Einsatz von Bundestrojanern

Der Bundestrojaner schwächt die IT-Sicherheit

von Prof. Norbert Pohlmann[*]

Künftig soll staatlich geförderte Schadsoftware eingesetzt werden, um an die Klartextdaten von potentiellen Straftätern auf PCs, Notebooks und Smartphones zu gelangen. Das ist aus Sicht der Strafverfolgungsorgane wünschenswert, wird aus Sicht der IT-Sicherheit aber katastrophale Nebenwirkungen haben.

Künftig soll staatlich geförderte Schadsoftware eingesetzt werden, um an die Klartextdaten von potentiellen Straftätern auf PCs, Notebooks und Smartphones zu gelangen. Das ist aus Sicht der Strafverfolgungsorgane wünschenswert, wird aus Sicht der IT-Sicherheit aber katastrophale Nebenwirkungen haben.

1. Ausgangssituation

IT-Sicherheit geht uns alle an. Sicherheitslücken bieten flächendeckend Einfallstore zu einer riesigen Anzahl von Endgeräten und ermöglichen Kriminellen die Begehung schwerer Straftaten und – das wird oft vernachlässigt – Wirtschaftsspionage mit enorm hohen Schadenssummen. Der jährliche finanzielle Schaden in diesem Bereich wird je nach Quelle mit 50-60 Mrd. Euro beziffert, allein in Deutschland. Um Straftaten und Wirtschaftsspionage wirksam zu verhindern, muss daher Ziel sein, die IT-Sicherheit im Internet nachhaltig zu verbessern.

In Anbetracht dieser Lage ist es aus Sicht der IT-Sicherheit umso positiver zu bewerten, dass immer mehr Verschlüsselung von Kommunikationsdaten zum Einsatz kommt. Durch die zunehmende Verwendung von öffentlich zugänglicher Verschlüsselungssoftware werden die Schutzziele Vertraulichkeit, Integrität und Authentizität nachhaltig gestärkt. Insgesamt folgt daraus das dringend benötigte höhere Schutzniveau im Internet für alle Bürger und die gesamte Wirtschaft.

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

2. Quellen-TKÜ

Um dieses Problem zu lösen, hat der Deutsche Bundestag am Ende der auslaufenden Legislaturperiode in einem Schnellverfahren das „Gesetz zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens“ beschlossen. Dieses Gesetz gibt den Strafverfolgungsbehörden u.a. die Möglichkeiten, Softwareschwachstellen auf dem Endgerät eines Verdächtigen auszunutzen, um mittels

[*] Prof. Norbert Pohlmann, if(is) – Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen.

aufgespielter Schadsoftware die Daten bereits vor der Verschlüsselung oder spätestens nach der Entschlüsselung abzugreifen. Dies wird als Quellen-TKÜ, z.B. mittels Bundestrojaners, bezeichnet.

3. Sicherheitsgefährdung

Aus technischer Sicht kann Quellen-TKÜ prinzipiell funktionieren. Die gesetzliche Bewilligung für den Einsatz von Softwareschwachstellen ist jedoch mit einer grundsätzlichen Schwächung der IT-Sicherheit aller Nutzer und der gesamten Wirtschaft im Internet verbunden.[1] Dieser Aspekt ist bei den Planungen zur Quellen-TKÜ völlig außer Acht gelassen worden, obwohl das BVerfG in seinem Urteil zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bereits auf den Zielkonflikt zwischen der Strafverfolgung und dem Schutz unserer IT-Systeme aufmerksam gemacht hat.

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

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

Theoretisch kann eine Veränderung der Integrität nur innerhalb des Kommunikationskanals erfolgen. Aus Sicht der IT-Sicherheit handelt es sich dabei um eine akzeptable Lösung, die dem Spannungsverhältnis zwischen IT-Sicherheit und Strafverfolgung gerecht wird.

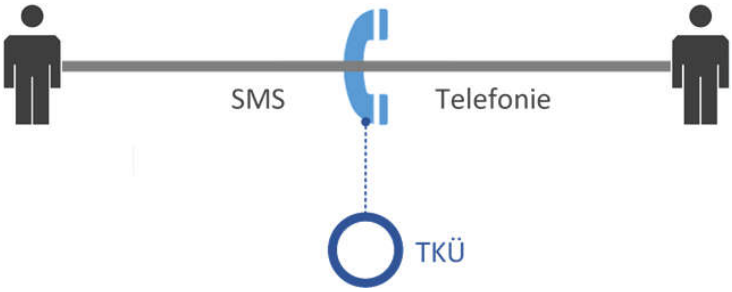

Abb. 1: Bisherige Form der Telekommunikationsüberwachung (TKÜ)

Anders sieht es jedoch bei der Quellen-TKÜ aus. Um an die Klartextdaten von potentiellen Straftätern zu gelangen, soll eine Abhörsoftware (Malware) auf das Endgerät des Verdächtigen aufgespielt werden. Im Zuge der effektiven Strafverfolgung wird das Aufspielen der Schadsoftware ohne das Wissen der verdächtigen Person erfolgen.

[1] *Pohlmann/Riedel*, DRiZ 2018, 52.

Diese Vorgehensweise stellt eine aktive Beeinträchtigung der Integrität des Endgerätes dar und wird deshalb aus Sicherheitsgründen von den aktuellen Betriebssystemen unterbunden. Aus diesem Grund muss eine Schwachstelle in der vorhandenen Software auf dem Endgerät des Verdächtigen ausgenutzt werden. Im Klartext: Behörden werden Sicherheitslücken, die ihnen bekannt geworden sind, nutzen, ohne die Bevölkerung vor ihnen zu warnen, um so ggf. Schäden in Millionenhöhe abzuwenden. Denn im Vergleich zur klassischen TKÜ kommt erschwerend hinzu, dass alle anderen Geräte der Bürger und der gesamten Wirtschaft im Internet durch dieselbe Schwachstelle in der verwendeten Software potentiell gefährdet sind.

Abb. 2: Quellen-TKÜ mit Hilfe des Bundestrojaners

Die Folgen können von den Strafverfolgungsbehörden nicht kontrolliert werden. 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 Staats, seine Bürger zu schützen, kaum zu vereinbaren.

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. ZDEs haben ihren Ursprung im Black Market. Für die Erstellung eines ZDEs 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 zugrundeliegende 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, Wissenschaftler, Hacker-Community oder weitere Akteure durch Hersteller finanziell 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 100-mal 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 betrachteten Akteure bewegen sich zusammen auf dem Markt für Schwachstellen in Software. Die einen nutzen diesen Markt für das Beheben von Softwarefehlern, die anderen für das gezielte Ausnutzen der Schwachstellen aus einem bestimmten Profitgrund.

Problematisch ist in diesem Zusammenhang die Tatsache, dass die durchschnittlichen finanziellen Belohnungen der Bug Bounty-Programme für kritische Schwachstellen 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, denn es ist davon auszugehen, dass sich Akteure der Bug Bounty-Programme zukünftig auf dem Black Market positionieren, um einen höheren finanziellen Profit zu erzielen. Diese Problematik wird durch den Kauf von Schwachstellen für den Betrieb des Bundestrojaners verschärft, denn es wird dadurch einseitig die Nachfrage an die Akteure des Grey/Black Markets erhöht. Durch die finanzielle Unterstützung des Grey Markets durch Strafverfolgungsbehörden würde indirekt auch dem Black Market zu mehr Wachstum verholfen werden. Damit würde unvermeidlich das Risiko, angegriffen zu werden, steigen und sich folglich der zu erwartende Schaden durch Cyberkriminalität im Internet erhöhen.

Die zunehmende Verwendung von Verschlüsselung im Internet sorgt unweigerlich dafür, dass die Strafverfolgungsbehörden ihre technischen Werkzeuge für die TKÜ an die neue Situation anpassen müssen. Das Ergebnis der angefertigten Analyse zeigt, dass durch die systematische Verwendung von Schwachstellen für die Installation des Bundestrojaners ein Bieterwettbewerb um Exploits gefördert wird, der bestehende Bug Bounty-Programme schwächt und im Ergebnis die IT-Sicherheit aller Endgeräte der Bürger und der gesamten Wirtschaft reduziert.[2] Mit der Reduzierung der IT-Sicherheit im Internet wird die angestrebte Erhöhung der öffentlichen Sicherheit zu einer Gefährdung der Gesellschaft durch Cyberkriminalität, Wirtschaftsspionage, Cyberwar durch Terroristen usw. Da zum aktuellen Zeitpunkt nicht klar ist, welcher Mehrwert bei der Aufklärung von Straftaten mittels Quellen-TKÜ tatsächlich erzielt werden kann, wirkt die Reduzierung der IT-Sicherheit umso schwerwiegender, weil der gesamtwirtschaftliche Schaden sehr groß sein wird.

Notwendig wäre hingegen eine gesamtgesellschaftliche Anstrengung, um die IT-Sicherheit in allen Bereichen messbar zu erhöhen. Die Bundesregierung sollte etwa darüber nachdenken, Bug Bounty- Programme aktiv zu

[2] *Pohlmann/Riedel*, DuD 2018, 367.

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.