Wien, am 9. August 2017

OFFENER BRIEF ZUR GEFÄHRDUNG DER CYBERSICHERHEIT DURCH DAS GEPLANTE SICHERHEITSPAKET

Sehr geehrte Mitglieder des Nationalrats,
sehr geehrte Damen und Herren,

die unterzeichnenden Vertreterinnen und Vertreter der IT-Branche möchten hiermit ihre Bedenken hinsichtlich des Entwurfs des „Sicherheitspakets" äußern. Die darin unter anderem vorgesehene neue Ermittlungsbefugnis des § 135a StPO soll es erlauben, ohne Zustimmung des Inhabers ein Programm zur Überwachung verschlüsselter Nachrichten auf einem Computersystem zu installieren. Darüber hinaus wird in den weiteren Novellierungen eine massive Ausweitung der Speicherverpflichtungen von Kundendaten festgesetzt, welche sich zum einen durch die erneute Einführung einer Vorratsdatenspeicherung („quick freeze") sowie zum anderen durch eine generelle Registrierungspflicht beim Erwerb von Prepaid-Karten bzw. entsprechendem Guthaben äußert. Hierdurch wird bei zweifelhaftem Nutzen für die Rechtsdurchsetzung ein enormer Aufwand verursacht und werden gleichzeitig, nicht zuletzt aufgrund der inhaltlichen Unbestimmtheit, kritische Fragen hinsichtlich Privatsphäre und Datenschutz aufgeworfen.
Obgleich es nachvollziehbar ist, dass eine Anpassung der Überwachungsmöglichkeiten an neue Technologien gefordert wird, möchten wir auf jene Aspekte hinweisen, die wir als Gefahr für die Cybersicherheit sehen, und den zu befürchtenden negativen Auswirkungen geschlossen entgegentreten:

Die Nutzung von IT-Sicherheitslücken für Ermittlungsmaßnahmen schwächt die Cybersicherheit und untergräbt das Vertrauen in österreichische Unternehmen
Nutzerinnen und Nutzer vertrauen derzeit darauf, dass ihre Daten in den von ihnen genutzten Diensten sicher vor fremden Zugriffen sind. Dieses Vertrauen basiert auf der intensiven Arbeit, welche die IT-Branche über Jahre in die Etablierung von Sicherheitsstandards, wie einer effektiven Verschlüsselung der Daten, investiert hat. Ein Hauptaugenmerk liegt dabei darauf, ständig nach vorhandenen Sicherheitslücken in den Systemen zu suchen und diese mittels Updates zu schließen. Zur unbemerkten Ferninstallation der vorgesehenen Überwachungssoftware werden jedoch gerade solche „backdoors" ausgenutzt. Um eine effektive Umsetzung der Ermittlungsmaßnahme zu garantieren, müssten solche Sicherheitslücken demnach offengehalten werden, anstatt sie dem jeweiligen Unternehmen zu melden. Die Auswirkungen solch bewusst nicht geschlossener „backdoors" haben sich zuletzt anhand krimineller Cyber-Attacken mittels Ransomware („WannaCry" bzw. „Petrwrap") gezeigt, die vor kurzem enormen Schaden für die Wirtschaft verursacht haben.
Die vorgeschlagenen Ermittlungsmaßnahmen untergraben damit auch das Vertrauen in österreichische Unternehmen und in den Wirtschaftsstandort Österreich, der bislang aufgrund der hohen Datenschutz- und Sicherheitsstandards geschätzt wird.

Das reine Ausleiten von Kommunikationsdaten ohne „Online-Durchsuchung" von Computersystemen ist technisch nicht möglich
In den Erläuterungen wird wiederholt betont, dass § 135a lediglich der Ausleitung von Kommunikationsdaten während des aufrechten Kommunikationsvorgangs dienen soll und keinesfalls einer „Online-Durchsuchung" gleichkommt. Aus technischer Sicht möchte die IT-Branche jedoch darauf hinweisen, dass ein solch „chirurgischer Eingriff" technisch nicht umsetzbar ist, und damit den Ausführungen in den Erläuterungen, welche die technische Umsetzbarkeit lediglich feststellen ohne diese zu erläutern, klar widersprechen. Der Grund hierfür liegt darin, dass für die Installation, den Betrieb und das Verstecken einer solchen Überwachungssoftware umfangreiche Zugriffsrechte auf dem Zielsystem benötigt werden. Hierdurch würden jedoch zahlreiche weitere Funktionalitäten erlaubt werden, inklusive des Durchsuchens, Manipulierens und Erstellens von Dateien. Eine technische Einschränkung der Software, um dies gänzlich zu unterbinden, ist nicht möglich. Darüber hinaus wären auch Backups in einer Cloud erfasst, was wiederum einer de facto Online-Durchsuchung gleichkommt. Diese Risiken wurden bereits von einer interministeriellen Arbeitsgruppe zur „Online-Durchsuchung" im Jahr 2008 thematisiert und konnten bislang nicht ausgeräumt werden.

Die ausgedehnte Definition der „Überwachung von Nachrichten“ birgt unabschätzbare Risiken für das „Internet der Dinge“

Verstärkt wird das Sicherheitsrisiko noch dadurch, dass die Novelle eine exzessive Ausdehnung des Begriffs „Nachricht“ vorsieht, durch welchen in Hinkunft nicht nur menschliche Gedankeninhalte, sondern auch Kommunikation im technischen Sinn erfasst werden soll. In Kombination mit der weiten Definition von „Computersystem“ im Strafgesetzbuch würde damit auch die Kommunikation zwischen Geräten im „Internet der Dinge“ miteingeschlossen werden, wodurch auch auf diesen Geräten entsprechende „backdoors“ notwendig wären und die potentiellen Missbrauchsmöglichkeiten noch weiter ansteigen.

Die staatliche Nutzung von Sicherheitsschwachstellen fördert einen Markt für Sicherheitslücken

Die Unterzeichner möchten sich deutlich gegen jegliche Kooperation des Staats mit zweifelhaften Dienstleistern, welche Sicherheitslücken am Markt für horrende Summen anbieten, aussprechen. Auch unter dem Gesichtspunkt des Schutzes der öffentlichen Sicherheit ist die Förderung eines „Markts für Sicherheitslücken“ nicht zu rechtfertigen, der sowohl von Kriminellen als auch von fremden Geheimdiensten sowie autokratischen Regimes zur Verfolgung von Dissidenten oder Industriespionage genutzt wird. Insbesondere kann nicht gewährleistet werden, dass die entsprechenden „backdoors“ ausschließlich dem anfragenden Staat mitgeteilt werden, wodurch das Missbrauchspotential noch weiter erhöht und zudem die Investitionen sowohl vom Staat als auch von Unternehmen in die Bemühungen um Cybersicherheit konterkariert werden.

Keine gesetzliche Grundlage vor Prüfung der technischen Umsetzbarkeit

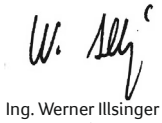
Abschließend sehen es die Unterzeichner kritisch, dass ein Gesetz beschlossen werden soll, dessen rechtmäßige technische Umsetzung in der Praxis erst im Anschluss während der Legisvakanz bis 2019 geprüft wird. Um ein unausgegorenes Lösungsmodell zu verhindern, welches Sicherheitsstandards und Grundrechte gleichermaßen gefährdet, fordern die Unterzeichner daher von einem Beschluss des § 135a StPO in dieser Form abzusehen und eine entsprechende Bestimmung zur Überwachung verschlüsselter Kommunikationsdienste nur dann in das Gesetz aufzunehmen, wenn die konkrete technische Umsetzung von unabhängigen technischen Experten geprüft und für unbedenklich deklariert wurde.

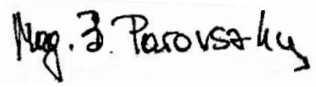
Hochachtungsvoll

AUSTRIAN Startups
AustrianStartups


Markus Raunig
Managing Director

Digital Society.at
Digital Society


Ing. Werner Illsinger
Präsident


Mag. Brigitte Parovszky
Generalsekretärin

OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY
Österreichische Computer Gesellschaft


Dipl.-Ing. Wilfried Seyruck
Präsident


Dr. Ronald Bieber
Generalsekretär

WKO
Unternehmensberatung · Buchhaltung · IT
WKO Fachverband UBIT


KommR Mag. Alfred Harl, MBA, CMC
Fachverbandsobmann


Dipl-Ing. Martin Zandonella
Berufsgruppensprecher IT


Mag. Philipp Graf
Geschäftsführer

Koordiniert durch:
ispa Internet Service Providers Austria
ISPA – Internet Service Providers Austria


Harald Kapper
Präsident


Dr. Maximilian Schubert
Generalsekretär