Norbert Pohlmann, Rene Riedel

Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen

Die Quellen-TKÜ bringt mit dem Bundestrojaner große Risiken für eine dringend notwendige vertrauenswürdige IT-Sicherheit und nachhaltige Digitalisierung.

Der zunehmende Einsatz von Verschlüsselung im Internet stellt die Strafverfolgungsbehörden aktuell vor eine neue Herausforderung: Um an die Klartextdaten von potentiellen Straftätern zu kommen, soll zukünftig staatlich geförderte Schadsoftware, sogenannte Bundestrojaner, eingesetzt werden. Dieser Artikel thematisiert die daraus resultierenden Probleme und negativen Auswirkungen aus Sicht der IT-Sicherheit. Der Bundestrojaner ist in der Gesamtbetrachtung nicht beherrschbar und verursacht wahrscheinlich mehr Cyberkriminalität anstelle von Aufklärung.

1 Einleitung

Im Internet werden zunehmend die Daten von Kommunikationsanwendungen verschlüsselt, z.B. bei WhatsApp, Skype, usw. Aus Sicht der IT-Sicherheit ist dieser Trend äußerst positiv zu bewerten, denn die Schutzziele: Vertraulichkeit, Integrität und Authentizität werden durch die Verwendung von Verschlüsselung nachhaltig gestärkt. Insgesamt folgt daraus ein höheres Schutzniveau im Internet.

Für die Strafverfolgungsbehörden und die öffentliche Sicherheit ergibt sich jedoch zeitgleich das Dilemma, dass die aktuellen Verschlüsselungstechnologien zunehmend auch von Kriminellen verwendet werden. Somit ist die klassische Telekommunikationsüberwachung (TKÜ) bereits heute überwiegend nicht nutzbar, weil die Daten nur in verschlüsselter Form abgegriffen werden können.

Da die Strafverfolgung einen wesentlichen Bestandteil des Schutzes der Gesellschaft darstellt, müssen die Strafverfolgungsbehörden bestehende Alternativen zur TKÜ weiter vorantreiben oder neue Ansätze entwickeln. Dazu hat der Deutsche Bundestag in einem Schnellverfahren das „Gesetz zur effektiven und praxistauglichen Ausgestaltung des Strafverfahrens“ am Ende der auslaufenden Legislaturperiode beschlossen.

Dieses Gesetz gibt den Strafverfolgungsbehörden unteranderem die Möglichkeiten, 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, z.B. mittels Bundestrojaner, bezeichnet und im weiteren Verlauf dieses Artikels behandelt.

Aus technischer Sicht kann Quellen-TKÜ bei verschlüsselter Kommunikation prinzipiell gewährleisten, die Kommunikationsdaten im Klartext abzugreifen, z.B. bei WhatsApp, Skype, usw. Die konkrete Umsetzung ist jedoch nur mit einer grundsätzlichen Schwächung der IT-Sicherheit aller Nutzer im Internet möglich, wie im weiteren Verlauf des Artikels gezeigt wird.

Die eigentliche Maxime unserer Gesellschaft sollte aber das Gegenteil von Schwächung der IT und des Internets sein. Denn zurzeit haben wir jährlich einen finanziellen Schaden im Bereich der Wirtschaftsspionage von 55 Milliarden Euro nur in Deutschland /Bitk17/. Außerdem müssen wir bezüglich der immer größer werdenden Gefahr durch Cyberwar, unsere Kritischen Infrastrukturen deutlich sicherer und vertrauenswürdiger gestalten, um unsere Gesellschaft angemessen zu schützen.

Prof. Dr. Norbert Pohlmann

ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

Rene Riedel

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

E-Mail: riedel@internet-sicherheit.de

Das Bundesverfassungsgericht hat in seinem Urteil zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ auf den Zielkonflikt zwischen dem staatlichen Interesse an der Infiltration fremder Systeme zur Gefahrenabwehr (gleiches dürfte für die Strafverfolgung gelten) und dem staatlichen Auftrag zur Gewährleistung einer hohen IT-Sicherheit hingewiesen. Die geplante Quellen-TKÜ lässt den zweiten Gesichtspunkt völlig außer Acht und blendet insoweit die Vorgaben des Bundesverfassungsgerichts /BVerfG08/ zu einer angemessenen Berücksichtigung dieses zentralen Abwägungskriteriums vollständig aus. In diesem Artikel wird an die fehlende Berücksichtigung der IT-Sicherheit bei der geplanten Umsetzung des „Bundestrojaners“ angeknüpft und analytisch gezeigt, dass eine Berücksichtigung aufgrund der Schwächung der IT-Sicherheit aller Nutzer dringend notwendig ist.

2 Schwachstellen in Software sind eine Gefahr für die Digitalisierung

Die Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, Smartphones, in sehr großen Rechenzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus, für neue Kommunikationsformen von sehr unterschiedlichen IT-Geräten, usw. Problematisch hierbei ist, dass die Sicherheit von Informationssystemen direkt mit der Sicherheit der installierten Softwarekomponenten verknüpft ist. Schwachstellen in Software ermöglichen es prinzipiell Angreifern, die Kontrolle über IT-Systeme zu übernehmen und immense Schäden zu verursachen. Ein großes IT-Sicherheitsproblem ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme und Anwendungen muss für die heutige Bedrohungslage deutlich besser werden. Die Fehlerdichte, die Anzahl der Softwarefehler pro 1.000 Zeilen Code, ist heute im Schnitt 0,3. Da gängige Betriebssysteme ca. 10. Mio. Zeilen Code haben, sind hier im Schnitt 3.000 Software-Fehler zu finden /Pohl14/. Teile dieser Softwarefehler sind Ziele für professionelle und erfolgreiche Angriffe von kriminellen Organisationen und jetzt auch von Strafverfolgungsbehörden.

Für die Steigerung des Schutzniveaus im Internet ist es deshalb wichtig, dass die Anzahl der Schwachstellen in Software minimiert wird. Hierfür müssen zukünftig zwei Dinge weiter vorangetrieben werden: Zum einen müssen effektivere Werkzeuge, wie z.B. sichere Programmiersprachen, unterstützende integrierte Entwicklungsumgebungen oder Compiler für die Unterstützung im Entwicklungs- und Integrationsprozess von Software geschaffen werden. Aufgrund der Komplexität von Software muss die Fehlerrate deutlich minimiert werden. Der zweite unerlässliche Aspekt bei der Minimierung von Schwachstellen ist das nachträgliche Aufspüren und Beheben nach dem Release einer Software.

Aktuell stellen immer mehr Unternehmen fest, dass der Aufwand für die nachträgliche Suche nach Schwachstellen in den eigenen Softwareprodukten unproportional hoch zu dem eigentlichen Entwicklungsprozess ist und somit nicht effizient von einem Unternehmen alleine realisiert werden kann. Gleichzeitig steigt aber das Bewusstsein der Unternehmen für die Notwendigkeit sicherer Softwareprodukte. Aus diesem Grund werden immer mehr sogenannte „Bug Bounty“-Programme (BBP) von den Unternehmen gegründet oder finanziell unterstützt.

2.1 „Bug Bounty“-Programme

„Bug Bounty“-Programme helfen den Herstellern von Produkten Schwachstellen zu finden, damit diese behoben werden können.

Die zentrale Idee von „Bug Bounty“-Programmen ist es, die Hacker-Community, Wissenschaftler oder weitere Akteure finanziell zu animieren, Schwachstellen in den eigenen Produkten zu finden, damit diese anschließend von den Unternehmen zeitnah behoben werden können. Eine Berkeley-Studie hat ergeben, dass die finanzielle Unterstützung von BBPs bis zu 100-mal kostenwirksamer ist, als eigenständige Bemühungen in einem Unternehmen /Finif13/. Die Effektivität von BBPs lässt sich außerdem anhand der Kennzahlen der Plattform „Bugcrowd“ verdeutlichen. Aus den jährlichen Reports von 2015-2017 /Bugc15//Bugc16//Bugc17/ geht hervor, dass sich die Anzahl der teilnehmenden Akteure in diesem Zeitraum jährlich verdoppelt hat und aktuell mehr als 60.000 Akteure umfasst. Die Anzahl der „Bug Bounty“-Programme hat sich im Jahr 2017 ebenfalls verdoppelt und umfasst aktuell mehr als 600 verschiedene Programme. Insgesamt wurden bis 2017 mehr als 96.000 Hinweise auf Schwachstellen eingereicht. Jedes Jahr werden durchschnittlich 221 kritische Schwachstellen bei der Plattform „Bugcrowd“ gemeldet. Diese Zahlen verdeutlichen, dass die Unternehmen immer mehr Geld in BBPs investieren, um die Anzahl an Schwachstellen in den eigenen Softwareprodukten erfolgreich zu reduzieren und damit einen dringend notwendigen höheren Level an IT-Sicherheit zu erreichen.

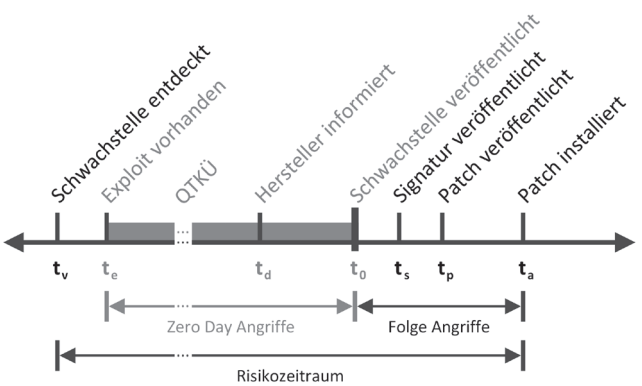
Bug Bounty Programme sind ein sehr effektives Mittel den Level an IT-Sicherheit in der IT und im Internet zu erhöhen (vgl. mit /Radi07/).

2.2 Zero Day Exploits

Schwachstellen in Software durchlaufen verschiedene Lebenszyklen. Die Gefahren und Handlungsempfehlungen zu einer Schwachstelle können in Abhängigkeit von dem aktuellen Zustand ermittelt werden. Bei der Verwendung von Schwachstellen zur Quellen-TKÜ muss der gesamte Risikozeitraum berücksichtig werden. In Abb. 1 (vgl. mit /Bilge12/) sind die verschiedenen Lebenszyklen und der Risikozeitraum dargestellt.

Der Lebenszyklus beginnt damit, dass eine Schwachstelle in einem Softwareprodukt gefunden wurde. Die größte Gefahr geht von einer gefundenen Schwachstelle aus, wenn diese dem Hersteller und der Öffentlichkeit unbekannt ist und bereits ein Exploit

Abb. 1 | Lebenszyklus einer Schwachstelle und Einfluss der Quellen-TKÜ darauf



zu der Schwachstelle programmiert wurde, die Angreifer nutzen können. Ein Exploit ist ebenfalls eine Software, die eine Schwachstelle automatisiert ausnutzen kann, um beispielsweise Zugriff auf ein Informationssystem zu erlangen. In diesem speziellen Fall wird von „Zero Day Exploits" (ZDE) gesprochen. Die besondere Gefahr von ZDEs resultiert direkt aus der Unwissenheit und der Tatsache, dass eine Schwachstelle potentiell automatisiert ausgenutzt werden kann. In dem Zeitraum von t_e bis t_0 existieren dementsprechend keine Schutzvorkehrungen oder Handlungsempfehlungen. In diesem Zeitraum sind „Zero Day Angriffe" (ZDA) besonders wirkungsvoll. Da die Strafverfolgungsbehörden ebenfalls ZDEs für die Installation des Bundestrojaners verwenden müssen (vgl. mit Kapitel 3.2), wird dadurch der Risikozeitraum deutlich erhöht (vgl. mit Kapitel 4.4). Ein schnelles Eliminieren der Schwachstelle durch den Hersteller wird damit verhindert.

Zum Zeitpunkt t_d wurde der Hersteller einer Software über eine Schwachstelle in seinen Produkten informiert. Diese Information kann ihm unteranderem durch ein „Bug Bounty"-Programm mitgeteilt worden sein. Der Hersteller hat nun die Möglichkeit, den entsprechenden Fehler zu beheben und ihn zu veröffentlichen, falls es noch nicht auf anderen Wegen geschehen ist.

Mit der Veröffentlichung einer Schwachstelle wird ein „Common Vulnerabilities and Exposures" (CVE) Eintrag erstellt. Dieser Eintrag enthält Erklärungen zu der Schwachstelle und Versionshinweise zu der betroffenen Software. Aus diesen Informationen können zum Zeitpunkt t_0 zum ersten Mal Schutzvorkehrungen und Handlungsempfehlungen abgeleitet werden. Zu diesem Zeitpunkt ist die Gefahr der Schwachstelle aber noch nicht gebannt, denn mit der Veröffentlichung eines CVE können weitere Angriffe motiviert werden.

Der Zeitraum von t_d bis zur Veröffentlichung einer Fehlerbehebung in t_p hängt von vielen verschiedenen Faktoren, wie z.B. der Größe eines Unternehmens, der Komplexität des Fehlers oder wie schwerwiegend eine Schwachstelle ist, ab. Mit der Veröffentlichung eines Patches nimmt die Gefahr einer Schwachstelle drastisch ab. Bis zum Zeitpunkt t_a kann die Schwachstelle aber weiterhin von Angreifern ausgenutzt werden, daher sollen die Anwender den vorhandenen Patch sofort einspielen. Es gibt viele Initiativen, den Zeitraum t_d bis t_a so klein wie nur möglich zu gestalten.

3 Unterschiede der TKÜ und Quellen-TKÜ

Die klassische TKÜ beruht auf passiven Abhören der Kommunikation zwischen zwei Kommunikationsteilnehmern (siehe Abb. 2). Für die technische Umsetzung des Abhörens sind die Telekommunikationsanbieter gesetzlich verpflichtet, eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) spezifizierte Schnittstelle in ihre Systeme zu integrieren. Das im Prinzip passive Abhören der Kommunikation erfolgt direkt in der Kommunikationsinfrastruktur. Aus diesem Grund wird die Integrität, die IT-Sicherheit, der beteiligten Endgeräte nicht verändert. Eine Veränderung der Integrität kann theoretisch nur innerhalb des Kommunikationskanals erfolgen.

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. Aus Sicht der IT-Sicherheit handelt es sich dabei um eine akzeptable und handhabbare Lösung.

Abb. 2 | Klassische TKÜ aus Sicht der IT-Sicherheit

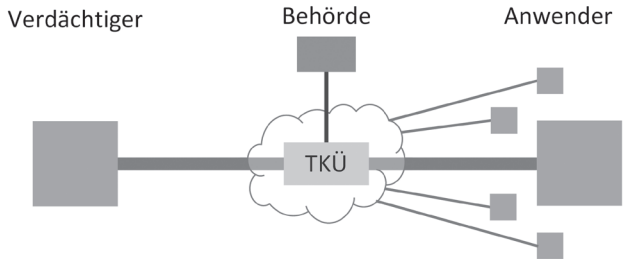
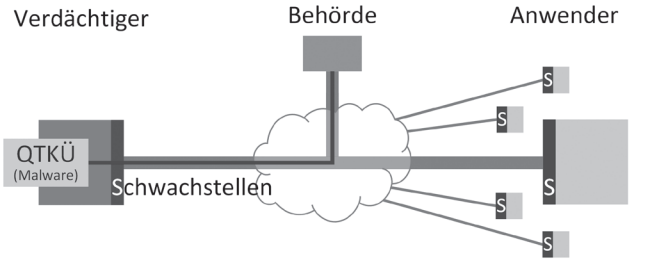


Abb. 3 | Quellen-TKÜ aus Sicht der IT-Sicherheit



Anders sieht es jedoch bei der Quellen-TKÜ aus (siehe Abb. 3). Für die technische Realisierung der Quellen-TKÜ muss zwingend eine Abhörsoftware (Malware) zum Abhören auf dem Endgerät der verdächtigen Person aufgespielt werden. Das Aufspielen der Abhörsoftware sollte im Sinne der Strafverfolgung überwiegend geheim erfolgen, also ohne das Wissen und die Zustimmung der verdächtigen Person. Somit wird durch das Aufspielen der Abhörsoftware im Hintergrund die Integrität des Endgerätes aktiv verändert.

Das Aufspielen von zusätzlicher, ungewollter Abhörsoftware im Hintergrund wird aus Sicherheitsgründen von allen gängigen Betriebssystemen verhindert. Aus diesem Grund muss eine Schwachstelle in der vorhandenen Software auf dem Endgerät des Verdächtigen ausgenutzt werden, weil der Verdächtigte diesen Vorgang ja eigentlich nicht möchte. Im Vergleich zur klassischen TKÜ kommt also erschwerend hinzu, dass alle anderen Geräte im Internet potentiell durch dieselbe Schwachstelle in der verwendeten Software gefährdet sind. Auch wenn die technischen Rahmenbedingungen bei der Quellen-TKÜ ebenfalls vom BSI spezifiziert werden, folgt daraus dennoch, dass es sich um eine Lösung mit starken Wechselwirkungen handelt. Diese können von den Strafverfolgungsbehörden nicht alleine kontrolliert werden. Der Level der IT-Sicherheit aller unbeteiligten Geräte (Nutzer) wird dadurch reduziert. Die Wechselwirkungen bezüglich der IT-Sicherheit werden in Kapitel 4 genauer erläutert.

3.1 Der Bundestrojaner

Die technische Umsetzung der Quellen-TKÜ, insbesondere die Verwendung von Schwachstellen und die Veränderung der Integrität des Endgerätes, ist gleichzusetzen mit der gängigen Vorgehensweise von Schadsoftware/Malware im Internet durch kriminelle Organisationen. Aufgrund dieser beiden Eigenschaften wird die auf dem Endgerät des Verdächtigen installierte Software als

„Bundestrojaner" bezeichnet. Trojaner sind im allgemeinen eine spezielle Form von Malware.

Aktuell wird Malware, insbesondere Ransomware, von kriminellen Hackern vermehrt verwendet, um finanziellen Profit zu erzielen. Hierfür wird das IT-System des Opfers zuerst mit der Ransomware infiziert. Mit Hilfe der Malware werden anschließend die Daten des Opfers auf dem IT-System durch kriminelle Organisationen verschlüsselt. Eine Entschlüsselung der Daten ist in den meisten Fällen nur möglich, indem die kriminelle Organisation den zugehörigen Schlüssel für die Entschlüsselung zur Verfügung stellt. Damit dies geschieht, müssen die Betroffenen in der Regel einen Geldbetrag (z.B. in Form von „Bitcoins") an die Kriminellen überweisen. Bei diesem Szenario wird also Malware für die Umsetzung einer Erpressung verwendet.

Bei der Quellen-TKÜ wird der Bundestrojaner (Malware) verwendet, um Kommunikationsdaten des Verdächtigen noch vor der Verschlüsselung oder nach der Entschlüsselung abzugreifen und an die Abhörsysteme der Strafverfolgungsbehörde zu versenden. Die Steuerung des Bundestrojaners erfolgt über eine „Command & Control" (C&C) Struktur. Diese kann beispielsweise verwendet werden, um nachträglich Funktionalitäten hinzuzufügen oder die Entfernung des Bundestrojaners vom Endgerät des Verdächtigen zu veranlassen.

3.2 Verteilung des Bundestrojaners

Angreifer (kriminelle Organisationen, politisch und wirtschaftlich orientierte Spione, Terroristen, usw.) und Strafverfolgungsbehörden nutzen Software-Schwachstellen und menschliche Unzulänglichkeiten aus, um Malware/Bundestrojaner auf IT-Endgeräten zu installieren. Über E-Mail-Anhänge oder unsichere Webseiten mit Hilfe von sogenannten „Drive-by Downloads" wird hauptsächlich Malware in IT-Endgeräte unbemerkt eingeschleust.

Die notwendigen Software-Schwachstellen werden dabei überwiegend in weit verbreiteten Softwareprodukten ausgenutzt, wie z.B. „Flash", „Java", „Internet Explorer", „Adobe PDF" oder „Office Produkten". Existieren kritische Schwachstellen in diesen Produkten, dann kann eine Schadsoftware schon während der Benutzung auf dem IT-Endgerät aufgespielt werden. So kann es beispielsweise sein, dass eine Schadsoftware bereits bei dem Besuch einer Webseite installiert wird.

Zum aktuellen Zeitpunkt gibt es keine Erkenntnisse zu der konkreten Umsetzung der Quellen-TKÜ. Aus diesem Grund muss davon ausgegangen werden, dass neben dem physischen Zugang zum Endgerät eines Verdächtigen, ebenfalls gängige und vergleichbare Strukturen aus dem Bereich der Cyberkriminalität für die Installation des Bundestrojaners verwendet werden (vgl. mit /CCC11/). Viele der aktuellen Infektionen mit Malware beruhen auf der Verwendung von sogenannten „Exploit Kits". Diese stellen grundsätzlich einen Baukasten mit allen notwendigen Modulen für das automatische Ausnutzen von Schwachstellen und der Installation von Malware im Hintergrund dar. Für den effektiven Betrieb des Bundestrojaners im Internet, wird es zwangsläufig einen vergleichbaren, modularen Baukasten geben. Dieser wird aufgrund von technischen Limitierungen, z.B. durch Sicherheitsmechanismen im Internet oder verschiedenen Softwarearchitekturen, vergleichbare Eigenschaften und Probleme von „Exploit Kits" aufweisen.

Diese Gemeinsamkeiten werden im weiteren Verlauf des Artikels genauer beschrieben. Es wird gezeigt, dass durch die Verwendung von ähnlichen Strukturen für die technische Realisierung der Strafverfolgung mittels Quellen-TKÜ die IT-Sicherheit auf viele verschiedene Weisen eingeschränkt wird.

3.3 Verstecken des Bundestrojaners

Während der Installation und Ausführung des Bundestrojaners müssen neben einer existierenden Schwachstelle, ebenfalls Techniken verwendet werden, um gängige Schutzmechanismen auf dem Endgerät des Verdächtigen zu umgehen. In erster Linie geht es hierbei um das Verstecken des Bundestrojaners vor Antiviren (AV) Software. Die Installation von AV Software wird von IT-Sicherheitsexperten in nahezu jeder Empfehlung für den sicheren Umgang im Internet genannt, so auch im IT-Grundschutz des BSI. Es ist also davon auszugehen, dass verdächtige Personen ebenfalls eine AV Software installiert haben, um sich beispielsweise vor dem Bundestrojaner zu schützen. Neben dem Verstecken des Bundestrojaners vor AV Software, müssen auch Funktionalitäten des Betriebssystems auf dem Endgerät manipuliert werden. Als Beispiele hierfür kann der Prozessmonitor von Windows, die Verwendung von Signaturen für den Schutz von Programmkomponenten oder das Rechtemanagement betrachtet werden. Der Prozessmonitor zeigt beispielsweise alle aktiven Anwendungen auf dem System an. Da es sich bei dem Bundestrojaner grundsätzlich auch um eine Anwendung handelt, würde diese im Prozessmonitor aufgeführt werden. Über den Prozessmonitor könnte der Bundestrojaner sogar an der Ausführung gehindert werden. Ohne entsprechende technische Vorkehrungen müssen die Strafverfolgungsbehörden damit rechnen, dass der Bundestrojaner von einer AV Software, dem Betriebssystem oder dem Verdächtigen erkannt und an der Ausführung gehindert wird.

Das Verstecken von Malware vor AV Software kann umgangssprachlich als „Katz-und-Maus-Spiel" bezeichnet werden. Für die technische Realisierung des Versteckens gibt es keine hundertprozentige Lösung, genauso, wie es andersherum keinen hundertprozentigen Schutz vor Malware gibt (vgl. mit Kapitel 5). Unabhängig von der konkreten Umsetzung des Versteckens, untergräbt bereits die Idee dahinter, einen wesentlichen Schutzmechanismus zur Schaffung von IT-Sicherheit im Internet, nämlich die Verwendung von effektiver AV Software. Die Säulen der IT-Sicherheit sollten im Zuge der Digitalisierung und den immer größer werdenden Gefahren der Computerkriminalität gestärkt werden. Eine staatliche Förderung von Mechanismen zur Untergrabung von AV Software stellt das komplette Gegenteil dar.

4 Negative Beeinflussung der IT-Sicherheit aller Bürgerinnen und Bürger, sowie aller Unternehmen, Behörden und weiteren Organisationen

Bei der Beschreibung der Unterschiede zwischen TKÜ und Quellen-TKÜ wurde bereits angedeutet, dass die Verwendung von Schwachstellen für das Aufspielen des Bundestrojaners mit Wechselwirkungen verbunden ist. In diesem Kapitel soll zum einen gezeigt werden, welche Wechselwirkungen konkret entstehen können und zum anderen soll anhand von Zahlen und Fakten verdeutlicht werden, warum die Wechselwirkungen nicht von einer Instanz alleine kontrollierbar sind. Anhand dieser beiden

Aspekte kann anschließend die negative Beeinflussung der IT-Sicherheit aller Endgeräte abgeleitet werden.

Der Schwerpunkt der Analyse beruht auf der Verwendung von „Drive by Downloads“ mittels „Exploit Kits“ als relevantesten Angriffsvektor für die Strafverfolgung (vgl. mit Kapitel 3.2).

Für die Aufbereitung von Zahlen und Fakten wurden öffentlich bekanntgewordene Schwachstellen (z.B. aus der CVE-Datenbank oder „Contagio“ /Cont15/), aus den Jahren 2012-2015, sowie Security Reports von Sicherheitsfirmen verwendet.

4.1 Viele Schwachstellen benötigt

Die Auswertung von prominenten „Exploit Kits“ aus den letzten Jahren hat ergeben, dass eine Schwachstelle alleine nicht ausreicht, um in der Praxis eine Schadsoftware effektiv auf viele Endgeräte zu verteilen. In Abb. 4 ist dargestellt, wie viele verschiedene Schwachstellen von den prominenten „Exploit Kits“ verwendet werden.

Abb. 4 | Anzahl verwendeter Schwachstellen von populären „Exploit Kits“

	Angler	Magnitude	Neutrino	Nuclear	Rig	Styx	SweetOrange	Blackhole	Ø
2012-2013	5	6	9	6	-	12	9	11	9
2014-2015	14	9	-	15	12	-	10	-	12

Im Jahr 2015 wurden **durchschnittlich 12 Schwachstellen** verwendet. Es ist anzunehmen, dass diese Zahl in der Praxis noch höher ist, da die Dunkelziffer bei der Analyse von Schadsoftware generell hoch ist und der modulare Aufbau von „Exploit Kits“ die Annahme von weiteren Funktionen erschwert.

Ein wesentlicher Unterschied zwischen der Verwendung von „Exploit Kits“ für die Strafverfolgung und der Verteilung von Schadsoftware aus anderen Profitgründen ist die Definition des „effektiven“ Verteilens. Stehen beispielsweise finanzielle Beweggründe im Vordergrund, dann ist eine Massenverbreitung effektiv. Geht es um die Strafverfolgung, dann ist eine zielgerichtete Infektion mit dem Bundestrojaner notwendig. Die grundsätzliche Problemstellung ist jedoch bei beiden Anwendungsszenarien identisch: Es werden Kombinationen von Schwachstellen benötigt, die eine effektive Verteilung im Kontext des jeweiligen Anwendungsszenarios ermöglichen.

Für die Strafverfolgungsbehörden ist es schwieriger, dieser Problemstellung gerecht zu werden, denn es wird zu einem bestimmten Zeitrahmen zwingend eine mögliche Kombination an Schwachstellen benötigt, damit das Abhören eines bestimmten Verdächtigen oder einer bestimmten Gruppe von Verdächtigen mit sehr unterschiedlichen Endgeräten begonnen und eine Straftat im besten Fall verhindert werden kann. Für einen Angreifer mit finanziellen Beweggründen ist es wahrscheinlich vernachlässigbar, wenn zu einem bestimmten Zeitpunkt eine bestimmte Personengruppe nicht zu erreichen ist.

In dem betrachteten Zeitraum von 2012 bis 2015 wurden überwiegend Endgeräte aus dem Desktop-Bereich mit „Exploit Kits“ angegriffen. Ab 2015 konnte ein signifikanter Anstieg der entdeckten Schwachstellen auf mobilen Endgeräten festgestellt werden /Sym16/. Der Anstieg verdeutlicht, dass Cyberkriminelle zunehmend ihre Werkzeuge für mobile Endgeräte optimieren und hierfür entsprechende Schwachstellen suchen. Es ist davon auszugehen, dass sich dieser Trend auf die zukünftigen „Exploit Kits“ auswirkt und die Anzahl der verwendeten Schwachstellen erhöht.

Aus diesen Überlegungen lässt sich folgern, dass Strafverfolgungsbehörden im Vergleich zu Cyberkriminellen höchstwahrscheinlich einen größeren „Pool“ an Schwachstellen benötigen, also mehr als durchschnittlich 12 Schwachstellen pro Jahr. Diese Annahme kann untermauert werden, indem die Anforderungen an die benötigten Kombinationen genauer betrachtet werden.

4.2 Kombinationen von Schwachstellen

In Kapitel 3.2 wurde bereits darauf eingegangen, dass die prominenten „Exploit Kits“ im Internet Schwachstellen in weit verbreiteter Software, wie z.B. „Flash“, „Java“, „Internet Explorer“, „Adobe PDF“ oder „Office Produkten“ verwenden. Hierbei handelt es sich überwiegend um Softwareprodukte, die interoperable für verschiedene Betriebssysteme entwickelt wurden. Aufgrund der Interoperabilität kann mit einer Schwachstelle eine große Menge von Anwendern angegriffen werden.

Grundsätzlich wird von IT-Sicherheitsexperten die Ansicht vertreten, dass das Schutzniveau im Internet drastisch erhöht werden kann, wenn die besonders anfälligen Softwareprodukte nicht mehr verwendet werden. Diese Tatsache kann für die Quellen-TKÜ ein Problem darstellen, denn die Verdächtigen könnten ebenfalls auf besonders anfällige Softwareprodukte verzichten. In diesem Fall wird die Menge der relevanten Softwareprodukte reduziert und somit die Suche nach möglichen Schwachstellen für eine Strafverfolgung drastisch erschwert. Für die Suche nach möglichen Kombinationen müssen die nachfolgenden Aspekte berücksichtigt werden.

- Neben „Windows“ müssen weitere Betriebssysteme, wie „MacOS“, „Linux“, „Android“, „iOS“ oder neue Betriebssysteme für „SmartWatches“, usw. bei der Suche nach Schwachstellen berücksichtigt werden.
- Jedes Betriebssystem bringt eine andere Architektur und unterschiedliche Sicherheitsmechanismen mit. Die Wahl des Betriebssystems kann also bereits zu einem höheren Schutz im Internet führen und somit die Installation des Bundestrojaners erschweren.
- Für die unterschiedlichen Betriebssysteme existieren unterschiedliche vorinstallierte Anwendungen zur Durchführung von Aufgaben im Internet. Diese Unterschiede werden besonders bei den Web-Browsern und E-Mail-Programmen deutlich.
- Schwachstellen sind häufig nur in bestimmten Versionen von Software enthalten. Diese speziellen Versionen müssen dann auf dem Endgerät des Verdächtigen vorhanden sein. Regelmäßige Updates können beispielsweise vor älteren Schwachstellen schützen.
- Betriebssysteme für mobile Geräte (insbesondere „Android“) weisen im Vergleich zu Betriebssysteme für Desktop-Computer (hierzu können beispielsweise auch Notebooks gezählt werden) eine hohe Fragmentierung mit großen Unterschieden in den verwendeten Softwarekomponenten auf. Die Gründe hierfür sind unterschiedliche Anforderungen und Umsetzungen der Gerätehersteller /Han12/. Inkompatibilitäten innerhalb verschiedener Versionen eines mobilen Betriebssystems führen häufig schon bei der normalen Entwicklung einer Software zu

Problemen. Die Fragmentierung der mobilen Betriebssysteme kann dazu führen, dass die Anzahl der benötigten Schwachstellen steigt. Dieses Problem tritt bei Desktop Geräten in der Regel nicht auf, da die Anforderungen an die Hardware direkt von den Herstellern des Betriebssystems festgelegt werden (vgl. z.B. mit „Windows Hardware Compatibility Program").

- Nicht alle Schwachstellen sind für die Installation des Bundestrojaners geeignet. Bei der Verwendung von „Exploit Kits" werden überwiegend kritische Schwachstellen (mit einem CVSS-Score > 9) benötigt (siehe Abb. 5).

Aus den genannten Punkten lässt sich ableiten, dass es sehr viele mögliche Kombinationen von Softwareprodukten gibt. Es ist davon auszugehen, dass die Anzahl der möglichen Kombinationen zukünftig weiter steigt. Beispielsweise ergeben sich durch die zunehmende Etablierung von „Wearables" (wie z.B. „SmartWatches") und der Diversifizierung von mobilen Betriebssystemen neue Kombinationen, die für die Quellen-TKÜ relevant sein können. Je mehr Kombinationen für die Strafverfolgung berücksichtigt werden müssen, desto ineffektiver ist die zielgerichtete Verwendung von „Exploit Kits".

4.3 Simultane Verwendung ist wahrscheinlich

Neben der Anzahl an Schwachstellen in den populären „Exploit Kits" (siehe Kapitel 4.1), kann aus den verwendeten Datenquellen ermittelt werden, wie wahrscheinlich eine simultane Verwendung der Schwachstellen von verschiedenen Instanzen ist. In Abb. 5 ist dargestellt, welche Schwachstellen im Zeitraum von 2012 bis 2015 simultan von verschiedenen „Exploit Kits" verwendet wurden.

Der Grafik kann entnommen werden, dass es sehr viele Überschneidungen bei den verwendeten Schwachstellen gibt. Der größte Anteil der dargestellten Schwachstellen hat den maximalen CVSS-Score von 10. Es handelt sich dabei also um äußerst kritische Schwachstellen. Mit Blick auf diese Daten muss davon ausgegangen werden, dass relevante Schwachstellen für die Quellen-TKÜ ebenfalls von Cyberkriminellen verwendet werden. Eine derartige Wechselbeziehung stellt eine große Gefahr für die IT-Sicherheit im Internet dar. Auf der einen Seite wird hierdurch deutlich, dass Schwachstellen höchstwahrscheinlich auf dem „Black Market" gehandelt werden. Auf der anderen Seite ergibt sich daraus eine parallele Gefahr für die Anwender im Internet, wenn durch die Quellen-TKÜ beispielsweise die Zeit für die Veröffentlichung von Fehlerbehebungen erhöht wird (vgl. mit Kapitel 2.2).

4.4 Kauf von Schwachstellen ist erforderlich

Das Bundesministerium des Innern (BMI) hat eine neue Bundesbehörde mit dem Namen „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS) geschaffen, die helfen soll, verschlüsselte Kommunikation, wie WhatsApp, Skype, usw. im Klartext mitlesen zu können.

ZITiS ist in München angesiedelt und soll bis 2022 bis zu 400 Beamte, davon viele IT-Spezialisten, eingestellt haben.

Die Infrastruktur von „Bug Bounty"-Programmen, insbesondere die Kostenwirksamkeit, kann von keinem Unternehmen alleine abgebildet werden, selbst wenn es sich um die eigenen Softwareprodukte handelt (vgl. mit Kapitel 2.1). Eine wichtige Frage ist, wie ZITiS die Aufgabe bezüglich der notwenigen Schwachstellen zukünftig für externe Softwareprodukte bewerkstelligen kann. Erschwerend kommt hinzu, dass im Internet sehr viele verschiedene Kombinationen von Softwareversionen und verschiedenen Betriebssystemen berücksichtig werden müssen, um einen lauffähigen Bundestrojaner langfristig betreiben zu können (vgl. mit Kapitel 4.2).

Abb. 5 | Simultan verwendete Schwachstellen der populären „Exploit Kits

CVE (2007-2015) \ Exploit Kit	Angler	Nuclear	Rig	SweetOrange	Magnitude	Blackhole	Neutrino	Styx		CVSS
CVE-2011-3544		x		x		x		x	4	10
CVE-2012-0507		x	x	x	x	x		x	6	10
CVE-2012-1723		x		x		x	x	x	5	10
CVE-2012-4681		x		x		x		x	4	10
CVE-2012-5076		x		x		x			3	10
CVE-2013-0074	x	x	x				x		4	9,3
CVE-2013-0422		x		x		x		x	4	10
CVE-2013-0431				x	x	x	x	x	5	5
CVE-2013-0634	x		x		x				3	9,3
CVE-2013-1493							x	x	2	10
CVE-2013-2423		x		x			x	x	4	4,3
CVE-2013-2460		x		x	x	x	x	x	6	9,3
CVE-2013-2463					x			x	2	10
CVE-2013-2465		x	x				x		3	10
CVE-2013-2471		x		x	x	x			4	10
CVE-2013-2551	x	x	x	x	x		x		6	9,3
CVE-2013-3896	x						x		2	4,3
CVE-2014-0322	x		x	x					3	9,3
CVE-2014-0497	x		x	x					3	10
CVE-2014-0515	x	x	x	x					4	10
CVE-2014-0569			x	x					2	10
CVE-2014-8439	x	x			x				3	10
CVE-2015-0311	x	x							2	10
CVE-2015-0336	x	x			x		x		4	9,3
CVE-2015-0359	x	x	x		x				4	10
Ø	11	17	10	15	10	9	10	10		
									3,7	9,2

Gehen wir positiv davon aus, dass von den 400 ZITiS-Mitarbeitern 300 IT-Sicherheitsexperten sein werden, die in der Lage sind, Schwachstellen zu finden, wie die Sicherheitsexperten bei „Bug Bounty"-Programmen.

Aus den Daten von „Bugcrowd" lässt sich ableiten, dass mit 300 IT-Experten statistisch gesehen 16 kritische Schwachstellen in einem Jahr gefunden werden können (siehe Abb. 6).

Abb. 6 | Anzahl kritischer Schwachstellen pro Mitglied (Vollzeit) der Plattform „Bugcrowd"

	2013-2015	2016	2017
Mitglieder	17994	26782	60000
Mitglieder (Vollzeit)	2699	4017	9000
Neue Kritische Meldungen (mit Duplikaten)	175	657	208
Anteil doppelter Einreichungen	35,8%	36,2%	36,0%
Neue Kritische Meldungen (ohne Duplikate)	112	419	133
Ø	221		

Kritische Meldungen pro Mitglied (Vollzeit)	0,0820	0,0551	0,0246
Ø	0,0539		
300 Mitglieder (Vollzeit)	16,1729		

In Kapitel 4.1 wurde gezeigt, dass die populären „Exploit Kits" durchschnittlich 12 Schwachstellen für die Installation von Malware auf Desktop Endgeräten verwenden. In dem betrachteten

Zeitraum von 2012 bis 2015 haben die Betriebssysteme: „Windows“, „MacOS“ und „Linux“ nahezu den gesamten Marktanteil im Desktop-Bereich abgedeckt /Stat17/. Die 12 Schwachstellen haben sich also über drei verschiedene Betriebssysteme hinweg gestreckt. In Kapitel 4.2 wurde auf die große Fragmentierung der Betriebssysteme für mobile Endgeräte und den damit verbundenen Inkompatibilitäten eingegangen. Im Juni 2016 wurden parallel acht verschiedene Versionen der gängigsten Betriebssysteme für mobile Endgeräte verwendet. Den größten Anteil daran hat das Betriebssystem „Android“ mit fünf verschiedenen Versionen /Stat16/. Wird die Anzahl der benötigten Schwachstellen im Desktop-Bereich betrachtet, dann werden hochgerechnet 32 Schwachstellen pro Jahr für den mobilen Bereich benötigt. Die höhere Anzahl an benötigten Schwachstellen resultiert aus der höheren Anzahl an verschiedenen Betriebssystemversionen, die potentiell eine Inkompatibilität untereinander aufweisen. Insgesamt werden also für die Abdeckung aller Endgeräte 44 Schwachstellen benötigt. Mit 16 selbst gefundenen Schwachstellen würde ZITiS also keine durchgehende Quellen-TKÜ mit dem Bundestrojaner auf allen Endgeräten gewährleisten können.

Die Erkenntnis, dass zu einem bestimmten Zeitpunkt innerhalb eines Jahres weitere unbekannte Schwachstellen für die effektive Verbreitung von Malware benötigt werden, ist insbesondere im Umfeld des „Black Markets“ nicht neu. Es ist gängige Praxis der Malware Entwickler, dass benötigte Schwachstellen eingekauft werden. Aus dieser Tatsache resultieren der Erfolg und das Wachstum des „Black Markets“. Damit die Quellen-TKÜ durchgängig realisiert werden kann ist davon auszugehen, dass die Strafverfolgungsbehörden Exploits auf dem „Grey Market“ kaufen.

Der „Grey Market“ ist grundsätzlich eine Abstufung des „Black Markets“. In der Praxis wird der „Grey Market“ als eine Instanz für die Vermarktung von Exploits für einen „vermeintlich positiven Zweck“, also z.B. für die Strafverfolgung mittels Bundestrojaner, betrachtet. Die Definition der Funktionsweise des „Grey Markets“ ist nur sehr schwammig möglich, insbesondere wenn es um die Interessen verschiedener Länder geht. Aufgrund der Aktivität einiger Akteure des „Grey Markets“ ist aktuell davon auszugehen, dass Exploits direkt zwischen dem „Grey Market“ und dem „Black Market“ gehandelt und gleichzeitig an verschiedene Instanzen (z.B. an autoritäre Regime zur Unterdrückung und Überwachung, an ausländisches Militär im Kontext von Cyberwar oder an ausländische Behörden zur Spionage) verkauft werden.

4.5 Schädliche Einschränkung von „Bug Bounty“-Programmen durch den Bundestrojaner

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“ vermarktet. Ein Exploit gilt solange als ZDE, bis die zugrundeliegende Schwachstelle dem Hersteller der Software gemeldet wurde und dieser einen entsprechenden Patch veröffentlicht hat (siehe Kapitel 2.2).

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. Der Wettbewerb hat direkt zur Folge, dass ein höherer Zielerreichungsgrad eines Akteurs, zu einem niedrigeren Zielerreichungsgrad des anderen führt. Die finanzielle Belohnung kann in diesem Zusammenhang als eine ausschlaggebende Komponente für die Definition des Zielerreichungsgrades betrachtet werden.

Problematisch ist in diesem Zusammenhang die Tatsache, dass die durchschnittlichen finanziellen Belohnungen der „Bug Bounty“-Programme für kritische Schwachstellen mit $1.776 weitaus geringer ausfallen, als der durchschnittliche Minimalpreis von $5.000 im „Black Market“. Für die „Bug Bounty“-Programme kommen 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 (vgl. mit /Allodi17/).

Daraus werden sich langfristig zahlreiche Probleme für die IT-Sicherheit ergeben, denn es ist davon auszugehen, dass sich Akteure von den „Bug Bounty“-Programmen zukünftig auf dem „Black Market“ positionieren, um einen höheren finanziellen Profit zu erzielen (vgl. mit /Radi07/). Diese Problematik wird durch den Kauf von Schwachstellen für den Betrieb des Bundestrojaners (siehe Kapitel 4.4) verschärft, denn es wird dadurch einseitig die Nachfrage an die Akteure des „Grey/Black Markets“ erhöht.

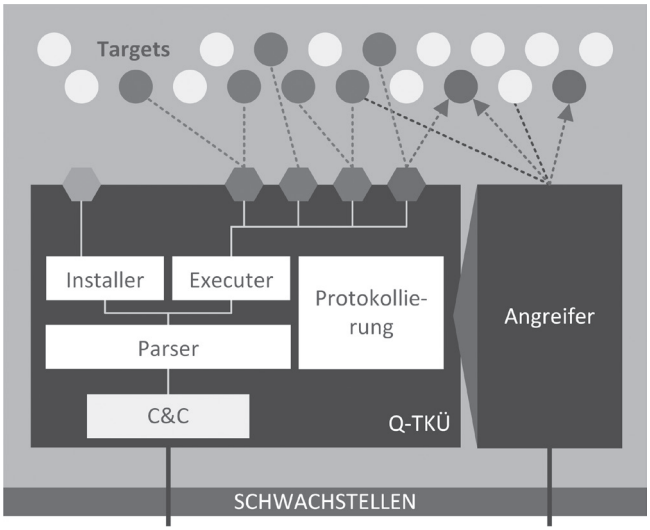
Durch die finanzielle Unterstützung des „Grey Markets“ durch ZITiS, würde indirekt auch dem „Black Market“ zu mehr Wachstum verholfen werden. Der Kauf von 28 Schwachstellen in einem Jahr hätte demnach zur Folge, dass sich die Anzahl der kritischen Meldungen bei der Plattform „Bugcrowd“ pro Jahr um 13% reduzieren würde (siehe Kapitel 4.4). Der jetzige Erfolg von „Bug Bounty“-Programmen würde dadurch sehr deutlich geschwächt, weil weniger Schwachstellen gepatcht und dadurch der Level an IT-Sicherheit aller Produkte reduziert werden (vgl. mit Kapitel 2.2). Damit würde unvermeidlich das Risiko angegriffen zu werden steigen und sich folglich der zu erwartende Schaden durch Cyberkriminalität im Internet erhöhen, weil mehr Angriffsfläche zur Verfügung steht.

5 Weitere Herausforderungen

In diesem Abschnitt werden weitere Herausforderungen diskutiert, die der Bundestrojaner hervorruft.
Abgesehen von den gesellschaftlichen Folgen durch die Reduzierung des Levels der IT-Sicherheit auf Basis des Bundestrojaners (siehe Kapitel 4), gibt es zahlreiche technische Hürden auf dem Endgerät des Betroffenen, die eine Strafverfolgung mittels Quellen-TKÜ erschweren können. Die Herausforderungen basieren im Wesentlichen auf dem sogenannten „Lying Endpoint Problem“ (LEP). In Abb. 7 ist die Problemstellung rund um das LEP dargestellt.

Zusammengefasst besagt das LEP, dass der Zustand eines Informationssystems nicht auf dem Informationssystem selber ermittelt werden kann (vgl. mit /Sahi07/). Mit anderen Worten: Die angestrebte revisionssichere Protokollierung durch den Bundestrojaner zum Zwecke der Forensik ist potentiell nicht realisierbar, da Manipulationen auf dem Endgerät des Verdächtigen nicht ausgeschlossen werden können.

Abb. 7 | Lying Endpoint Problem



Aus technischer Sicht kann aus dem LEP eine weitere Gefahr abgeleitet werden, denn Software auf einem Informationssystem kann im Allgemeinen entwendet und für andere Zwecke weiterverwendet werden. So können Hacker beispielsweise den Bundestrojaner als „Backdoor" für das Einschleusen eigener Schadsoftware verwenden, falls dieser ebenfalls Schwachstellen enthalten sollte. Denkbar ist ebenfalls, dass der Bundestrojaner insgesamt von Hackern entwendet wird und zusammen mit einer nachträglich implementierten C&C-Struktur für die Durchführung weiterer Angriffe im Internet verwendet wird (vgl. mit /CCC11/).

6 Zusammenfassung

Für die Gewährleistung der öffentlichen Sicherheit ist die Strafverfolgung ein wichtiger und notwendiger Bestandteil. Die zunehmende Verwendung von Verschlüsselung im Internet sorgt unweigerlich dafür, dass die Strafverfolgungsbehörden ihre technischen Werkzeuge für die TKÜ an die neue und zukünftige Situation anpassen müssen.

In diesem Artikel wurde die Verwendung von Schwachstellen als Basis für die Umsetzung einer Quellen-TKÜ analysiert. Das Ergebnis der 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 IT-Geräte (Nutzer) reduziert**. 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 abschließend geklärt 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.

Die aktuellen Probleme rund um die klassische TKÜ sind ein wesentlicher Auslöser für die Diskussion über die Einführung des Bundestrojaners. Die Quellen-TKÜ ist aber nicht das einzige Werkzeug für die Umsetzung einer Strafverfolgung. Die Ergebnisse dieses Artikels sollen dazu motivieren, die bestehenden Alternativen zur Quellen-TKÜ mittels Bundestrojaner zu diskutieren und ebenfalls in den Kontext der IT-Sicherheit zu setzen, um deutlich sicherere Lösungen für die notwenige Strafverfolgung unserer modernen Gesellschaft nutzen zu können.

Literatur

/Pohl14/ N. Pohlmann: „Die Vertrauenswürdigkeit von Software", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 10/2014

/Bitk17/ Bitkom: „Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro". Stand: 21.07.2017. https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html (abgerufen am 20.11.2017)

/Bugc17/ Bugcrowd: „State of Bug Bounty Report – Bugcrowd's third annual analysis of the global bug bounty economy". Stand: 2017. https://pages.bugcrowd.com/hubfs/Bugcrowd-2017-State-of-Bug-Bounty-Report.pdf (abgerufen am 21.09.2017)

/Bugc16/ Bugcrowd: „The State of Bug Bounty – Bugcrowd's second annual report on the current state of the bug bounty economy". Stand: Juni 2016. https://pages.bugcrowd.com/hubfs/PDFs/state-of-bug-bounty-2016.pdf (abgerufen am 21.09.2017)

/Bugc15/ Bugcrowd: „The State of Bug Bounty". Stand: Juli 2015.

/Sym16/ Symantec: „Internet Security Threat Report". Stand: April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (abgerufen am 18.09.2017)

/Sahi07/ Ravi Sahita, Uday R. Savagaonkar, Prashant Dewan, and David Durham: „Mitigating the Lying-Endpoint Problem in Virtualized Network Access Frameworks". In: Proceedings of the Distributed systems: operations and management, 18th IFIP/IEEE international conference on Managing virtualization of networks and services, San José, CA, 2007

/Finif13/ Matthew Finifter, Devdatta Akhawe, and David Wagner: "An empirical study of vulnerability rewards programs". In: Proceedings of the 22nd USENIX conference on Security, Washington, D.C., 2013

/Cont15/ Contagio: "A collection of the latest malware samples, threats, observations, and analyses". Stand: 25.05.2015. http://contagiodump.blogspot.de (abgerufen am 14.11.2017)

/Bilge12/ Leyla Bilge, Tudor Dumitras: "Before we knew it: an empirical study of zero-day attacks in the real world", In: Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, North Carolina, 2012

/BVerfG08/ Urt. v. 27.2.2008 – Az. 1 BvR 370/07, 1 BvR 595/07, Rn. 241.

/CCC11/ Chaos Computer Club: „Analyse einer Regierungs-Malware". Stand: 08.10.2011. http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (abgerufen am 14.11.2017)

/Radi07/ J. Radianti, J. J. Gonzalez: „Understanding Hidden Information Security Threats: The Vulnerability Black Market", In: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, Waikoloa, HI, 2007

/Allodi17/ L. Allodi: „Economic Factors of Vulnerability Trade and Exploitation: Empirical Evidence from a Prominent Russian Cybercrime Market". In: arXiv:1708.04866, 2017

/Stat16/ Statista: "Fragmentierung von mobilen Betriebssystemen". Stand: 27.06.2016. https://www.statista.com/chart/5118/mobile-os-fragmentation (abgerufen am 20.11.2017)

/Stat17/ StatCounter, "Market share of the leading operating system editions in Germany from January 2009 to March 2017", Stand: April 2017. https://www.statista.com/statistics/461815/operating-systems-market-share-germany (abgerufen am 20.11.2017)

/Han12/ D. Han, C. Zhang, X. Fan, A. Hindle, K. Wong, E. Stroulia: "Understanding Android Fragmentation with Topic Analysis of Vendor-Specific Bugs", In: 19th Working Conference on Reverse Engineering, 2012