Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Entwurf der Cybersicherheitsstrategie für Deutschland 2021 vom 8.6.2021

Stellungnahme anhand ausgewählter Fragen des Aufrufs der Bundesregierung zur Kommentierung des Entwurfs

Sachverständiger

Dr. Daniel Guagnin – daniel.guagnin@fiff.de

8. September 2021

Vorbemerkung

Die jüngsten Nachrichten unterstreichen, dass IT-Sicherheit in erster Linie auf den Schutz informationstechnischer Systeme abzielen muss, und die Bestrebungen, den sogenannten Sicherheitsbehörden Zugriff auf die Systeme von Kriminellen und potentiellen Angreifer:innen zu gewähren, geeignet sind, die IT-Sicherheit **aller** zu gefährden.

1. Der **Angriff auf die Verwaltung des Landkreises Anhalt-Bitterfeld** zeigt, wie essentiell IT-Systeme in allen Bereichen sind und wie hier Sicherheitslücken durch Organisierte Kriminalität ausgenutzt werden, um großen Schaden anzurichten.[1] An erster Stelle sollte daher alle Energie darauf verwendet werden, Sicherheitslücken zu schließen. Stattdessen basiert die Überwachung und Infiltration krimineller Netzwerke durch Trojaner großteils darauf, Sicherheitslücken offen zu halten, was schließlich Kriminalität fördert, da diese Sicherheitslücken nicht exklusiv für die „Sicherheitsbehörden“ vorgehalten werden können, sondern in allen Systemen und für alle Angreifer:innen gleichermaßen vorhanden sind. Eine Bekämpfung der Angreifer:innen erscheint vor dem Hintergrund ihrer Vielzahl und der breiten Angriffsmöglichkeiten unzureichend gesicherter Systeme zudem wenig zielführend für die Erhöhung des Sicherheitsniveaus.
2. Sicherheitslücken in iOS ermöglichten beispielsweise die Installation der **Spähsoftware „Pegasus" der NSO Group**[2], die zwar nach eigenen Angaben Trojaner nur zur Bekämpfung von Kriminalität und Terrorismus verkauft, diese aber nachweislich gegen Journalist:innen, Menschrecht**s**anwälte[3] und Politiker:innen[4] eingesetzt wurden. Ebenso wie Sicherheitslücken kann auch die Anwendung von Überwachungssoftware nicht wirksam auf den Einsatz gegen „Kriminelle und Terroristen" beschränkt werden. Vielmehr wird diese hier von verschiedenen Staaten eingesetzt, um kritische Journalisten und politische Gegner zu überwachen. Zudem wird in autoritären Regimen Kritik kriminalisiert[5] und so der Einsatz von Überwachungssoftware und die Verfolgung der Kritiker:innen legitimiert. Als demokratischer Rechtsstaat ist es eine besondere Verantwortung für Deutschland, eine demokratische und freiheitliche IT-Sicherheitspolitik zu pflegen und vorzuleben und sich hier durch eine Politik der technischen Sicherheit **zu** profilieren, anstelle die invasiven überwachenden Sicherheitsstrategien autoritärer Staaten nachzuahmen.
3. In der Begründung zur Entscheidung über die Verfassungsbeschwerde der Gesellschaft für Freiheitsrechte **e. V.** (GFF) gegen gegen die Novelle des Polizeigesetzes Baden-Württemberg vom November 2017, die den umfangreichen Einsatz von Staatstrojanern zur Überwachung von Zielpersonen erlaubt, wird folgendes deutlich: **Das Bundesverfassungsgericht bestätigt die Auffassung, dass staatliche Stellen Grundrechte verletzen, wenn sie Sicherheitslücken in IT-Systemen geheim halten, ohne ihre Risiken zu bewerten.**[6] Es ist kaum zu vermeiden, dass Cyberkriminelle und ausländische Geheimdienste von den Sicherheitslücken profitieren, die deutsche Behörden bewusst nicht schließen lassen.

1 https://www.heise.de/news/LKA-Loesegeldforderung-bei-Hackerangriff-in-Anhalt-Bitterfeld-6136714.html
2 https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
3 https://www.amnesty.de/informieren/aktuell/projekt-pegasus-spionage-software-medien-zivilgesellschaft
4 https://www.tagesschau.de/investigativ/ndr-wdr/spionage-software-pegasus-frankreich-101.html
5 https://netzpolitik.org/2021/internet-sicherheitsgesetz-amnesty-kritisiert-massive-einschraenkung-der-meinungsfreiheit-in-bangladesch/
6 https://freiheitsrechte.org/pm-grundsatzentscheidung-it-sicherheit/

1. Zu Kapitel 4: Zielstellung der Cybersicherheitsstrategie und generelle Anmerkungen zur Strategie

Die Bedeutung und Tragweite von IT-Sicherheit wird in der Zielstellung benannt, allerdings liegt der Strategie grundlegend die zweifelhafte Annahme zugrunde, dass Cybersicherheit vorrangig durch die Bekämpfung der Angreifer:innen erhöht werden kann, **statt** konsequent und kompromisslos auf technische Sicherheit zu setzen.

1. Wie richtigerweise in der Zielstellung ausgeführt wird, finden Angriffe häufig durch staatlich vorgelagerte Stellen statt. Ebenso wird festgestellt, dass die Angriffe in der Regel nicht oder nur schwer lokalisierbar sind. Die Verfolgung und Bekämpfung der Angreifenden kann somit nicht das erste und wirksamste Mittel der Erhöhung von Cybersicherheit sein.
2. Gegenangriffe auf Akteure im Cyberraum sowie die Infiltration und Kompromittierung der Systeme vermeintlicher Angreifer basieren in aller Regel auf der Unsicherheit ihrer Systeme. Die technischen Systeme sind in aller Regel breitflächig (auf allen Seiten etwaiger Konflikte) homogen. Daher führt das Vorhalten von Angriffsmöglichkeiten und insbesondere die damit verbundene ausbleibende Behebung wichtiger Sicherheitslücken zur allgemein IT-Unsicherheit. Daher steht das in der Strategie an vielen Stellen vorherrschende Verständnis von Sicherheit - im Sinne einer Abwehr-Aktivität der sogenannten Sicherheitsbehörden - den Interessen einer technisch robusten und resilienten IT-Sicherheit diametral entgegen.

Im Sinne der Steigerung des Niveaus der IT-Sicherheit wäre es daher zielführend, sogenannte Maßnahmen der Gegenwehr, die notwendigerweise die Verletzlichkeit der Systeme bedingen, aus einer Sicherheitsstrategie zu streichen.

Einige Elemente der Strategie sind durchaus begrüßenswert in ihrem Bestreben, die IT-Sicherheit durch sinnvolle Prozesse und Maßnahmen zu stärken, werden aber konterkariert durch unverhältnismäßige Bestrebungen der Ausweitung von sogenannten Abwehrmaßnahmen, die das Potential haben, die sinnvollen Maßnahmen unwirksam oder gar unmöglich zu machen.

3. Zu Kapitel 7: Leitlinien

Zu 7.1. Cybersicherheit als gemeinsame Aufgabe von Staat, Wirtschaft und Gesellschaft

Eine vertrauensvolle Zusammenarbeit ist die Basis für eine gewinnbringende Kooperation der verschiedenen Akteure. Für eine resiliente und robuste IT-Infrastruktur müssen alle an einem Strang ziehen. Dafür ist eine vertrauensvolle Beziehung zwischen Staat, Wirtschaft und Gesellschaft hilfreich, um gemeinsam Sicherheitslücken zu bekämpfen und so die Gefahren von Angriffen, und dem daraus resultierenden Ausfall von relevanten IT-Strukturen – wie auch kritischer Infrastrukturen – zu vermeiden. Ein Generalverdacht gegenüber Bürger:innen, wie er mit invasiver Überwachung, und bei leichteren Vergehen, oder gar ohne Anfangsverdacht **vorgesehen ist**, ist hier kontraproduktiv. Ein BSI, das verpflichtet ist, Sicherheitslücken für die Behörden der inneren Sicherheit geheim zu halten, kann wenig Kooperation aus Unternehmen, Wissenschaft und Zivilgesellschaft erwarten. Ein unabhängiges BSI aber, das nicht den Interessen des BMI unterliegt und frei vom Verdacht einer Kooperation mit den Behörden der inneren Sicherheit ist, kann als zentrale Vermittlungsstelle und Koordinationszentrale für die Stärkung resilienter, vertrauenswürdiger IT-Systeme unterstützend wirken.

Zu 7.2. Digitale Souveränität stärken

Notwendige Schritte und Maßnahmen zur Erreichung einer Unabhängigkeit von Herstellern (wie bspw.

ganz zentral Microsoft) werden nicht benannt. Vielmehr fokussiert auch hier die Strategie auf die eigene Herstellung von Überwachungssoftware, anstatt auf die vielfältigen Potentiale offener Softwaresysteme in allen öffentlichen Bereichen zu fokussieren. Die Stärkung und der Ausbau von Freier Software (Open Source Software) ist hier das Mittel der Wahl, und zwar basierend auf Lizenzmodellen, die die Software nicht lediglich quelloffen und einsehbar machen, sondern auch eine Modifikation und Weiterverteilung erlauben. Hierbei sei auch auf das vom BMI in Auftrag gegebene Gutachten verwiesen, das explizit die Rolle von Open Source Software zur Minderung der Abhängigkeit von internationaler Firmen und zur Stärkung der digitalen Souveränität Deutschlands hervorhebt:[7]

- Der Markt ist derzeit auf wenige Software-Anbieter konzentriert, dies begünstigt Abhängigkeiten grundsätzlich. Die strategische Ausrichtung dieser Anbieter droht diese Abhängigkeiten künftig noch zu verstärken. Dazu gehört der konstante Ausbau des eigenen digitalen Ökosystems, die zunehmende Umstellung von on-premise auf cloudbasierte Lösungen und ein stärkeres Engagement dieser Anbieter bei der Open Source-Software (OSS)-Entwicklung. Neben den marktführenden Produkten gibt es aber auch andere proprietäre und Open Source -Alternativen am Markt, die teilweise hinsichtlich der Leistungsfähigkeit vergleichbar sind.

- Insbesondere die Abhängigkeit von Microsoft-Produkten führt gemäß den Ergebnissen der vorliegenden Analyse zu Schmerzpunkten bei der Bundesverwaltung, die im Widerspruch zu den strategischen Zielen der IT des Bundes stehen. Als kritisch befunden werden vor allem eingeschränkte Informationssicherheit und (datenschutz-)rechtliche Unsicherheit; beides Punkte, die die digitale Souveränität des Staates gefährden.

- Nationale und internationale Beispiele zeigen, dass viele Organisationen bereits heute auch andere Lösungen einsetzen oder deren Nutzung erwägen, um ihre Abhängigkeiten von einzelnen Software-Anbietern zu mindern. Ein Großteil davon zielt darauf ab, Microsoft-Produkte durch Open Source-Lösungen zu ersetzen. Die Analyse ausgewählter Vorhaben zeigt potenzielle Erfolgsfaktoren dieser Lösungsansätze auf.

Ein wichtiges Potential von Freier Software ist hier die Möglichkeit der Anpassung nach spezifischen Bedarfen der Behörden und Verwaltungen und die nachhaltige Kontrolle über die Entwicklungspfade und die Gestaltung der Software. Dies ist mit finanziellen Aufwänden verbunden, die aber eine große Wirksamkeit auf die Erreichung des Zieles digitaler Souveränität zeitigen. Die eingesparten Lizenzgebühren können schließlich stetig in die bedarfsgerechte Anpassung und Weiterentwicklungen der Software fließen. Freie Software ist also keineswegs kostenlos, aber statt in Lizenzen kann und muss in die eigene Weiterentwicklung investiert werden. Schließlich profitieren alle gesellschaftlichen Akteure von einer nutzerfreundlichen und robusten Software und der Unabhängigkeit von einzelnen Herstellern.
Freie Software ist außerdem ohne lizenzrechtliche Probleme auditierbar, hier müssen im Sinne einer Sicherheitsstrategie Maßnahmen der Qualitätskontrolle und Sicherheitsaudits vorgesehen und finanziert werden. Die gefundenen Schwachstellen können direkt zur Behebung in Auftrag gegeben werden und somit das Sicherheitsniveau gesteigert werden – ein weiterer Vorteil Freier Software und eine praktische sicherheitspolitische Dimension der Unabhängigkeit von den Herstellern.

Zu 7.4. Ziele messbar und transparent ausgestalten

Generell ist eine stärkere Transparenz der Verfahren notwendig und demokratisch erforderlich. Die frühe Einbindung während des Entwurfsstadiums der Strategie beispielsweise ist hierbei ein Schritt in die richtige Richtung. Allerdings sind die Beteiligungsfristen regelmäßig extrem kurz, was eine ernsthafte Auseinandersetzung - insbesondere ehrenamtlich - nahezu unmöglich macht. Außerdem **fiel** die Berücksichtigung der Kritik – selbst von eigens zu Anhörungen eingeladenen Sachverständigen im Bundestag – in der Vergangenheit häufig äußerst dürftig aus. Das schadet dem Partizipationsprozess generell und der Gesellschaft im Ganzen, da wichtige Perspektiven aus der Gesellschaft – die die Folgen der Gesetzgebung zu tragen hat – fehlen.
Die kritische Überprüfung von Gesetzen und Maßnahmen ist unbedingt notwendig. Allerdings darf diese nicht nur versprochen werden, sondern muss dann auch umgesetzt werden. Außerdem bleibt die Überprüfung im vorliegenden Entwurf beschränkt darauf festzustellen, ob Kontrollkompetenzen und invasive Überwachungs-Maßnahmen ausgeweitet werden müssen, und nicht etwa kritisch zu prüfen, ob bspw. im

7 https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

Sinne einer Überwachungsgesamtrechnung[8] Maßnahmen sinnvoll und angemessen sind, um ggf. unverhältnismäßige oder hinfällig gewordene Kompetenzen und Befugnisse wieder zurück zu nehmen.

Zu Kapitel 8: Handlungsfelder

Widerstrebende Interessen

An vielen Stellen offenbart sich in den Handlungsfeldern ein inhärenter Widerspruch, der oben aufgezeigt wurde: Offensive und invasive Maßnahmen der sogenannten Sicherheitsbehörden führen im Bereich der IT-Sicherheit faktisch zu Unsicherheit, da nur Systeme, die kompromisslos auf Vertraulichkeit, Integrität und Verfügbarkeit ausgerichtet sind, eine Chance haben, gegen Angriffe zu bestehen. Alle Maßnahmen, die darauf abzielen, Verletzlichkeiten nicht zu bekämpfen, sondern als potentielle Einfallstore vorzuhalten, müssen den gesellschaftlichen Sicherheitsinteressen folglich zuwider laufen. Angriffspunkte in informatischen Systemen dienen niemals nur den eigenen Interessen, sondern auch allen Angreifenden.

Die genannten positiven Handlungsfelder wie Verbraucherschutz, sichere Identitäten, Verschlüsselung, Stärkung der Sicherheit der Unternehmen und der Digitalwirtschaft, Sicherheitsstandards, Security-by-Design, kryptografische Standards **sowie** Cybersicherheit von Behörden und bei Wahlen werden dadurch geschwächt oder gar grundlegend unterwandert. Die Forderung von Sicherheit durch Verschlüsselung trotz Verschlüsselung zeigt hier eine paradigmatische Fehlannahme und damit den fundamentalen Fehlschluss einer Sicherheit durch invasive Überwachung technischer Systeme. Jegliche Hintertüren oder Vordertüren, Zugriffsmöglichkeiten und Angriffspunkte beschädigen die Integrität technischer Systeme und machen damit erst Angriffe möglich. Es kann nur Sicherheit durch Verschlüsselung und nur durch Verschlüsselung geben. Die potentielle Aufklärungsarbeit und Bekämpfung von Kriminalität darf diese nicht zuerst ermöglichen.

Vertrauen

Eine „Zusammenarbeit von Staat, Wirtschaft, Wissenschaft und Zivilgesellschaft im Bereich der Cybersicherheit" (8.2.2) kann nur dann gelingen, wenn es eine gemeinsame Vertrauensbasis gibt, insbesondere durch die Gewissheit, dass gemeldete Schwachstellen nicht für invasive Angriffs- und Überwachungsmaßnahmen instrumentalisiert, sondern schnellstmöglich geschlossen werden. Dafür ist es notwendig einen unabhängigen Bundesakteur zu haben, der nicht in die Pflicht genommen werden kann, mit den sogenannten Sicherheitsbehörden zu kooperieren. Das BSI könnte so ein Akteur sein, insofern es unabhängig vom Innenministerium ist. In der aktuellen Konstellation und mit den aktuellen Bestrebungen, das BSI auch mit offensiven Befugnissen auszustatten, steht eine vertrauensvolle Zusammenarbeit mit Wirtschaft und Zivilgesellschaft auf dem Spiel.

Ein gegenseitiger Austausch von Perspektiven, Erfahrungen und Bedarfen in Sachen IT-Sicherheit, wie er bspw. in der „Allianz für Cybersicherheit“ (ACS) gepflegt oder im „Dialog für Cybersicherheit“ des BSI angestoßen wird, ist erstrebenswert und ausbaufähig. Echte Partizipation, angemessene Beteiligungsformate und vor allem Beteiligungszeiträume sowie eine ernsthafte Berücksichtigung von Anregungen sind hier unabdingbar.

Digitale Kompetenz

Die Ausbildung von Kompetenz in der Bevölkerung und einem Grundverständnis digitaler Infrastrukturen ist ein zentrales Element eines selbstbestimmten Umgangs mit digitalen Technologien. Ein wichtiger, allseits vernachlässigter Aspekt ist hier der Bereich der Bildung. Bis heute wurde es versäumt, Strukturen der Kompetenzvermittlung für die heranwachsende Bevölkerung zu schaffen. Ehrenamtliche Initiativen wie bspw. das Format „Chaos Macht Schule" des CCC sind regelmäßig stark nachgefragt, können aber die Nachfrage gar nicht abdecken. Vielmehr muss Schulen Budget für die fachliche Inhaltsvermittlung

8 Vgl. zum Beispiel: https://netzpolitik.org/2021/ueberwachungsgesamtrechnung-mehr-als-die-summe-der-einzelteile/

und Schulungen der Lehrkräfte zur Verfügung gestellt werden und nicht lediglich für die Anschaffung technischer Mittel.

Dennoch können die Verbraucher:innen aber die Verantwortung der IT-Sicherheit keineswegs alleine schultern. Insbesondere nicht, wo IT-Sicherheit von Herstellern vernachlässigt oder durch Sicherheitsbehörden systematisch untergraben wird. Die Anhebung vorgeschriebener Mindeststandards und die kompromisslose Unterstützung von Sicherheit durch starke und sichere Verschlüsselung sind hier die Mittel der Wahl und dringend geboten.

„Gefahrenabwehr“

Die Annahme, den vermehrten Tätigkeiten anderer Länder im Feld offensiver Methoden durch eine eigene Aufrüstung an Methoden und Kompetenzen begegnen zu können, ist ein Fehlschluss. Jegliche Maßnahmen, die die Kompromittierung von IT zum Ziel haben, schwächen strukturell die eigene Software, da diese mit der Software potentieller Angreifender in aller Regel identisch ist. Vielmehr sollte international darauf hingewirkt werden, gemeinsam für eine resiliente IT-Struktur Politik zu machen, um global Angriffsflächen zu minimieren und die zunehmend auf IT basierenden Alltagstechnologien zu schützen.

Der formulierten Erwartung *„... für die Gefahrenabwehr besonders schwerer und bedeutender Cyberangriffe werden die Möglichkeiten für eine effektive Cyberabwehr erweitert. Gegen die Ursachen schwerer Cyberangriffe kann aktiv vorgegangen werden, um deren schädliche Wirkung im besten Fall komplett zu unterbinden. Damit steigt das gesamtstaatliche Cybersicherheitsniveau."* liegt ein fataler Fehlschluss zugrunde. Gegenwehr – so es denn überhaupt möglich ist, Angreifende korrekt zu lokalisieren - ist wenig aussichtsreich in Anbetracht der einfachen Mittel für Cyberangriffe. „Waffen" sind kopierbar, Angriffs-Computer austauschbar, häufig kommen breite Botnetze zum Einsatz. Hingegen ist das Vorhalten von Angriffspunkten auf Systemen Dritter für potentielle Gegenangriffe ein Eigentor, da in Zeiten der Globalisierung alle auf denselben Systemen arbeiten (z. B. Microsoft). Angriffspunkte für die Gegner erhöhen also immer auch die eigene Angreifbarkeit.

Die in der Strategie angelegte stetige Ausweitung der Befugnisse der Sicherheitsbehörden ist vor dem Hintergrund bereits erfolgter Ausweitungen der letzten Jahre höchst fragwürdig und müsste zumindest mit entsprechenden Kontrollmechanismen einhergehen. Angebracht wäre außerdem eine kritische Überprüfung der Wirksamkeit invasiver Überwachungsmaßnahmen[9] hinsichtlich der tatsächlichen Abwehr von Gefahren im Verhältnis zur Steigerung von Gefahren durch Hintertüren und Sicherheitslücken.

Die Vermischung technischer IT-Sicherheit mit geopolitischen Machtinteressen fördert nicht die Cybersicherheit, da gegenseitige Ausspähung systematisch Unsicherheit auf der Ebene der IT-Systeme fördert. Cybersicherheit kann nur strategisch und kooperativ funktionieren, denn sie beruht nicht auf der absichtlichen Herstellung von Unsicherheit in „anderen" Systemen, sondern auf der Herstellung von robusten Systemen. Hier kann Kooperation sehr fruchtbar sein, da gemeinsame Investitionen zur Absicherung von Systemen, wie bspw. Sicherheitsaudits und die Behebung von Sicherheitslücken, schließlich allen zugute kommen.

Förderung von Forschung und Wissenschaft

Die Förderung unabhängiger Forschung und Standards ist eine wichtige Maßnahme, die zu einer Stärkung der Cybersicherheit führen kann. Allerdings ist es wichtig, im Rahmen politischer Prozesse auch auf die kritischen Stimmen aus der Wissenschaft zu hören und somit das gewonnene Potential aus dieser sinnvollen Investition zu ziehen. Diese sind sich weitgehend einig, dass eine Stärkung der offensiven „Sicherheitsmethoden“, wie hier ausführlich beschrieben, die technische Sicherheit digitaler Systeme massiv unterwandert.

9 vgl. z.B. den Verweis zur Überwachungsgesamtrechnung in FN 8

4. Frage zur klaren Linie der Strategie

Eine klare Linie ist leider nicht zu erkennen. Stattdessen stehen Maßnahmen, die tatsächlich die IT-Sicherheit erhöhen können, im direkten Widerspruch zum Ausbau invasiver Befugnisse, die die IT-Sicherheit schwächen. Der Kampf gegen die Angreifer ist im Cyberraum wenig erfolgversprechend – im Gegensatz zum Aufbau einer resilienten und robusten Informationstechnik, hier ist aber eine klare Linie nicht zu erkennen.

Im Sinne einer widerspruchsfreien Strategie wäre daher anzudenken, Maßnahmen und Ziele der technischen IT-Sicherheit gänzlichen von aktiven Maßnahmen der Behörden der inneren Sicherheit getrennt zu verhandeln.