Hannover IT

Position zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, Niedersächsisches Polizei- und Ordnungsbehördengesetz

Zusammenfassung

Online Durchsuchungen sowie Quellen-Telekommunikationsüberwachung basieren auf einem fundamentalen Eingriff in die technischen Geräte, denen Bürgerinnen und Bürger im Alltag vertrauen. Sie basieren technisch auf denselben Methoden, eine Eingrenzung einer „Durchsuchungssoftware“ auf diese oder jene Inhalte bleibt auf die Art der Datenausleitung beschränkt, und eine Unterscheidung der Inhalte ist nicht klar definierbar.

Die Nutzung von Technologie schafft viele neue Möglichkeiten und Chancen, ist aber immer auf Vertrauen ihrer Nutzerinnen und Nutzern angewiesen. Dieses Vertrauen wird durch den manipulativen Eingriff in alltäglich genutzte Geräte untergraben. Die missbräuchliche Nutzung von Informations- und Kommunikationstechnik hat weitreichende Folgen für die Kernbereiche der Privatsphäre Einzelner, aber auch für die Funktionsfähigkeit der Gesellschaft und der Wirtschaft insgesamt.

Für die sinnvolle und effiziente Nutzung von IKT muss daher Vertrauen in die Technik gestärkt werden, dies kann nicht auf leeren Versprechen beruhen, sondern muss auf nachvollziehbaren Tatsachen gründen. Dieses Vertrauen durch eine solide technische Basis zu stärken ist unser tägliches Brot. Die Anwendung von Online-Durchsuchungen und Quellen-TKÜ basiert aber immer auf einer lückenhaften Sicherheit informationstechnischer Geräte, und unterwandert damit ganz grundsätzlich die Informationssicherheit im Allgemeinen. Die dafür benötigte Software untergräbt die Vertraulichkeit und Integrität der anvisierten Systeme und ist somit selbst *Schadsoftware,* deren Schaden nicht auf die anvisierten Betroffenen begrenzt bleibt.

Sicherheitslücken schaden allen

Für einen Fernzugriff auf informationstechnische Geräte ist entweder die Installation von Hardware oder von Software erforderlich. Eine verdeckte Installation wird üblicherweise softwareseitig durchgeführt, und erfordert eine listige Täuschung der Betroffenen, die Manipulation der Netzwerkinfrastruktur, die Zusammenarbeit mit Softwareherstellern oder, und vor allem, die Ausnutzung von Sicherheitslücken.[1]

Sicherheitslücken in Software entstehen aufgrund der praktischen Unvermeidbarkeit von Fehlern und machen die ständige Überprüfung und Weiterentwicklung von Software notwendig. Verantwortungvolle Entwickler und Entwicklerinnen informieren die Hersteller über entdeckte Sicherheitslücken, damit diese sie beheben können. Bedauerlicherweise hat

[1]Vgl. Rehak, Rainer. 2014. “Angezapft - Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung”, S. 18ff. https://doi.org/10.18452/19264

sich aber ein Schwarzmarkt entwickelt, auf dem entdeckte Sicherheitslücken zur missbräuchlichen Nutzung verkauft werden. Wenn staatliche Akteure Sicherheitslücken für eigene Schadsoftware benötigen, müssen sie entweder selbst neue Sicherheitslücken finden, also eigene Ressourcen aufwenden, oder aber diese von anderen kaufen. Der Handel mit Sicherheitslücken gefährdet die allgemeine Sicherheit, da dadurch ein Interesse entsteht dieses möglichst lange offen zu halten, anstatt sie schnellstmöglich zu schließen. Je länger eine Sicherheitslücke besteht, desto mehr Akteure können Schadsoftware entwickeln, die diese Lücken ausnutzt. Im Falle des Einsatzes von staatlicher Schadsoftware wird damit aktiv gegen die allgemeine IT-Sicherheit gearbeitet. Die Folgen solchen Handelns wurden im Zuge des WannaCry-Vorfalls deutlich wo unzählige Organisationen, darunter auch Kliniken und die Deutsche Bahn,[2] lahmgelegt wurden, durch eine Sicherheitslücke die der NSA lange bekannt war. Eine frühzeitige Meldung der Schwachstelle an den Hersteller hätte erheblichen ökonomischen Schaden abwenden können.

Durch die eigene Entwicklung von Schadsoftware zum Zwecke der Onlinedurchsuchung und Quellen-TKÜ unterstützt der Staat somit strukturell die Unsicherheit der informationstechnischen Infrastruktur. Durch die strukturelle Förderung von Schwachstellen werden nicht zuletzt auch kriminellen und terroristischen Aktivitäten Möglichkeiten gegeben zivile Informationstechnik anzugreifen und zu missbrauchen. Somit wirkt dies dem eigentlichen Zweck der Polizei, dem Schutz der Bevölkerung, direkt entgegen. Vor dem Hintergrund der wachsenden Bedeutung von IKT in allen gesellschaftlichen Bereichen ist dies ein Risiko, das nicht hingenommen werden darf.

Spähsoftware enthält Lücken und kann verbreitet werden

Ungeachtet der Sicherheitslücken, an denen Schadsoftware ansetzt, kann diese selbst Schwachstellen enthalten und weiteren Missbrauch ermöglichen.[3] Software zur Online-Durchsuchung von Computern erfordern weitreichende Rechte auf den betroffenen Geräten, und sind daher im Falle eines Missbrauchs durch dritte besonders problematisch, und bergen somit zusätzliche Sicherheitsrisiken. Aufgrund der im Vorfeld unbekannten, unterschiedlichen Konfigurationen von persönlichen Geräten, und der fehlenden Möglichkeiten die Software im Vorfeld ausgiebig zu testen, sind Fehler hier sehr wahrscheinlich.

Wird die Software über einen Weblink oder einen Email Anhang verbreitet besteht außerdem die Gefahr der Verbreitung auf Unbeteiligte, durch Weiterleitung durch den Betroffenen. Darüber hinaus können die Sicherheitslücken auf denen die Schadsoftware aufsetzt, sowie die Schwachstellen der Software selbst anderen bekannt werden, und somit weiteren Missbrauch ermöglichen.[4]

Schadsoftware schädigt Wirtschaft und Gesellschaft

Die staatliche Entwicklung von Schadsoftware für die Zwecke der Online-Durchsuchung und der Quellen-TKÜ wirkt also fundamental den Zwecken der Bekämpfung von Kriminalität und

[2]https://www.tagesspiegel.de/weltspiegel/ransomware-wanna-cry-wie-hacker-mit-cyber-attacken-millionen-erpressen/19797626.html

[3]Vgl. dazu die Analyse des Bundestrojaners 2011 durch den CCC: https://www.ccc.de/de/updates/2011/staatstrojaner

[4]Vgl. Rehak, Rainer. 2014. “Angezapft“, S. 18.

Terrorismus entgegen. Die Notwendigkeit von Sicherheitslücken, an denen sie Schadsoftware ansetzt, sowie notwendiger Weise entstehende Schwachstellen der eigenen Schadsoftware führen zu einem vergrößerten Potential von Kriminalität und Terrorismus.

Über den konkreten Schaden, der bei einzelnen Bürgerinnen und Bürgern, durch vorgehaltene Sicherheitslücken zu erwarten ist, ergibt sich ein gesamtgesellschaftliches Gefahrenpotential, da zentrale Organisationen und Infrastrukturen heute auf IKT basieren.

Darüber hinaus wird das Vertrauen der Bürgerinnen und Bürger in Informationstechnik gefährdet, und damit das wirtschaftliche und gesellschaftliche Potential der Weiterentwicklung digitaler Infrastrukturen vermindert.

Nicht ohne Grund hat das Bundesverfassungsgericht die Vertraulichkeit und Integrität informationstechnischer Systeme als Grundrecht bestätigt.[5] Daher appellieren wir an den Gesetzgeber, die strukturelle Verbreitung von Schadsoftware durch staatliche Behörden unbedingt zu unterlassen. Vielmehr sollten Ressourcen zur Verbrechensbekämpfung defensiv eingesetzt werden, beispielsweise durch das proaktive Finden und Beheben von Sicherheitslücken oder durch die Etablierung einer Kultur der IT-Sicherheit und eine aktive Bekämpfung des Handels mit Sicherheitslücken.

Wer ist Hannover IT?

Hannover IT ist das führende Netzwerk der Informations- und Kommunikationswirtschaft (IKT) im Raum Hannover.

Wir vertreten die wirtschafts- und sozialpolitischen Interessen der IKT-Branche im Raum Hannover, die in einem stark wachsenden Markt mehr als 25.000 Menschen beschäftigt. Ein wichtiges Ziel unserer Arbeit ist, die Wettbewerbsfähigkeit unserer Branche im nationalen und internationalen Wettbewerb um Standorte und Arbeitsplätze zu sichern. Wir wollen das Wissen rund um die vielfältigen Facetten der Digitalisierung vermehren und teilen. Hierzu erarbeiten wir u.a. gemeinsam Positionen sowohl zu fachlichen als auch strategischen Fragestellungen.

[5] BVerfG-Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07.
Vgl. https://www.telemedicus.info/article/677-Das-IT-Grundrecht-im-Detail.html