Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)12

Schriftliche Stellungnahme
zum Fragenkatalog für das öffentliche Fachgespräch
des Ausschusses Digitale Agenda des Deutschen Bundestages

zum Thema IT-Sicherheit
am Mittwoch, dem 7. Mai 2014

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Fragenkatalog für das öffentliche Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema „IT Sicherheit“ am 7. Mai 2014

Antworten des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Frage 1:
Der Ausspähskandal durch ausländische Nachrichtendienste, die zahlreichen Fälle von Identitätsklau und zuletzt die OpenSSL-Sicherheitslücke haben die Verletzlichkeit der digitalen Infrastrukturen offensichtlich gemacht. Inwieweit ist eine sichere Kommunikation über die bestehenden Infrastrukturen aus Ihrer Sicht heute überhaupt noch möglich? Welche Erkenntnisse gibt es zu den Angriffsmöglichkeiten und Kompromittierungen der Informations- und Kommunikationsinfrastruktur (Hard- und Software, Netzwerktechnik, Normen und Standards etc.)? Welche Maßnahmen (a) müssen ergriffen werden, um den Grundrechtsschutz und die Vertraulichkeit der Kommunikation wieder sicherzustellen?

Antwort:
Aufgrund der Quantität und Qualität der unterschiedlichen Angriffsmöglichkeiten im Cyberraum muss im Allgemeinen von einer kritischen Gefährdungslage ausgegangen werden. Technische Standardschutzmaßnahmen stellen bereits ein wirkungsvolles Instrument dar, um die damit verbundenen Risiken zu minimieren. Kommunikation kann insbesondere durch den Einsatz vertrauenswürdiger Kryptographie, den stärksten IT-Sicherheitsmechanismus, gesichert werden. Gegen Identitätsdiebstähle können beispielsweise Zwei-Faktor-Authentifizierungen für sichere Identitäten (wie z.B. beim neuen Personalausweis) verwendet werden. Die Verfügbarkeit von Daten lässt sich insbesondere durch den Einsatz von Redundanzen und Back-Up-Systemen sicherstellen. Mit Blick auf die Zielgruppe der Bürgerinnen und Bürger stellen zudem bereits grundlegende Maßnahmen wie das regelmäßige Einspielen von Updates oder die Verwendung einer regelmäßig aktualisierten Anti-Viren-Software ein zentrales Element zur Erhöhung des Sicherheitsniveaus dar. Besonders gefährdete „Hochwert-Ziele“ in Behörden und Wirtschaft benötigen jedoch weitergehende, speziell auf die Bedrohungslage abgestimmte hochwertige Schutzmaßnahmen.

Das BSI verfolgt einen breiten Handlungsansatz, der neben der Unterstützung gesetzgeberischer Maßnahmen insbesondere kooperative Elemente wie z.B. Handlungsempfehlungen und Angebote für unterschiedliche Zielgruppen umfasst. Die Regierungsparteien haben in ihrem Koalitionsvertrag verschiedene Maßnahmen zur Förderung der IT-Sicherheit angekündigt, wozu u.a. auch gesetzgeberische Maßnahmen zählen. Als nachgeordnete Behörde unterstützt das BSI mit seinem technischen Know-how und seiner Erfahrung die Bundesregierung bei ihren gesetzgeberischen Überlegungen. Von zentraler Bedeutung aus BSI-Sicht ist in diesem Zusammenhang das im Koalitionsvertrag angekündigte IT-Sicherheitsgesetz, das „verbindliche Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen“ sowie eine „Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle“ enthalten soll. Das BSI befürwortet ein entsprechendes IT-Sicherheitsgesetz.

Frage 2:
Welche Abwehrmöglichkeiten (Hard- und Software) stehen privaten Nutzerinnen und Nutzern, Unternehmen, Behörden und Verfassungsorganen heute zur Verfügung, um die eigene Datensicherheit in kompromittierten Kommunikationsinfrastrukturen zu erhöhen und welche Möglichkeiten gibt es für den Gesetzgeber, diese auszubauen?

Antwort:
Die Herausforderung in kompromittierten Kommunikationsinfrastrukturen besteht zum einen darin, dass über das IT-System Daten, Anwendungen und Prozesse selbst angegriffen und kompromittiert werden können, und zum anderen darin, dass die Kommunikation über diese unsicheren

Infrastrukturen belauscht und manipuliert werden kann. Durch die Umsetzung von grundlegenden technischen Sicherheitsmaßnahmen, wie sie beispielsweise in den IT-Grundschutz-Katalogen aufgeführt sind, können nach Einschätzung des BSI bereits rund 80 Prozent der Standard-bedrohungen abgewehrt werden. Darüber hinaus ist es aus Sicht der IT-Sicherheit von zentraler Bedeutung, vertrauenswürdige Informationstechnik, z.B. vertrauenswürdige Kryptogeräte, für alle Anwenderkreise verfügbar zu machen und diese in die Lage zu versetzen, IT-Sicherheits-maßnahmen eigenverantwortlich umzusetzen. Neben seiner Kernaufgabe als zentraler IT-Sicherheitsdienstleister der Bundesverwaltung unterstützt das BSI durch Kooperations- und Informationsangebote wie die Allia

.

Frage 3:
Welche Maßnahmen können Anbieter/Betreiber von Kommunikationsdiensten und -infrastruktur ergreifen und welche Möglichkeiten gibt es für den Gesetzgeber, sie hierbei zu unterstützen?

Antwort
Anbieter/Betreiber von Kommunikationsdiensten und -infrastrukturen sind nach TKG und TMG verpflichtet, durch entsprechende Maßnahmen das Fernmeldegeheimnis und den Datenschutz zu gewährleisten. Die BNetzA gibt dazu im Benehmen mit dem BSI und der BfDI einen Sicherheitskatalog als Grundlage für die Sicherheitskonzepte heraus. Die Sicherheitskonzepte können von der BNetzA geprüft werden, sehr schwerwiegende Sicherheitsvorfälle müssen gemeldet werden, von der BNetzA kann zudem eine Untersuchung veranlasst werden. Vorfälle im Bereich des Datenschutzes müssen den zuständigen Datenschutzbehörden gemeldet werden. Eine Untersuchung obliegt den Datenschutzbehörden.

Viele Telekommunikationsbetreiber versuchen darüber hinaus, ihre Kunden bei Fragen der IT-Sicherheit zu unterstützen. Dazu werden Kunden z.B. gewarnt, wenn Informationen über Sicherheitsvorfälle bei Kundensystemen vorliegen. Darüber hinaus haben die meisten TK-Anbieter auch kostenpflichtige Sicherheitslösungen im Produkt-Portfolio. Zur Vollständigkeit der Abwehr aktueller Angriffe müsste das Portfolio in vielen Fällen aber noch ergänzt werden.

Frage 4:
Inwieweit kann die Sicherheit bei der Nutzung von Kommunikationsdiensten wie De-Mail, E-Mail und anderen Messaging-Diensten weiter erhöht werden? Wie werden die bisherigen gesetzlichen Grundlagen hierzu eingeschätzt? Welchen Beitrag können öffentliche Stellen (z. B. Bundesdruckerei, Bundesamt für die Sicherheit in der Informationstechnik) leisten, wenn diese Zertifikate zur Verschlüsselung zur Verfügung stellen würden?

Antwort:
Nach Inkrafttreten des De-Mail-Gesetzes im Jahr 2011 und der daran anschließenden Akkredi-tierung von De-Mail-Diensteanbietern steht einem breiten Anwenderkreis mit der De-Mail ein Angebot zur Verfügung, durch das der verbindliche und vertrauliche Versand elektronischer Nachrichten deutlich einfacher geworden ist. Eine weitere Erhöhung der Sicherheit ist durch eine Ende-zu-Ende-Verschlüsselung der Nachrichten zu erreichen. Hierzu bieten De-Mail-Angebote z.B. die Hinterlegung des benötigten Schlüsselmaterials in einem Verzeichnisdienst an, was einen komfortablen Zugriff auf die öffentlichen Schlüssel der Kommunikationspartner ermöglicht. Zur Erhöhung der Vertrauenswürdigkeit der verwendeten Schlüssel gibt es derzeit Aktivitäten des BSI zur Schaffung eines über das Internet erreichbaren Dienstes zur Schlüsselzertifizierung mit einer starken Authentisierung des Nutzers durch den Einsatz der eID-Funktion des Personala
-Mail verdeutlicht zudem, dass der Staat durch die Schaffung von Rahmen-bedingungen die Herausbildung von Standards und Normen fördern kann, auf deren Grundlage eine vertrauensfördernde Prüfung und Zertifizierung der Angebote erfolgt.

Frage 5:
Wie können Privatpersonen sowie klein- und mittelständische Unternehmen zur stärkeren Nutzung sicherer Kommunikationsverbindungen und Verschlüsselungsverfahren bewegt werden? Besteht hier politischer Handlungsbedarf?

Antwort:
Privatanwender von IT sowie klein- und mittelständische Unternehmen benötigen zielgerichtete Informationen über die Gefährdungen im Cyberraum sowie die verfügbaren Schutzmöglichkeiten, die sie selbst ergreifen können (Hilfe zur Selbsthilfe) oder die ihnen von Dritten (z.B. von Internet- und Dienste-Providern, IT-Unternehmen etc.) angeboten werden. Dies betrifft insbesondere die Möglichkeiten, Daten durch Verschlüsselung zu schützen. Handlungsbedarf besteht in diesem Zusammenhang hinsichtlich der Initiierung von Vorhaben zur Entwicklung und Bereitstellung einfach anwendbarer Ver- und Entschlüsselungswerkzeuge wie beispielsweise Verschlüsselungs-Apps für die mobile Internetnutzung durch Smartphones und Tablets.

Frage 6:
Inwieweit besteht politischer Handlungsbedarf zur Verbesserung der Datensicherheit und des Datenschutzes bei neuen Kommunikationsdiensten wie mobilen Instant-Messengern (WhatsApp etc.)?

Antwort:
Die Anbieter der populären Kommunikationsdienste (z.B. Whatsapp, Threema, Skype etc.) sind fast ausschließlich Unternehmen, deren Firmensitz außerhalb Deutschlands oder der EU liegt, sodass die Einflussmöglichkeiten auf die Ausgestaltung der Angebote mitunter begrenzt sind. Wo die Möglichkeit einer Auswahl zwischen verschiedenen Angeboten oder Diensten gegeben ist, ist es aus der Perspektive der IT-Sicherheit jedoch wünschenswert, dass die Nutzerinnen und Nutzer bei der Auswahl eines Angebotes oder Dienstes auf ein möglichst hohes Niveau an Datensicherheit achten. Auch wäre die verstärkte Entwicklung von Open-Source-Angeboten, die durch Dritte geprüft oder zertifiziert werden können, wünschenswert, sodass eine größtmögliche Transparenz hinsichtlich des gebotenen Niveaus an Datensicherheit gewährleistet wird.

Frage 7:
Welchen Beitrag können Vorschläge wie Deutschland-Mail oder Schengen-Routing tatsächlich leisten und müsste nicht die zentrale Maßnahme sein, schnell vertrauenswürdige und wirksame Ende-zu-Ende-Verschlüsselungen durchzusetzen? Welche Maßnahmen müssen ergriffen werden, um hierfür die jeweiligen Systemumgebungen abzusichern und zugleich die Handhabbarkeit zu erleichtern? Inwieweit sollten Telekommunikationsanbieter zu einer Transportverschlüsselung verpflichtet werden?

Antwort
Die an der Initiative “E-Mail Made in Germany” teilnehmenden Provider verschlüsseln E-Mails auf dem Transportweg. Auf den Servern der Anbieter liegen die E-Mails dagegen im Klartext vor. Das ermöglicht den Anbietern, E-Mail-Postfächer auf Schadprogramme zu untersuchen und die betroffenen Kunden zu warnen. Eine Ende-zu-Ende-Verschlüsselung muss hierbei durch den Kunden selbst angestoßen werden. Die Lösung des Anbieters darf einer solchen Ende-zu-Ende-Verschlüsselung zumindest nicht entgegen stehen.

Frage 8:
Wo sehen Sie gesetzgeberischen Handlungsbedarf (z. B. im Strafrecht, aber auch im TKG, im TMG oder auch in den Sicherheitsgesetzen), um den Grundrechtsschutz und den Schutz der

Vertraulichkeit der Kommunikation sicherzustellen?

Antwort:
Auf die Antwort zu Frage 1 wird verwiesen.

Frage 9:
Welchen Beitrag kann das Bundesamt für die Sicherheit in der Informationstechnik (BSI) zur Erhöhung der IT-Sicherheit und zur Unterstützung des Selbstschutzes der Bürgerinnen und Bürger sowie der Unternehmen leisten, welche Rahmenbedingungen müssen hierfür erweitert und welche personellen sowie materiellen Grundlagen geschaffen werden? Inwieweit müssen welche Kapazitäten des BSI und auch des Cyber-Abwehrzentrums ausgebaut werden? Wie kann das BSI in seiner Rolle als neutraler Berater der Bürgerinnen und Bürger gestärkt werden? Inwieweit ist eine effektive Koordinierung mit dem Bundesministerium des Innern und den anderen Ressorts der Bundesregierung gesichert?

Antwort:
Als nationale IT-Sicherheitsbehörde verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die IT-Sicherheit in Deutschland durch auf Prävention ausgerichtete Maßnahmen und Angebote zu fördern. Aus Sicht der IT-Sicherheit ist es von zentraler Bedeutung, vertrauenswürdige Informationstechnik für alle Anwenderkreise verfügbar zu machen und diese in die Lage zu versetzen, IT-Sicherheitsmaßnahmen eigenverantwortlich umzusetzen. Neben seiner Kernaufgabe als zentraler IT-Sicherheitsdienstleister der Bundesverwaltung unterstützt das BSI durch Kooperations- und Informationsangebote wie die Allianz für Cybersicherheit oder BSI für Bürger auch Wirtschaft und Bürger bei der Umsetzung präventiver Maßnahmen. Mit dem fachaufsichtführenden Bundesministerium des Innern sowie anderen Ressorts der Bundesregierung besteht eine vertrauensvolle und intensive Kooperation, die ständig weiterentwickelt wird. Um den angesichts einer kritischen Gefährdungslage im Cyberraum und der fortschreitenden Digitalisierung der Gesellschaft ansteigenden Beratungsbedarf der Zielgruppen des BSI abdecken zu können, ist eine weitere Verbesserung der Ressourcenausstattung des BSI erforderlich. Das BSI begrüßt in diesem Zusammenhang das im Koalitionsvertrag formulierte Ziel, die Kapazitäten des BSI sowie des Cyber-Abwehrzentrums auszubauen.

Frage 10:
Die gravierende Sicherheitslücke Heartbleed in OpenSSL ist auch ein Beleg dafür, welche Folgen es hat, wenn derart zentrale Funktionalitäten nicht unabhängig überprüft werden. Wie können beispielsweise angemessene IT-Sicherheitsaudits für Open-Source-Security-Software ermöglicht werden und wie können das BSI oder andere, auch nicht-staatliche Stellen, derartige Audits unterstützen?

Antwort:
Die mit freier Software (Open-Source-Software) verbundene Transparenz stellt eine wesentliche Voraussetzung für die Überprüfbarkeit und Zertifizierbarkeit von Software dar, die eine Bewertung der Vertrauenswürdigkeit von Software ermöglicht. Eine vollständige Auditierung aller wichtigen Open-Source-Produkte mit Sicherheitsrelevanz ist keine allein durch das BSI leistbare Aufgabe. Das BSI führt jedoch zielgerichtet projektbezogene Sicherheitsuntersuchungen durch und stellt dem Open-Source-Ansatz folgend die Projektergebnisse der Öffentlichkeit zur Verfügung.

Zu Frage 11:
Sehen Sie die Vorschläge der EU-Datenschutzgrundverordnung als ausreichend an, um ausländische Unternehmen (Facebook, Google, WhatsApp etc.), die in Europa ihre Dienste anbieten, zur Wahrung der europäischen Datenschutzgrundsätze zu verpflichten oder wo besteht hier aus Ihrer Sicht noch Handlungsbedarf? Welche Möglichkeiten bestehen, europäische Bürgerinnen und Bürger

bei der Nutzung entsprechender Angebote vor dem Ausspähen durch ausländische Dienste zu schützen? Wie schätzen Sie weitere EU-Legislativen (z. B. Die Cybercrime-Richtlinie) diesbezüglich ein?

Antwort:
Das BSI begrüßt das Ziel, zu einer gemeinsamen europäischen Datenschutzgrundverordnung zu gelangen. Zu den vorgesehenen Regelungsinhalten zählt dabei auch ein einheitliches Mindestniveau hinsichtlich der Sicherheit der Verarbeitung personenbezogener Daten. Der in Deutschland vorherrschende hohe Anspruch an die Datensicherheit sollte in diesem Zusammenhang erhalten bleiben.

Mit Blick auf die weiteren aktuellen EU-Rechtsetzungsverfahren ist für das BSI als zivile und auf Prävention ausgerichtete IT-Sicherheitsbehörde insbesondere der sich im Gesetzgebungsverfahren befindliche NIS-Richtlinienentwurf von Relevanz (Vorschlag für eine EU-Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS) in der Union, KOM(2013)48 vom 07.02.2013). Der Richtlinienentwurf dient der Erhöhung der Netz- und Informationssicherheit im Wesentlichen bei institutionellen Anwendern und Anbietern von IT-Dienstleistungen (z.B. den Betreibern kritischer Infrastrukturen), nicht jedoch bei Bürgerinnen und Bürgern. In diesem Kontext unterstützt das BSI a
(Ergebnis der ersten Lesung vom 13.03.2014), nach dem die für NIS zuständige Behörde in einem Mitgliedstaat eine zivile Behörde und kein Nachrichtendienst sein sollte. Aus Sicht des BSI ist die Netz- und Informationssicherheit ein eigenständiges Aufgabengebiet. Die Trennung von anderen Aufgaben (Strafverfolgung, Datenschutz, Nachrichtendienst etc.) hat sich in Deutschland seit Jahren bewährt. Außerdem sollten in der NIS-Richtlinie die Befugnisse der zuständigen Behörden so ausgestaltet werden, dass sie nur den Zielen der Richtlinie dienen und nicht für andere Zwecke missbraucht werden können.