An das
Bundesministerium für Inneres
Abteilung III//A/4
Herrengasse 7
1010 Wien

bmi-III-A-4-stellungnahmen@bmi.gv.at

Wien, am 25. September 2024

Stellungnahme der ISPA zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich, in Zusammenhang mit der öffentlichen Konsultation (Geschäftszahl: 2024-0.148.142) des Bundesministeriums für Inneres betreffend einen Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz (SNG) geändert wird, Stellung zu nehmen.

Der vorliegende Entwurf geht auf eine lange öffentliche Debatte zurück, in deren Rahmen von den staatlichen Sicherheitsbehörden wiederholt auf unzulängliche nachrichtendienstliche Befugnisse hingewiesen und insbesondere der Wunsch nach der Überwachung verschlüsselter Kommunikation geäußert wurde. Neben anderen Aspekten soll der vorliegende Entwurf eben dies sicherstellen, in dem die Direktion Staatsschutz und Nachrichtendienst (DSN) mittels einer ins Endgerät der überwachten Person eingebrachten Schadsoftware (Trojaner) Zugriff auf die unverschlüsselten Nachrichten erhält.

Die dem Entwurf vorausgehende Diskussion zur „Messenger-Überwachung“ spiegelt zwei schwer miteinander zu vereinbarende Interessen wider. Auf der einen Seite steht das Anliegen der staatlichen Sicherheitsbehörden, die zum Schutz der Bürger und zur Abwehr verfassungsgefährdender Angriffe verpflichtet sind. Angesichts des technologischen Wandels in der Kommunikation möchten sie ihre gesetzlichen Befugnisse an die neuen Gegebenheiten anpassen, um mit den technischen Möglichkeiten der überwachten Personen Schritt halten zu

können. Auf der anderen Seite steht das gesamtgesellschaftliche Interesse an privater Kommunikation und sicheren Informationsinfrastrukturen, verbunden mit der Sorge vor einem möglichen Missbrauch dieser Befugnisse. Zusätzlich zur rechtspolitischen Diskussion müssen auch klare verfassungsrechtliche Schranken beachtet werden, wie sie der österreichische Verfassungsgerichtshof in seinem Erkenntnis vom 11. Dezember 2019 formuliert hat, als er das 2018 beschlossene „Sicherheitspaket“, das ebenfalls Befugnisse zur Überwachung verschlüsselter Kommunikation enthielt, aufgehoben hat.[1]

Die ISPA kann in ihrer Stellungnahme nicht auf sämtliche Aspekte dieser Debatte eingehen. Als Vertreterin der österreichischen Internetwirtschaft beschränkt sie sich dabei grundsätzlich auf die Wiedergabe der Perspektive der betroffenen Unternehmen und auf offene Fragen, die sich aus dem Entwurfstext ergeben. Sie hofft, dadurch ihren Beitrag im Diskurs zu leisten.

Durch den Einsatz eines Trojaners kommt der Staat in einen Interessenkonflikt:

Der Entwurf gibt der DSN die Möglichkeit, eine Schadsoftware (Trojaner) in das Computersystem der überwachten Person einzubringen, welches den Zugriff auf gesendete und empfangene Nachrichten im unverschlüsselten Zustand ermöglicht. Ein derartiger Trojaner setzt für seine Installation eine Sicherheitslücke im Computersystem der überwachten Person voraus, etwa im Betriebssystem des Endgeräts oder in konkreten Anwendungen. Diese Sicherheitslücke darf nur dem Entwickler des Trojaners, nicht aber dem Anbieter des Betriebssystems/der Software bekannt sein, da letztere die Lücke ansonsten beheben würde und der Trojaner nicht mehr einsatzfähig wäre.

Dadurch gelangt der Staat aber in einen Interessenkonflikt. Einerseits hat er ein Interesse an einem hohen Niveau an Cybersicherheit, das auch mittels entsprechender Rechtsnormen (z.B. NIS-2-Gesetz) sichergestellt werden soll. Wenn etwa eine Sicherheitslücke in einem Betriebssystem besteht, das ja nicht nur von Gefährdern, sondern auch von Privatpersonen, Unternehmen und in der Verwaltung genutzt wird besteht, hat der Staat grundsätzlich ein Interesse daran, diese zu beheben, da ansonsten große Nachteile durch Angriffe Dritter drohen. Mit der im Entwurf vorgesehenen Einsatzmöglichkeit für Trojaner sind die staatlichen Sicherheitsbehörden nun aber für die Überwachung von Nachrichten auf die Existenz bestimmter Sicherheitslücken angewiesen und haben daher ein genau gegenläufiges Interesse, nämlich dass diese Sicherheitslücken nicht geschlossen werden. Dieser Interessenkonflikt spitzt sich dabei gerade im Innenministerium zu, bei dem nicht nur die DSN,

[1] VfGH 11.12.2018, G73/2019 ua.

sondern auch die für das novellierte Netz- und Informationssicherheitsgesetz 2024 (NIS-G 2024) zuständige neu zu schaffende Cybersicherheitsbehörde angesiedelt sein wird.

Dies ist insofern brisant, als es den Sicherheitsbehörden möglich sein könnte, aus dem ihnen zur Verfügung stehenden Trojanern Rückschlüsse auf die ausgenutzten Sicherheitslücken zu ziehen (etwa mittels Reverse Engineering), welche dann vom Anbieter für deren Behebung genutzt werden könnten. Gerade dies werden die Sicherheitsbehörden in eigenem Interesse aber nicht machen, obwohl dadurch ein erhebliches Sicherheitsrisiko für andere, legitime Anwender ausgeräumt werden könnte.

Die entsprechenden Sicherheitslücken bleiben also bis zu ihrer anderweitigen Entdeckung und Behebung bestehen und können auch von böswilligen Akteuren genutzt werden. Diese unterliegen dann aber freilich nicht jenen strengen Einschränkungen, die im Entwurf für den Einsatz durch die DSN vorgesehen sind. Jüngsten Medienberichten zufolge ist dies auch bereits tatsächlich passiert.[2]

Unklar, wie gesetzliche Anforderungen in der Praxis sichergestellt werden:

Der Entwurf sieht in § 15a Abs. 5 vor, dass die Funktion des eingespeisten Trojaners technisch beschränkt sein soll. Der Trojaner darf nur innerhalb des Bewilligungszeitraums gesendete/empfangene Nachrichten überwachen, nur notwendige Veränderungen am Computersystem vornehmen und nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig werden. Zu diesen explizit genannten Beschränkungen treten noch implizite, sich aus der Gesamtschau des Entwurfs ergebende Beschränkungen. So darf der Trojaner selbstredend auch nur der DSN und nicht Dritten die Einsicht in die Kommunikation der überwachten Person ermöglichen. Auch darf er nur die Kommunikation, nicht aber die am Endgerät gespeicherten Daten auslesen.

Für die ISPA stellt sich die Frage, wie diese gesetzlichen Anforderungen in der Praxis sichergestellt werden können. Da von vielen Experten ausgeschlossen wird, dass die DSN diesen Trojaner in Eigenentwicklung herstellen kann, kommt in der Praxis nur dessen Erwerb von Dritten, wie etwa anderen Staaten oder privaten Anbietern in Frage. Auch wenn die genauen Modalitäten der Beziehung zwischen dem Verwender des Trojaners (in diesem Fall die DSN) und dessen Anbieter für Dritte nicht transparent sind, so kann doch aufgrund des

[2] Der Standard, 1.09.2024: *Die Tricks des „Bundestrojaners" sind in die Hände Moskaus gefallen*. Online abrufbar unter https://www.derstandard.at/story/3000000234720/die-tricks-des-bundestrojaners-sind-in-die-haende-moskaus-gefallen .

Interesses des Anbieters an der Wahrung seiner Betriebs- und Geschäftsgeheimnisse (konkret, welche Sicherheitslücke ausgenutzt wird) davon ausgegangen werden, dass dem Verwender nicht der Quellcode des Trojaners offengelegt wird. Vielmehr ist zu erwarten, dass der Trojaner und die für dessen Installation notwendige Software entweder in kompilierter Version als ausführbare Anwendung oder aber überhaupt als Dienstleistung (Malware-as-a-Service) durch den Anbieter zur Verfügung gestellt wird. Bei beiden Varianten gibt es aber mangels Einblicks in den Quellcode letztlich keine Möglichkeit, mit einem Code Review die Funktionalität des Trojaners endgültig zu überprüfen. Die DSN müsste sich daher hinsichtlich der Einhaltung der im Entwurf vorgesehenen technischen Beschränkungen auf vertragliche Zusagen des Anbieters verlassen. Dies kann insbesondere dann ein Problem werden, wenn der Trojaner nicht von befreundeten Staaten mit vergleichbarer Rechtslage, sondern von privaten Anbietern bezogen wird, die häufig in Drittstaaten ansässig sind. Die DSN kann sich damit im Ergebnis niemals sicher sein, ob der verwendete Trojaner tatsächlich nur das macht, was er nach österreichischer Rechtslage darf oder ob er etwa darüberhinausgehende Überwachungsmaßnahmen vornimmt oder die ausgelesenen Daten sogar an Dritte übermittelt. Der Entwurf beinhaltet lediglich die Verpflichtung zu den erwähnten technischen Beschränkungen, lässt aber offen, ob etwa bloße vertragliche Zusagen über die Funktion des Trojaners ausreichend sind oder die DSN zu einer umgehenden technischen Überprüfung verpflichtet ist, bevor dieser eingesetzt werden darf.

Aus Sicht der ISPA wäre es daher zweckmäßig, wenn der Entwurf diesbezüglich Klarstellungen vornimmt, dass ein Trojaner nur dann eingesetzt werden kann, wenn in Abwägung aller Umstände und gegebenenfalls nach einer eingehenden technischen Überprüfung kein vernünftiger Zweifel daran besteht, dass er die in Österreich geltenden technischen Beschränkungen einhält.

Mitwirkungspflichten der Anbieter sind unklar geregelt:

Für die Überwachung unverschlüsselter wie auch verschlüsselter Nachrichten wird die DSN in der Praxis auf die Mitwirkung privater Anbieter angewiesen sein, die für die überwachte Person Kommunikationsinfrastruktur oder entsprechende Dienste bereitstellen. Für diese sieht der Entwurf in § 11 Abs. 2 Mitwirkungs- und Auskunftspflichten vor, lässt deren genaue Ausgestaltung und Adressatenkreis aber offen.

Da sowohl § 11 Abs. 2 Z8 wie auch Z9 des Entwurfs auf die Bestimmungen zur Überwachung von Nachrichten in § 134 Z3 Strafprozessordnung (StPO) verweisen, sind die darin enthaltenen Begriffsbestimmungen maßgeblich. Der Begriff des Anbieters bezieht sich gem.

§134 Z6 StPO sowohl auf Betreiber öffentlicher Kommunikationsnetze, Bereitsteller von Diensten der Informationsgesellschaft (§ Z 2 E-Commerce-Gesetz - ECG) und Anbieter von Vermittlungsdiensten (§ 3 Z4a ECG). Während bei der klassischen Telekommunikationsüberwachung nach dem Vorbild der StPO nur die Betreiber öffentlicher Kommunikationsnetze sinnvollerweise mitwirken konnten, ist bei der Überwachung verschlüsselter Kommunikation mittels eines Trojaners auch eine Mitwirkung anderer Diensteanbieter denkbar – etwa bei der Einschleusung manipulierter Updates für Applikationen oder Betriebssysteme durch deren Hersteller oder im Extremfall sogar durch den absichtlichen Einbau von Sicherheitslücken (Backdoors), die für die Installation des Trojaners genutzt werden können. All diese Möglichkeiten reichen extrem weit und werfen komplexe technische, rechtliche, gesellschaftspolitische und finanzielle Fragen auf, die zuvor geklärt werden müssen. Der Entwurf nimmt hier jedoch keinerlei Eingrenzungen vor und auch in den Erläuterungen werden keine Angaben dazu gemacht, welche Arten von Diensteanbietern in welcher Weise mitwirken sollen. In einem allfälligen neuen Entwurf müsste dies unbedingt klargestellt und ggf. anhand einer Folgenabschätzung eingegrenzt werden, wobei eine vorhergehende öffentliche Debatte über die weitreichenden Implikationen unabdingbar ist.

Auch die Mitwirkungspflichten speziell für Betreiber öffentlicher Kommunikationsnetze lassen viele Fragen offen. Während sich diese Pflichten im Fall der Überwachung unverschlüsselter Nachrichten nach dem Vorbild der Telekom-Überwachung in §134 Z3 StPO richten, ist im Fall der Überwachung verschlüsselter Nachrichten unklar, welche Mitwirkung von den Netzbetreibern bei der Installation des Trojaners verlangt wird. Je nach Art des verwendeten Trojaners bzw. der ausgenutzten Sicherheitslücke gibt es unterschiedliche Weisen, wie dieser am Endgerät installiert werden kann – z.B. Zero-Click, One-Click – womit auch eine unterschiedliche Mitwirkung der Netzbetreiber theoretisch denkbar ist. Aus Sicht der Anbieter von Telekommunikationsdiensten ist eine Mitwirkung dieser bei der Installation des Trojaners abzulehnen, da ansonsten ein massiver Vertrauensverlust in die Integrität elektronischer Kommunikation droht. Insbesondere Manipulationen am Datenverkehr durch den ISP wären ein absoluter Tabubruch und dürfen keinesfalls in Erwägung gezogen werden.

Im Entwurf sollten daher die Mitwirkungspflichten der Anbieter genauer geregelt und eingegrenzt werden. Für Mitwirkungspflichten, die über die derzeitigen Pflichten hinausgehen, müsste auch die Überwachungskostenverordnung (ÜKVO) angepasst werden. Die darin geregelten Bestimmungen zum Kostenersatz für die Überwachung von Nachrichten (§ 9 ÜKVO) beziehen sich nämlich auf die klassische Telekommunikationsüberwachung und damit einen anderen Sachverhalt. Je nach Ausgestaltung der Mitwirkungspflichten wären ggf. auch

Investitionen erforderlich, die nach der Investitionskostenersatzverordnung (IKEV 2023) abgegolten werden müssen. Damit der Kostenersatz geltend gemacht werden kann, wären die entsprechenden Bestimmungen in ÜKVO, IKEV 2023 und TKG auch um Verweise auf die Verpflichtung nach dem SNG zu ergänzen.

Anordnungen müssen jedenfalls Geheimhaltungsverpflichtung beinhalten:

Der Entwurf sieht in § 11 Abs. 3 vor, dass die DSN dem entsprechenden Anbieter dessen Mitwirkungsverpflichtung und ihren Umfang sowie die Verpflichtung, mit der Ermächtigung oder gerichtlichen Bewilligung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, aufzutragen hat. Es ist von zentraler Bedeutung, dass die DSN auch tatsächlich eine derartige Geheimhaltungsverpflichtung in ihre Anordnungen aufnimmt. Bei Auskunftsanordnungen in Bezug auf Informationen über ihre Nutzer:innen sind Anbieter von Vermittlungsdiensten gemäß Art. 10 Abs. 5 des Gesetzes über digitale Dienste (Digital Services Act – DSA) nämlich dazu verpflichtet, den betroffenen Nutzer grundsätzlich spätestens zum Zeitpunkt der Befolgung der Anordnung oder zu einem Zeitpunkt, den die erlassende Behörde in ihrer Anordnung angegeben hat, über diese zu informieren. Eine zeitnahe Information der Nutzer:innen über eine Überwachungsmaßnahme wird aber in aller Regel kontraproduktiv sein und die Überwachung torpedieren. In allen einschlägigen Anordnungen – auch abseits des SNG – in denen etwa Betreiber von Kommunikationsnetzen zu bestimmten Auskünften ihre Nutzer:innen angewiesen werden, muss daher unbedingt eine derartige Geheimhaltungsverpflichtung enthalten sein.

Wertungswiderspruch durch Backup-Überwachung:

Die im Entwurf angedachte Überwachung durch den Trojaner (§ 11 Abs. 1 Z9) bezieht sich ausschließlich auf Nachrichten, d.h. Kommunikationsvorgänge. Auch den Erläuterungen zum Ministerialentwurf zufolge scheidet eine Durchsuchung des gesamten Computersystems inklusive lokal gespeicherter Daten aus. Allerdings sind nach den Erläuterungen nicht nur Nachrichten über internetbasierte Apps wie Whatsapp oder Telegramm von der Überwachung erfasst, sondern auch über einen Cloud-Diensteanbieter an einen Cloud-Server übermittelte Datenpakete. Letzteres scheint aber somit auch Backups des Geräts zu erfassen, die an einem Backup-Server übermittelt werden. Damit wäre es für die Ermittler zwar einerseits unzulässig, die lokal am Endgerät gespeicherten Daten (wie unter anderem gespeicherte Standortdaten, Notizen, Bilder, Musik, Videos, Gesundheitsdaten von Wearables etc.) mittels des Trojaners auszulesen. Sobald diese Dateien aber in Form eines Backups an einen Server übermittelt werden, wäre der Zugriff darauf auf einmal rechtlich unproblematisch. Da diese

Daten typischerweise erheblich umfangreicher und teils auch sensibler sind als diejenigen, die über bloße Chats übermittelt werden, sollte die Legitimität des Zugriffs durch Ermittlungsbehörden nicht davon abhängen, ob die überwachte Person die Backupfunktion auf dem Telefon aktiviert hat. Dieser Wertungswiderspruch sollte in einem überarbeiteten Entwurf aufgelöst werden, etwa durch eine Klarstellung, dass auch derartige automatisierte Backups als M2M-Kommunikation (die nicht von der Überwachung erfasst ist) zu verstehen ist.

Begriff des Computersystems zu weit gefasst:

Der Entwurf ermöglicht das Einbringen eines Programms in ein „Computersystem“ eines Betroffenen (§ 11 Abs. 1 Z9). Der Begriff „Computersystem“ umfasst dabei nach der Legaldefinition von § 74 Abs. 1 Z8 StGB „einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen“. Vom Wortlaut ist dies damit nicht auf solche Computersysteme begrenzt, die sich in der physischen Verfügungsgewalt des Betroffenen befinden (insb. dessen Endgeräte). Vielmehr könnten vom Begriff her auch durch den Betroffenen genutzten, aber von Dritten betriebene Cloud-Systeme umfasst sein. Ein Einbringen eines Trojaners in ein solches Cloud-System birgt aber unabsehbare Sicherheitsrisiken für den jeweiligen Anbieter und dessen Nutzer:innen, weshalb der Entwurf diese Möglichkeit nicht eröffnen sollte. Auch die Formulierung in den Erläuternden Bemerkungen, wonach die Ermittlungsmaßnahmen auch „andere Geräte, die eine Internetverbindung ermöglichen“ umfassen (S.4), würde beispielsweise auch eine Kompromittierung von Smart-Home-Systemen ermöglichen, was aus Sicherheitsgründen ebenfalls abzulehnen ist. Dies sollte im Entwurf entsprechend geändert und eingegrenzt werden.

Mit freundlichen Grüßen,

Stefan Ebenberger

Generalsekretär ISPA

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675
DVR-Nr.: 0931977

Die ISPA – Internet Service Providers Austria – ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von über 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

UniCredit Bank Austria AG
Konto-Nr.: 00660 491 705, **BLZ:** 12000
BIC: BKAUATWW
IBAN: AT59 1200 0006 6049 1705

UID-Nr.: ATU 54397807
ZVR-Zahl: 551223675
DVR-Nr.: 0931977