medienimpulse
Beiträge zur Medienpädagogik

Weshalb der sogenannte Bundestrojaner eine schlechte Idee ist

Gedanken angesichts eines zunehmenden Überwachungspopulismus

AutorIn:Herbert Gnauer

Schon mehrfach wurden in Österreich zusätzlicheÜberwachungsmaßnahmen geplant. Herbert Gnauer berichtet den LeserInnen der MEDIENIMPULSE vom Scheitern dieser Pläne und sensibilisiert für aktuelle Probleme der Überwachung ...

I. Einleitung: Der Status Quo

Zu Jahresbeginn 2017 kehrte Innenminister Wolfgang Sobotka mit einer langen Wunschliste aus dem Weihnachtsurlaub zurück. Einmal mehr verlangte er im unmittelbaren Gefolge eines Attentates[1] nach Verschärfung bzw. Ausweitung von Überwachungsmaßnahmen, obwohl das Polizeiliche Staatsschutzgesetz (PStSG) erst ein knappes halbes Jahr zuvor in Kraft gesetzt worden war und sich die Bedrohungslage seit damals nicht im Geringsten geändert hatte. Eine Evaluation diesbezüglicher Bestimmungen wurde sowieso noch nie durchgeführt, so auch hier nicht. Besagte ministerielle Wunschliste war bereits Thema eines Post Scriptums zum Artikel HEAT - Das 1x1 der Überwachungs-Gesamtrechnung in Ausgabe 4/2016 der MEDIENIMPULSE[2].

Noch im Jänner wurden die einzelnen Begehrlichkeiten Punkt für Punkt ins Arbeitsübereinkommen der Bundesregierung[3] übernommen. Lediglich der Idee, Fußfesseln für nicht verurteilte "Gefährder" einzuführen, erteilte Justizminister Wolfgang Brandstetter später per Erlass eine Absage[4]. In den folgenden Monaten war das sogenannte Sicherheitspaket zwar immer wieder Gegenstand politischer Auseinandersetzungen und medialer Stellungnahmen, aber mit Ausnahme einer Verschärfung des Versammlungsrechts[5] wurden diesbezüglich keine weiteren Gesetzesentwürfe vorgelegt. Letztere wurde Ende März recht plötzlich als Initiativantrag im Nationalrat eingebracht und bereits knappe vier Wochen später beschlossen.

Erst als schon niemand mehr damit rechnete - zwischenzeitlich war die Koalitionsregierung zerbrochen - wurden die Karten auf den Tisch gelegt. Am 10. Juli 2017 schickte das Bundesministerium für Justiz (BMJ) das Strafprozessrechtsänderungsgesetz 2017 (325/ME)[6] in Begutachtung. Am selben Tag wurde dem Nationalrat seitens des Bundesministeriums für Inneres (BMI) ein Entwurf zur Änderung des Sicherheitspolizeigesetzes (326/ME)[7] übermittelt. Damit lag nun das gesamte Paket in Form konkreter Gesetzestexte vor.

Wer gehofft hatte, dass zumindest einige Forderungen angesichts der zahlreichen kritischen Stimmen[8] und vielfach geäußerten Warnungen[9] abgemildert worden wären, wurde enttäuscht. Ganz im Gegenteil fanden sich zur allgemeinen Überraschung sogar bis dahin unangekündigte Maßnahmen in den Entwürfen, so etwa eine Einschränkung des Briefgeheimnisses[10]. Auch die geplante Einrichtung von Sicherheitsforen[11] ließ aufhorchen, insbesondere der in diesem Zusammenhang vorgesehene Datenaustausch mit Privatpersonen machte viele stutzig. Ansonsten hatten, mit Ausnahme der oben erwähnten Fußfessel, alle zu Jahresbeginn geäußerten Ansinnen des Innenministers Eingang in die nun vorgelegten Entwürfe gefunden. Eine kritisch kommentierte Auflistung der wichtigsten Punkte ist auf der Website der Bürgerrechts-NGO epicenter.works[12] nachzulesen.

Dass die Begutachtungsfrist just in die Sommermonate fiel, wurde mit wenig Begeisterung zur Kenntnis genommen. Nicht wenige sahen darin einen Versuch, die Vorhaben möglichst unbemerkt an einer breiteren Öffentlichkeit vorbeizuschwindeln. Sollte dieser Plan je existiert haben, ist er jedenfalls gründlich gescheitert. Nicht zuletzt, weil epicenter.works ein Online-Tool anbot, das es erlaubte, mittels weniger Mausklicks aktiv am parlamentarischen Begutachtungsprozess teilzunehmen und eine Stellungnahme abzugeben[13]. So wurde die

Thematik erfolgreich breiteren Bevölkerungsschichten nähergebracht. Zudem wurden die von kritischen Stimmen gerne als 'Überwachungspaket' apostrophierten Gesetzesvorhaben immer wieder im beginnenden Wahlkampf aufgegriffen und in den Medien heftig diskutiert. Bis zum Ende der Frist am 21. August waren zu den beiden Entwürfen jeweils mehr als 9000 Stellungnahmen eingegangen[6], [7]. Das stellte einen einsamen Rekord dar und veranlasste epicenter.works, zwecks übersichtlicher Darstellung und erleichterter Analyse eine eigene Seite einzurichten[14].

Auch im öffentlichen Diskurs gewannen die kritischen Stimmen immer deutlicher Überhand, bis die Entwürfe schlussendlich nur noch von VertreterInnen der ÖVP in all ihren Punkten verteidigt wurden. Zuletzt wurde das in einer Sitzung des nationalen Sicherheitsrates deutlich, die kurzfristig für Freitag 31. August anberaumt worden war. Seither wird das Vorhaben in vorliegender Form überwiegend als vorläufig gescheitert angesehen[15], [16]. In der Tat scheint es trotz vereinzelter anderslautender Aussagen unwahrscheinlich, dass hier vor den Neuwahlen am 15. Oktober nochmals Bewegung eintreten könnte.

II. Der Bundestrojaner

Dass die einzelnen Punkte der Gesetzesvorhaben während der letzten Wochen öffentlich diskutiert und in den Medien dargestellt worden sind, ist grundsätzlich sehr zu begrüßen. Auch der Ruf nach einer längst überfälligen Evaluation bisheriger Überwachungsmaßnahmen[2] war zuletzt immer öfter zu hören. So darf ich einiges als bekannt voraussetzen und möchte mich hier vorrangig zwei sehr grundlegenden Aspekten widmen, die in so engem Zusammenhang miteinander stehen, dass sie gemeinsam behandelt werden können: Die Überwachung verschlüsselter elektronischer Kommunikation und der Einsatz von Spionagesoftware, besser bekannt unter dem allgemein verbreiteten Begriff Bundestrojaner.

Beides basiert auf der Ausnützung von Sicherheitslücken in den Betriebssystemen und installierten Programmen bzw. Apps auf Computern, Laptops, Tablets und Mobile Phones. Eine mit ausreichend starkem Key korrekt ausgeführte End-To-End-Verschlüsselung ist nach heutigem Stand der Technik mit vertretbarem Aufwand kaum zu knacken. Sollte eines Tages der Quantencomputer Wirklichkeit werden, dürfte es selbst mit der theoretischen Möglichkeit vorbei sein. Es kann daher in aller Regel nur vor der Verschlüsselung einer Nachricht oder umgekehrt nach ihrer Entschlüsselung angesetzt werden. Beides muss direkt auf einem der involvierten Geräte geschehen, Voraussetzung dafür ist die Installation besagter Spionagesoftware, vulgo Bundestrojaner. Selbst wenn es gelingt, sich physischen Zugang zu den betreffenden Geräten zu verschaffen, bleibt dort zumeist noch ein Sicherheitssystem zu überwinden. Das gilt insbesondere wenn ein professioneller Hintergrund vorliegt, wie es bei organisierter Kriminalität und großangelegten terroristischen Aktionen der Fall ist, wo verschlüsselte elektronische Kommunikation teils eine Rolle spielt. Deshalb ist Remote-Installation bei Spionagesoftware meist Mittel der Wahl. Aus denselben Gründen kann es ohne Sicherheitslücken diesbezüglich kein Auskommen geben.

Exploits[17] (von engl. ***to exploit*** 'ausnutzen') - d. h. heisst Einbrüche unter Ausnutzung von Sicherheitslücken und Fehlfunktionen in Betriebsystemen und Anwendungen - sind also eine notwendige Voraussetzung jeder Form von Online-Überwachung, bergen aber eine Menge von Gefahren in sich. Da wäre zunächst einmal die Entwicklung unerwünschter Eigeninteressen seitens der involvierten Sicherheitsinstitutionen. Sobald sie mithilfe von Exploits arbeiten und auf ihnen aufbauen, geraten sie unvermeidlich in eine gewisse Abhängigkeit. Eine geschlossene Schwachstelle steht ja auch für den eigenen Gebrauch nicht mehr zu Verfügung. So bekommen Institutionen, die für den Schutz von BürgerInnen - nicht zuletzt auch vor Cyberattacken zuständig sind - plötzlich Interesse am Fortbestand von Exploits. Diese Paradoxie ist nicht aufzulösen und wirkt im Sinn einer verbesserten Sicherheitslage kontraproduktiv.

Womit wir bei einem weiteren Problem angelangt wären. Denn die 'guten' Sicherheitsbehörden und Nachrichtendienste sind keineswegs die einzigen potenziellen Nutznießer. Zwar scheint der weit verbreitete Irrglaube zu bestehen, es gäbe an einem Exploit eine Art exklusives Nutzungsrecht. Dem ist aber nicht so, vielmehr können jederzeit weitere Personen unbemerkt Kenntnis von der betreffenden Schwachstelle erlangen. Sei es durch Zufall, sei es aufgrund gezielter Suche, sei es durch Kauf. Denn für derlei Informationen existieren dunkle und hoch

dotierte Märkte. Dem Argument, diese Märkte ließen sich im Fall einer Teilnahme beeinflussen, kann ich nichts abgewinnen. Der Handel mit Information und Know How, und um nichts anderes geht es hier, ist kaum kontrollierbar. Die Vorstellung, dass staatliche Stellen Gelder der öffentlichen Hand direkt oder indirekt in kriminelle Strukturen investieren, ist schwer erträglich und mit Demokratie eigentlich unvereinbar.

Selbst wenn die Software im eigenen Haus, das heisst im Auftrag eines der beteiligten Ministerien oder einer nachgereihten Dienststelle entwickelt werden sollte, müsste immer noch das Wissen um die Exploits angekauft werden, weil das Aufspüren von Schwachstellen unkalkulierbare Aufwände mit sich bringt. Davon abgesehen ist es mit einem einzigen Trojaner nicht getan. Schließlich sind mit Windows, MacOS und Linux schon einmal drei grundsätzlich unterschiedliche Plattformen verbreitet, die es wiederum in zahlreichen Versionen gibt. Dazu kommen die Betriebssysteme für mobile Geräte. Hier ist zwar Android mit großem Abstand am häufigsten, von dem allerdings wiederum vielerlei Varianten und Ableger existieren. Die mögliche Nutzungsdauer der einzelnen Schwachstellen ist höchst unterschiedlich. Während einige bereits nach kurzer Zeit geschlossen werden, überstehen andere ganze Generationen von Updates, wenn sie sich in unveränderten Abschnitten des Codes befinden und in die neuen Versionen unbemerkt hinüberrrutschen. Wird noch hinzugerechnet, dass eventuell auch auf dem jeweiligen Gerät installierte Programme bzw. Apps zu berücksichtigen sind, ergibt sich eine Fülle möglicher Kombinationen. Auch nur die häufigsten abzudecken, dürfte enormen Aufwand verursachen, weshalb Eigenentwicklungen in diesem Bereich entsprechend dotierte IT-Abteilungen voraussetzen. Bedenkt man ferner, dass Architektur und Funktionsumfang derartiger Spionagesoftware mittels Audits zu prüfen ist und gegebenfalls auch Anpassungen vorgenommen werden müssen, lässt sich erahnen, mit welchen Kosten tatsächlich zu rechnen sein wird.

III. Von Backdoors und Schadprogrammen: WannaCry und Stuxnet

So oder so, Sicherheitslücken können nicht im Tresor gelagert und für den Einsatz aus edlen Motiven reserviert werden. Das gilt gleichermaßen für zufällig oder durch fehlerhafte Programmierung entstandene Scherheitslücken, wie auch für teils vom Hersteller bewusst eingebaute Backdoors[18]. Sie alle sind stets in Gefahr, unbemerkt in falsche Hände zu geraten und stellen daher eine allgemeine Bedrohung dar. Dieser Umstand ist absolut unvermeidbar und durch nichts in den Griff zu bekommen. Wer meint, dass Staaten hier mithalten und sich aufrüsten sollten, denkt in den veralteten Schemata materieller Waffenarsenale. Cyberwaffen sind unsichtbar, lassen sich weder quantitativ noch qualitativ einschätzen und können daher auch keine abschreckende Wirkung nach Muster des Kalten Krieges entfalten.

Das Mai 2017 im wahrsten Sinn virulent gewordene Schadprogramm WannaCry[19] beruhte auf einer Schwachstelle im Netzwerkprotokoll SAMBA. Mehr als fünf Jahre war die Lücke bereits bekannt und wurde vor dem Hersteller Microsoft vorsätzlich geheimgehalten, damit sie von der US-amerikanischen National Security Agency (NSA) weiterhin genutzt werden konnte. Wenn dieser Zero Day[20] auch (vor allem hierzulande) glücklicherweise noch halbwegs glimpflich verlief, waren weltweit doch etliche Spitäler, Transport- und Logistikunternehmen und weitere in sensiblen Bereichen tätige Institutionen betroffen. Ohne den mehr oder minder zufällig relativ frühzeitig entdeckten 'Kill Switch'[19] hätte der Schaden zweifellos noch ganz andere Dimensionen angenommen.

Dabei scheint der erwartbare Nutzen im Verhältnis zu den Gefahren sehr gering, denn professionelle TäterInnen können sich der Überwachung durch sogenannte Bundestrojaner gleich auf mehreren Wegen entziehen. Auf niedrigster Stufe wäre da zunächst schlichte Neuinstallation von Betriebssystem und Software, wodurch die allermeisten Schadprogramme vom System verbannt werden können. Ausgenommen sind lediglich jene Programme, die in der Lage sind, sich auf der Hardware des Gerätes festzusetzen. Gegen sie hilft ein Wechsel des betreffenden Gerätes. Dem Vernehmen nach gehört eine größere Anzahl von Mobiltelefonen schon heute zur Grundausstattung organisiert tätiger Krimineller. Des Weiteren besteht auch die Möglichkeit, eigene Kommunikationssysteme abseits bekannter Messenger zu betreiben, die noch dazu verhältnismäßig leicht zu verbergen sind. Die Wirksamkeit derartiger Überwachungsmethoden ist also begrenzt, sobald professionell agierende Personen und Institutionen auf den Plan treten.

Dem gegenüber stehen übermäßig große Gefahren. Wer weiss zu sagen, welche Arten von Schadprogrammen bereits verbreitet wurden und auf Computersystemen in aller Welt unbemerkt schlummernd auf ihre Aktivierung warten? Niemand kann ermessen, wieviele Programme vom Schlage eines Stuxnet[21] existieren. Malware, die eigens dafür entwickelt wurde, lebenswichtige Systeme zu übernehmen, in ihrer Funktion zu stören oder gegebenenfalls ausser Gefecht zu setzen. Im vielbeschworenen Internet of Things (IoT)[22] soll jeder Haushalt über dutzende Geräte mit Internetanbindung verfügen. Jedes einzelne davon wäre im Fall eines Cyberwars ein potenzielles Angriffsziel. Allein durch die Möglichkeit, mittels Überhitzung Brände auszulösen, ließe sich immenser Schaden anrichten. Wer dieses Beispiel zu drastisch findet, kann sich auch mit der Vorstellung lahmgelegter Stromnetze begnügen. Als Angriffsziele kämen im Grunde sämtliche elektronisch gesteuerten Systeme in Frage, die in irgendeiner Form vernetzt sind. Bei Licht besehen, leben wir bereits seit geraumer Zeit in einer überaus verletzlichen Umgebung.

Überdies könnten findige Kriminelle den Spieß einfach umdrehen und die staatlichen Spionageprogramme dazu nutzen, Sicherheitsbehörden gezielt mit Falschinformation zu versorgen. Schadprogramme lassen sich einerseits durchaus enttarnen, weshalb auch die Hersteller von Virenscannern mitspielen müssten, damit ihre Produkte die Überwachungssoftware nicht im Zug von Scans melden oder gar außer Gefecht setzen. Andererseits könnten auch ausgesuchte Geräte absichtlich exponiert werden, um als sogenannte Honey Pots eine Infektion mit Spionagesoftware bewusst zu provozieren. Solcherart könnten Behörden in die Irre geführt, Einsatzkräfte an falsche Stellen gelockt und vom eigentlichen Zielort ferngehalten werden.

IV. Gegenstrategien

Die einzige wirksame Taktik gegen Exploits ist die konsequente Durchsetzung einer Informationspflicht. Im ersten

Schritt ist der Hersteller zu informieren. Sollte er das Sicherheitsproblem nicht innerhalb einer angemessenen Frist beheben, ist es weltweit bekannt zu machen. Damit wäre einerseits der Handel mit diesem Exploit unterbunden, denn niemand würde für öffentlich vorliegende Informationen bezahlen. Zweitens könnten Interessensvertretungen von Verbraucher*innen auf unwillige Hersteller Druck ausüben. Oder sich, im Fall von Open Source[23], selbst schützen, indem entsprechende Hotfixes[24] in Auftrag gegeben werden. Möglicherweise gelingt es eines Tages, im Rahmen der Produktgewährleistung einen Rechtsanspruch auf rasche Behebung von Sicherheitslücken zu erwirken. Da derlei Informationen über das Internet quasi in Echtzeit global verteilt werden können, ließen sich hier sehr effektive Strukturen entwickeln. Politische Unterstützung eines solchen Vorhabens wäre im Interesse der allgemeinen Sicherheit mehr als angebracht, erscheint aber bis auf Weiteres utopisch. Wie eben dargelegt, werden in diesem Zusammenhang derzeit (noch) andere Konzepte verfolgt.

Eine ausführlichere Darstellung der hier umrissenen Problematik findet sich in Otmar Lendls 'Thesen zu aktuellen Gesetzesentwürfen'[25]. Der Autor ist leitender Mitarbeiter des österreichischen Computer Emergency Response Team CERT.at und zählt unbestreitbar zu Österreichs führenden IT-Sicherheitsexperten. Sehr detailliert und kaum widerlegbar begründet er, weshalb jede Schwächung von Verschlüsselung letztlich eine Schwächung der allgemeinen Sicherheit mit sich bringt.

V. Conclusio

All dies vor Augen, kann Überwachung verschlüsselter elektronischer Kommunikation keineswegs als zeitgemäße Fortführung von Telefonüberwachung gesehen werden. Schon aufgrund technischer Implikationen bedeutet sie sehr viel mehr. Neben dem weiteren Verlust von Privatsphäre bringt sie unvermeidlich eine Gefährdung aller NutzerInnen digitaler Technologien mit sich. Im Namen vorgeblich erhöhter Sicherheit wird eine weltweite, völlig unkalkulierbare Bedrohung vorangetrieben. Durch das vorläufige Scheitern des Sicherheitspaketes wurde Zeit gewonnen. Es steht zu hoffen, dass sie für gründliches Nachdenken und einen faktenbasierten Diskurs genützt werden kann.

Linkliste

[1] Wikipedia-Artikel: Anschlag auf den Berliner Weihmachtsmarkt an der Gedächtniskirche:
https://de.wikipedia.org/wiki/Anschlag_auf_den_Berliner_Weihnachtsmarkt_an_der_Ged%C3%A4chtniskirche

[2] Medienimpulse 4/2016: HEAT - Das 1x1 der Überwachungs-Gesamtrechnung:
http://medienimpulse.at/articles/view/1008?navi=1

[3] Arbeitsprogramm der Bundesregierung 2017/2018:
http://archiv.bundeskanzleramt.at/DocView.axd?CobId=65201

[4] Kurier: Fußfessel für Gefährder nur Alternative zur U-Haft, Klarstellung per Erlass:
https://kurier.at/politik/inland/fussfessel-fuer-gefaehrder-nur-alternative-zur-u-haft/256.749.845

[5] Initiativantrag zur Änderung des Versammlungsgesetzes (2063/A):
https://www.parlament.gv.at/PAKT/VHG/XXV/A/A_02063/index.shtml#tab-Uebersicht

[6] Bundesgesetz, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017) (325/ME):
https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00325/index.shtml

[7] Ministerialentwurf zur Änderung von Sicherheitspolizeigesetz, Bundesstraßen-Mautgesetz 2002, Straßenverkehrsordnung 1960 und Telekommunikationsgesetz 2003 (326/ME):
https://parlament.gv.at/PAKT/VHG/XXV/ME/ME_00326/index.shtml

[8]

Kurier: Kritik an "überschießen-den Eingriffen" durch geplantes Sicherheitspaket:
https://kurier.at/politik/inland/kritik-an-ueberschiessenden-eingriffen-durch-geplantes-sicherheitspaket/277.393.758

[9] Salzburger Nachrichten: Gastkommentar VfGH-Präsident Gerhart Holzinger:
http://www.salzburg.com/nachrichten/oesterreich/politik/sn/artikel/hoechstrichter-holzinger-weist-staat-in-die-schranken-249769/

[10] Stellungnahme von epicenter.works zu 325/ME
https://epicenter.works/sites/default/files/epicenter.works_-_strafprozessaenderungsg_2017_325_me_xxv_gp_0.pdf

[11] Stellungnahme von epicenter.works zu 326/ME
https://epicenter.works/sites/default/files/epicenter.works_-_spg_bstmg_stvo_und_tkg_326_me_xxv_gp.pdf

[12] Website epicenter.works: Das steckt im Überwachungspaket
https://epicenter.works/thema/ueberwachungspaket

[13] Kampagnen-Website:
https://www.überwachungspaket.at

[14] Übersicht und Analyse der öffentlichen Stellungnahmen
https://www.überwachungspaket.at/konsultation

[15] Wiener Zeitung: Nationaler Sicherheitsrat - In die nächste Runde
http://www.wienerzeitung.at/nachrichten/oesterreich/politik/914410_In-die-naechste-Runde.html

[16] Futurezone: Nationaler Sicherheitsrat: Kein Nein, kein Ja der SPÖ zum Sicherheitspaket
https://futurezone.at/netzpolitik/nationaler-sicherheitsrat-kein-nein-kein-ja-der-spoe-zum-sicherheitspaket/283.803.101?utm_source=futurezone.at&utm_campaign=2df88d342d-newsletter_futurezone_at&utm_medium=email&utm_term=0_667c8ddbb8-2df88d342d-109944929

[17] Wikipedia-Artikel: Exploit
https://de.wikipedia.org/wiki/Exploit

[18] Wikipedia-Artikel: Backdoor
https://de.wikipedia.org/wiki/Backdoor

[19] Wikipedia-Artikel: WannaCry
https://de.wikipedia.org/wiki/WannaCry

[20] Wikipedia-Artikel: Zero Day
https://en.wikipedia.org/wiki/Zero-day_(computing)

[21] Wikipedia-Artikel: Internet der Dinge
https://de.wikipedia.org/wiki/Internet_der_Dinge

[22] Wikipedia-Artikel: Stuxnet
https://de.wikipedia.org/wiki/Stuxnet

[23] Wikipedia-Artikel: Open Source
https://de.wikipedia.org/wiki/Open_Source

[24] Wikipedia-Artikel: Hotfix
https://de.wikipedia.org/wiki/Hotfix

[25] Otmar Lendl: Ein paar Thesen zu aktuellen Gesetzesentwürfen
http://cert.at/services/blog/20170731130131-2076.html

Tags

überwachung, sicherheit, trojaner, gesetzgebung

Impressum und Offenlegung gemäß §25 des Mediengesetzes
Medieninhaber: Republik Österreich, Bundesministerium für Bildung
Zuständigkeit: Laut Bundesministeriengesetz 1986 in der jeweils geltenden Fassung
Hersteller: Bundesministerium für Bildung
Verlagsort: Wien
Herstellungsort: Wien
Kontakt: Bundesministerium für Bildung, Abteilung IT/3, Minoritenplatz 5, 1014 Wien
http://bmb.gv.at