Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)11

Chaos Computer Club

Effektive IT-Sicherheit fördern

Stellungnahme zur 7. Sitzung des Ausschusses Digitale Agenda des Deutschen Bundestages

Linus Neumann,
Mittwoch, 7. Mai 2014

Einleitung

Sowohl technische Aspekte der Geheimdienst-Spähskandale um NSA und GCHQ als auch Apples „Goto Fail“ und der als „Heartbleed“ bekanntgewordene OpenSSL-Bug zeigen teilweise jahrelange Versäumnisse bei der Implementierung, aber auch im Design von weit verbreiteter sicherheitsrelevanter Software und darauf basierender Architekturen.

Zur Sicherung zukünftiger IT-Infrastrukturen sind nun einige grundlegende Weichenstellungen notwendig: Damit Sicherheitslücken vor ihrer Ausnutzung behoben werden, muss die Qualität von Open-Source-Software durch regelmäßige Auditierungen sichergestellt werden. Bei vielen IT-Architekturen – insbesondere im Bereich der Kommunikation – ist ein Paradigmenwechsel von Perimetersicherheit zu mehrschichtigen Sicherheitssystemen mit Ende-zu-Ende-Verschlüsselung überfällig. Auf politischer Ebene ist die Arbeit der Geheimdienste in klare Grenzen zu weisen, und die Politik mit Mitteln auszustatten, deren Einhaltung wirksam zu erzwingen.

1. Qualität von Open-Source-Software sicherstellen

Ziel politischer Förderung sollte in Zukunft die Incentivierung der Qualitätssicherung von freier und offener Software sein, insbesondere solcher, deren Einsatz weit verbreitet ist. Die Qualitätssicherung von Open-Source-Software stellt kommerzielle Akteure vor ein klassisches Dilemma: Die Allgemeinheit – und auch die Konkurrenz – profitiert von den individuellen Investitionen in das öffentliche Gut, wodurch eine Trittbrettfahrer-Mentalität befördert wird.

Regelmäßige unabhängige Prüfungen durchführen

So ist es zu erklären, dass namhafte Anbieter weltweit das OpenSSL-Projekt zum Grundstein der Übertragungssicherheit ihrer Kommunikation erheben, jedoch nur geringe oder gar keine Investitionen in dessen Qualitätssicherung tätigen. Nicht nur „Heartbleed“ hat jedoch gezeigt, dass sicherheitskritische Softwarekomponenten – egal ob quelloffen oder proprietär – einer regelmäßigen Auditierung bedürfen. Der Vorteil von Open-Source-Software besteht gerade darin, dass solche Auditierungen unabhängig und zum Nutzen aller in offenen Verfahren durchgeführt werden können.

Eine regelmäßige und eingehende Prüfung von sicherheitsrelevanter Open-Source-Software ist daher unerlässlich und fällt in den Bereich des öffentlichen Interesses. Die Veröffentlichung aller Befunde dieser Auditierungen sowie das allgemeine Zugänglichmachen aller Bugfixes sind dabei selbstverständliche Grundvoraussetzungen.

Bisher unternimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch allerhand Zertifizierungen den Versuch, einen ähnlichen Effekt auf anderem Wege zu erzielen: Lange Kataloge definieren Designanforderungen, die Angriffsmöglichkeiten – auf dem Papier – ausschließen sollen. Tatsächlich erfolgreiche Angriffe – auch das zeigt „Heartbleed“ – setzen jedoch genau an den Stellen an, die übersehen oder nicht bedacht wurden oder nicht bedacht werden konnten, wie zum Beispiel simple Programmierfehler mit weitreichenden Folgen. Genau diese Arten von Fehlern sind in Zertifizierungskatalogen nicht abbildbar; verlangt wird nur das sprichwörtliche Häkchen auf der Check-Liste. Darüber hinaus errichten die teuren Zertifizierungsprozesse einerseits Markteintrittsbarrieren, während sie andererseits für die zertifizierenden Instanzen einen Interessenkonflikt hervorrufen: Der Auftraggeber bezahlt nicht für eine Liste fundamentaler nderungen, die das Einhalten von Projektplänen gefährden, sondern erwartet eine möglichst konfliktfreie, zeitnahe Zertifizierung. Darüber hinaus werden Zertifizierungen üblicherweise an Versionsnummern gebunden und behindern dadurch einen dynamischen Weiterentwicklungsprozess der Software.

Als Gegenmodell zu diesem bürokratischen und mit nicht zielführenden Anreizen versehenen Vorgehen sind regelmäßige Auditierungen vorzuziehen. Durch eine Auftragsvergabe nach Kompetenzkriterien kann hier außerdem die Chance ergriffen werden, bezahlte Auditierung für kleine und mittelständische Anbieter attraktiv zu machen. Da oft keine eigene ökonomische Incentivierung besteht, quelloffene Software aufwendig zu auditieren (OpenSSL ist hier ein perfektes Beispiel), wird der Staat die fehlenden Anreize dazu schaffen müssen. Das ist auch langfristig in seinem Interesse, da die Qualität weit verbreiteter Open-Source-Anwendungen strukturell verbessert wird. Praktisch bedeutet das, ein staatliches Budget dafür zu reservieren, kritische Open-Source-Komponenten auf Sicherheitslücken auditieren zu lassen. Bei der Auftragsvergabe muss das Prinzip vieler Augen Anwendung finden und der gleiche Auftrag mehrmals an verschiedene Auditoren vergeben werden.

Bug Bountys ausloben

Als besonders erfolgreich für das Aufspüren und Beheben von Sicherheitslücken haben sich darüber hinaus so genannte „Bug Bounty“-Programme erwiesen, bei denen Belohnungen für das Finden kritischer Sicherheitslücken bedingungslos ausgelobt werden. Diese internationalen unbürokratischen Anreize tragen zur allgemeinen Erhöhung der Sicherheit von Open-Source-Software bei. Sie treten zudem in direkte Konkurrenz mit dem bestehenden Schwarzmarkt für Sicherheitslücken, der heute vom Geld der Geheimdienste und Kriminellen unterhalten wird.

Parallel ist eine generelle Förderung der Entwicklung von Open-Source-Software wünschenswert und mit ökonomischen Anreizen zu versehen: Wirkliche Beherrschung von IT-Systemen ist nur möglich, wenn einzelne Nutzer und Wirtschaftsunternehmen, aber auch staatliche Stellen Hoheit über ihre Systeme haben. Strategisch sollten daher die richtigen Weichen gestellt werden in Richtung einer soliden Open-Source-Infrastruktur im Hinblick auf Software, Services und Hardware.

Haftung der Anbieter sicherstellen

Eine weitere damit zusammenhängende Frage betrifft die Haftung von Anbietern für Sicherheitslücken bzw. für deren zeitnahe Eindämmung und Beseitigung. In der Tat wird zu Recht die Frage gestellt, weshalb kommerzielle Software-Lieferanten und Dienste-Anbieter größtenteils ohne jegliche Haftung operieren dürfen. Für kommerzielle Anbieter wäre eine derartige Haftung in der Tat zielführend, da sie nennenswerte Anreize zur Qualitätssicherung schaffen würde. Das Beispiel OpenSSL macht allerdings eindrücklich deutlich, weshalb Haftung für Open-Source-Software nicht möglich ist: Eine kleine internationale Community entwickelte dieses Tool größtenteils ehrenamtlich, während weltweit Banken und Konzerne einerseits kaum zur Entwicklung beitrugen, andererseits sehr große finanzielle Werte mittels OpenSSL absicherten. Eine Haftung für nicht überprüfbare, kommerzielle Software bei einem gleichzeitigen Haftungsausschluss für quelloffene Sicherheitstechnik kling nur auf den ersten Blick wie ein Widerspruch: Die resultierenden Anreize würden sowohl bei quelloffener als auch bei proprietärer Software zur Code-Qualität beitragen und zugleich Anbieter von Sicherheitslösungen in Richtung des zu bevorzugenden Open-Source-Ansatzes bewegen.

2. Dezentrale Sicherheitssysteme mit Ende-zu-Ende-Verschlüsselung ausbauen

Ein vielfach kritisierter Aspekt der bundesdeutschen IT-Sicherheitsbemühungen betrifft den durch die Anbieterbindung entstehenden Interessenkonflikt: Verfahren wie De-Mail verlangen von den Anbietern zwar eine teure Zertifizierung, versprechen dafür jedoch dank Zentralität und Inkompatibilität mit anderen Verfahren einen starken „Lock-in-Effekt", der die Kunden dauerhaft binden soll. Ergebnis dieser Wirtschaftsförderungsmaßnahmen sind stark zentralisierte Infrastrukturen, die besonders attraktive Angriffsziele darstellen. Den Kontroll- und Überwachungsambitionen deutscher Geheimdienste und Strafverfolgungsbehörden ist es sicherlich auch zu verdanken, dass konzeptionelle Fehler in diesen Architekturen dank der unverschlüsselten Datenvorhaltung zu dauerhaften und absichtlichen Risiken führen.

Zentrale Strukturen aufbrechen

In der Kommunikationssicherheit sollte der Anbieter daher nie gleichzeitig der einzige Dreh- und Angelpunkt des Sicherheitsmodells sein, da seine Kompromittierung dann jene weitreichenden Folgen hat, die nun im Rahmen der Snowden-Enthüllungen öffentlich wurden. Leider ist auch in den initialen Reaktionen deutscher Unternehmen darauf kein nachhaltiges Umdenken zu erkennen: Das über viele Jahre versäumte Einschalten von Transportverschlüsselung wird mit einer aufdringlichen Werbekampagne geradezu gefeiert, während man mittels „Schengen-Routing" und einer „Deutschland-Cloud" die Zentralisierung weiter vorantreiben möchte, um Marktanteile zu gewinnen, die aus gutem Grund nie erreicht wurden. Bedauerlicherweise wirkt auch der größere Teil der Programme des BSI bisher immer wieder auf derartige Modelle hin, statt mittels dezentraler, offener Standards auch auf eine Senkung der Attraktivität für Angreifer hinzuwirken. Ein entsprechender Paradigmenwechsel hin zu dezentralen Diensten mit Ende-zu-Ende-Verschlüsselung ist überfällig, denn nur so steigen die Angriffskosten auf ein Niveau, das Massenspionage unmöglich macht.

Parallel muss auch die notwendige Infrastruktur für eine Dezentralisierung geschaffen werden. Hier ist insbesondere der Breitbandausbau zu benennen. Entgegen der landläufigen Auffassung und momentan vorherrschenden Nutzungsweise ist das Internet als Netz gleichberechtigter Teilnehmer konzipiert, in dem jeder Teilnehmer direkte Verbindungen zu jedem anderen aufbauen kann: Das Internet kennt keine Unterscheidung in Sender und Empfänger. Heutige DSL-Angebote führen eine solche Unterscheidung künstlich ein, indem die Anschlussgeschwindigkeiten für das Empfangen von Daten um ein Vielfaches höher sind als die Übertragungsraten für das Senden. Dieser Umstand erschwert es für kleine mittelständische Unternehmen und Privatpersonen, Dienste selbst vorzuhalten, statt die Dienstleistungen großer, meist wenig vertrauenswürdiger Anbieter in Anspruch zu nehmen. Die Folge sind genau jene Datensilos, die Massenüberwachungen überhaupt erst möglich machen.

Starke Sicherheitsstandards umsetzen

Neben diesen grundsätzlichen Weichenstellungen für ein resilientes, offenes und verteiltes Kommunikationsnetz ist von gesetzgeberischer Seite auf das Einhalten von Sicherheitsstandards hinzuwirken und diese auch im eigenen IT-Beschaffungsverhalten bei Behörden und mtern zu berücksichtigen. So sollte Verschlüsselung grundsätzlich vorgeschrieben und die Verwendung unsicherer Verschlüsselungsverfahren, wie sie beispielsweise im Mobilfunk seit Jahren wider besseren Wissens und trotz der Existenz sicherer Alternativen zum Einsatz kommen, ausgeschlossen werden. Eine Ende-zu-Ende-Verschlüsselung von Kommunikation muss als verpflichtender Stand für Behörden, Berufsgeheimnisträger und schrittweise für alle Kommunikationsunternehmen eingeführt werden, um Sicherheit gegen

Ausforschung – insbesondere gegen Massenüberwachung – zu erlangen. Die im vergangenen Jahr erwirkten Absenkungen des Schutzniveaus durch das E-Government und das E-Justice-Gesetz sind zu korrigieren.[1] [2]

Ende-zu-Ende-Verschlüsselung zum Standard machen

Ein von Befürwortern zentraler Infrastrukturen immer wieder vorgetragenes Argument betrifft die angeblich erschwerte Nutzung von Ende-zu-Ende-Verschlüsselung, da diese zusätzliche Softwarekomponenten erfordere. Bei dieser Argumentation beißt sich die Katze in den Schwanz: Zusatzkomponenten für Ende-zu-Ende-Verschlüsselung waren lange Zeit vor allem deshalb notwendig, weil bewusst auf sie verzichtet wurde. Alle gängigen E-Mail-Clients und Messenger-Applikationen, auch die bei Smartphones mitgelieferten, beweisen heute das Gegenteil: Die Mehrzahl unterstützt Ende-zu-Ende-Verschlüsselung – nur ist sie oft nicht Standard, sondern muss erst zusätzlich eingeschaltet werden. Da die meisten Nutzer Standardeinstellungen nicht ändern, ist hier einer der Hauptgründe für die mangelnde Verbreitung zu suchen, dem jedoch leicht Abhilfe geleistet werden kann.

Betrieb kritischer Infrastruktur absichern

An dieser Stelle sei darauf hingewiesen, dass kritische Infrastrukturen (z. B. Energie- und Wasserversorgung) von funktionierenden IT-Diensten abhängig sind. Ausfälle dieser IT-Dienste lassen sich nicht vermeiden, daher muss sichergestellt werden, dass sie keinen Ausfall kritischer Infrastrukturen zur Folge haben. Auch hier kann eine hohe Resilienz nur durch dezentrale Strukturen erreicht werden. Weiterhin müssen kritische Infrastrukturen in Netzen betrieben werden, die unabhängig vom Internet sind und keine Angriffsfläche über das Internet bieten. Derartige Festverbindungen sind jedoch in ihrer technischen Realisierung teurer und entbinden auch nicht vom allgemeinen Verschlüsselungsgebot, so dass nicht selten darauf verzichtet wird.

Natürlich gilt es hier aber ebenso wie für normale Kommunikation, Angriffe auf die IT-Systeme zu erschweren und ihre möglichen Folgen gering zu halten. Eine zeitgemäße Zugangssicherung mit Zwei-Faktor-Authentifizierung ist hierzu ebenso notwendig wie eine Ende-zu-Ende-Verschlüsselung jeglicher Steuer- und Diagnosebefehle. Fatal ist darüber hinaus die wechselseitige Abhängigkeit zwischen kritischen Infrastrukturen. Die Studie „Was bei einem Blackout geschieht“ des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB33) kommt zu der Schlussfolgerung, „dass bereits nach wenigen Tagen im betroffenen Gebiet die bedarfsgerechte Versorgung der Bevölkerung mit lebensnotwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist. Auch wird deutlich gemacht, dass „erhebliche Anstrengungen erforderlich sind, um die Durchhaltefähigkeit kritischer Infrastrukturen zu erhöhen, sowie die Kapazitäten des nationalen Systems des Katastrophenmanagements weiter zu optimieren.“[3] Der Chaos Computer Club hat sich diesem Thema im Februar 2014 mit einer ausführlichen Stellungnahme gewidmet.[4]

---

[1] Chaos Computer Club (2014): Gutachten unterstreicht Untauglichkeit der De-Mail für rechtsverbindliche Kommunikation, online: http://ccc.de/de/updates/2013/de-mail-unqualifizierte-makulatur

[2] Chaos Computer Club (2014): Sicherheit von De-Mail nur ein schlechter Witz, online: http://ccc.de/de/updates/2013/de-mail-unqualifizierte-makulatur

[3] Petermann, Thomas/Bradke, Harald/Lüllmann, Arne/Poetzsch, Maik/Riehm, Ulrich (2011): Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Bd. 33, online: http://www.tab-beim-bundestag.de/de/pdf/publikationen/buecher/petermann-etal-2011-141.pdf

[4] Chaos Computer Club (2014): Stand der Technik nicht genug: CCC fordert unabhängige Risikobewertung für Sicherheit im Stromnetz, online: http://ccc.de/de/updates/2014/BNetzA

3. Unabhängige und evidenzbasierte Sicherheits- und Geheimdienstpolitik sicherstellen

Nach den Enthüllungen von Edward Snowden ist die Rolle von Geheimdiensten, Überwachungsbehörden und deren kommerzieller Partnern grundlegend neu zu bewerten, da sie strukturell gegen die IT-Sicherheit gearbeitet haben und weiterhin arbeiten. Das weder politisch-parlamentarisch noch gesellschaftlich hinreichend kontrollierte Wirken der Geheimdienste und ihrer Partner hinsichtlich der Unterminierung der IT-Sicherheit kann nicht weiterhin akzeptiert werden.

Sinn und Effektivität von Überwachungsmaßnahmen regelmäßig prüfen

Der seit mehr als einem Jahrzehnt vorherrschende Teufelskreis aus Zentralisierung und Überwachung muss durchbrochen werden, schon um die Sinnhaftigkeit in der Terrorismus- oder Kriminalitätsbekämpfung erstmals einem ernsthaften überprüfenden Blick auszusetzen. So werden mit öffentlichen Mitteln sowohl Deutschlands als auch der EU in großem Umfang Projekte gefördert, die eine effizientere, flächendeckendere Überwachung der Bürger zum Ziel haben. Diese Forschung findet weiterhin unter dem Vorwand statt, diese Überwachung würde zu mehr Sicherheit führen. Ein Effekt dieser großzügigen Förderung ist, dass sich ein wachsender Industriezweig gebildet hat, der aus reinem Gewinninteresse auf den Ausbau von Überwachungssystemen drängt. Dieser Mechanismus ist nur durch Zudrehen des Geldhahnes für solche Technologien zu durchbrechen.

Im Sinne einer zukunftsorientierten, rationalen Sicherheitspolitik, bei der sowohl die Bürger- und Freiheitsrechte als auch die ökonomischen Interessen der von den Geheimdiensten ausspionierten Wirtschaftsunternehmen und -verbände berücksichtigt werden, ist eine fortlaufende Evaluation aller Überwachungsgesetze und -bestimmungen anzustreben. Die Annahme, dass mehr Überwachungsmöglichkeiten auch mehr Sicherheit gegen Terrorismus brächten, beruht vorwiegend auf anekdotischen Argumenten der Behörden. Sicherheitspolitik im digitalen Zeitalter erfordert jedoch ein hohes Maß an Transparenz und Kontrolle, um Auswüchse zu verhindern, wie sie durch Snowden zwar bekannt wurden, aber weiterhin bestehen.

Eine in regelmäßigen Abständen – etwa alle zwei bis drei Jahre – stattfindende unabhängige wissenschaftliche, öffentliche Evaluation von Effizienz, Kosten, Wirksamkeit und Missbrauchsgeschehen von Überwachungs- und Eingriffsbefugnissen muss selbstverständlich werden. Damit diese Evaluation ernsthaft und wirksam ist, bedarf es eines Automatismus, so dass ein Gesetz außer Kraft tritt, wenn keine positive Evaluation stattgefunden hat oder die betreffenden Behörden die Kooperation mit den evaluierenden Wissenschaftlern verweigern. Diese sind im Gegenzug personell so auszustatten, dass sie die nötige Datenbasis auch bereitstellen und aktuell halten können.

Unabhängigkeit des BSI sicherstellen

Bisher unterliegt die Zusammenarbeit von BND, MAD und BfV mit ausländischen Partnerdiensten keiner ausreichenden politischen Kontrolle. Laut dem ehemaligen Kanzleramtsminister Ronald Pofalla werden die entsprechenden Abkommen im Detail von den Diensten selbst ausgehandelt und angepasst. Dabei legt schon das reine Volumen der durch die NSA über deutsche Bürger gesammelten Daten den Verdacht nahe, dass diese kaum ohne die Kenntnis deutscher Dienste – wenn nicht sogar deren Unterstützung – gesammelt werden können. Es ist notwendig, hier politische Kontrolle und Transparenz gegenüber dem Parlament und der Öffentlichkeit herzustellen. Mit welchen Diensten aus welchen Gründen welche Daten ausgetauscht werden, ist für die Öffentlichkeit und Politik wesentlich, um über das Fortbestehen solcher Kooperationen entscheiden zu können. Die Geheimhaltungsinteressen der Dienste dürfen dabei nicht weiter sakrosankt sein. Was aus welchen Gründen wie lange geheim zu halten ist, darf nicht länger der Entscheidungsgewalt der Dienste unterliegen, da die Geheimhaltung regelmäßig dazu dient, Fehlverhalten zu kaschieren und Gesetze zu überdehnen.

Mit dem BSI verfügt die Bundesregierung über eine Institution, die aktuell viele Möglichkeiten ungenutzt lässt, auf den skizzierten grundsätzlichen Paradigmenwechsel hinzuwirken. Wirtschaft und Bürger müssen jedoch das zweifelsfreie Vertrauen haben können, dass das BSI ausschließlich der Sicherheit von Computern und Netzen verpflichtet ist und nicht Informationen über Lücken und Schwachstellen mit Geheimdiensten und Polizeibehörden teilt oder gezielt auf eine Schwächung von Kommunikationsinfrastrukturen hinarbeitet.

Dazu muss das BSI aus dem Verantwortungsbereich des Innenministeriums (BMI) herausgelöst und einen starken Status als unabhängige Bundesbehörde bekommen. Bei einer Weisungsbefugnis des BMI steht immer der Verdacht im Raum, dass das BSI ähnlich wie die NSA seine erheblichen Zugangsmöglichkeiten, die mit der Begründung der IT-Sicherheit eingeräumt und vermutlich demnächst erweitert werden, für andere Überwachungszwecke nutzt. Solange das BSI dem Innenminister untersteht, ist trotz aller Versicherungen anzunehmen, dass deutsche Geheimdienste und über deren internationalen Austausch auch die NSA und weitere ausländische Dienste Kenntnis von Schwachstellen erhalten, die Wirtschaft und Bürger dem BSI mitteilen. Dies gilt es zu vermeiden. Ein starkes, unabhängiges BSI mit unzweideutigem Sicherheitsauftrag – auch gegen staatliche Angreifer – ist der einzige Weg, das notwendige Vertrauen im Bereich der IT-Sicherheit aufzubauen.