Auf (un)verschlüsselten Wegen

Hintertürdiskussion: Sicherheitsforscher kritisieren fehlende Transparenz beim Messenger Whatsapp

Von Nina May und Stefanie Gollasch

Sicherheitslücke oder Entscheidung im Dienste der Nutzerfreundlichkeit? Whatsapp und Facebook stehen in der Kritik. FOTO: DPA

Auf der Website von Whatsapp hört es sich so einfach an: „Unsere Ende-zu-Ende-Verschlüsselung sorgt dafür, dass Ihre Kommunikation nur von Ihnen und Ihrem Chatpartner gelesen werden kann. Und von niemandem in der Mitte, nicht einmal Whatsapp." An diesem Versprechen sind nun Zweifel aufgekommen. Eine Hintertür soll es theoretisch möglich machen, dass etwa Nachrichtendienste wie die NSA oder Datenjäger aus der Wirtschaft Chats hacken können.

Die Sicherheitslücke liegt im Verschlüsselungsprozess während der Handyregistrierung: Wenn jemand sein Telefon verliert oder die SIM-Karte wechselt, können Nachrichten zunächst nicht zugestellt werden. Dem Absender wird dies mit nur einem einzelnen Haken hinter der Nachricht angezeigt. Meldet sich der Adressat mit einem neuen Schlüssel an, wird die Nachricht erneut gesendet, worauf ein zweiter Haken hinweist. Für die Nutzer hat das erst mal den Vorteil, dass Nachrichten nicht verloren gehen. Doch genau hier sehen Datenschützer die Schwachstelle: Ein Hacker könnte nun das Handy unter dem Namen des ursprünglichen Besitzers registrieren und so auf die automatisch neu versendeten Nachrichten zugreifen.

Moxie Marlinspike, der die von Whatsapp genutzte quelloffene Verschlüsselungstechnik erfand, wies die Vorwürfe zurück: „Es gibt keine vorsätzliche Hintertür", schreibt der Hacker und Hausbesetzer im Blog seiner Organisation Open Whisper Systems. Es handele sich vielmehr um eine Design-Entscheidung zugunsten der Nutzerfreundlichkeit, die verhindere, dass Millionen von Nachrichten verloren gingen.

Die Diskussion, die am Wochenende hohe Wellen schlug, ist Wasser auf die Mühlen der Kritiker, die den Messengerdienst seit der Übernahme durch Facebook im Jahr 2014 für die Inkarnation eines Datendealers halten. Mit der Einführung der Ende-zu-Ende-Verschlüsselung im April 2016 hatte das Unternehmen um Vertrauen gebuhlt. Ausgelöst hat die aktuelle Debatte der Deutsche Tobias Boelter, derzeit Doktorand an der University of California in Berkeley, mit einem Blogeintrag. Der Kölner Matheabsolvent und ehemalige Mitarbeiter aus der Kryptografie-Forschungsabteilung von SAP erklärte dem Redaktions-Netzwerk Deutschland (RND), dass ihm noch kein konkreter Fall bekannt sei, dass die von ihm identifizierte Hintertür bereits genutzt wurde, um Chats abzuhören. Er sagt weiterhin: „Das eigentliche Problem ist, dass Whatsapp gesagt hat, dass sie unter keinen Umständen Nachrichten lesen können. Das wurde nun widerlegt. Bei anderen Diensten wie zum Beispiel dem Facebook Messenger ist von vornherein klar, dass Facebook Zugriff auf die Nachrichten hat."

Der Sicherheitsforscher Ahmad-Reza Sadeghi von der TU Darmstadt verweist darauf, dass Nutzer der Applikation sowieso vertrauen müssen. Für den aktuellen Fall sei das Thema lediglich für diejenigen relevant, die mit ihren Kommunikationspartnern bei einem persönlichen Treffen einen individuellen Schlüssel ausgetauscht haben. Sonst könne Whatsapp ohnehin theoretisch immer mitlesen.

Der Sicherheitsforscher Roland Schilling von der Technischen Universität Hamburg sagt gegenüber dem RND: „Für die Nutzer von Whatsapp spielt es keine Rolle, ob es sich um eine Bequemlichkeitsentscheidung oder eine absichtlich platzierte Hintertür handelt. Es geht hier um einen möglichen Angriff auf ihre Privatsphäre." Schilling kritisiert zudem, dass der Code des Verschlüsselungsprotokolls von Whatsapp nicht öffentlich ist. „Nutzer müssen sich daher blind auf das Versprechen verlassen, dass der Anbieter ihre Privatsphäre respektiert." Der Sicherheitsforscher verweist auf eine technische Alternative für dieselbe Funktion – Neuaussendung von Nachrichten bei Fehlzustellung –, die ihm zufolge nicht ohne Weiteres missbraucht werden könnte: „Die gibt es in der Form von Warnungen, die der Nutzer erst bestätigen muss. Dies lässt ihm die Chance, auf einem unabhängigen Kanal, zum Beispiel per Telefon, bei seinem Kommunikationspartner nachzufragen. Dann kann er selbst die Entscheidung treffen, ob er Nachrichten an einen Empfänger mit diesem neuen Schlüssel schicken möchte." Diese Variante werde etwa von dem Messenger Signal praktiziert, den Whatsapp als Vorbild nennt. Marlinspike wies diese Möglichkeit in seiner Stellungnahme jedoch als nutzerunfreundlich zurück.

Uneinigkeit herrscht darüber, in welchem Ausmaß die Sicherheitslücke für Hacker genutzt werden könnte. Boelter meint, der Whatsapp-Server könne nachträglich komplette Unterhaltungen abrufen und nicht nur einzelne Nachrichten. Udi Yavo, Mitgründer und Geschäftsführer des US-Datenschutzunternehmens enSilo, ruft hingegen gegenüber dem RND zur Mäßigung auf: „Wenn es sich hier um ein Hintertürchen handelt, dann ist es ein ziemlich schlechtes. Der Hacker hat schließlich nur Zugriff auf die ungelesenen Nachrichten, das ist eine sehr beliebige Auswahl. Und das Opfer muss offline sein, das mindert die Macht des Angriffs zusätzlich."

Stashcat: Sicherer Messenger für Unternehmen

Eine sichere Kommunikation verspricht der Messenger Stashcat. Der Dienst für Unternehmen und Behörden verweist beim Austausch von Nachrichten und Dokumenten auf eine Ende-zu-Ende-Verschlüsselung und Server in Deutschland. Die Madsack Mediengruppe ist am Stashcat-Entwickler heinekingmedia beteiligt.

IN KÜRZE

„Sherlock"-Macher appellieren an Fans

London. Mit Spannung haben Fans auf die finale Folge der jüngsten Staffel aus der Detektivserie „Sherlock" mit Benedict Cumberbatch gewartet. Kurz vor der Ausstrahlung im BBC-Fernsehen ist nun offenbar eine russische Synchronfassung der Folge im Internet aufgetaucht. Die Macher reagierten mit einem Aufruf, die Version nicht zu verbreiten. Die vierte Sherlock-Staffel lief am 1. Januar an. Die dritte und letzte Folge stand am Sonntagabend im BBC-Fernsehprogramm. In Deutschland sollen die Folgen im Frühjahr bei der ARD zu sehen sein. Zuvor sind sie aber auch bei iTunes verfügbar.

Satirepreis für Gerhard Glück

Göttingen. Gerhard Glück (72) hat den Satirepreis „Göttinger Elch" erhalten. Der in Kassel lebende Zeichner, Maler und Fotograf nahm die Auszeichnung am Sonntag in Göttingen für sein satirisches Lebenswerk entgegen. In der Würdigung der Jury hieß es, Glück sei einer „der ganz Großen der komischen Kunst". Der „Göttinger Elch" wird seit 1997 jährlich für ein satirisches Lebenswerk verliehen, er ist mit 3333 Euro und einer silbernen Elchbrosche dotiert. Frühere Preisträger waren unter anderem Otto Waalkes und zuletzt Max Goldt.

TV-QUOTEN

Die meistgesehenen Sendungen am Sonnabend:

RTL: „Ich bin ein Star …"
7,26 Mio. Zusch. / 28,6 % Marktant.
ZDF: „Wilsberg"
6,52 Mio. / 19,7 %
ARD: „Tagesschau"
5,9 Mio. / 19,6 %
RTL: „DSDS"
5,41 Mio. / 16,5 %
ARD: „Biathlon-Weltcup"
5,06 Mio. / 29,9 %

MEDIA CONTROL

-1° -7° Überwiegend freundlich

Sonnenaufgang 08:23 Sonnenuntergang 16:39
Mondaufgang 21:47 Monduntergang 10:21

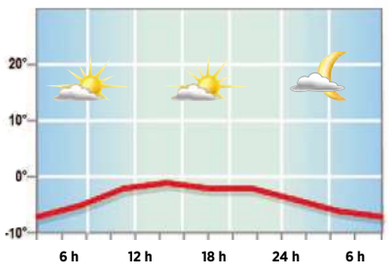
WETTERLAGE

Zwischen einem Tief über Italien und Hochs über Westeuropa sowie Südskandinavien kommt kalte Luft nach Mitteleuropa. Die Temperaturen steigen kaum noch über die 0-Grad-Marke. Winterlich bleibt es auch in Osteuropa und Skandinavien.

VORHERSAGE

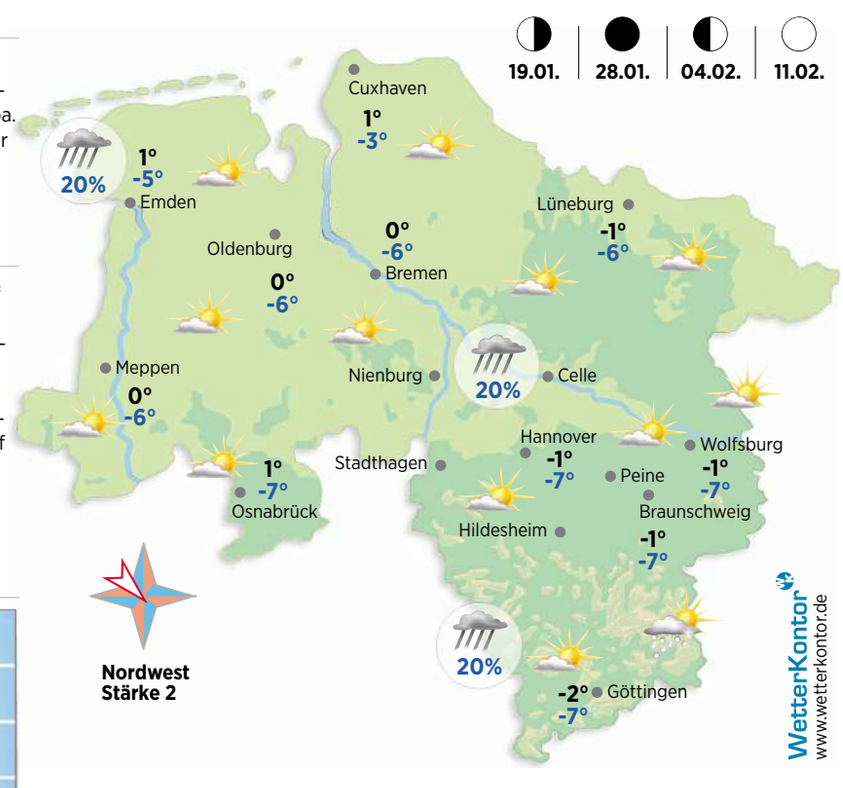
Häufig scheint die Sonne, im Tagesverlauf ziehen aber auch zeitweise Wolkenfelder vorüber. Es bleibt weitgehend trocken. Minus 2 bis plus 1 Grad werden erreicht. Der Wind weht schwach aus Nordwest. In der kommenden Nacht ist der Himmel nur gering bewölkt. Die Temperaturen sinken auf minus 3 bis minus 7 Grad. Morgen zeigt sich das Wetter nach anfänglichem Nebel meist freundlich und trocken.

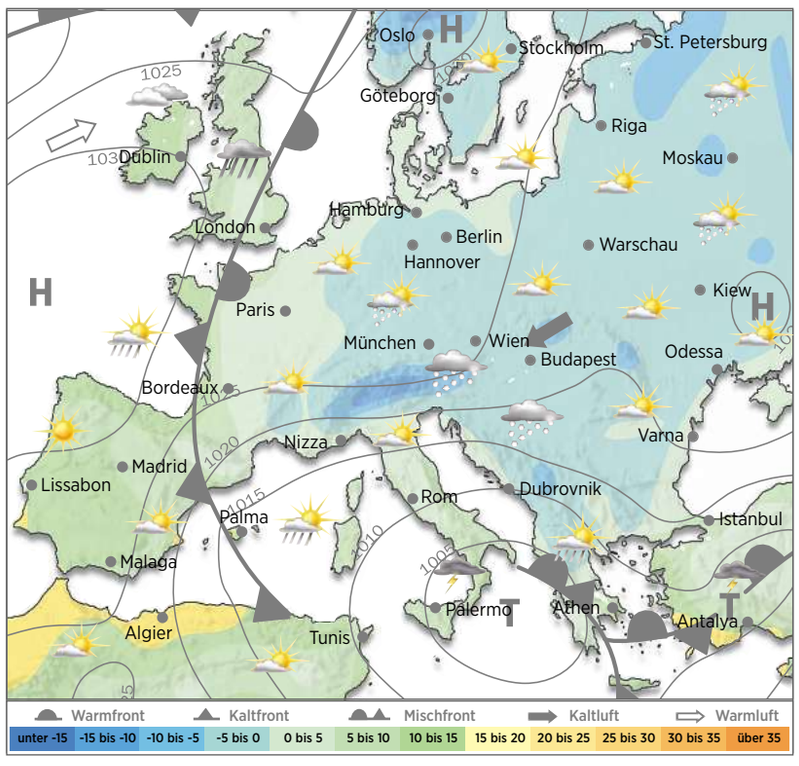
TAGESVERLAUF



BIOWETTER

Die Wetterlage beschert uns einen erholsamen Schlaf. Dadurch wacht man morgens ausgeschlafen auf und ist voller Energie. Die kalte Luft macht jedoch besonders Rheumakranken zu schaffen. Sie müssen sich auf eine Verschlimmerung ihrer Schmerzen einstellen. Trotz der Schmerzen tut den Gelenken ein Spaziergang gut.





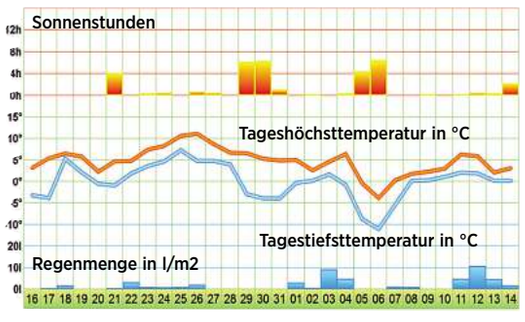
EUROPA

Algarve/Faro	17°	heiter
Amsterdam	2°	sonnig
Barcelona	13°	wolkig
Bozen	5°	wolkig
Florenz	5°	bedeckt
Istanbul	7°	Regen
Kopenhagen	1°	wolkig
Larnaka	17°	wolkig
Locarno	4°	sonnig
Malaga	18°	heiter
Mailand	3°	sonnig
Oslo	-4°	sonnig
Rhodos	16°	Regen
Teneriffa	22°	wolkig
Venedig	6°	wolkig
Wien	-1°	wolkig
Zürich	-3°	wolkig

DIE WELT

Bangkok	34°	Schauer
Buenos Aires	30°	wolkig
Dubai	26°	sonnig
Hongkong	17°	wolkig
Kairo	19°	wolkig
Kapstadt	26°	sonnig
Los Angeles	17°	wolkig
Miami	23°	wolkig
New York	5°	wolkig
Peking	1°	heiter
Rio de Janeiro	32°	Gewitter
Sao Paulo	28°	Gewitter
Sydney	30°	sonnig
Tel Aviv	20°	wolkig
Tokio	7°	heiter

DAS WETTER DER VERGANGENEN TAGE



DEUTSCHLAND HEUTE

Berlin	-1°	Schn.sch.
Braunlage	-4°	Schn.sch.
Brocken	-9°	Schn.sch.
Dresden	-3°	Schnee
Frankfurt	0°	wolkig
Hamburg	1°	wolkig
Kassel	-1°	wolkig
Leipzig	-2°	Schn.sch.
München	-3°	Schn.sch.
Nürnberg	-3°	Schn.sch.
Sylt	2°	heiter

REISEWETTER

Österreich, Schweiz: Im Norden bewölkt und gebietsweise Schneefall, sonst freundlich, später im Süden Österreichs ebenfalls dichte Wolken mit Schnee. Bis 5 Grad.

Großbritannien, Irland: Bewölkt, zum Teil neblig-trüb, gebietsweise Regen oder Nieselregen. Werte zwischen 4 und 12 Grad.

Italien: Im Norden freundlich und trocken, sonst wechselnd bis stark bewölkt, gebietsweise Regen oder Schnee. 4 bis 12 Grad.

Spanien, Portugal: Im Norden und Nordosten viele Wolken und örtlich Regengüsse. Sonst viel Sonnenschein und trocken. Temperaturen zwischen 7 und 18 Grad.

Frankreich: Im Westen und Südwesten sowie über der Mitte viele Wolken und örtlich Regen, im Bergland Schnee. Sonst wechselnd bewölkt und trocken. 0 bis 11 Grad.

Griechenland, Türkei: Wechselnd bis stark bewölkt, häufig Regengüsse, im Norden und Nordwesten Griechenlands Schneefälle. Örtlich Gewitter. 5 bis 17 Grad.

Mallorca: Mal mehr, mal weniger Wolken, im Laufe des Tages einige Regenschauer. Höchstwerte von 11 bis 14 Grad.

Kanaren: Teils heiter, teils wolkig, aber nur vereinzelt Regenschauer. Temperaturen am Nachmittag zwischen 19 und 23 Grad.

SCHNEEHÖHEN

Brocken	105 cm	Oberstdorf	120 cm
Harz	80 cm	Neuhaus a. R.	60 cm
Fichtelberg	100 cm	Oberhof	70 cm
Großer Arber	70 cm	Zinnwald	50 cm
Schneekoppe	140 cm	Zermatt	120 cm
Klingenthal	70 cm	Zugspitze	280 cm

Dienstag -1° -5° | Mittwoch 0° -3° | Donnerstag 1° -2° | Freitag 1° -2° | Sonnabend 1° -2°