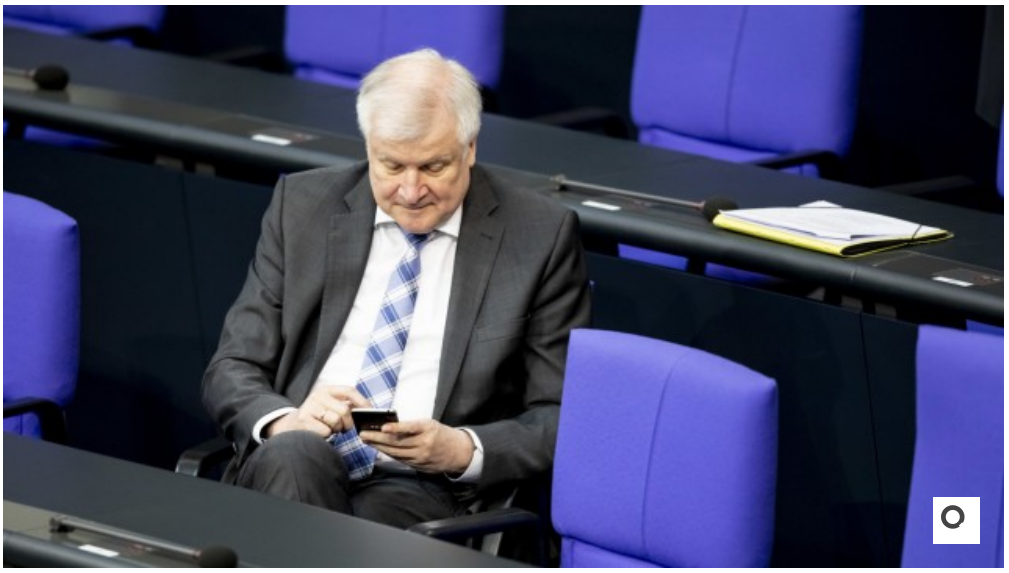
**11. Juni 2019, 15:11 Uhr** **Seehofers Hintertüren**

# Der Cyberunsicherheitsminister



Sicherheistlücken a
Seehofers eigenes
Der Innenminister
Hintertüren für
Messengerdienste
Experten halten da
gefährliches Signal
dpa)

In einem offenen Brief warnen Bürgerrechtler und IT-Experten vor den Forderungen des Bundesinnenministers, Hintertüren in Messengern wie Whatsapp und Threema einzubauen.

Feedback

Um den Ermittlungsbehörden Zugriff auf die Kommunikation von Verdächtigen zu gewähren, riskiere Seehofer die Sicherheit aller Nutzer, schreiben die Experten.

Unterzeichnet haben den Brief über 100 Organisationen und Einzelpersonen, darunter der CCC und die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger.

*Von Max Muth*

Es passiert nicht oft, dass sich bekannte Cybersecurity-Experten am anderen Ende der Welt über Horst Seehofer unterhalten. Namentlich erwähnt haben der Australier Patrick Gray und Ex-Facebook-Security-Chef Alex Stamos den deutschen Innenminister in ihrem wöchentlichen Branchenpodcast "Rizky.Biz" nicht. Doch die Nachricht, dass Deutschland im Jahr 2019 beschlossen habe, sich für Hintertüren in Messengern wie Whatsapp und Threema einzusetzen, fanden die beiden dann doch erwähnenswert. Stamos' Fazit ist wenig schmeichelhaft für den deutschen Innenminister: Ähnliche Überlegungen kenne er von US-Sicherheitspolitikern - von vor fünf Jahren. Deutschland hinke der Debatte also wohl ein bisschen hinterher.

Am Dienstag legten deutsche Experten nach. In einem offenen Brief, der der *SZ* vorliegt, wenden sich Bürgerrechtsorganisationen, IT-Experten, Politiker und Verbände an den Bundesinnenminister. Ihr Fazit: Der geplante Eingriff in die Verschlüsselung von Messenger-Diensten hätte "fatale Konsequenzen" für die IT-Sicherheit in Deutschland. Die Unterzeichner "warnen ausdrücklich vor einem solchen Schritt und fordern eine sofortige Abkehr von diesem oder ähnlichen politischen Vorhaben auf deutscher wie europäischer Ebene." Ein solcher Schritt würde die Sicherheit von Millionen Nutzern senken und Einfallstore für Internetkriminelle und ausländische Nachrichtendienste schaffen. Zu den Unterzeichnern gehören 100 Organisationen und Einzelpersonen, darunter der Chaos Computer Club, der ehemalige Bundesbeauftragte für den Datenschutz, Peter Schaar, der PGP-Erfinder Phil Zimmerman und die ehemalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger.

## Kommunikation ohne Verschlüsselung ist unsicher

"Crypto War" ("Verschlüsselungskrieg") und "Going Dark" ("Verdunkelung"), das sind die Schlagwörter unter denen Seehofers aktuelle Bemühungen global seit vielen Jahren verhandelt werden. Im Kern geht es dabei darum, wie Polizei und Geheimdienste sich auch heute die Ermittlungsmöglichkeiten der frühen Internetjahre erhalten können. In der analogen Welt können Wohnungen durchsucht, Briefe abgefangen, Telefonate abgehört werden. Und jahrelang funktionierte das mindestens genauso im Internet, jedenfalls so lange E-Mail-Nachrichten im Klartext über ungeschützte Verbindungen in offenen W-Lan-Netzwerken verschickt wurden. Oder Menschen über Social-Media-Accounts kommunizierten, die mit dem Passwort "123456" oder über eine banale Sicherheitsfrage gesichert waren.

**Verschlüsselung**

### Seehofer will Whatsapp, Telegram & Co. zum Entschlüsseln zwingen

Wenn sie nicht mitmachen, sollen sie abgeschaltet werden. Der Plan zielt auf Kriminelle, könnte aber die Verschlüsselung aller Nutzer in Frage stellen.

**Von Constanze von Bullion und Jannis Brühl**

Unsichere oder für mehrere Accounts genutzte Passwörter sind zwar immer noch nicht ausgemerzt, wie unter anderem die Mega-Leaks von Kundenlogins im Lauf der vergangenen Monate oder der Skandal um gehackte Politiker-Daten Anfang des Jahres zeigen. Doch spätestens seit den Enthüllungen von Edward Snowden wissen Menschen weltweit um die Unsicherheit ihrer Kommunikation im Netz - und es gibt Technologien, die ihnen dabei helfen, sich zu schützen.

Die Antwort auf die allermeisten dieser Probleme heißt Ende-zu-Ende-Verschlüsselung (E2EE). Die Grundidee ist einfach: Wer eine Nachricht schreibt, verschlüsselt diese vor dem Absenden mit einem Algorithmus, den selbst starke Prozessoren nur durch jahrelanges Ausprobieren knacken könnten. Verschickt wird nur Zeichengulasch. Das kommt beim Empfänger an, der dieses Gulasch dann wieder in die Textfassung zurückverwandelt. Das ist gut für Unternehmen,

auf die Kommunikation haben wollen, weil sie jemanden eines Verbrechens verdächtigen, ist es weniger gut.

## Von der Cäsar-Chiffre zu PGP und Threema

Verschlüsselung existiert seit Jahrtausenden. Schon der römische Kaiser Julius Cäsar hat sich mit der Cäsar-Chiffre in der Kryptographie-Geschichte verewigt. Er verschob Buchstaben des Alphabets systematisch um drei Positionen: A wurde also zu D, B zu E und so fort. Solche Systeme funktionieren, solange zwar Empfänger den Schlüssel (Bei Cäsar: 3 Stellen zurück) kennen, nicht aber gegnerische Spione, die die Nachrichten abfangen. Im Lauf der Jahrhunderte wurden solche Substitutions-Chiffren immer ausgefeilter, auch die berühmte Enigma-Maschine der Nationalsozialisten im 2. Weltkrieg nutzte die Technik noch. Der Nachteil: Nur wer eine Enigma hatte, konnte die Nachrichten entschlüsseln.

Heute ist Verschlüsselung deutlich einfacher: PGP zum Beispiel. Das steht für "Pretty Good Privacy" ("Ziemlich guter Privatsphäreschutz") und erlaubt es, Nachrichten zu verschlüsseln, ohne dass Sender und Empfänger alle Schlüssel direkt austauschen müssen. PGP kann mittlerweile per Extensions in Programme wie Outlook integriert werden und ist auch für Laien recht einfach nutzbar.

Noch leichter machen es den Nutzerinnen aber Messenger wie Signal, Threema oder Whatsapp. Beim Austausch der Telefonnummer regelt die App alles weitere weitgehend automatisch, die Kommunikation ist sicher. Zu sicher - finden Sicherheitsbehörden weltweit und der deutsche Innenminister. Um heute an Mails oder Chats von Verdächtigen zu kommen, müssen Ermittler Trojaner auf den Endgeräten installieren. Das ist aufwendig und schwierig, deutlich schwieriger jedenfalls, als Whatsapp einen Gerichtsbeschluss zu schicken, das im Gegenzug die Nachrichten rausrückt.

Doch der Trend geht spätestens seit den Snowden-Veröffentlichungen klar zur Verschlüsselung. Und auch Cyber-Experten von Regierungen geben mittlerweile zu, dass sich diese Entwicklung wohl nicht umkehren lassen wird. Gray und Stamos zitieren in eingangs erwähntem Podcast auch den ehemaligen Chef-Anwalt des FBI, Jim Baker, der soll zum Thema "Crypto-War" gesagt haben: "Der Crypto War? Den haben wir doch längst verloren!"

Diese Botschaft der Amerikaner ist beim deutschen Innenminister offensichtlich noch nicht angekommen. Vor zwei Wochen wurden die Pläne Seehofers bekannt, die Messenger-Dienste zum Einbau von Backdoors verpflichten zu wollen. Vergangene Woche dann beschlossen die Innenminister von Bund und Ländern, dass auch das deutsche 5G-Netz bitte nicht zu gut verschlüsselt werden soll.

**Privatsphäre**

## Zehn Regeln für Ihre digitale Sicherheit

Die geleakten Datensätze zeigen: Selbst, wer sich selbst für vollkommen uninteressant hält, besitzt Daten über Dritte, die er schützen muss. Die wichtigsten Grundregeln im Überblick.

**Von Simon Hurtz**

zur Startseite

Diskussion zu diesem Artikel auf: Rivva
Themen in diesem Artikel: Bundesinnenministerium Cyber-Angriff Horst Seehofer IT-Sicherheit



Mehr zum Thema

Hacker früher und heute
**Alles für alle - und Assange gegen alle**

Cyber-Sicherheit
**Hacker-Waffe der NSA legt Baltimore lahm**

Verschlüsselung

**Entschlüsseln zwingen**

IT-Sicherheit
**Wie der Netzbetreiber Innogy den Cyber-Ernstfall probt**

IT in Israel
**Wo die Militär-Geheimdienst-Start-up-Szene boomt**

Stuttgart - Süd, Stuttgart - Nord, Stuttgart - West, Stuttgart - Mitte

**Finanzierungsberater Baufinanzierung B2B Frankfurt (m/w/d)**
Interhyp Gruppe
60318 Frankfurt am Main, Frankfurt am Main

Alle Angebote

## Leser empfehlen im Ressort Digital

1 Landwirtschaftsministerin **Medienanstalt will Klöckners Nestlé-Video prüfen**

2 Klöckner und das Nestlé-Video **Die Politik sollte mehr Distanz schaffen**

3 Tierschutz **Warum die Niederlande verbieten, Möpse zu züchten**

## Meistgelesene Artikel

1 Brasilien **Neue Zweifel an Urteil gegen Lula**

2 Biologie **Tropische Hyalomma-Zecke hat in Deutschland überwintert**

3 Unwetter im Großraum München **"Eisbrocken schlugen wie Gewehrsalven auf uns ein"**

zur Startseite