Fazit

Die Dynamik der IT-Entwicklung und der Gefährdungen wird uns auch in Zukunft vor weitere Herausforderungen stellen. Der Gesetzentwurf stellt aus meiner Sicht als BSI-Präsident einen wichtigen Schritt zur Verbesserung der IT-Sicherheit sowohl für Kritische Infrastrukturen wie auch für Bürgerinnen und Bürgern als Internetnutzer in Deutschland dar. Die neuen Aufgaben wird das BSI aktiv angehen.