Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)07

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

von

Pascal Kurschildgen | IT-Sicherheitsberatung

Pascal Kurschildgen | IT-Sicherheitsberatung

Marktplatz 14
40764 Langenfeld

Tel: +49 2173 9939 298-0
Fax: +49 2173 9939 298-9
Mail: pascal@kurschildgen.com
Web: www.kurschildgen.com

Bankname: Stadt Sparkasse Langenfeld
Konto: 210 13 339
BLZ: 375 517 80

IBAN:
DE19375517801032105247
BIC: WELADED1LAF

Inhaber:
Pascal Kurschildgen

Steuer 135/165/2497

Inhaltsverzeichnis

1. Frage1

1.1. Frage:

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 (auch gesetzgeberische) müssen ergriffen werden, um den Grundrechtsschutz und die Vertraulichkeit der Kommunikation wieder sicherzustellen?

1.2. Antwort:

Da eine vertrauliche Kommunikation aus gutem Grund nicht alleine aus den gesicherten Übertragungswegen und der Infrastruktur sondern aus einem mehrschichtigen System besteht, kann unter gewissen Umständen weiterhin sicher kommuniziert werden. Wobei der Begriff „sichere Kommunikation“ noch nicht abschließend definiert wurde.
Die offengelegte OpenSSL Sicherheitslücke zeigt beispielsweise, dass lediglich ein Teil der sicher geglaubten Übertragungswege eine Schwäche aufweist.
Hiermit ist es nun auch in der Öffentlichkeit angekommen, dass die Übertragunsgwege nicht grundsätzlich vor Einsichtnahme durch Dritte gesichert sind und man sich selber um die Vertraulichkeit seiner zu übermittelnden Informationen und Inhaltsdaten kümmern muss.

Um den Grundrechtsschutz und die Vertraulichkeit der Kommunikation sicher zu stellen, muss ein speziell dafür geschaffenes Gesetz entwickelt werden oder bestehende Gesetze und Verordnungen erweitert werden, um die notwendige Informationssicherheit sicher zu stellen.
Konkret kann hier unter anderem für Anbieter von Kommunikationsinfrastrukturen verbindlich vorgeschrieben werden, eine dem Stand der Technik entsprechenden Transportverschlüsselung umzusetzen. Als Grundlage kann hier zum Beispiel der RFC 2487[1] zitiert werden, der sich mit der „Service Extension for Secure SMTP over TLS“ befasst. Dieser Standard ist im Januar 1999 definiert aber nicht flächendeckend umgesetzt worden. Die Umsetzung dieses über 20 Jahre alten Standards, ist als „E-Mail made in Germany“ bekannt. Umgesetzt durch web.de, GMX und Telekom[2].

[1] http://tools.ietf.org/html/rfc2487

[2] http://www.e-mail-made-in-germany.de/

Um einen Grundrechtsschutz und einen gewissen Anteil an Vertraulichkeit herzustellen, muss den Anbietern von Kommunikationsdiensten unter anderem das Speichern und Übermitteln von unverschlüsselten Passwörtern gesetzlich untersagt werden. Ein Verstoß gegen ein solches Gesetz, muss mindestens als grob fahrlässige Handlung definiert werden, um die Anbieter entsprechend in die Haftung nehmen zu können.

Weiterhin sollte der Gesetzgeber eine Grundlage dafür schaffen, die Entwicklung von sicherheitskritischer Software wie OpenSSL zu fördern und entsprechend zu überprüfen. Eine Überprüfung von freier Software vor dem Einsatz in kritischen Infrastrukturen wie dem Internet, muss gesetzlich geregelt werden.

2. Frage 2

2.1. Frage:

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

2.2. Antwort:

Eine Möglichkeit der Abwehr, besteht aus einer richtig installierten und angewandten Ende zu Ende Verschlüsselung. Die heute am Markt erhältlichen Lösungen sind S-MIME , PGP und spezielle Entwicklungen wie zum Beispiel die E-POST Businesslösung für Berufsgeheimnisträger. In der Praxis zeigt sich in vielen Systemen allerdings das Problem, der durch den Nutzer nicht zu bedienenden und verstandenen Sicherheitssoftware. Bei der Erstellung von S-MIME Zertifikaten kommt es zum Beispiel auch heute noch vor, dass Anbieter von für Privatanwender kostenlosen Zertifikaten, diese inklusive privatem Schlüssel selbst erzeugen und diese dann dem Nutzer auf unverschlüsselten Übertragungswegen zusenden. S-MIME Zertifikate muss der Nutzer inklusive dem privaten Schlüssel selbst lokal erzeugen, um sicher zu stellen, dass kein Dritter den für die Entschlüsselung wichtigen privaten Schlüssel als Kopie vorrätig hält.

Die Probleme übertragen sich nahtlos auf die heutzutage immer weiter verbreiteten mobilen Lösungen wie smartphones und tablets. Dort ist es zum Beispiel mangels eines etablierten Standards auf den sich die Hersteller von mobilen Kommunikationsgeräten noch nicht geeinigt haben, für Private Nutzer und kleine Unternehmen nicht ohne weiteres möglich plattformübergreifend verschlüsselt zu kommunizieren. Der Aufwand ist nur durch Experten und IT-Techniker zu bewältigen.

Weiterhin gehören auch aktuelle Betriebssysteme und regelmäßige Sicherheitsupdates sämtlicher zum Einsatz kommender Hard- und Software zur Grundvoraussetzung für eine sichere Kommunikation. Eine Ende zu Ende Verschlüsselung kann nicht auf leicht zu kompromittierenden Betriebssystemen und Software sicher gestellt werden. Hier ist aktuell der Nutzer, die Behörde oder das Unternehmen in der Pflicht immer mit aktuellen Systemen zu arbeiten und diese dem Nutzer zur Verfügung zu stellen.
Der Gesetzgeber kann hier nach meiner Einschätzung insofern zum Einsatz kommen, in dem er die Hersteller von Hard- und Software wirksam in die Pflicht nimmt. Das kann bedeuten, dass Hersteller von Software verpflichtet werden, durch konkrete Erweiterungen des Produkthaftungsgesetzes zum Beispiel, wirksame Vorkehrungen zu treffen, die dazu in der Lage sind, ein Produkt

möglichst fehlerfrei auszuliefern und Hersteller sich an diesem Ziel auszurichten haben.
Die Hersteller müssen ebenso verpflichtet werden, erkannte und bekannte Sicherheitslücken unverzüglich zu schließen und Sicherheitsupdates zeitnah zur Verfügung zu stellen. Eine Veröffentlichungspflicht, analog dem §42a des Bundesdatenschutzgesetz der vorschreibt, dass Betroffene informiert werden müssen, kann hier zur Sensibilisierung der Hersteller im Vorfeld führen. Dies kann bedeuten, dass Hersteller von Hard- und Software ihre Nutzer oder die Öffentlichkeit über Sicherheitslücken unverzüglich informieren und Sicherheitsupdates mit Installationsanleitungen zur Verfügung stellen müssen.

3. Frage 3

3.1. Frage:

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

3.2. Antwort

Die Anbieter können grundlegend eine sichere Transportverschlüsselung nach dem Stand der Technik umsetzen und erweiterte Sicherheitsmaßnahmen wie zum Beispiel eine „Zwei Faktor Authentifizierung“ einsetzen und Benutzerpasswörter nicht im Klartext speichern. Unter einer Zwei Faktor Authentifizierung versteht man das nutzen von mindestens zwei Merkmalen eines Identitätsnachweis. Ein Identitätsnachweis kann etwas sein was ich weiß (Passwort), was ich habe (Token, Karte, etc) und etwas was ich bin (Fingerabdruck, Stimme, etc.).
Dies kann in einem noch zu schaffenden oder zu erweiternden Gesetz, wie unter 1.2 beschrieben, vorgeschrieben werden.

4. Frage 4

4.1. Frage:

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?

4.2. Antwort

Kommunikationsdienste, wie zum Beispiel der in der Frage genannte DE-Mail Dienst, bieten grundsätzlich nur eine Transportverschlüsselung zwischen dem Nutzer und den Servern untereinander und keine Inhaltsverschlüsselung. Diese muss der Nutzer selber durch zusätzlich zu installierende Software, Schlüsselerstellung und Schlüsselverwaltung sicherstellen.

Die bisherigen geltenden Gesetze, gehen nur sehr ungenügend auf die Bedürfnisse einer verbindlichen- und Ende zu Ende verschlüsselten Kommunikation ein.

Ein guter Ansatz ist die „Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.März in Hamburg“ zur Gewährleistung der Menschenrechte bei der elektronischen Kommunikation[3]. Hier wird unter anderem eine sichere Verschlüsselung beim Transport und bei der Speicherung von Daten mit Produkten und Verfahren nach bekannten sicheren kryptographischen Algorithmen gefordert.

Einen unterstützenden Beitrag könnte die Bundesdruckerei mit einem leicht zu bedienenden Personalausweis und Sicherheitszertifikat leisten. Dieser sollte dem Bürger kostenlos zur Verfügung gestellt werden, damit die Akzeptanz sich einen solchen anzuschaffen, durch die Bürger gesteigert wird. Auch, wenn das Angebot an Anwendungen für Bürger noch sehr überschaubar ist und derzeit noch hauptsächlich Behörden mit sehr eingeschränkten Dienstleistungen dort auf der Homepage des Bundesministerium des Inneren[4] aufgelistet sind.

---

[3] http://www.datenschutz.sachsen-anhalt.de/konferenzen/nationale-datenschutzkonferenz/entschliessungen/entschliessungen-der-87-datenschutzkonferenz-27-bis-28-maerz-2014-in-hamburg/gewaehrleistung-der-menschenrechte-bei-der-elektronischen-kommunikation/

[4] http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html

5. Frage 5

5.1. Frage:

Wie können Privatpersonen sowie klein- und mittelständische Unternehmen zur stärkeren Nutzung sicherer Kommunikationsverbindungen und Verschlüsselungs- verfahren bewegt werden? Besteht hier politischer Handlungsbedarf?

5.2. Antwort:

Unternehmen können und sollten in die Pflicht genommen werden, entsprechende Maßnahmen umzusetzen, die geeignet sind, die Offenlegung von Geschäftsgeheimnissen oder personenbezogenen Daten durch unverschlüsselte Kommunikation zu verhindern.
Eine erste Erwähnung findet sich da bereits in den umzusetzenden technischen und organisatorischen Maßnahmen zum Zugangs- und Zugriffsschutz und der Weitergabekontrolle gem. Anlage zu §9 des Bundesdatenschutzgesetzes. Hier ist ein dem Stand der Technik entsprechendes Verschlüsselungsverfahren einzusetzen.

Privatpersonen können nur durch Aufklärung zur Nutzung sicherer Kommunikationsverbindungen bewegt werden. Die Aufklärung muss für Bürger sämtlicher Altersgruppen und zielgruppenorientiert erfolgen. Durch groß angelegte Präventionskampagnen zur Aufklärung, wie es zum Beispiel bereits seit 1987 durch die Bundeszentrale für Gesundheitliche Aufklärung mit der Kampagne „gib AIDS keine Chance“ bundesweit erfolgt. Ohne jedoch hier die Gefahr die durch die Krankheit ausgeht vergleichen zu wollen, ist eine Kampagne vergleichbaren Ausmaßes und Durchdringung von Nöten. Der politische Handlungsbedarf kann hier durch die Schaffung einer solchen Einrichtung zur Aufklärung gedeckt werden. Denkbar ist hier der Ausbau und Nutzung des für Bürger vollkommen unbekannten Portals „BSI für Bürger“[5]. Dieses Portal sollte grundsätzlich zur Aufklärung der Bürger dienen. Hier kann massiv ausgebaut werden um die Bürger zur Nutzung von sicheren Kommunikationsverbindungen zu bewegen.

[5] https://www.bsi-fuer-buerger.de/

6. Frage 6

6.1. Frage:

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

6.2. Antwort:

Wenn es ein Gesetz gibt wie in Antwort 1.2 formuliert kann die Datensicherheit bei solchen Diensten und Programmen enorm gesteigert werden. Grundlegend muss aber hier beachtet werden, dass die Datenverarbeitung der meisten Messaging Dienste, in Rechenzentren außerhalb der EU betrieben werden. nur durch gesetzgeberisch erzwungene Aufklärung der Nutzer durch die Anbieter etwas verbessert werden kann. Der politische Handlungsbedarf kann sich hier auf die Schaffung eines Gesetzes oder einer Vorschrift zur Nutzeraufklärung und transparenten Datennutzung erstrecken.

7. Frage 7

7.1. Frage:

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?

7.2. Antwort:

Eine Ende-zu-Ende-Verschlüsselung ist einer Deutschland-Mail oder Schengen-Routing Maßnahme unbedingt zu bevorzugen. Die Umsetzung bestehender Lösungen, wie beispielsweise das Patent zum Verfahren für die sichere Übertragung einer digitale Nachricht[6], liefern einen sehr guten Ansatz für die Umsetzung einer sicheren Ende zu Ende Verschlüsselung.
Die Telekommunikationsanbieter sollten ergänzend ebenso zu einer Transportverschlüsselung mit dem Stand der Technik entsprechenden Verschlüsselungsverfahren verpflichtet werden.

[6] Patent DE102012222995 B3, Verfahren für die sichere Übertragung einer digitalen Nachricht von M.Bobinski und J.Pabel

8. Frage 8

8.1. Frage:

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?

8.2. Antwort:

Das Strafrecht sollte im „§203 Verletzung von Privatgeheimnissen“ um die grob fahrlässige Handlung durch Unternehmen und deren Geschäftsführer erweitert werden, wenn unbefugt Geschäftsgeheimnisse oder vertrauliche Kommunikation durch fehlerhafte, fehlerhaft umgesetzte oder fehlende Sicherheitsmaßnahmen offenbart werden.
Der §109a des Telekommunikationsgesetzes erscheint mir für Diensteanbieter als ausreichend reguliert.

9. Frage 9

9.1. Frage:

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?

9.2. Antwort

Das BSI kann und sollte unbedingt frühzeitig an Schulen und Bildungseinrichtungen Aufklärung und Sensibilisierung für IT-Sicherheit betreiben. Schüler, Lehrer und Eltern sollten in einem Gesamtkonzept berücksichtigt werden, damit ein ausgeglichenes Wissensniveau vorherrscht. Ziel eines solchen Konzeptes muss ein aufgeklärter Bürger und Nutzer von IT-Systemen sein. Ein solches Konzept sollte bundeseinheitlich erstellt und umgesetzt werden.

Ein in vielen Diskussionen immer wieder auftauchender und, so genannter „Internetführerschein“ darf allerdings nicht die Grundvoraussetzung sein, um an einer Kommunikation teilnehmen zu dürfen. Ein Zugang zu Medien muss immer und uneingeschränkt zur Verfügung stehen.

Die Aufgaben und Ziele des Cyber Abwehr Zentrums sind der Bevölkerung nicht wirklich bekannt und verwirren durch die Namensgebung. Hier ist eine breite Aufklärung der Öffentlichkeit erforderlich.

10. Frage 10

10.1. Frage:

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?

10.2. Antwort:

IT-Sicherheitsaudits müssen verbindlich vorgeschrieben werden. Eine Selbstverpflichtung kann meiner Meinung nach nicht zum Ziel führen. Denn ein IT-Sicherheitsaudit ist sehr kostspielig und zeitintensiv in der Umsetzung. Ein möglicherweise noch zu schaffendes IT-Sicherheitsgesetz, könnte einen vergleichbaren Paragraphen wie den §9a im Bundesdatenschutzgesetz zum Datenschutzaudit beinhalten. Auch wenn dieser im Bundesdatenschutzgesetz mangels eines noch zu schaffenden Gesetzes nie wirklich angewendet worden ist. Dazu fehlte meiner Meinung nach der Anreiz für Unternehmen dieses zu verlangen. Ein IT-Sicherheitsaudit könnte in Deutschland für eine gewisse Übergangszeit nach Inkraftsetzung eines IT-Sicherheitsgesetzes gefördert werden. Dies könnte die Akzeptanz erhöhen ein solch aufwendiges IT-Sicherheitsaudit durchzuführen.
Die IT-Sicherheitsaudits sollten dazu allerdings vom Hersteller und nicht vom Anwender durchgeführt und in Auftrag gegeben werden müssen. Ein IT-Sicherheitsaudit muss vom Hersteller durchgeführt oder in Auftrag gegeben und dem Anwender vorgewiesen werden.
Bei Open-Source-Security-Software sollte ein IT-Sicherheitsaudit sofort staatlichen Einrichtungen wie dem BSI oder eine dafür ins Leben zu rufende Stiftung zufallen. Hier ist eine Stiftung IT-Sicherheit, ähnlich der Stiftung Datenschutz von der Bundesregierung zu gründen und mit dem notwendigen Grundkapital auszustatten, deren Aufgabe es unter anderem ist, Open Source Sicherheitssoftware zu überprüfen oder überprüfen zu lassen.

11. Frage 11

11.1. Frage:

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?

11.2. Antwort:

Ein Schutz vor Geheim- und Nachrichtendiensten ist meiner Meinung nach nicht möglich. Hier sollte und muss das Instrument der Aufklärung und Transparenz gewählt werden, um größere Schäden oder Beeinträchtigung der schützenswerten Bedürfnisse der Nutzer zu verhindern.
Die erwähnte Cybercrime Richtlinie ist ein guter Ansatz, um eventuell entdeckte Straftaten zu ahnden. Sie ist aber nur und ausschließlich dazu geeignet, Straftaten aufzudecken oder zu ahnden, aber nicht um sie zu verhindern.

Eine EU-Datenschutzverordnung sehe ich als nicht geeignet an, um Daten von europäischen Nutzern bei außereuropäischen Unternehmen zu schützen. Denn ein US-Amerikanischer Bundesbezirksrichter hat beispielsweise am 25. April einen Durchsuchungsbeschluss für E-Mail Daten eines Microsoft Kunden erlassen[7]. Die Daten des besagten Kunden sind in einem Rechenzentrum in Dublin, also Irland gespeichert.
Da der erwirkte Durchsuchungsbeschluss in diesem Fall wie eine richterliche Anordnung behandelt wird, ist es unerheblich wo die Daten gespeichert sind, die vom US-Amerikanischen Konzern Microsoft herausgegeben werden müssen. Somit kann und wird eine EU-Datenschutzverordnung nicht zur Anwendung kommen. Microsoft hat angekündigt gegen die Entscheidung vorzugehen[8].

Auch wenn dies nur ein erster Vorstoß eines einzelnen Bundesbezirksrichter darstellt, zeigt es doch die Unzulänglichkeiten der EU-Datenschutzgrundverordnung, beim Versuch, die Daten europäischer Bürger bei US-Amerikanischen Unternehmen standortunabhängig schützen zu wollen.

---

[7] http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425

[8] http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspx