Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)09

Stellungnahme von Thorsten Schröder zum Fragenkatalog für das öffentliche Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema „IT Sicherheit“ am Mittwoch, dem 7. Mai 2014

Thorsten Schröder
modzero GmbH
Berlin, den 4. Mai 2014

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

   a) Eine sichere Kommunikation über die bestehenden Infrastrukturen ist möglich, solange die Wirkung starker Verschlüsselung nicht mutwillig oder fahrlässig durch Hersteller oder Dritte beeinträchtigt wird.
   b) Die gesicherten Erkenntnisse beschränken sich auf die bislang an die Öffentlichkeit gelangten Informationen über praktische, erfolgreich durchgeführte Angriffe auf Systeme, Protokolle und Geräte. Anhand dieser Erkenntnisse können Angriffsszenarien, die bislang als unwahrscheinlich galten, neu klassifiziert werden – zum Beispiel, weil durch eine Veröffentlichung der Aufwand und die Kosten eines bestimmten Angriffstyps auf eine bestimmte Fehlerklasse geringer geworden sind. In so einem Fall erhöht sich die Eintrittswahrscheinlichkeit, und der Grad der Bedrohung muss anhand spezifischer Risiken neu berechnet werden. In den meisten Fällen kann davon ausgegangen werden, dass nicht die Frage der Machbarkeit eines Angriffs im Vordergrund steht, sondern die Frage nach der Zeit und den Ressourcen eines Angreifers.
   c) Grundsätzlich sind Angriffe gegen Hard- und Software-Komponenten möglich, also auch gegen sogenannte Embedded Systeme, Netzwerkkomponenten, etc. Besonders gefährlich sind Fehler, die sich bereits in Normen und Standards eingeschlichen haben (oder mutwillig eingebaut worden sind). Die Auswirkungen hier sind sehr groß, da Hersteller diese Normen als Grundlage heranziehen, um ihr Produkt kompatibel mit standardisierter Technologie zu gestalten.
   d) Das Benennen von konkreten Maßnahmen, durch die Grundrechte geschützt und eine vertrauliche Kommunikation ermöglicht würde, ist in diesem Kontext schwierig. Denn der Schutz der Grundrechte hängt nicht allein von etwaigen Fehlern in Software oder Standards ab – auch nicht vom Finden und Veröffentlichen solcher Fehler. Außerdem kann die Vertraulichkeit der digitalen und analogen Kommunikation grundsätzlich nicht sichergestellt, sondern nur erhöht werden. Die Erhöhung der Sicherheit und Vertraulichkeit der Kommunikation ist allerdings oft mit erheblichen Kosten bei der Einführung neuer Standards verbunden, etwa, weil sich jeder Nutzer oder Anbieter komplett

neue Hardware zulegen müsste, die mit den aktuellen, sichereren Standards kompatibel wäre.
Die Gesetzgebung könnte Telekommunikationsanbietern also zwar grundsätzlich vorschreiben, welche Mindeststandards gelten müssen, allerdings müsste die entsprechende Technologie für Anbieter und Konsumenten erschwinglich gestaltet - also etwa subventioniert -werden.

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?*

   a) Die beste und zuverlässigste Abwehrmöglichkeit bedeutet einen Verzicht auf Komfort. Denn ein höheres Sicherheitsniveau geht immer mit dem Einschnitt in die Bedienbarkeit einer Anwendung einher. Das bedeutet, Nutzer können sich häufig nur schützen, indem sie auf eine bestimmte Technik verzichten, die das Leben erleichtern sollte. (Cloud-Dienste, Indizierung von Dokumenten und E-Mails, vermeintlich kostenlose Hilf lugins, usw.)
   b) Bei Verwendung starker Kryptografie für den Versand und die Speicherung sensibler Daten (z. B. via E-Mail) können Unbefugte nur mit großer Mühe Einsicht nehmen.
   Damit ist allerdings noch keine Bedrohung abgewehrt, sondern vielmehr werden der Aufwand und somit die Kosten für einen erfolgreichen Angriff erhöht.
   Die Verwendung starker Kryptografie für den Versand und die Speicherung sensibler Daten bedeutet allerdings einen Verzicht auf Komfort, da z. B. ein komfortables Durchsuchen der gespeicherten Daten nicht mehr möglich ist.
   c) Außerdem gibt es Techniken und Software, welche die Integrität von verschlüsselten Kanälen überwachen; solche Verfahren sind ebenfalls geeignet, um die Authentizität von Diensten im Internet zu bewerten. Die Verwendung solcher Werkzeuge bedeutet jedoch für die Nutzer ebenfalls größere Umstände, einen geringeren Komfort – und vor allem viel technisches Wissen. Die Warnungen eines solchen Werkzeugs müssen gelesen und verstanden werden, um ein erhöhtes Schutzniveau zu erreichen und angemessene Maßnahmen einleiten zu können. Um solche Programme - wie in 2b) und 2c) angesprochen – sinnvoll nutzen zu können, müssen die Verbraucher sensibilisiert und geschult werden. Dabei sollte die Regierung sie unterstützen.

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

   a) Anbieter müssen beispielsweise darauf verzichten, Cloud-Dienste als Opt-Out-Service an ihre Produkte oder Dienstleistungen zu binden. Gesetzgeber sollten den Endnutzer (und nicht den Anbieter/Betreiber) durch eine klare Regelung hinsichtlich Opt-In in Schutz nehmen. Ziele einer solchen Maßnahme sind: Datensparsamkeit und das Vermeiden der Speicherung unnötiger Informationen über Kunden und Benutzer, um die Ausmaße eines etwaigen Zwischenfalls von vorneherein einzuschränken. Ausländische Anbieter und Betreiber von

Kommunikationsdiensten werden sich möglicherweise nicht an die Vorgaben deutscher oder europäischer Behörden richten.

b) Betreiber von SSL/TLS-gesicherten Servern bzw. Diensten können Chipkarten oder andere Hardware-basierte Security-Token-Systeme verwenden, um zu vermeiden, dass kryptografisches Schlüsselmaterial über Netzwerke in unbefugte Hände gelangt. Letzteres war durch die kürzlich publik gewordene sogenannte Heartbleed Schwachstelle in OpenSSL der Fall.

c) Der Gesetzgeber muss darüber hinaus auf die Vorratsdatenspeicherung auf Seiten der Kommunikationsdienste-Anbieter verzichten. Denn diese senkt das Sicherheitsniveau auf Seiten des Betreibers erheblich.

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?*

a) Grundsätzlich stellen die Antworten 2c), 3b) und 3c) eine erste geeignete Maßnahme für ein erhöhtes Sicherheitsniveau bei der Verwendung dieser Dienste dar. Die Aufwände für ein höheres Sicherheitsniveau werden auf allen Seiten erhöht: Benutzer müssen sensibilisierter mit der Technik umgehen und Warnungen korrekt interpretieren können, Betreiber müssen auf Opt-Out-Mechanismen verzichten und können Hardware-Module für SSL-gesicherte Verbindungen verwenden. Behörden müssen rechtliche Vorgaben liefern und auf verdachtsunabhängige Massenüberwachung auf Seiten der Betreiber verzichten.

b) Weder öffentliche Stellen wie das BSI, noch privatwirtschaftliche Unternehmen wie die Bundesdruckerei GmbH leisten einen Beitrag zur Erhöhung der Sicherheit, wenn sie (kostenlose oder kostenpflichtige) Zertifikate zur Verschlüsselung zur Verfügung stellen. Die D-TRUST GmbH, an der die Bundesdruckerei 100% der Anteile hält, stellt bereits Zertifikate zur Verfügung[1]; eine wesentliche Erhöhung des allgemeinen Sicherheitsniveaus der SSL Public Key Infrastruktur (PKI) konnte hierdurch offenbar nicht gewährleistet werden.

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

a) Aufklärung, Bildung und eine Vorbildfunktion sind entscheidend für die flächendeckende Verbreitung sinnvoller kryptografischer Maßnahmen. Verständlich formulierte und visualisierte Informationen müssen bestenfalls schon früh im Schulunterricht vermittelt werden; Unternehmensgründer sollten geeignete Informationsmaterialien an die Hand bekommen, in denen die Gefahren und Gefahrenquellen benannt und geeignete Gegenmaßnahmen erläutert werden.

b) Das BSI könnte aktiv und regelmäßig den Deutschen IP-Adressraum nach Diensten absuchen (Monitoring), die keine oder nur minderwertige

[1] https://www.d-trust.net/fileadmin/dokumente/2.Preisinformationen.pdf

Verschlüsselungsoptionen bieten. Da IP-Adressen in der Regel bestimmten Organisationen und Verwaltungsberechtigten zuzuordnen sind, können Verantwortliche automatisiert per E-Mail über Missstände und Gegenmaßnahmen informiert werden.

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

   a) Telekommunikationsanbieter, die ein neu verpacktes oder altes Instant-Messenging-Verfahren auf dem Markt anbieten, müssen sich an die geltenden Bestimmungen und Gesetze hinsichtlich des Daten- und Verbraucherschutzes halten.
   b) Unabhängige Forscher und Personen, die Mängel und Sicherheitslücken in den Protokollen und Instant-Messenging-Produkten identifizieren und aufdecken, müssen vor anschließender Strafverfolgung geschützt werden. Zumindest, sofern die Veröffentlichung nicht grob fahrlässig die Existenz der betreffenden Unternehmen aufs Spiel setzt.

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?*

   a) Deutschland-Mail kann keinen sinnvollen Beitrag zur Erhöhung der IT-Sicherheit bieten. Die sinnvolle Ende-zu-Ende Verschlüsselung stellt lediglich eine Option dar. Somit ist die offizielle Werbebotschaft

      „De-Mails können nicht von Dritten abgefangen und verändert werden, weil sie auf ihrem Weg durch das Internet immer verschlüsselt sind.“ (Quelle: http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/Sicherheitsmerkmale/sicherheitsmerkmale_node.html)

      irreführend, und widerspricht den empfohlenen Maßnahmen in Absatz 5a).

   b) Schengen-Routing bietet für eine technische Umsetzung sicherlich zahlreiche interessante Problemstellungen. Jedoch kann auch eine Sicherstellung der räumlichen Eingrenzung des Datenverkehrs nicht verhindern, dass ein deutsches Unternehmen mit den Daten zahlreicher deutscher Teilnehmer an eine US-Firma verkauft wird. Zwei bekannte Beispiele hierfür sind Unternehmen der Samwer-Brüder: alando.de wurde an das US-amerikanische Unternehmen eBay, die Jamba GmbH an den US-amerikanischen Konzern VeriSign verkauft.

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?*

Zur Sicherstellung des Schutzes und der Vertraulichkeit der Kommunikation und der Grundrechte müssen Maßnahmen ergriffen werden, die sicherstellen, dass Überwachungsmaßnahmen wie z. B. eine Quellen-TKÜ lückenlos dokumentiert und begründet werden können. Massenhafte Überwachung der gesamten oder großer Teile der Bevölkerung mittels Vorratsdatenspeicherung muss per Gesetz ausgeschlossen werden.

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?*

a) Damit die Informationen des BSI für die Nutzer als verlässlich und vertrauenswürdig gelten, ist es zwingend notwendig, dass das BSI Transparenz zu seinem wichtigsten Grundsatz erhebt.
b) Es ist begrüßenswert, dass das BSI sich zum Wohl der Wirtschaft und der Bevölkerung für die Sicherheit von Open-Source Software einsetzt. Allerdings braucht es weitere finanzielle Mittel, um transparent Ausschreibungen für den Review von Open-Source-Produkten durchführen zu können. Das BSI benötigt darüber hinaus Beratung für die detaillierte Definition öffentlicher Ausschreibungen besonders komplexer Konzepte und Lösungen.
c) Die noch vor Bekanntwerden der Heartbleed-Schwachstelle in OpenSSL vom BSI ausgeschriebene Sicherheitsanalyse des OpenSSL-Quellcodes[2] weist für IT-Sicherheits-Unternehmen zu wenige sinnvolle Rahmenbedingungen auf. Die hier geforderten Zielsetzungen sind für ein kommerziell agierendes Unternehmen aus der Privatwirtschaft nicht praktikabel; die im konkreten Beispiel genannte Zielsetzung birgt zu viele inhaltliche und finanzielle Gefahren für ein kleines, effizient arbeitendes Team mit Spezialisierung auf solchen Dienstleistungen.

[2] http://www.evergabe-online.de/download/bekanntmachung65725.pdf?verfahrenID=65725

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*

    Das BSI hat bereits einen derartigen Audit ausgeschrieben.[3]

    b) Angemessene Sicherheitsaudits der sehr komplexen OpenSSL-Bibliothek beschränken sich auf einzelne wichtige Teilaspekte. Jeder Teilaspekt muss durch mehrere voneinander unabhängig agierenden Auditoren-Teams durchgeführt werden, ein einzelner Audit der Code-Basis wird keine sonderlich hohe Sicherheit gewährleisten.

    c) Zusätzlich könnte ein offizielles Bug-Bounty-Programm[4] eingeführt werden. Strenge Richtlinien müssen eingehalten und dessen Einhaltung überwacht werden, damit etwaige Sicherheitslücken nicht durch Bundesbehörden für den Bau digitaler Waffen missbraucht werden können. Das Preisgeld für einen Fehler muss hoch genug sein, um den Findern einen Anreiz zu bieten, ihr Wissen nicht auf dem Schwarzmarkt zu verkaufen.

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 Datenschutzgrund- sätze 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?*

    Da ich zu den genannten EU-Verordnungen über ein zu geringes Vorwissen verfüge, verzichte ich auf die Beantwortung der Fragen aus Punkt 11.

Kontakt

Thorsten Schröder
modzero GmbH
Tongrubenweg 58A
12559 Berlin
ths@modzero.ch

[3] http://www.evergabe-online.de/download/bekanntmachung65725.pdf?verfahrenID=65725
[4] http://en.wikipedia.org/wiki/Bug_bounty_program