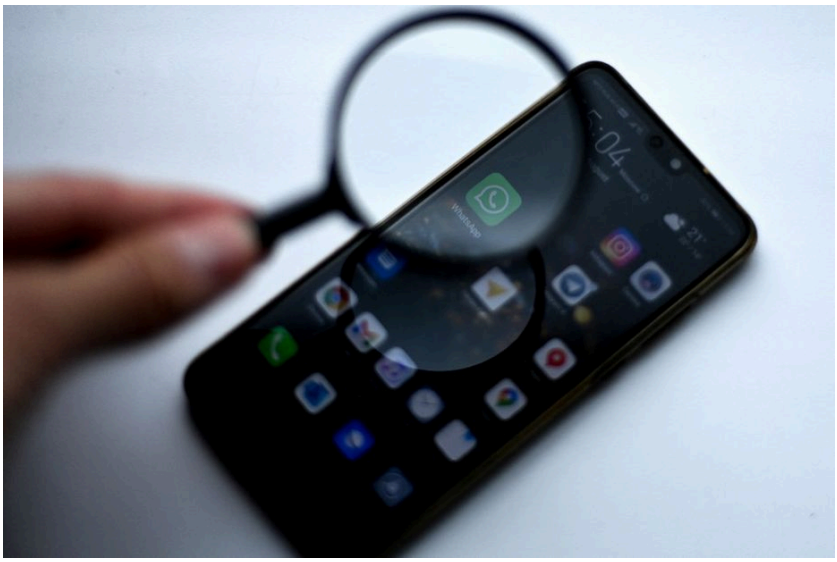
FRAGE UND ANTWORT

Chatkontrolle: Wie die EU die Messenger-Verschlüsselung aushebeln will

Schon bald will die EU-Kommission ihre Pläne offiziell enthüllen. Wie das technisch gehen könnte, welche Probleme das aufwirft und warum Kritiker schon jetzt auf die Barrikaden gehen

Andreas Proschofsky
23. März 2022, 08:00



Einblick in die Chats aller Nutzer haben: Das ist zwar nicht das offizielle Ziel der Chatkontrolle, Kritiker befürchten aber, dass es darauf hinauslaufen könnte.
Foto: KIRILL KUDRYAVTSEV / AFP

Langsam wird es ernst: Bereits Ende März will die EU-Kommission laut aktuellen Informationen [http://www.derstandard.at/story/2000134204045/eu-kommission-will-bald-ernst-mit-aushebelung-der-chatverschluesselung-machen] den Entwurf für ein schon im Vorfeld äußerst umstrittenes Gesetz vorstellen: die Chatkontrolle. Deren postuliertes Ziel: die Bekämpfung des sexuellen Missbrauchs von Kindern. Eine Zielsetzung, der wohl kaum jemand widersprechen wird. Dass dies nun für solchen Wirbel sorgt, liegt daran, wie man das erreichen will.

Wie aus einem im Vorjahr geleakten früheren Entwurf hervorgeht, sollen Messenger wie Whatsapp oder Signal sowie E-Mail-Anbieter dazu verpflichtet werden, nach sogenanntem Child Sexual Abuse Material (CSAM) zu suchen und die Nutzer dann an die Behörden zu melden.

Das würde einer Aushöhlung von effektiver Verschlüsselung gleichkommen, warnen angesichts solcher Perspektiven Kritikerinnen – samt brandgefährlicher Konsequenzen. Was damit gemeint ist und wie das Ganze überhaupt technischen ablaufen könnte, soll im Folgenden näher unter die Lupe genommen werden.

Frage: Wenn von "Aushebelung der Verschlüsselung" die Rede ist – was ist damit gemeint? Ich dachte, Ende-zu-Ende-Verschlüsselung verhindert, dass jemand anderer mitlesen kann?

Antwort: Das tut sie auch – aber eben nur auf dem Transportweg. Die Idee der EU setzt an ganz anderer Stelle an, und zwar direkt am Smartphone der User. Dort ist ein Zugriff auf die Inhalte natürlich möglich, und das lässt sich auch technisch nicht verhindern. Immerhin muss die betreffende App selbst die Chats ja auch den Nutzern am Bildschirm anzeigen, sie zwischenspeichern und verarbeiten. Genau diese Position soll nun genutzt werden, die Apps sollen also dazu verpflichtet werden, selbst nach problematischen Inhalten zu suchen. "Client Side Scanning" nennt sich dieses Konzept.

Frage: Wie könnte das dann in der Praxis aussehen?

Antwort: Mit vollständiger Sicherheit lässt sich das noch nicht sagen. Immerhin sind die Pläne der EU derzeit noch in Entwicklung. Insofern ist auch nicht ganz klar, wie man sich die Umsetzung in der Praxis vorstellt. Die realistischste Variante ist aber, dass man

schlicht eine recht grobe Aufgabe – das regelmäßige Scannen nach solchen Inhalten – stellt und den einzelnen Herstellern dann die Implementation überlässt.

Frage: Gibt es zumindest schon eine Idee davon, wie das technisch laufen könnte?

Antwort: Allerdings, und das ist Apple zu "verdanken". Hat der iPhone-Hersteller doch Mitte des vergangenen Jahres ein ebensolches System vorgestellt – und zwar ebenfalls unter den Vorzeichen des Kampfs gegen sexuellen Missbrauch von Kindern. Sehr vereinfacht sieht dieses so aus: Es wird eine Datenbank mit digitalen Fingerabdrücken einschlägiger Materialien erstellt, die laufend auf dem Smartphone aktuell gehalten wird. Diese wird dann zum Abgleich mit den in den betreffenden Apps verschickten Bildern genutzt.

Frage: Was passiert jetzt, wenn es einen "Treffer" gibt?

Antwort: Im System von Apple wäre es so gewesen, dass nach einer gewissen Zahl an Übereinstimmungen zunächst eine Meldung an Apple erfolgt – mit den betreffenden Bildern. Diese sollten dann noch einmal geprüft werden und erst nachdem sich herausstellt, dass es sich tatsächlich um solche Materialien handelt, wäre dann eine Meldung an die Behörden erfolgt.

Frage: Wieso reden wir hier im Konjunktiv? Also was ist mit dem Apple-System passiert?

Antwort: Es wurde nach massiven Protesten von Nutzern und Privatsphärenexperten vorerst wieder eingestellt beziehungsweise liegt es derzeit auf "Eis". Und "massiv" ist hier keine Untertreibung, selbst Apple-Mitarbeiter liefen öffentlich Sturm gegen die Pläne [http://www.derstandard.at/story/2000128897537/iphone-foto-scans-apples-umstrittene-massnahmen-gegen-kinderpornografie-fuehren-zu] . NSA-Whistleblower Edward Snowden sprach gar davon, dass Apple damit der "Privatsphäre den Krieg erklärt" habe [http://www.derstandard.at/story/2000129218793/edward-snowden-apple-hat-der-privatsphaere-den-krieg-erklaert] .

Frage: Bevor wir zur Kritik kommen, würden mich aber noch ein paar Details interessieren. Also etwa: Wer liefert in so einem Modell überhaupt diese Datenbank mit digitalen Fingerabdrücken? Wie kann ich diesen vertrauen?

Antwort: Im Fall von Apple wären es diverse auf den Kampf gegen die sexuelle Ausbeutung von Kindern spezialisierte NGOs gewesen. Das wird wohl bei einer EU-weiten Lösung kaum anders sein. Immerhin würde es wenig Sinn ergeben, wenn die Hersteller eigene Datenbanken erstellen – aus vielen Gründen. Einfach weil damit viel Arbeit unnötig dupliziert würde, aber auch weil das Sichten solcher Materialien eine emotional enorm belastende Tätigkeit ist, die nicht noch mehr Menschen vornehmen sollten.

Frage: Wie zuverlässig ist so ein System?

Antwort: Generell war das Apple-System technisch recht durchdacht. So liefert es etwa digitale Fingerabdrücke, die auch leicht veränderte Bilder erkannten und nicht nur das Original. Aber klar, es wird immer Tricks geben, falsche Treffer zu erzeugen. Auch beim [http://www.derstandard.at/story/2000129038191/iphone-fotoscan-forscher-zeigen-wie-sich-apples-umstrittene-technologie-austricksen] Apple-Ansatz hatten Sicherheitsforscher schnell solche Defizite gefunden. Das sind aber jetzt wirklich Detailfragen, die beim aktuellen Stand nur schwer zu beantworten sind – und die dann von den Lösungen der einzelnen Hersteller abhängen werden, wenn das Gesetz tatsächlich beschlossen wird.

Frage: Das klingt doch alles wohlüberlegt. Welches Problem haben die Kritiker damit?

Antwort: Es gibt eine Fülle von unterschiedlichen Kritikpunkten. Im Kern steht aber ein Vorwurf: Solch ein System wäre das Einfallstor für eine Massenüberwachung sämtlicher Kommunikation. Oder wie es vor wenigen Tagen dutzende Bürgerrechtsorganisationen, darunter die angesehene Initiative European Digital Rights (EDRi), in einem offenen Brief an die EU-Kommission formulierten [http://www.derstandard.at/story/2000134250136/offener-brief-chatkontrolle-macht-eu-zum-weltmarktfuehrer-bei-der-massenueberwachung] : Es werde ein "gefährlicher Präzedenzfall für die massenhafte Ausspähung privater Kommunikation" geschaffen.

Frage: Wie das?

Antwort: Nun, ist so ein System einmal da, könnte es natürlich auch mit anderen Daten gefüttert werden. Theoretisch wäre es durchaus möglich, ganz andere digitale Fingerabdrücke in die Datenbank einzuspeisen. Also nach beliebigen Bildern suchen zu lassen, je nachdem, welche Gruppe man damit anvisiert. Insofern wäre das ein sehr, sehr mächtiges Tool, um Überwachung aller Art vornehmen zu können.

Frage: Ja gut, aber die Beschränkung auf dieses eine Thema sollte ja problemlos gesetzlich festgeschrieben werden können.

Antwort: Da ist zwar richtig, aber nur weil etwas festgeschrieben ist, heißt das nicht, dass es nicht wieder geändert werden kann. Wer etwa die politisch aufgeheizte Stimmung nach Terroranschlägen kennt, der weiß, dass hier recht flott solche Forderungen

kommen würden.

Frage: Aber auch da hätte ich jetzt nicht das große Problem damit ...

Antwort: Selbst wenn wir außer Acht lassen, dass das noch immer eine Massenüberwachung der Kommunikation eines großen Teils der Bevölkerung darstellen würde – und somit prinzipiell hochproblematisch ist –, verweisen Kritikerinnen noch auf einen anderen Punkt: Nämlich dass es auf der Welt noch andere Länder gibt. Mit ganz anderen Gesetzgebungen. In dem Moment, in dem man so ein System aufbaue, würden rasch Begehrlichkeiten von autoritären Regimen kommen, die damit gegen die Opposition vorgehen wollen. Und auch in vermeintlich stabilen Demokratien kann es schnell zu einem Regierungswechsel kommen.

Frage: Das wirft eine allgemeinere Frage auf, nämlich wie sollen die App-Hersteller dazu gezwungen werden, überhaupt an so einem System teilzunehmen? Könnten die das nicht einfach ignorieren?

Antwort: Gute Frage, auch hier gilt es zunächst auf die finale Fassung des Gesetzes zur Chatkontrolle zu warten. Aber dieses wird sicher Sanktionen für nicht willige Firmen vorsehen. Im schlimmsten Fall könnte dies darauf hinauslaufen, dass Messengern, die sich nicht daran halten, der Betrieb in der EU komplett untersagt wird.

Frage: Ich kann mir trotzdem nicht vorstellen, dass solch eine Blockade lückenlos funktioniert. Wenn ich mal ein bisschen herumnerden darf: Einige dieser Messenger sind Open Source, also im Quellcode verfügbar. Was hindert nun jemanden daran, einfach eine überwachungsfreie Version dieser Programme anzubieten, die ich mir dann manuell installieren kann?

Antwort: Ein gar formidabler Punkt. Genau das zeigt nämlich eine Realität auf, die sich bei solchen Konzepten immer wieder zeigt. Sie sind nie lückenlos und treffen primär jene, die sich nicht genügend mit dem Thema beschäftigen. Jetzt ist aber natürlich das Problem: Wer Fotos eines sexuellen Missbrauchs von Kindern teilt, der hat ein gesteigertes Interesse daran, sich nach ebensolchen Alternativen umzusehen – und so die "Chatkontrolle" ins Leere laufen zu lassen.

Frage: Wäre es da nicht sinnvoller, das gleich auf der Ebene der Betriebssysteme zu etablieren, also etwa direkt bei Android und iOS solche Filter einzubauen, die dann die Inhalte sämtlicher Chat-Apps durchsuchen? Das würde doch auch verhindern, dass jeder Messenger-Anbieter für sich ein eigenes System bauen muss?

Antwort: Für die Kritiker dieser Pläne ist das der Albtraum schlechthin. Spinnt man die Befürchtungen weiter, wäre das endgültig eine – zumindest potenzielle – Massenüberwachungsschnittstelle für (fast) alle Smartphones. Aber dem Gedankenexperiment zuliebe ignorieren wir das jetzt einmal. Insofern: Ja, technisch wäre das wohl die sauberere Lösung. Zumindest Apple würde sich wohl auch schwertun, gegen die Aufnahme solcher Funktionen zu argumentieren, immerhin wollte man so etwas Ähnliches ja schon von sich aus ausliefern. Aber auch das macht es für jene, die unentdeckt bleiben wollen, nur schwieriger, aber nicht unmöglich. Gibt es doch auch freie Android-Varianten, die jeder selbst installieren kann – und die so ein System sicher nicht übernehmen werden.

Frage: Mir fällt noch ein ganz anderer Punkt ein: Wäre so ein System nicht auch ein Sicherheitsproblem?

Antwort: Das sehen Sicherheitsexperten tatsächlich so. Jede solche Schnittstelle ist ein zusätzlicher Angriffspunkt, die potenziell auch von Dritten für Spionage genutzt werden könnte. Wobei man ehrlicherweise auch sagen muss, dass es meist für Angreifer komfortablere Wege gibt, die Nutzer auszuspionieren, wenn sie es einmal aufs Smartphone geschafft haben.

Frage: Langsam frag ich mich: Wozu das Ganze eigentlich? Also was ist die Motivation?

Antwort: Zum Teil steckt dahinter fraglos eine gute Intention, nämlich eben der Kampf gegen die Verbreitung von Bildern, die sexualisierte Gewalt gegen Kinder zeigen. Tatsächlich ist das Aufspüren entsprechender Inhalte durch die zunehmende Nutzung verschlüsselter Chat-Dienste zuletzt schwerer geworden. Denn was man bei all dem nicht vergessen darf: Auf den eigenen Servern scannen Firmen wie Google, Facebook und Apple schon seit Jahren nach solchen Inhalten.

Frage: Warum dann die Aufregung?

Antwort: Weil die Nutzer das Smartphone viel mehr als Ihres, als ihren höchst privaten Bereich ansehen. Wohingegen die Privacy-Erwartungen an irgendwelche Server großer Unternehmen erheblich geringer sind.

Frage: Zurück zur Intention, irgendwie kann ich mir nicht vorstellen, dass nicht auch ganz andere Interessen dahinterstehen ...

Antwort: Mit Spekulationen gilt es immer vorsichtig zu sein, um hier nicht ins Verschwörungstheoretische abzugleiten. Gleichzeitig ist es kein Geheimnis, dass effektive Verschlüsselung Geheimdiensten und Strafverfolgungsbehörden seit Jahren ein Dorn im Auge

ist. Die Sicherheitsverschärfungen, die viele Unternehmen infolge der Snowden-Enthüllungen vorgenommen haben, haben die Arbeit dieser Behörden erheblich erschwert – vor allem was die Massenüberwachung anbelangt. Sie werden also über die aktuellen Entwicklungen zumindest nicht ganz unglücklich sein. Das nicht zuletzt mit der Hoffnung darauf, diese Hintertür irgendwann auch für die eigenen Zwecke nutzen zu können.

Frage: Kritik ist ja schön und gut, aber was ist die Alternative? Immerhin will ja niemand, dass solche Inhalte verbreitet werden ...

Antwort: Bürgerrechtsorganisationen sagen dazu: gezielte Fahndung und Überwachungsmaßnahmen unter richterlicher Aufsicht. Also quasi "gute alte Polizeiarbeit" statt Massenüberwachung mit all ihren hochproblematischen Nebeneffekten.

Frage: Abschließende Worte?

Antwort: Wie auch immer der Entwurf der EU-Kommission schlussendlich aussehen wird, sie darf sich schon einmal auf gehörigen Widerstand einstellen. Wenn selbst Publikums-Darling Apple mit einem ähnlichen System gescheitert ist, werden die Pläne der EU sicher nicht besser aufgenommen. Einen ersten Vorgeschmack gab es schon vor einigen Monaten, als sich 20 EU-Abgeordnete quer durch die Fraktionen zu Wort meldeten und davor warnten, dass mit der Chatkontrolle "chinesische Verhältnisse" drohen – in Anspielung auf die umfassende Überwachung des Internets durch die dortigen Machthaber. (Andreas Proschofsky, 23.3.2022)

Zum Thema

EU-Kommission will bald ernst mit Aushebelung der Chatverschlüsselung machen [http://www.derstandard.at/story/2000134204045/eu-kommission-will-bald-ernst-mit-aushebelung-der-chatverschluesselung-machen]

Offener Brief: Chatkontrolle macht "EU zum Weltmarktführer bei der Massenüberwachung" [http://www.derstandard.at/story/2000134250136/offener-brief-chatkontrolle-macht-eu-zum-weltmarktfuehrer-bei-der-massenueberwachung]

Wie finden Sie den Artikel? 41 Reaktionen

4 ♡ | 32 informativ | 3 hilfreich | 1 berührend | 1 unterhaltsam

Zu diesem Inhalt können keine Reaktionen mehr gespeichert werden.