Quellen-TKÜ als Gefahr für die allgemeine IT-Sicherheit

Künftig soll mit dem Bundestrojaner staatlich geförderte Schadsoftware eingesetzt werden, um an die Klartextdaten von potenziellen Straftätern zu gelangen. Das ist aus Sicht der Strafverfolgungsorgane wünschenswert, wird aus Sicht der IT-Sicherheit aber schwerwiegende Nebenwirkungen haben. *Von Norbert Pohlmann und Rene Riedel*

Einführung

IT-Sicherheit geht uns alle an. Durch Sicherheitslücken in IT-Systemen sind nicht nur Nutzer gefährdet, die vergessen haben, die neueste Firewall herunterzuladen. Sicherheitslücken bieten flächendeckend Einfallstore, um auf eine riesige Anzahl von Endgeräten zuzugreifen und ermöglichen Kriminellen die Begehung schwerer Straftaten. Insbesondere im Bereich der Wirtschaftsspionage entstehen dabei enorm hohe Schadenssummen. Der jährliche finanzielle Schaden in diesem Bereich wird allein in Deutschland mit 50 bis 60 Milliarden Euro beziffert. Wie unausgeglichen das Verhältnis zwischen dem aktuellen Schutzniveau im Internet und den möglichen Angriffsflächen zugunsten der Hacker und Cyberkriminellen ist, wurde zuletzt bei den Sicherheitslücken „Spectre" und „Meltdown" deutlich. Um Straftaten und Wirtschaftsspionage wirksam zu verhindern, muss die IT-Sicherheit im Internet nachhaltig verbessert werden.

Es ist daher grundsätzlich positiv zu bewerten, dass immer mehr Kommunikationsdaten verschlüsselt werden. Durch die zunehmende Verwendung öffentlich zugänglicher Verschlüsselungssoftware werden die Schutzziele Vertraulichkeit, Integrität und Authentizität nachhaltig gestärkt und das Schutzniveau im Internet für alle Bürger und die gesamte Wirtschaft deutlich erhöht.

Von den Vorteilen der Verschlüsselung profitieren aber natürlich auch kriminelle Personen und Gruppierungen, die ihre Aktivitäten über das Internet, zum Beispiel bei WhatsApp oder Skype, organisieren. Für die Strafverfolgungsbehörden ergeben sich daraus Probleme, denn die Telekommunikationsüberwachung (TKÜ) in der bisherigen Form ist nicht für die Überwachung von verschlüsselten Kommunikationskanälen geeignet.

Der Deutsche Bundestag hat daher am Ende der letzten Legislaturperiode in einem Schnellverfahren das „Gesetz zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens" beschlossen. Dieses Gesetz gibt den Strafverfolgungsbehörden die Möglichkeit, Softwareschwachstellen auf dem Endgerät eines Verdächtigen auszunutzen, um mittels aufgespielter Schadsoftware die Daten bereits vor der Verschlüsselung oder spätestens nach der Entschlüsselung abzugreifen. Dies wird als Quellen-TKÜ bezeichnet.

Die Ausnutzung von Softwareschwachstellen durch die Quellen-TKÜ ist jedoch mit einer grundsätzlichen Schwächung der IT-Sicherheit aller Nutzer und der gesamten Wirtschaft im Internet verbunden. Dieser Aspekt ist bei den Planungen zur Quellen-TKÜ völlig außer Acht gelassen worden, obwohl das Bundesverfassungsgericht bereits in seinem Grundsatzurteil aus dem Jahr 2008 zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" auf den Zielkonflikt zwischen der Strafverfolgung und dem Schutz unserer IT-Systeme aufmerksam gemacht hat.

Im Ergebnis werden Behörden nun ermächtigt, die gleichen Methoden zu nutzen wie Kriminelle. Das sollte aber nicht die Lösung des Problems sein. Im Gegenteil: Der Schutz aller müsste so nachhaltig erhöht werden, dass es Kriminellen prinzipiell erschwert wird, Straftaten zu begehen.

Unterschiede der TKÜ und Quellen-TKÜ

In der bisherigen Form der TKÜ werden die Kommunikationsdaten von potenziellen Straftätern direkt in der Telekommunikationsinfrastruktur abgegriffen. Es handelt sich dabei um ein passives Abhören des Kommunikationskanals ohne die Integrität, das heißt die IT-Sicherheit der beteiligten Endgeräte, zu beeinträchtigen.

Der Zugriff auf die Daten erfolgt über eine spezielle Schnittstelle, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) spezifiziert wurde. Diese Schnittstelle muss gesetzlich verpflichtend von den Betreibern einer Telekommunikationsinfrastruktur eingebunden werden. Durch spezifizierte Zugriffskontrollen und weitere Schutzmechanismen kann weitestgehend sichergestellt werden, dass nur die Strafverfolgungsbehörden Zugriff auf die Kommunikation erhalten. Die IT-Sicherheit der klassischen TKÜ hängt also von der Sicherheit der spezifizierten Schnittstelle und der Verwendung durch die Strafverfolgungsbehörden ab. Es handelt sich dabei um eine akzeptable Lösung, die dem Spannungsverhältnis zwischen IT-Sicherheit und Strafverfolgung gerecht wird.

Anders sieht es bei der Quellen-TKÜ aus. Um an die Klartextdaten von potenziellen Straftätern zu gelangen, wird eine Abhörsoftware (Malware) auf das Endgerät des Verdächtigen aufgespielt. Im Zuge der effektiven Strafverfolgung erfolgt das Aufspielen der Schadsoftware dabei ohne das Wissen der verdächtigen Person. Diese Vorgehensweise stellt eine aktive Beeinträchtigung der Integrität des Endgerätes dar, sie wird deshalb aus Sicherheitsgründen von den aktuellen Betriebssystemen grundsätzlich unterbunden. Um das Aufspielen dennoch zu ermöglichen, muss eine Schwachstelle in der Software auf dem Endgerät des Verdächtigen ausgenutzt werden. Die Behörden nutzen dabei ihnen bekannte Sicherheitslücken, ohne die Bevölkerung über die Gefahren der Softwareschwachstellen zu informieren. Damit ist im Vergleich zur klassischen TKÜ nicht nur ein Zugriff auf die Daten Verdächtiger möglich, potenziell sind die Daten aller Nutzer der verwendeten Software gefährdet. Es wäre etwa theoretisch denkbar, dass eine Sicherheitslücke, von der deutsche Strafverfolger wissen und die sie gerade nutzen, um eine Diebesbande zu verfolgen, zur selben Zeit von Kriminellen ausgenutzt wird, um Millionenbeträge zu erbeuten. Das ist mit dem Auftrag des Staates, seine Bürger zu schützen, kaum zu vereinbaren.

Einordnung des Bundestrojaners

Die technische Umsetzung der Quellen-TKÜ, insbesondere die Verwendung von Schwachstellen und die Veränderung der Integrität des Endgerätes, entspricht der gängigen Vorgehensweise von kriminellen Organisationen im Internet. Die auf dem Endgerät des Verdächtigen installierte Software wird als „Bundestrojaner" bezeichnet. Bei Trojanern handelt es sich um eine spezielle Form von Malware. Diese wird im Rahmen der Quellen-TKÜ verwendet, um Kommunikationsdaten des

Verdächtigen noch vor der Verschlüsselung oder nach der Entschlüsselung abzugreifen und an die Abhörsysteme der Strafverfolgungsbehörde zu versenden.

Einordnung der Abhörinfrastruktur

Das technisch anspruchsvollste Problem bei der Arbeit mit einem Trojaner ist, bisher unbekannte Sicherheitslücken ausfindig zu machen, über die die Malware aufgespielt werden kann. Für die Koordination und technische Realisierung des Abhörens von verschlüsselter Kommunikation wurde durch das Bundesministerium des Innern (BMI) eine neue Bundesbehörde mit dem Namen „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS) geschaffen. ZITiS ist in München angesiedelt. Bis 2022 sollen dort 400 Beamte, davon viele IT-Spezialisten, eingestellt werden.

Wie die Autoren dieses Beitrages in einer eigens erstellten Analyse mit dem Thema „Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen" aufgezeigt haben, wird die geplante Ausstattung von ZITiS höchstwahrscheinlich nicht ausreichen, um vergleichbare Strukturen und Mechanismen wie Cyberkriminelle aufzubauen. Das bedeutet konkret, dass ZITiS alleine nicht in der Lage sein dürfte, genügend Schwachstellen in Softwareprodukten zu finden, um den Bundestrojaner im punktuellen Bedarfsfall auf dem Endgerät eines Verdächtigen, zum Beispiel auf dem Smartphone, dem Tablet oder dem Computer, aufzuspielen. Alle diese Endgeräte haben unterschiedliche Betriebssysteme, etwa von Microsoft/Windows, Apple/iOS, Google/Android und LINUX, die entsprechend berücksichtigt werden müssen.

Weil die Suche von Schwachstellen in Softwareprodukten so aufwendig und schwierig ist, hat sich ein „Black Market" entwickelt, auf dem Cyberkriminelle Schwachstellen in Softwareprodukten einkaufen, um Engpässe bei der Verbreitung von Schadsoftware zu vermeiden. Die eigenständige Suche nach Schwachstellen wird zunehmend irrelevant. Stattdessen etablieren sich professionelle Marktteilnehmer auf dem „Black Market", die „Malware-as-a-Service" oder vergleichbare Dienste als innovative Verkaufsstrategien im Internet anbieten. Bei diesen Diensten ist es unter anderem möglich, für kleine Geldbeträge punktuelle Installationen von Schadsoftware zu veranlassen.

Daneben existiert auch der „Grey Market", der die Vermarktung von Schwachstellen für einen „vermeintlich positiven Zweck" betreibt, etwa an Staaten. Die Übergänge zwischen den Märkten sind fließend, insbesondere werden auf dem „Grey Market" wahrscheinlich auch Schwachstellen an autoritäre Regime verkauft. Damit die Quellen-TKÜ durchgängig realisiert werden kann, ist davon auszugehen, dass ZITiS in einer vergleichbaren Art und Weise Schwachstellen auf dem „Grey Market" einkaufen wird.

Schwächung von bestehenden Bemühungen

Angriffe auf Basis von „Zero Day Exploits" (ZDE) haben in der Vergangenheit verdeutlicht, welche wirtschaftlichen oder gesellschaftlichen Schäden durch unbekannte Schwachstellen in Software verursacht werden können. ZDE haben ihren Ursprung im „Black Market". Für die Erstellung eines ZDE muss zuerst eine unbekannte Schwachstelle identifiziert werden. Zu dieser Schwachstelle wird anschließend ein Exploit programmiert. Dieser Exploit wird am Ende als Produkt auf dem „Black Market" verkauft. Ein Exploit gilt solange als ZDE, bis die zugrunde liegende Schwachstelle dem Hersteller der Software über „Bug Bounty"-Programme oder vergleichbare Bemühungen gemeldet wurde und dieser einen entsprechenden Patch veröffentlicht hat.

Die zentrale Idee von „Bug Bounty"-Programmen ist es, Wissenschaftler, die „Hacker"-Community oder weitere Akteure durch finanzielle Anreize zu animieren, Schwachstellen in Produkten der Hersteller zu finden, damit diese anschließend die Schwachstellen beheben können. Eine Berkeley-Studie hat ergeben, dass die finanzielle Unterstützung von „Bug Bounty"-Programmen bis zu hundertmal kostenwirksamer ist als eigenständige Bemühungen der Hersteller.

Wirtschaftswissenschaftlich betrachtet stehen die „Bug Bounty"-Programme in einem Wettbewerb zu den Akteuren des „Grey/Black Markets". Alle Akteure bewegen sich zusammen auf dem Markt für Softwareschwachstellen. Die einen nutzen diesen Markt für das Beheben von Softwarefehlern, die anderen für das gezielte Ausnutzen der Schwachstellen.

Problematisch ist in diesem Zusammenhang die Tatsache, dass die finanziellen Belohnungen der „Bug Bounty"-Programme für kritische Schwachstellen in der Regel weitaus geringer ausfallen als der durchschnittliche Minimalpreis im „Black Market". Für die „Bug Bounty"-Programme kommt erschwerend hinzu, dass in der Regel nur einmalig eine Belohnung erzielt werden kann. Auf dem „Black Market" hingegen kann ein ZDE mehrere Male an verschiedene Interessenten verkauft werden. Daraus werden sich langfristig zahlreiche Probleme für die IT-Sicherheit aller Endgeräte ergeben. Es ist davon auszugehen, dass sich Akteure der „Bug Bounty"-Programme zukünftig auf dem „Black Market" positionieren, um einen höheren finanziellen Profit zu erzielen.

Der Kauf von Schwachstellen für den Betrieb des Bundestrojaners unterstützt diese Entwicklung, weil er die Nachfrage auf dem „Grey Market" erhöht. Im Ergebnis würde die finanzielle Unterstützung des „Grey Markets" durch ZITiS auch dem „Black Market" zu mehr Wachstum verhelfen. Damit würde unvermeidlich das Risiko für die allgemeine IT-Sicherheit steigen und sich folglich der zu erwartende Schaden durch Cyberkriminalität im Internet erhöhen.

Fazit

Die zunehmende Verwendung von Verschlüsselung im Internet zwingt die Strafverfolgungsbehörden unweigerlich dazu, ihre technischen Werkzeuge für die TKÜ an die neue Situation anzupassen.

Die Quellen-TKÜ ist hierfür jedoch nicht das geeignete Mittel. Die systematische Verwendung von Schwachstellen für die Installation des Bundestrojaners fördert den Bieterwettbewerb um Exploits und schwächt bestehende „Bug Bounty"-Programme. Dadurch wird nicht nur die IT-Sicherheit aller Endgeräte der Bürger und der gesamten Wirtschaft erheblich reduziert, sondern auch die Gefahr von Cyberkriminalität, Wirtschaftsspionage und auch Cyberwar durch Terroristen erhöht. Da zum aktuellen Zeitpunkt nicht klar ist, welcher Mehrwert bei der Aufklärung von Straftaten mittels Quellen-TKÜ tatsächlich erzielt werden kann, wiegt die Reduzierung der IT-Sicherheit umso schwerer.

Notwendig wäre eine gesamtgesellschaftliche Anstrengung, um die IT-Sicherheit in allen Bereichen messbar zu erhöhen. Die Bundesregierung sollte etwa darüber nachdenken, Bug Bounty-Programme aktiv zu unterstützen. Ziel muss sein, den „Black Market" auszutrocknen, nicht ihn staatlich zu unterstützen. Nur dieser Weg bietet auf lange Sicht die Möglichkeit, Kriminalität und Wirtschaftsspionage im Internet wirksam zu begegnen.

Dieser Ansatz löst natürlich nicht das konkrete Problem der Strafverfolger, die in vielen Fällen Nachrichten nicht mehr lesbar machen können. Aber die Quellen-TKÜ ist aus den genannten Gründen hierfür eben auch der falsche Ansatz. Es ist notwendig, dass Experten aus den verschiedenen Bereichen gemeinsam nach sichereren und risikoärmeren Lösungen für die Strafverfolgung suchen, die im Kontext der IT-Sicherheit funktionieren.

Professor Dr. Norbert Pohlmann
ist Vorstand Ressort IT-Sicherheit bei eco – Verband der Internetwirtschaft.

Rene Riedel
ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen.