Fakten für politische Entscheidungsträger:

6 Gründe warum „Rechtmäßiger Zugriff“ auf Verschlüsselung unsere Sicherheit gefährdet

Sichere Verschlüsselung brauchen alle

Wer vertraulich miteinander redet, möchte nicht dabei abgehört oder gestört werden. Das gilt für die analoge wie die digitale Welt, für private Kommunikation und für geschäftliche. Die Sicherheit vor Eingriffen kann lebenswichtig sein, wenn es um die Steuerung von Maschinen und Geräten (Energie, Verkehr, Gesundheit ...) geht. Auch politische Aktivisten in totalitären Systemen sind oft auf sichere, vertrauliche Kommunikation angewiesen. Also: auch wer „nichts zu verbergen hat“ braucht Verschlüsselung, die Sicherheit schafft.

Ein hohes Maß an Sicherheit für die Kommunikationspartner im digitalen Raum bietet die End-to-End-(E2E)-Verschlüsselung dann, wenn nur der Empfänger den Schlüssel zur Nachricht besitzt.

Müssen Sicherheitsdienste mithören können?

Genutzt wird die E2E etwa bei Messengern, online Shopping, online Banking, Stromversorgung, Steuerungsanlagen. Aber sicher auch von Kriminellen und Terroristen. Seit Jahren – und nach jedem aktuellen Vorfall wieder aufs Neue – fordern Sicherheitsbehörden von Regierungen die Möglichkeit, verschlüsselte Kommunikation einfacher zu überwachen, um Verbrechen besser verhindern und aufklären zu können. Damit soll unser aller Sicherheit erhöht werden.

Es ist zweifelhaft, ob Kommunikationsüberwachung tatsächlich signifikant vor Verbrechen schützen kann. Fakt ist jedoch, dass jedweder Eingriff in sichere Verschlüsselung – legal oder kriminell – die Sicherheit von uns allen beeinträchtigt. Als Folge werden damit auch die – teilweise lebenswichtigen – Systeme, die von vertraulicher Kommunikation abhängen, sowie das Internet insgesamt, gefährdet.

Hier 6 wichtige Punkte:

1

Missbrauch ist möglich
Wer eine Hintertür für rechtmäßigen Zugriff in ein System einbaut, der gibt auch Hackern, Kriminellen und fremden Regierungen eine Chance, diese zu nutzen. Undichte Stellen bei Behörden oder für diese tätigen Sicherheitsfirmen lassen sich erfahrungsgemäß nicht vermeiden. Sensible Daten können so abgefischt und missbraucht werden.

2

Nationale und private Sicherheit wird gefährdet
Durch Hintertüren sind z. B. persönliche Daten, Bankdaten, Zugangsdaten und Staatsgeheimnisse weniger geschützt. U. a. werden Spionage, Identitätsdiebstahl, Erpressung und Marktmanipulation dadurch erleichtert.

3

Terroristen werden sich tarnen
Sichere Verschlüsselung ist kein Hexenwerk. Kriminellen und Terroristen wird es technisch ein Leichtes sein, Systeme und Anwendungen mit Hintertüren zu meiden. Gefährdet werden die, die dem Staat vertrauen und Anwendungen nutzen, die rechtmäßige Zugriffe auf Verschlüsselung erlauben.

4

Lebensbedrohliche Schwachstellen
Verschlüsselte End-to-End-Kommunikation schützt die Identität von Journalisten, Aktivisten, Zeugen, Geheimagenten, Polizei und anderen. Hintertüren gefährden die Leben dieser Menschen, denn sie erleichtern auch unrechtmäßigen Zugang.

5

Überwachung schädigt die Infrastruktur
Kryptographie wird auch genutzt um Identität und Authentizität zu sichern. Zum Beispiel bei der Zertifizierung von Websites oder im Namenssystem (DNS) des Internet, das mit Kryptographie dafür sorgt, dass `my.bank.de` die richtige Website adressiert und nicht von Hackern auf `phishers.com` umgeleitet werden kann. Wenn die Verschlüsselung durch Hintertüren für gesetzliche Überwachung geschwächt ist, wird das Internet unsicherer.

6

Und wenn 193 Staaten Hintertüren wollen?
Würde rechtmäßiger Zugriff auf Kryptographie die Sicherheit in einem Staat erhöhen, wäre es vermutlich konsequent, dass alle Staaten – respektive deren Sicherheitsdienste – ebenfalls Hintertüren für einen solchen Zugriff fordern. Die Vorstellung, dass jeder Staat beliebig auf geschützte Informationen – und seien es nur die, die sein Land durchlaufen – zugreifen kann, ist absurd und beängstigend. Die negativen wirtschaftlichen und politischen Auswirkungen sind kaum vorstellbar.

Jedes Land hat das Recht und die Pflicht seine Bürger zu schützen. Das gilt auch im Internet. Privatpersonen, die Wirtschaft und der Staat sind auf eine funktionierende und vertrauenswürdige Infrastruktur angewiesen.

Nur mit einer starken und nicht durch Hintertüren korrumpierte Verschlüsselung erreichen wir die dafür erforderliche Sicherheit.

Internet Society German Chapter ISOC.DE

Frei nach: Factsheet For Policymakers: 6 Ways "Lawful Access" Puts Everyone's Security At Risk
https://www.internetsociety.org/wp-content/uploads/2019/05/FactSheet-EncryptionVsLawful-Access-EN.pdf