Sebastian Alscher
sebastian.alscher@piratenpartei.de
Borys Sobieski
borys.sobieski@piratenpartei.de
Marco Holz
trojaner@marcoholz.de
Hanno Wagner
hessentrojaner@rince.de

08.06.2021

„Hessentrojaner“ – Fachtechnische Stellungnahme

In dieser Stellungnahme wird zum geplanten Einsatz einer Überwachungssoftware („Staatstrojaner“, „Hessentrojaner“) für Online-Durchsuchungen und Quellen-Telekommunikationsüberwachung durch die Landespolizei Hessen Stellung genommen. Es wird insbesondere um die technische Beherrschbarkeit und Kontrollierbarkeit des Einsatzes von Überwachungssoftware gehen, sowie die gesellschaftlichen und wirtschaftlichen Begleiterscheinungen der Beschaffung und des Einsatzes von Überwachungssoftware.

Einleitung

Im Rahmen der Änderung des HSOG im Juni 2018 werden den Polizeibehörden erweiterte Rechte in Bezug auf die Datenerhebung durch den Einsatz technischer Mittel eingeräumt, insbesondere die Telekommunikationsüberwachung an informationstechnischen Systemen (§ 15b HSOG) und die Onlinedurchsuchung solcher Systeme (§ 15c HSOG).

Ziel der Schadsoftware/Trojaner

Für einen verdeckten Eingriff in informationstechnische Systeme wird hierzu einer Zielperson eine Software auf das zu überwachende System aufgespielt. Dafür wird eine oder mehrere Sicherheitslücken ausgenutzt, um die Überwachungssoftware auf dem System aufzubringen.

Ziel ist die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht, seine Speichermedien ausgelesen werden können, sowie gegebenenfalls mithilfe des Systems die weitere Umgebung überwacht werden kann, mit Ausnahme von Daten, die den Kernbereich privater Lebensgestaltung betreffen. Ebenso ist das Ziel, Benutzereingaben zu erfassen, bevor sie zu Kommunikationszwecken verschlüsselt übertragen werden (Quellen-Telekommunikationsüberwachung). Voraussetzung ist daher, dass die Person diese Maßnahme nicht bemerkt, sowie dass genau dieser Funktionsumfang von der Software bereitgestellt wird .

Mit dieser Überwachungssoftware werden Vertraulichkeit und Integrität der informationstechnischen Systeme verletzt, um beispielsweise Schaden für Leib und Leben abzuwenden.

Funktionen und Aufbau von Trojaner-Software zur Überwachung

Für eine solche Maßnahme kann als Überwachungssoftware eine Trojaner-Software eingesetzt werden. Von dieser Software wird in einem bestehenden Programm eine Hintertür geöffnet, durch die Informationen gesammelt oder Funktionen und Aufgaben ausgeführt werden können. In der Regel ist das Öffnen einer Hintertür bei diesem bestehenden Programm und die Exfiltration von Daten vom Besitzer des informationstechnischen Systems nicht gewollt, und die Verletzung von Vertraulichkeit und Integrität des IT-Systems stellt für diesen einen Schaden dar. Zusätzlich kann durch das Ausnutzen derartiger Hintertüren auch Änderungen am informationstechnischen System selbst durchgeführt werden, welche vom Verwender weder gewollt noch authorisiert wurden (Beispiel Kryptotrojaner/Ransomware). Daher kann man die Überwachungssoftware auch als Schadsoftware bezeichnen. Damit eine solche Schadsoftware zur Erfüllung der Überwachungsziele erfolgreich eingesetzt werden kann, muss sie bestimmte Mindesteigenschaften besitzen:

- Sie muss in der Lage sein, sich in einem Speicher auf dem Zielsystem anzusiedeln. Hierzu muss sie in Speichersysteme schreiben können.

- Sie muss auf dem Zielsystem Daten und/oder Datenströme lesen können, um Informationen zu gewinnen, die dem Einsatzzweck entsprechen.
- Sie muss auf dem Zielsystem in der Lage sein, eine Verbindung nach außen herzustellen, beispielsweise um Daten aus der Überwachung an die Angreifer zu übermitteln, oder um Informationen zu liefern, mit denen festgestellt werden kann, welche Software-Komponenten notwendig sind, um sich auf dem System einzunisten (Persistenz).
- Sie muss auf dem Zielsystem in der Lage sein, Daten zu empfangen, beispielsweise Daten, die Befehle enthalten, damit das Zielsystem ferngesteuert werden kann, oder damit Daten auf dem Zielsystem mit dem Angreifer geteilt werden können, der sie für weitergehende Analysen verwendet.

Neben der vorgesehenen Fernsteuerung durch Angreifer ist häufig das Nachladen weiterer Funktionen wichtig. Es werden Programmteile nachgeladen, um beispielsweise privilegierte Rechte auf dem Zielsystem zu erhalten, damit der Angreifer bestimmte notwendige Programm-Funktionen ausführen kann, um zu vermeiden, dass installierte Virenscanner Warnhinweise auszulösen, oder um bestimmte Programme zu kompromittieren, die auf dem Zielsystem ausgeführt werden. Für die erfolgreiche Einschleusung dieser Sorte von Schadsoftware müssen Sicherheitsfunktionen des anzugreifenden Systems dauerhaft überwunden werden. Damit wird das informationstechnische System weiter geschwächt und ist gegen Angriffe Dritter verletzbar.

Weitere Funktionen sind die Überwachung des Datenflusses von, zu und durch das System, der Analyse gespeicherter Daten auf der Festplatte, sowie weiteren angeschlossenen Medien und/oder derzeit in flüchtigen Speichern vorliegender Daten.

Um die beschriebenen Funktionen für den Angreifer erfüllen zu können, muss sich die Überwachungssoftware im Zielsystem einnisten können. Sie muss in der Lage sein, diese Funktionen ungestört und gleichzeitig unbemerkt ausüben zu können. Auch beispielsweise nach einem Neustart des Systems muss die Software in der Lage sein, die Funktion wieder aufnehmen zu können. Damit das erreicht wird, ist Schadsoftware häufig modular aufgebaut. Typischerweise enthält sie nur die für den nächsten Schritt notwendigen Daten. Damit ist es möglich, die Größe der Datei klein zu halten, gleichzeitig nur die Daten für die wirklich benötigten Funktionen auf dem Zielsystem zu hinterlassen und nicht mehr benötigte Daten zu entfernen. Beispielsweise wird zuerst eine kleine Datei auf dem Zielsystem hinterlegt, die – vereinfacht gesagt – eine Installationsroutine enthält, die den Virenscanner deaktiviert oder die ermittelt, welche Version einer Chat-Anwendung die Zielperson auf dem System betreibt, um anschließend den zu dieser Software passenden Schadcode zum Auslesen der Kontaktliste herunterzuladen und auszuführen. Weitere Funktionalität, die nachgeladen wird, dient beispielsweise zur Übertragung oder Ausleitung von Daten aus dem Zielsystem an den Angreifer.

Risiken bei der Entwicklung von Überwachungssoftware

Für eine informationstechnische Überwachung muss die Schadsoftware auf das Zielsystem zugeschnitten sein. Die Bemühungen von Behörden, eine Schadsoftware zur Überwachung informationstechnischer Systeme selber zu entwickeln, haben sich als überaus schwierig herausgestellt. Ein bereits entwickelter Trojaner aus dem Jahre 2011 verursachte durch Design- und Implementierungsfehler weitere Sicherheitslücken, die auch von Dritten ausgenutzt werden konnten.[1]

Bei dem Erwerb von Überwachungssoftware bei Dritten besteht das Problem, dass bei dieser üblicherweise nicht der Quellcode übergeben wird und nicht der volle Funktionsumfang bekannt ist, sondern nur angenommen werden kann. Sie wird immer mindestens den angeforderten Funktionsumfang bereitstellen, dies lässt sich auch verhältnismäßig leicht überprüfen. Unklar ist aber, welche **weiteren Funktionen** im Code stecken, die jedoch nicht dokumentiert sind.

Zur Entwicklung einer Software, die für die Umsetzung einer Maßnahme nach § 15b oder c HSOG benötigt wird, bieten sich die folgenden Möglichkeiten.

Fremdentwicklung

Die Überwachungssoftware kann bei einem Drittanbieter erworben werden, der die Software nach entsprechenden Vorgaben programmiert. Dies schließt damit auch den Erwerb von Zero-Days ein, also von Sicherheitslücken, die der Allgemeinheit bisher noch nicht bekannt sind, und für die bisher noch keine Software-Aktualisierungen existieren, die diese Sicherheitslücke schließen.

Problem: Der Erstellungsprozess, ebenso wie die verwendeten Software-Bibliotheken, müssen dokumentiert werden. Andernfalls ist die Kontrolle über die Funktionalität, insbesondere der **nicht über die Vorgaben hinausgehenden Funktionalität**, nicht sicherzustellen. Bisher gibt es aber für Spionage-Schadsoftware keine Qualitätsstandards, an denen sich ein Anbieter orientieren kann.

Denn: Extern verfügbare Sicherheitslücken und der Code, der diese ausnutzt, sind üblicherweise nicht mit dem Ziel programmiert, einen eingeschränkten Funktionsumfang zur Verfügung zu stellen. Der Code soll vorrangig dazu zu dienen, schnellstmöglich ein Ziel zu erreichen, denn auch die Hersteller von Überwachungssoftware stehen im Wettbewerb und Konkurrenzkampf. Das bedeutet, dass die Zeit wertvoll ist, bis eine Lücke durch ein Software-Update beseitigt ist. Daher geht hier häufig Geschwindigkeit vor Präzision.

Generell gilt, dass der Hersteller mehr Kenntnis über den Funktionsumfang der Software hat als die Behörden.

1https://www.ccc.de/de/updates/2011/staatstrojaner

Von einer Software, die in ihren Funktionen nicht vollständig bekannt ist, gehen unkalkulierbare Risiken aus. Denn schließlich lässt sich nicht eindeutig sagen, was die Software, wenn sie auf dem Zielsystem aufgespielt ist, machen wird. Das gleiche gilt für die Software, die zur Kontrolle der Überwachungssoftware dient, die seitens der Polizeibehörden betrieben werden muss. Daher müssen unerwünschte Begleiterscheinungen ausgeschlossen oder zumindest beherrschbar werden.

Hierfür muss man ausschließen können, dass defekte Software eingekauft wird. Eine Überprüfung kann aber nur geleistet werden, wenn der Hersteller den Quellcode der Anwendung zur Verfügung stellt, damit eine Überprüfung in Bezug auf die enthaltenen Funktionalitäten überhaupt vorgenommen werden kann. Üblicherweise liefern Unternehmen lediglich den kompilierten Binärcode aus, was eine vollständige Überprüfung auch für Expertinnen und Experten unmöglich macht. Diese Überprüfung sollte regelmäßig von einer unabhängigen Stelle übernommen werden, wie dem BSI oder dem Bundes- oder Landesdatenschutzbeauftragten, da andernfalls ein Interessenkonflikt besteht.

Vollständige Eigenentwicklung

Eine öffentliche Behörde entwickelt die Überwachungssoftware für den jeweiligen Einsatzzweck selbst.

Problem: Eine bisher unbekannte Sicherheitslücke zu finden und einen entsprechenden Schadcode dafür zu entwickeln (Zero-Day) ist verhältnismäßig teuer. Im internationalen Vergleich von Sicherheitsbehörden gibt es solche Eigenentwicklungen in der Regel bei den Nachrichtendiensten, die mit sehr hohen Budgets ausgestattet sind.

Nur bei einer vollständigen Eigenentwicklung besteht seitens der Angreifer Gewissheit darüber, welche Funktionen durch welchen Code (ausschließlich) ausgeführt werden können. Nur durch eine Eigenentwicklung für einen jeweiligen (richterlich genehmigten) Einsatzzweck kann garantiert werden, dass nicht über die entsprechende Genehmigung hinaus Eingriffe in die Persönlichkeitsrechte erfolgen.

Teilweise Eigenentwicklung

Ein Teil externer verfügbarer Software-Module wird eingebunden, ein Teil der Module selbst entwickelt. Dies bietet zumindest für die selbst entwickelten Module eine höhere Gewissheit, welche Funktionalität durch den Code der Schadsoftware bereitgestellt wird.

Dennoch ist auch in diesem Fall die Eigenentwicklung sehr aufwändig, technisch sehr komplex und erfordert viel Fachwissen. Eine solche Entwicklung wäre in der Bundesrepublik das technisch schwierigste Softwareentwicklungsprojekt der öffentlichen Verwaltung, viel komplexer als beispielsweise die Entwicklung eines eGovernment-Systems.

Weitergehende Schwierigkeit:

Die Art der Entwicklung bietet auch keine Garantie, dass die von einer Überwachungssoftware **nachgeladenen** Module in ihrer Funktionalität nicht über das hinausgehen, was im Rahmen der Maßnahme festgelegt wurde. Es wird hier nur beschrieben, in wieweit der Funktionsumfang von Modulen überhaupt eingeschätzt werden kann.

Gefahren für die Gesellschaft aus der Bereithaltung von Überwachungssoftware

Um unbemerkt Zugang zu einem informationstechnischen System zu gewinnen, müssen Sicherheitslücken in der Software der Zielperson ausgenutzt werden. Diese Sicherheitslücken entstehen durch Fehler in der Programmierung, beispielsweise im Software-Design oder bei der unmittelbaren Umsetzung in Softwarecode.

Der Eingriff in Informationssysteme erfolgt über Zero-Day-Exploits, also mit Schadsoftware, die Sicherheitslücken ausnutzt, die bisher nicht öffentlich bekannt sind. Von besonderem Interesse hierbei sind Sicherheitslücken bei weit verbreiteten Betriebssystemen und Anwendungen wie Browsern, da sie bei mehr Überwachungsmaßnahmen bzw. Zielpersonen eingesetzt werden können. Dies ist der Fall, weil es wahrscheinlicher ist, dass eine Zielperson eine „übliche“ Software nutzt, als eine Spezialanwendung mit wenigen Nutzern. Auch wenn ein Einsatz dieser Cyberwaffe gegenüber der von einer Maßnahme betroffenen Person gerechtfertigt ist, so bleiben die Auswirkungen daher nicht auf diese Person beschränkt. Denn die Überwachungssoftware verwendet Lücken, die auch in den Systemen weiterer Bürgerinnen und Bürger vorliegen. Wer von einer solchen Lücke in seinem informationstechnischen System weiss, würde zur Gewährleistung der Vertraulichkeit und der Integrität seines informationstechnischen Systems diese Lücke mit einem Software-Update schnellstmöglich schließen wollen, oder die Software deinstallieren, um seine Daten nicht zu gefährden.

Die Geheimhaltung der Sicherheitslücke sowohl gegenüber der Zielperson als auch gegenüber dem Hersteller der Software verhindert jedoch, dass Bürgerinnen und Bürger sich selbst schützen können und der Hersteller diese Aktualisierung mit Code, der diese Lücke schließt, entwickeln kann. Nachdem der Hersteller für eine Sicherheitslücke eine Aktualisierung zur Verfügung gestellt hat, vergeht weitere Zeit, bis auf die entsprechenden Systeme die Aktualisierung aufgespielt wird. Daher ist es sehr wichtig, dass Softwareupdates so schnell wie möglich verfügbar sind, um eingespielt werden zu können, damit IT-Systeme geschützt werden können.

Gefahr für die Zivilgesellschaft

Das Offenhalten einer solchen Sicherheitslücke betrifft nicht nur den Einzelfall einer von der Überwachungsmaßnahme betroffenen Person. Eine Lücke kann nicht für eine einzelne Person offen gehalten werden und für alle anderen Bürgerinnen und Bürger geschlossen werden. Stattdessen wird sie die Si-

cherheit der informationstechnischen Systeme von den weitaus mehr Bürgerinnen und Bürger betreffen, die die gleichen Systeme einsetzen. Eine Sicherheitslücke in einem Protokoll unter Windows 10 betrifft beispielsweise alle Windows 10-Systeme, solange keine Aktualisierung zur Verfügung steht und installiert wurde, die diese Lücke schließt. Betroffen ist davon nicht nur die Zielperson der Überwachungsmaßnahme.

Um nicht entdeckt zu werden oder andere Module der Schadsoftware nachladen zu können ohne eine Warnung durch den Virenscanner auszulösen, werden häufig die Aktualisierungen/Signatur-Updates des Virenscanners beim überwachten System verhindert. Wenn für eine Sicherheitslücke eine Schadsoftware existiert, mit der erreicht wird, dass ein Virenscanner nicht aktualisiert wird, dann birgt dies für alle Bürgerinnen und Bürger ein erhebliches Risiko.

Im Gegensatz zur Herstellung ist die Verbreitung von Schadsoftware häufig mit geringem Aufwand möglich. Die Verbreitung und schließlich der Befall kann bei Verwendern informationstechnischer Systeme, die von einer Überwachungsmaßnahme gar nicht betroffen sind, erhebliche Konsequenzen haben. Ein Virenscanner, der nicht aktualisiert wird, führt zu einem verwundbaren System. Beispielsweise werden jeden Tag 350.000 neue Schadprogramme (Malware) registriert, die den Virenschutzsystemen zur Erkennung zugeführt werden.[2] , Da es eine rege Aktivität bei der Entwicklung von Viren gibt, steigt das Risiko für Unbeteiligte erheblich, obwohl sie von einer Überwachungsmaßnahme eigentlich überhaupt nicht betroffen sind, aber trotzdem keine Updates ihres Virenscanners mehr erhalten. Da sie von der Maßnahme nichts wissen, ist ihnen erschwert, ihr Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme wahrzunehmen. Der Virenscanner entdeckt dann nicht mehr den Trojaner, der sich im Browser eingenistet hat, und beispielsweise genutzt wird, um Daten beim Online-Banking auszulesen. Die Infektionen von Windows-PCs mit Finanz-Schadsoftware, so genannten Banking-Trojanern, ist in den ersten sechs Monaten des Jahres 2019 auf nahezu 140.000 Fälle gestiegen, es handelt sich also um eine sehr ernstzunehmende Gefahr für Privatpersonen.[3]

Regelmäßig gelingt es, an die Informationen zu kommen, welche Sicherheitslücken von staatlichen Akteuren ausgenutzt werden und somit nicht geschlossen werden.[4] Im Grunde genommen ist es nicht besonders schwierig, eine solche Lücke zu finden, denn eine Person, die befürchtet mit Hilfe einer solchen Schadsoftware überwacht zu werden, braucht ihr informationstechnisches System lediglich forensisch untersuchen zu lassen. Hierbei kann eine solche Schadsoftware dann entdeckt und festgestellt werden, welche Sicherheitslücke ausgenutzt wurde. Das Interesse an einer gründlichen Untersuchung ist erheblich, da ein florierender Markt für Sicherheitslücken besteht, auf dem Teilnehmer bereit sind, hohe Summen für das Wissen um Schwachstellen zu bezahlen. Daher ist davon auszugehen, dass die Geheimhaltung nicht vollständig gewährleistet werden kann. Das Ausnutzen von absichtlich offen gehaltenen Sicherheitslücken muss daher immer Teil des Risikoabschätzung sein.

2https://www.av-test.org/en/statistics/malware/
3https://www.springerprofessional.de/it-sicherheit/bank-it/zahl-der-banking-trojaner-steigt-massiv-an/16202052
4FIfF-Kommunikation 2/17, S. 18 (https://faui1-files.cs.fau.de/public/publications/fiff-2017-02-staatliche-spaehsoftware-nemetz.pdf)

Gefahr für Behörden, Gerichte und kritische Infrastruktur

Auch Behörden oder Gerichte leiden unter Sicherheitslücken, die nicht zeitnah geschlossen werden konnten, und für die Schadsoftware geschrieben wurde. Besondere Herausforderungen bestehen immer dort, wo eine Vielzahl unterschiedlicher Softwareprogramme auf einem System laufen, für die eine hohe Verfügbarkeit gewährleistet werden muss, wo jedoch eine Aktualisierung dazu führen kann, dass Programme nicht mehr funktionieren. Hier kann das Einspielen einer Betriebssystem-Aktualisierung erst nach ausgiebigen Tests erfolgen. Es ist daher ungemein wichtig, so schnell wie möglich eine Gegenmaßnahme gegen eine Lücke zu entwickeln, ansonsten kann der Ausfall von Krankenhäusern, Behörden, Gerichten oder anderen kritischen Infrastrukturen die Sicherheit im Land gefährden.

Krankenhäuser und Gesundheitseinrichtungen stellen aufgrund ihrer zentralen Bedeutung für das Allgemeinwohl eine der wichtigsten Institutionen einer Gesellschaft dar. Ein Ausfall oder eine Störung hat das Potenzial, signifikante Folgen für die öffentliche Sicherheit nach sich zu ziehen. Daher werden sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zu den sogenannten Kritischen Infrastrukturen (KRITIS) gezählt. So wurden 2019 Krankenhäuser Opfer der als „Emotet“ bekannt gewordenen Erpresser. Verbreitungswege von Emotet waren die EternalBlue-Sicherheitslücke und die DoublePulsar-Schwachstelle.[5] Die EternalBlue-Sicherheitslücke greift Windows-Systeme an und nutzt eine Schwachstelle im SMB-Protokoll. Mittlerweile wird allgemein angenommen, dass die Schadsoftware für EternalBlue von der U.S. National Security Agency (NSA) entwickelt wurde.

Auch beim Kammergericht Berlin kam es zu einem schwerwiegenden Befall der IT-Infrastruktur, und eine Infektion mit bekannter Malware wurde festgestellt, und zwar durch die Malware „Emotet“ und Trickbot. Die Module letzterer waren klar auf Datenabfluss ausgerichtet. So muss also davon ausgegangen werden, dass unter Ausnutzung einer Schwachstelle, für die von einer öffentlichen Stelle ein Schadcode entwickelt wurde, ein unbekannter Urheber des Angriffs über den vollen Zugriff auf den Datenbestand des Kammergerichts verfügte.[6]

Ein Beispiel für den Befall kritischer Infrastruktur durch Schadsoftware, die ursprünglich für zielgerichtete Überwachung programmiert wurde, ist die Deutsche Bahn. Die Schadsoftware WannaCry nutzt die gleiche Schwachstelle und befiel 450 Rechner der Deutschen Bahn.

Gefahr für Unternehmen

Darüber hinaus werden nicht nur Bürgerinnen und Bürger oder öffentliche Stellen davon betroffen sein, sondern eine Vielzahl weiterer Systeme bei Unternehmen und anderen Organisationen. Die häufigsten Risiken liegen hier im Bereich der Spionage und der Betriebsunterbrechung.

5https://de.malwarebytes.com/emotet/
6https://www.berlin.de/sen/justva/presse/pressemitteilungen/2020/pressemitteilung.887323.php

Betriebsunterbrechung

Malware, die auf Sicherheitslücken basierte, welche für Verfolgungsbehörden entwickelt wurde, wurden genutzt, um Ransomware zu verbreiten. Diese Schadsoftware nutzt die offene Sicherheitslücke, um informationstechnische Systeme zu verschlüsseln und unbrauchbar zu machen, und diese gegen Zahlung eines Geldbetrags wieder freizugeben.

So berichtete der Vorsitzende des Logistikunternehmen Maersk Jim Hagemann Snabe auf dem Weltwirtschaftsforum in Davos, dass durch die Ransomware „NotPetya“ eine Schadensumme von mehreren hundert Millionen Dollar entstanden sei. Die Reederei transportiert mit ihren Containerschiffen knapp 20 Prozent des gesamten Welthandels. Durch den Angriff der Ransomware am 27. Juni 2017 erlitt Maersk einen Totalausfall aller IT-Systeme: 45.000 Client-Rechner sowie 4.000 Server rund um den Globus seien ausgefallen. Auch andere Großunternehmen, wie der Pharmariese Merck, der durch den NotPetya-Angriff eine Schadensumme von über 300 Millionen beklagte, und das Logistikunternehmen FedEx gehörten zu den Opfern.

Beachtenswert ist, dass diese Unternehmen gar nicht das eigentliche Ziel des Angriffs waren, es hat nie eine Lösegeldforderung gegeben. Vielmehr wollte der Urheber der Schadsoftware eine Sicherheitslücke einer in der Ukraine häufig genutzten Software ausnutzen, und eigentlich einen auf die Ukraine begrenzten Schaden anrichten.[7] Der Schaden für die Kollateralopfer ist unstrittig erheblich, und diese Fälle machen deutlich, wie weitreichende Folgen das Nicht-Schließen von Sicherheitslücken haben kann — bis zu einer massiven Gefährdung der deutschen Wirtschaft.

Spionagerisiko

Für Unternehmen ist eine sichere Infrastruktur nicht nur für den Unternehmensbetrieb notwendig, sondern auch zu Wahrung der Vertraulichkeit von Geschäftsgeheimnissen und dem Schutz geistigen Eigentums, der häufig den Konkurrenzvorteil ausmacht.

Nicht geschlossene Sicherheitslücken und insbesondere die Verfügbarkeit von Schadsoftware, die diese Lücken ausnutzt, stellen daher ein signifikantes Risiko dar, weil sie zur Spionage durch unbefugte Dritte eingesetzt werden können. Stellt eine interessierte Hackergruppe oder gar ein staatlicher Akteur fest, dass eine Sicherheitslücke besteht und diese zur Überwachung im Interesse öffentlicher Stellen offen gehalten wird, so kommt dies einer Einladung gleich, sie für deutsche Unternehmen auszunutzen, um gleichermaßen die Kommunikation zu überwachen und Firmengeheimnisse auszuleiten. Es sind zahlreiche staatsnahe Hackergruppen im Ausland bekannt, die, mit entsprechenden Mitteln versehen, diese Lücken in unserer Informationsinfrastruktur auszunutzen versuchen. Lücken, derer man sich zumindest für dein Einsatz der eigenen Überwachungssoftware bewusst ist und die eigentlich geschlossen werden könnten.

Der Schaden durch Industriespionage in Deutschland kann aufgrund der hohen Dunkelziffer und der Unkenntnis über eine Infiltration Dritter nur geschätzt werden. Bitkom berichtet 2019, dass auf Basis von mehr als 1.000 befragten Unternehmen 43% der Unternehmen vermutlich vom Ausspähen digita-

7https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2017-2018.pdf

ler Kommunikation betroffen sind und 42% der Unternehmen vermutlich von digitaler Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen. Digitale Angriffe haben bei 70% der Unternehmen einen Schaden verursacht. Der Gesamtschaden bei Unternehmen in Deutschland innerhalb der letzten zwei Jahre wurde 2019 auf 205,7 Milliarden Euro (inklusive Kosten für Ermittlungen und Ersatzmaßnahmen, Rechtsstreitigkeiten, etc) geschätzt.[8] Im Rahmen der Abwägungen zum absichtlichen Offenhalten von Sicherheitslücken von informationstechnischen Systemen müssen diese Folgeschäden, die für Unternehmen in Deutschland existenzgefährdend sein können, mit berücksichtigt werden.

Vorgaben an den IT-Grundschutz durch das BSI

Wie oben beschrieben kann nicht angenommen werden, dass die Kenntnis einer Sicherheitslücke exklusiv bei den Staatsorganen vorliegt. Es ist stattdessen wahrscheinlich, dass sie weiteren Kreisen bekannt ist.

Das Bundesinnenministerium schreibt: Der Staat ist verfassungsrechtlich verpflichtet, die Bevölkerung zu schützen. Dafür ist er mit bestimmten Handlungsbefugnissen ausgestattet. Bedient er sich dieser Rechte, um eine Person zu schützen, bedeutet das aber unter Umständen, dass er gleichzeitig in die Rechte einer anderen Person eingreift. (https://www.bmi.bund.de/DE/themen/sicherheit/sicherheit-node.html)

Im Falle der Sicherheitslücken, die bei dieser Schadsoftware ausgenutzt werden, wird nicht ausschließlich in die Rechte einer einzelnen verdächtigen Person eingegriffen, sondern eine Gefährdungslage für breite Personengruppen und auch Organisationen und Unternehmen geschaffen. Das BSI gibt vor, wie ein IT-Grundschutz für Unternehmen auszusehen hat:[9]

> „Die folgenden Anforderungen MÜSSEN für den Baustein Schutz vor Schadprogrammen vorrangig umgesetzt werden:
>
> OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen (B)
>
> Es MUSS ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Außerdem MUSS festgehalten werden, wie der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so SOLLTEN die identifizierten IT-Systeme NICHT betrieben werden. Das Konzept SOLLTE nachvollziehbar dokumentiert und aktuell gehalten werden."

Man muss zum Ergebnis kommen, dass ein verlässlicher Schutz nicht möglich ist, wenn Sicherheitslücken bekannt sind, aber dennoch offen gehalten werden. Der Bau bzw. die Verwendung eines Trojaners gefährdet damit die Sicherheit der Infrastruktur für die Bürger, aber auch für Behörden und Organisationen.

8https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf

9*BSI, IT-Grundschutz-Kompendium, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.html*

Gefahr für das Verhältnis zwischen Zivilgesellschaft und Staat

Für den Einsatz der Überwachungssoftware werden offene, aber noch nicht der Öffentlichkeit bekannte Sicherheitslücken ausgenutzt. Bedingung für die erfolgreiche Durchführung einer Maßnahme mit einer erworbenen Spionagesoftware ist daher, dass diese Sicherheitslücke bis zum Beginn der Maßnahme besteht und nicht bis dahin geschlossen wird.

Auch für weitere erfolgreiche Durchführungen von Überwachungsmaßnahmen mit dieser Software muss sichergestellt werden, dass diese Angreifbarkeit informationstechnischer Systeme weiterhin besteht. Ein Schließen von Sicherheitslücken wäre dringend zu vermeiden, da dann eine neue Überwachungssoftware entwickelt werden müsste, was die oben beschriebenen Kosten und Entwicklungszeiten mit sich bringt. Es liegt also seitens der öffentlichen Stellen das dringende Bedürfnis vor, alles dafür zu tun, dass es keine Möglichkeit gibt, sich vor dieser Sicherheitslücke zu schützen, um so die Möglichkeit zur Ausübung einer Überwachungsmaßnahme zu verbauen.

Gleichzeitig stellt diese Lücke ein Risiko für alle Bürgerinnen und Bürger dar - entweder weil ihre eigenen informationstechnischen Systeme betroffen sein könnten, oder weil Systeme betroffen sind, auf denen z.B. ihre vertraulichen Daten liegen, oder weil sie von der Funktionstüchtigkeit von Systemen von Behörden oder Einrichtungen abhängig sind, wie bei Stadtwerken, Krankenhäusern oder im Personennahverkehr.

Wenn beispielsweise durch das Ausnutzen einer Sicherheitslücke in die IT-Infrastruktur einer Krankenkasse oder eine Knochenmarkspender-Datenbank eingebrochen werden würde, so wären damit sensible Daten von Personen im Umlauf, die ihrerseits weder im Zusammenhang mit der Überwachungsmaßnahme stehen, noch selber über möglicherweise anfällige informationstechnische Systeme verfügen.

Durch eine Ausweitung der Befugnisse und der damit einhergehenden Zunahme der Häufigkeit der Einsätze wird die Menge an benötigten Sicherheitslücken und der Zeitraum, in dem Systeme durch diese Lücken uneingeschränkt verfügbar sind, zunehmen - und damit auch die Bereitschaft des Staates, die Sicherheit der Zivilgesellschaft zu gefährden. Gleichzeitig gibt das Gesetz keinerlei Regeln und Maßnahmen vor, wie die Risiken, die durch den Einsatz der Software entstehen, minimiert werden, und wie die Gefahr durch die Sicherheitslücken so weit wie möglich eingeschränkt werden soll, dass der Schutz der Allgemeinheit aufrechterhalten werden kann.

Der Staat kommt nicht mehr im gleichen Maße der Aufgabe nach, seine Bürgerinnen und Bürger und die Wirtschaft vor Schadsoftware zu schützen und ihr Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu verwirklichen.

Durch das Gesetz gelangen die Polizeibehörden stärker in eine Rolle, die nicht mehr nur ausschließlich dem Schutz der Bürgerinnen und Bürger dient. Stattdessen führt der inhärente Konflikt bei der Ausübung ihrer Aufgaben dazu, dass sie die Risiken ausweiten, die zu einer Gefährdung führen. Je höher die Wahrscheinlichkeit ist, dass es zu einem Schaden kommt, der im Zusammenhang mit einer

bewusst in Kauf genommenen Gefährdung der Bürgerinnen und Bürger einhergeht, umso mehr kommt es zu einer Belastung der Vertrauensbasis zwischen Zivilgesellschaft und Staat, die bis zu einem Bruch desselben führen kann. Und diese Wahrscheinlichkeit steigt mit der Anzahl der Einsätze sowie der damit beschäftigten Personen.

Risiken beim und Fragestellungen zum Einsatz von Überwachungssoftware

Neben den grundsätzlichen Gefährdungen für die Institutionen und die Zivilgesellschaft ergeben sich weitere Risiken aus dem Einsatz selbst, bzw. aus der Bereithaltung für einen Einsatz durch die Polizeibehörden des Landes.

Risiko von Missbrauch und Nutzung zur Erpressung

Überwachungssoftware ist ein mächtiges Werkzeug, das dazu dient, Informationen zu beschaffen, die die Zielpersonen nicht in der Hand Dritter wissen möchten. Daher war der Einsatz bestimmter Software bis vor Kurzem auch auf das BKA beschränkt und nur zu bestimmten Sachverhalten im engen Rahmen erlaubt. Die Ausdehnung der Befugnisse, diese Software einzusetzen, bring es mit sich, dass mehr Menschen Zugriff auf dieses Werkzeug bekommen, unabhängig davon, wie die Software am Ende aussieht.

Gleichzeitig ist es unstrittig, dass viel Macht im Einsatz der Software liegt, da Informationen erlangt werden können, oder auch weil bei einem Eingriff in ein fremdes informationstechnisches System Daten verändert werden können, so dass sie einer Person Schaden zufügen. Es ist von außen nicht erkennbar, welche Veränderung der Besitzer des informationstechnischen Systems und welche der Verantwortliche für den Trojaner durchgeführt hat. Die Möglichkeit für einen Missbrauch (wie beispielsweise Erpressung oder Bedrohung) nimmt mit steigender Anzahl befugter Behörden zu. Wenn mit einem Trojaner kompromittierendes Material auf einem Computer hinterlegt wird, beispielsweise im Rahmen eines verdeckten Eingriffs in informationstechnische Systeme, so kann selbst für unbescholtene Menschen eine Bedrohung entstehen. Hierbei geht es nicht um einen systematischen Einsatz, sondern um menschliches Fehlverhalten, welches allein mit einem Anstieg der Anzahl der Personen mit entsprechender Möglichkeit auch häufiger auftreten wird.

Beispielsweise wurde im Rahmen der Snowden-Veröffentlichungen bekannt, dass NSA-Mitarbeiter ihre Spionagewerkzeuge routinemäßig für private Zwecke missbraucht haben. Aber auch bei deutschen Strafverfolgungsbehörden wurden Systeme, die zu besonderen Einsatzzwecken zu verwenden sind, für persönliche Interessen missbraucht. So wurden bei einem Konzert der Bardin Helene Fischer in Frankfurt 83 Personenabfragen durchgeführt, um an Informationen über Helene Fischer zu kom-

men.[10] Auch für die Bedrohung von Politikern (z.B. Frau Janine Wissler[11]) oder Anwälten in Strafprozessen (z.B. Frau Basay-Yildiz[12]) wurden durch Beamte der hessischen Polizei bereits unzulässige Mittel zur Informationsbeschaffung verwendet. Mit dem „Hessentrojaner“ wird sowohl das Missbrauchspotenzial als auch ein daraus hervorgehender Schaden deutlich größer, weil damit Zugriff auf Endgeräte von Bürgerinnen und Bürgern besteht.

Wenn diese Einsatzwerkzeuge gegen Personen, die als Kontrollinstanz dienen, oder auch aus einer anderweitigen politischen Motivation verwendet würden so wäre der Schaden für diese Personen und auch die Demokratie als Ganzes erheblich, auch wenn es sich nur um Einzelfälle handeln würde. Würde beispielsweise kompromittierendes Material (in Text oder Bild) auf dem System zurückgelassen und anschließend als Zufallsfund festgestellt, so wäre in der öffentlichen Meinung und auch vor Gericht ein möglicher Unschuldsbeweis nahezu ausgeschlossen und ein irreparabler Schaden bereits entstanden. Ebenfalls wäre alleine die Androhung einer solchen Veröffentlichung maßgeblich genug, um Verhalten zu beeinflussen.

Unterstützung illegaler Bezugswege

Wenn im Rahmen der Entwicklung von Zero-Day-Exploits auf Drittanbieter zurückgegriffen wird, sei es durch Teile der Software oder als ganzes, unterstützt der Staat durch den Erwerb des Schadcodes eine Schattenindustrie, die sich zu wesentlichen Teilen im illegalen Raum bewegt. Denn auch die Drittanbieter entwickeln Softwarekomponenten zur Ausnutzung einer spezifischen Sicherheitslücke (sogenannte Exploits) in der Regel nicht selbst, sondern kaufen diese in einem gut organisierten Markt ein. Diese Schwachstellen werden vor allem für den Einsatz im Rahmen von Spionage, Erpressung und weiteren Menschenrechtsverletzungen, insbesondere durch totalitäre Regime, entwickelt. Damit wird das Land Hessen Unterstützer einer Industrie, die von der Verletzung von Menschenrechten profitiert.

Wie oben beschrieben haben Personen, die vermuten können, dass sie Teil einer solchen Überwachungsmaßnahme sind, ein hohes Interesse, die auf ihrem System eingesetzte Überwachungssoftware festzustellen und sich dagegen zu schützen. Für entsprechende aktuelle, noch nicht erkannte und von außen nutzbare Sicherheitslücken (sogenannte Remote Execution; Schadsoftware wie Trojaner, für die man keinen physischen Zugriff zu dem Gerät benötigt) werden sehr hohe Preise bezahlt. Diese hohen Preise werden insbesondere von staatlichen Akteuren bezahlt, die die finanzielle Ausstattung für einen Erwerb mitbringen. Da der Staat also einen Markt mit antreibt, auf dem sechs- bis siebenstellige Beträge für entsprechende Sicherheitslücken verdient werden können, sinkt das Interesse der Entdecker solcher Fehler, diese Lücken dem Hersteller der Software zu melden. Eine Ausweitung der Einsatzmöglichkeiten und damit verbunden eine höhere Notwendigkeit zur Beschaffung von Sicherheits-

10https://www.fr.de/hessen/hessen-beamte-missbrauchen-polizeisystem-infos-ueber-helene-fischer-kommen-zr-12875917.html
11https://www.hessenschau.de/politik/rechtes-netzwerk-bei-der-polizei-innenminister-beuth-wirft-lka-schwere-versaeumnisse-nach-drohmails-gegen-wissler-vor,wissler-nsu-beuth-100.html
12https://www.hessenschau.de/gesellschaft/nach-luebcke-mord--weitere-drohschreiben-an-frankfurter-anwaeltin-aufgetaucht,neuer-drohbrief-100.html

lücken treibt daher einen Markt an, der die informationstechnische Infrastruktur für Bürgerinnen und Bürger ebenso wie Unternehmen erheblichen Risiken aussetzt.

Unterscheidung Telekommunikationsüberwachung und verdeckter Eingriff in IT-Systeme

Das Gesetz unterscheidet zwischen der Quellen-Telekommunikationsüberwachung und der allgemeinen Datenerhebung. Eine solche Unterscheidung ist fraglich, denn auch um die Telekommunikationsüberwachung einzuleiten ist es bereits erforderlich, mehr Informationen zu erlangen, als nur die Telekommunikationsdatenströme an sich.

Da das Ziel der Maßnahme ist, Daten vor der Verschlüsselung und einer folgenden Übertragung abzufangen und auszuleiten, werden also zwangsläufig zunächst Daten erfasst, bevor sie verschlüsselt und gesendet werden. Damit ist zu diesem Zeitpunkt unklar, ob es sich um Telekommunikationsdaten handelt, da ihnen der Charakter fehlt, gesendet worden zu sein. Gleichzeitig lässt sich aus den gesendeten Daten nur schwer bis gar nicht ermitteln, in wieweit sie mit dem zuvor aufgezeichneten Daten (Tastatureingaben, Aufnahmen des Mikrofons oder der Webcam) übereinstimmen. Beispielsweise kann die Software Skype eine Gesprächsübertragung übermitteln, die Person hat jedoch die Tonübertragung stumm geschaltet. In diesem Fall würden die vom Mikrofon aufgezeichneten Daten gespeichert werden, auch wenn sie nie zur Übertragung gedacht waren und auch nie gesendet wurden.

Den Gedanken, dass im Rahmen einer solchen Maßnahme keine Daten erlangt würden, die nicht auch durch eine „konventionelle“ TKÜ erfasst würden, muss man folglich verwerfen. Damit ist eine Unterscheidung in § 15b und § 15c, die im ersteren Falle eine weitreichendere Befugnis erteilt, unangemessen.

Betroffenheit

Bei verdeckten Eingriffen in informationstechnische Systeme ist zu beachten, dass das Auslesen von Smartphone-Daten oder angeschlossener Cloud-Speicher nicht mehr nur das Überfliegen von Kalender-Einträgen oder Urlaubsphotos ist. Mittlerweile bildet sich in Smartphones das gesamte Leben der Benutzer ab, insbesondere gewährt es Zugänge zu vielen weiteren angeschlossenen Diensten. Auf Smartphones werden nicht nur Emails, Termine, Bilder, Aktienportfolios oder anzügliche Liebesbotschaften gespeichert, es finden sich dort auch Passwörter zu Online-Diensten und beispielsweise in Kürze auch die elektronische Gesundheitsakte, auf der Krankheitsbefunde der Person gespeichert sind.

Diese Daten zu durchsuchen bedeuten, das Leben einer Person vollumfänglich in allen Facetten vor sich ausgebreitet zu sehen.

Ein weiterer nicht zu vernachlässigender Aspekt ist die Verwendung von IT-Systemen durch mehrere Benutzer. Bedingt durch die Corona-Pandemie haben Menschen mehr Zeit zu Hause verbracht. Dies

betrifft auch die Arbeits- und Ausbildungszeit. Im Rahmen von Home Office haben Arbeitnehmer den Computer zu Hause für ihre beruflichen Verpflichtungen genutzt. Wegen der Schließung der Schulen haben Schüler den Computer anderer Familienmitglieder und Freunde genutzt, um ihren schulischen Verpflichtungen nachzukommen. Üblicherweise wird an Heimcomputern keine Benutzerverwaltung betrieben, wie dies an professionellen Systemen der Fall ist. Mit anderen Worten, in diesen Fällen ist davon auszugehen, dass sich Daten mehrerer Personen auf den informationstechnischen Systemen befinden.

Dies kann zur Folge haben, dass bei einer Datenerhebung aus einem solchen System eine korrekte Attribution erschwert oder gar unmöglich ist. Verwenden alle Mitglieder eines Haushalts beispielsweise den gleichen Heimcomputer, so kann man allein aus dem Vorliegen eines Dokuments technisch nicht feststellen, wer dieses erstellt hat, oder wer dieses über das E-Mail-Programm an einen Dritten versendet hat.

Hieraus wird deutlich, dass die Forderung, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist, keine ausreichende Sicherheitsmaßnahme ist, um den Einsatzzweck auf eine Einzelperson zu beschränken.

Fragestellungen zur richterlichen Anordnung

Der Einsatz erfolgt nach richterlicher Anordnung. Das bedeutet, dass der Richter den Einsatz der Überwachungssoftware der Art und dem Umfang nach als angemessen beurteilt und eine damit verbundene Schädigung Dritter als unvermeidbar aber angemessen bewertet wird.

Damit dies möglich ist, müssen mindestens folgende Bedingungen erfüllt sein:

- Der Funktionsumfang der Überwachungssoftware muss im für die Überwachung abgesteckten Rahmen für diesen Einsatz klar definiert und für den Richter verständlich sowie überprüfbar sein.
- Die Rahmenbedingungen der Überwachung müssen für den Zeitraum des Einsatzes unveränderlich sein, ebenso der Funktionsumfang der Überwachungssoftware.
- Die Beurteilung der eingesetzten Software muss für einen Richter möglich sein.
- Eine Kontrolle der Einhaltung der Rahmenbedingungen, unter denen die Anordnung erlassen wurde, muss jederzeit möglich sein.

Funktionsumfang der Überwachungssoftware klar definiert

Für die Maßnahme muss eine Überwachungssoftware entwickelt worden sein, die keine über die für die jeweilige Maßnahme hinaus beschlossenen Fähigkeiten besitzt. Hierzu ist eine ausführliche Dokumentation der Software nötig, die insbesondere die bestehende Funktionalität dokumentiert. Beispiels-

weise wenn die Software Zugriffsmöglichkeiten auf Speicherplatz des informationstechnischen Systems besitzt, muss sich durch die Dokumentation nachvollziehbar sicherstellen lassen, dass nur notwendige Daten gelesen werden. Gleichermaßen muss sichergestellt werden, dass die Software keinen Schreibzugriff auf Speicherbereiche hat, die es ermöglichen, Daten dort abzulegen, die im Rahmen einer späteren Strafverfolgung fälschlicherweise dem Überwachten zugeschrieben werden könnten. Das muss mit Methoden der Dokumentation - auch im Quellcode - nachgewiesen werden. Es muss hierzu eine ausführliche und vor allem für sachkundige Dritte verständliche Dokumentation des Quellcodes der Überwachungssoftware mit Beschreibung der jeweiligen Code-Blöcke und zugehörige Funktionen existieren, es muss also der Quellcode verfügbar sein.

Unveränderlichkeit des Funktionsumfangs der Überwachungssoftware

Die Möglichkeiten zum Nachladen von Modulen, die die Fähigkeiten der Überwachungssoftware erweitern, muss nachvollziehbar dokumentiert werden. Eine Überwachungssoftware wird üblicherweise als kleines Datenpaket auf dem Zielsystem installiert und lädt anschließend Module nach, mit denen sich weitere Funktionen ausführen lassen. Dies kann beispielsweise die Funktionalität zur Überwachung mit Hilfe einer Laptopkamera sein, oder zur Ausleitung von Daten an die Angreifer.

Die Software selbst ist im Zeitpunkt nach der Installation auf dem Zielsystem bereit, Module jeder Art zu empfangen und auf diese Weise in der zukünftigen Funktionalität nur durch die nicht überwindbaren Restriktionen des Zielsystems eingeschränkt. Das bedeutet, dass es theoretisch möglich ist, Module mit jeder beliebigen Funktionalität nachzuladen. Lediglich die Erreichbarkeit der Schadsoftware auf dem Zielsystem und die Verfügbarkeit der Module schränken die Möglichkeiten ein. Hier gilt also „the sky is the limit“. Diese Funktionalität muss daher zwingend ausgeschlossen werden, da sie sonst unkontrollierbar ist.

Diese Einschränkung muss aus dem Quellcode zweifelsfrei hervorgehen, durch den anordnenden Richter überprüfbar sein, und entsprechend dokumentiert werden.

Beurteilbarkeit der eingesetzten Software durch einen Richter

Ein Richter, der im Rahmen einer Anordnung die Verwendung einer Überwachungssoftware genehmigt, muss eine Prüfung vornehmen können. Es kann nicht angenommen werden, dass Richter ohne weiteres beurteilen können, welche Eigenschaften der Code von Schadsoftware überhaupt mit sich bringt. Das gilt insbesondere dann, wenn die Software nicht im Quellcode vorliegt - in diesem Fall ist eine Beurteilung unmöglich. Diese Prüfung wird erschwert, wenn eine solche Überwachungssoftware weitere Softwaremodule nachladen kann. Auch diese müssten dann zuvor durch einen Richter geprüft werden. Das ist notwendig, um eine Qualitätssicherung zu gewährleisten, denn fehlerhafte Programmierung kann zu technischen wie auch rechtlichen Problemen führen, beispielsweise wenn über einen Befehl aus der Ferne die Überwachungsfunktion nach Beendigung der Maßnahme nicht mehr abgeschaltet werden kann. In früher eingesetzten Versionen von Staatstrojanern der Firma Digitask mit

Sitz in Haiger (Lahn-Dill-Kreis) konnten Fehler belegt wurden.[13] Ein Richter kann das in der Regel allein schon aufgrund des Arbeitsaufwands technisch nicht beurteilen.

An mehreren Stellen wurde deutlich, dass eine Mindestvoraussetzung für die Beurteilung der Eigenschaften das Vorliegen eines dokumentierten und nachvollziehbaren Quellcodes ist. Ein solches Erfordernis ist im Gesetz allerdings nicht dokumentiert. Daher steht zu befürchten, dass eine Beurteilung durch einen Richter erschwert wird oder gar außerhalb des Möglichen liegt. Dies wäre aber notwendig um zu beurteilen, ob diese Software dem Einsatzzweck der beantragten Maßnahme gerecht wird. Dies ist ebenso notwendig, um abwägen zu können, wie tiefgreifend der Eingriff in die Persönlichkeitsrechte tatsächlich sein wird.

Auch das Verständnis der Überwachungssoftware im Hinblick auf die Funktionen und Eigenschaften zu überprüfen, setzt hohe fachliche Kompetenz voraus. Diese kann man jedoch nicht erwarten, denn das Gesetz schreib eine solche erweiterte Qualifikation, wie die Kompetenzen aus einem Studiengang für IT-Sicherheit, für das Richteramt nicht vor. Darüber hinaus sind doppelt qualifizierte Richter gewiss keine nachhaltige Lösung für das Rechtssystem in Deutschland. Die Schlussfolgerung muss also ein Regelwerk sein, das Qualitätsstandards und Anforderungen an die Beschaffenheit und Funktionalität der Software definiert. Sei es im Gesetz, oder dass das Gesetz zum Erlass von Verordnungen ermächtigt, die dieses Standards ausprägen. Ebenso sollten diese anschließend auch einer als hinreichend unabhängig anzusehenden Institution eine Kompetenz zuweisen, über diese Standards zu befinden, beispielsweise durch eine Zertifizierung. Dieses Prüfsystem, die Unbedenklichkeitserklärung einer unabhängigen Quelle, würde dann aufgrund entsprechender Bescheinigung den Richter in die Lage versetzen, auf dieser Grundlage eine Entscheidung zu treffen.

Anordnung von Einschränkungen im Rahmen der Maßnahme

Liegt es im Bereich des Möglichen, dass die Überwachungssoftware weitere Funktionalität besitzt, die im Rahmen der Maßnahme unangemessen ist, oder lässt sich der Funktionsumfang durch den Richter gar nicht erst beschließen, so lässt sich dieser Mangel nicht durch eine Verpflichtung der Antragsteller beheben.

Die Verpflichtung der Antragsteller durch den Richter, dass die Funktionsweise des Überwachungsprogramms sicherstellen muss, dass die Überwachung und Weiterleitung anderer als der von dieser Anordnung umfassten Daten ausgeschlossen ist, kann nicht funktionieren. Denn die Maßnahme kann ja nur zugelassen werden, wenn dies im Rahmen des Richtervorbehalts bereits feststeht.

Ebenso wäre eine Verpflichtung des Antragstellers durch den Richter, selbst fachkundig zu prüfen, ob die Funktionsweise entsprechend eingeschränkt ist, zu hinterfragen, denn damit sind die Überprüfer personengleich mit den Überprüften, was an der Wirksamkeit der Kontrolle stark zweifeln lässt. Das gleiche gilt, wie oben ausgeführt, für den Ankauf der Software von einem privaten Hersteller, der eine Prüfung aus eigener technischer Sachkunde vornimmt. Eine solche unabhängige Prüfung kann nur

13Stellungnahme des Chaos Computer Clubs zum Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen an den Hessischen Landtag vom 4.2.2018

von einer anderen unabhängigen Stelle vorgenommen werden, hier ist zwingend eine Funktionstrennung vorzunehmen: Der Antragsteller darf nicht selbst prüfen, da er ein starkes Interesse an der Durchführung der Überwachung hat, daher ist er als befangen anzusehen. Der Hersteller ist ebenfalls befangen, da er die Software verkaufen möchte. Ein Richter ist neutral und soll prüfen ob der Einsatz gerechtfertigt ist.

Ebenso muss eine unabhängige Stelle die Prognose vornehmen, ob die jeweilige Schwachstelle dazu geeignet ist, bei Geheimhaltung der Sicherheitslücke einen großen Anteil der Bevölkerung, kritische Infrastrukturen oder die Wirtschaft in besonderer Weise zu schädigen. Eine solche Regelung findet sich im Gesetz nicht.

Darüber hinaus stellt das Gesetz keine Anforderungen, dass die dargestellten Risiken der Überwachungssoftware minimiert werden müssen, wie beispielsweise durch die Veröffentlichung der Sicherheitslücke bei Bekanntwerden.

Codecontrolle

Im Verlauf des Einsatzes kann es notwendig werden, dass die Überwachungssoftware weitere Codeteile nachlädt. Um zu jedem Zeitpunkt nachzuvollziehen, wie die Überwachungssoftware als ganzes aussieht, verwendet man ein Versionierungssystem für Softwarecode. Hierin wird der Quellcode sowie die Programmdokumentation abgelegt. Angesichts des weitreichenden Eingriffs in die Persönlichkeitsrechte und um jederzeit anlassbezogen eine Analyse der Schadsoftware vornehmen zu können, wäre ein Hinterlegen dieser Versionen beim Datenschutzbeauftragten angemessen. Dabei muss zu jeder Zeit einer Überwachung sichergestellt werden, dass nur Software verwendet wird, die sich auch im Versionierungssystem befindet und dass diese nicht bei der Nutzung manipuliert werden konnte. Es muss nachprüfbar sein, welche Version der Software zu welchem Zeitpunkt bei welcher Zielperson im Einsatz war.

Dokumentation flüchtiger Veränderungen

Zur Überwachung eines informationstechnischen System wird die Schadsoftware auf dem Zielsystem eingebracht. Damit die Maßnahme durchgeführt werden kann, ist die Manipulation eines weiteren Programms notwendig, um den Code auszuführen. Dieser ausgeführte oder auszuführende Code liegt nicht nur auf einer Festplatte oder anderem dauerhaften Speicher, sondern befindet sich häufig auch bereits im Hauptspeicher des Systems, da es zur Ausführung schon geladen wurde. Das bedeutet, dass die Manipulation des Systems auch im flüchtigen Speicher stattfindet oder stattfinden kann.

Zur Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen legt § 28 (1) HSOG fest, dass die eingesetzten Mittel, der Zeitraums des Einsatzes, die Angaben, die die Feststellung der erhobenen Daten ermöglichen, sowie die Organisationseinheit, die die Maßnahme durchführt protokolliert werden müssen.

§ 28 (2) Nr 5 und 6 HSOG erfordern darüber hinaus für die Telekommunikationsüberwachung an informationstechnischen Systemen sowie die verdeckten Eingriffe in informationstechnische Systeme weitergehende Dokumentation. Diese bezieht sich auf die Beteiligten, die Angaben zur Identifizierung des informationstechnischen Systems, aber auch, welche Veränderungen an den informationstechnischen Systemen vorgenommen wurden. Der Text spezifiziert jedoch nicht ausreichend, was genau dokumentiert werden muss, im Hinblick auf die Veränderung – er stellt nicht sicher, dass auch der Ausgangszustand von welchen aus in den neuen Zustand die Speichermedien versetzt wurden, festgehalten wird. Damit ist es nicht zwangsläufig nachvollziehbar, wie genau eingegriffen wurde und worauf zugegriffen wurde.

Command & Control-Infrastruktur

Nachdem eine Schadsoftware auf dem informationstechnischen System der Zielperson eingebracht wurde, meldet sie sich bei einem voreingestellten Server im Internet, um von dort gegebenenfalls Module nachzuladen oder Befehle zu empfangen, was sie jetzt auf dem Zielsystem machen soll. Diese Server nennt man „Command & Control“-Server, also Server die auf der einen Seite Befehle geben können, aber auch kontrollieren, ob die Schadsoftware ihre Aufgabe erledigt. Dorthin werden auch die Ergebnisse einer Überwachung gesendet, also alle vertraulichen und auch geheimen Daten (auch aus dem privaten Lebensbereich, bis dahin fand ja keine Trennung statt), die auf Anordnung gesammelt wurden.

Zwar erfolgt durch diesen Teil der Einsatz-Software keine unmittelbare Grundrechtseinschränkung, allerdings ist sie die kommunikative Schnittstelle dahingehend, als dass sie Adressat der Überwachungssoftware ist. Wer Kontrolle über die Kontrolleinheit und den Weg der Daten dorthin hat, der hat Kontrolle über die Überwachungssoftware.

Wenn eine Behörde Sicherheitslücken des Zielsystems für eine Überwachungsmaßnahme gezielt ausnutzt, besteht eine Gefährdung mindestens des Zielsystems insbesondere dann, wenn die Infiltration des Zielsystems durch die Polizei — auch unabsichtlich — Dritten ermöglicht, in das System einzudringen oder die Kontrolle über die Kommunikation mit der Überwachungssoftware zu übernehmen. Das kann insbesondere dann passieren, wenn eine unzureichende Authentifizierung von Schadsoftware oder Kontrolleinheit besteht oder auch eine Verschlüsselung mangelhaft implementiert oder grundsätzlich unzureichend ist (z.B. Passwort leicht auszuspähen), und erst recht wenn es so unberechtigten Dritten ermöglicht wird, eine Nachladefunktion von Modulen zum eigenen Vorteil zu nutzen.

Wenn dies gelingt, dann haben die Polizeibehörden unbefugten Dritten den Zugang zu Informationen des Kernbereichs persönlicher Lebenshaltung eingerichtet. Möglich ist auch, dass mit dem Wissen um die Vorgehensweise bei der Infiltration für die Überwachungsmaßnahme auch auf weitere informationstechnische Systeme zugegriffen werden kann, bei denen die gleiche Überwachungssoftware aktuell im Einsatz ist oder nicht gelöscht wurde. So entsteht nicht nur ein Reputationsschaden ungeheuren Ausmaßes der Polizeibehörden, vielmehr machen sich damit öffentliche Stellen im Auge der Bürge-

rinnen und Bürger zum Handlanger von Kriminellen. Dies wird einen nachhaltigen Vertrauensschaden nach sich ziehen.

Da die Schadsoftware umfangreich mit der Kontrolleinheit kommuniziert ist es auch wichtig, sicherzustellen, dass dieser Datentransfer, der die sensiblen Daten enthält, verschlüsselt ist. Ebenso muss sichergestellt sein, dass sich sowohl das Zielsystem, bzw. die Software auf dem Zielsystem, als auch der Kontrollserver gegenseitig authentifizieren, also ihre Identität einwandfrei bestätigen und damit sicherstellen, dass die gewünschten Systeme miteinander kommunizieren, ohne unerwünschte Dritte. So kann die Wahrscheinlichkeit sowohl eines reines Abhörens der Daten, als auch von Angriffen wie ein Man-in-the-Middle-Angriff verringert werden. Ein gängiger Weg der Authentifizierung ist über digitale Zertifikate, beispielsweise mit dem weithin anerkannten X.509-PKI-Standard.

Wird der Datenverkehr unverschlüsselt oder leicht zu entschlüsseln übertragen, so gelangen die Daten, die möglicherweise auch den Kernbereich privater Lebenshaltung betreffen, in die Hände unbefugter Dritter. Bei einem Man-in-the-Middle-Angriff sitzt ein unbefugter Dritter zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Er täuscht dabei den Kommunikationspartnern vor, das jeweilige Gegenüber zu sein.

Fazit

Mit dem Einsatz von Schadsoftware zu Überwachungszwecken auf informationstechnischen Systemen gehen erhebliche Risiken einher. Die Risiken, die durch den Eingriff in die informationstechnischen Systeme der Zielperson erfolgen, verletzen das Recht auf Privatsphäre. Diese Risiken alleine zu betrachten reicht allerdings nicht aus, denn die Gefährdung ist weitreichender. Es bestehen weitere Risiken für die Zielperson, indem die eingesetzte Software mehr Funktionen hat, als für den Einsatz notwendig, oder indem Dritte Kontrolle über die Schadsoftware erlangen und diese missbrauchen, oder indem im Rahmen der Ausleitung der Daten von Unbefugten mitgelesen werden kann.

Darüber hinaus entstehen Risiken für die Allgemeinheit, da seitens der Hessischen Polizeibehörden ein Interesse besteht, die allgemeine Kommunikationsinfrastruktur dauerhaft unsicher zu halten und Sicherheitslücken nicht zu schließen und so potentiell jeden Menschen zu gefährden. Darüber hinaus besteht ein erhebliches Risiko für Unternehmen, Behörden und Organisationen, dass diese Sicherheitslücken zu deren Nachteil ausgenutzt werden, verbunden mit dem Risiko für den Fortbestand der Unternehmung oder die Aufrechterhaltung der öffentlichen Verwaltung. Aufgrund dieser Ausgangssituation ist deutlich, dass mit jeder weiteren Überwachungsmaßnahme auch das Risiko steigt, dass die Software entdeckt und zu Missbrauchszwecken verwendet wird.

Mit einer Ausweitung der berechtigten Antragsteller für diese Maßnahmen steigt folglich auch die Häufigkeit des Einsatzes der Überwachungssoftware und damit die Wahrscheinlichkeit, dass sich ein solches Risiko materialisiert und es zu einem erheblichen Schaden kommt.

Es müssen daher Rahmenbedingungen geschaffen werden, die die Begleiterscheinungen einer Beschaffung und Nutzung von Überwachungssoftware beherrschbar und kontrollierbar machen, um diese gewichtigen Kollateralschäden zu verhindern.

Nötig sind also Standards für Empfehlungen an Richter im Rahmen der Abwägungen zur Genehmigung von Maßnahmen durch das Amtsgericht. Insbesondere wird die Notwendigkeit der angemessenen Informationsgrundlage deutlich, um die Richter für eine Entscheidung zur richterlichen Anordnung in die Lage zu versetzen, eine Überwachungssoftware entsprechend ihrer Funktionalität zu beurteilen. Hierfür muss ein Schwachstellenmanagement eingerichtet werden. Darüber hinaus gilt es, vor einer Anordnung eine unabhängige Folgeabschätzung für jeden weiteren Einsatz zu treffen.

Im Rahmen der DSGVO hat man gelernt, wie man Software insbesondere hinsichtlich der Funktionalität korrekt dokumentieren muss. Bei einer Spionage-Schadsoftware ist das dagegen bisher nicht definiert. Daher ist es überaus schwierig für einen beurteilenden Richter oder ein Kontrollgremium nachzuvollziehen, in wieweit die eingesetzte Spionage-Schadsoftware während der gesamten Einsatzzeit nur auf den vorgeschriebenen Umfang beschränkt ist. Ebenso schwierig ist es zuzusichern, dass ausschließlich die berechtigten öffentlichen Stellen Zugriff auf die Schadsoftware haben — und damit nur sie in der Lage sind, sowohl Zugriff auf den vollen Funktionsumfang zu haben, als auch die Möglichkeit, Module nachzuladen sowie Informationen auszuleiten.