Junge Welt / 16.05.2026 / Schwerpunkt / Seite 9

Den Köder geschluckt

Ranghohe CDU-Funktionäre fielen offenbar auf Phishingangriffe per Signal-App herein. Geheimdienste und Medien machen Russland verantwortlich

Von Marc Bebenroth

Noch immer sind Bundesregierung und EU-Kommission nach Kräften bemüht, ihre Geheimdienste und Polizeien rechtlich sowie technisch in die Lage zu versetzen, sämtliche Chats der Bevölkerung mitlesen zu können. Ein Hindernis sind Ende-zu-Ende-verschlüsselte Messenger-Apps. »Ich nutze Signal jeden Tag«, hatte der US-Whistleblower Edward Snowden vor diesem Hintergrund im November 2015 öffentlich erklärt. Mehr als zehn Jahre später ist der von einer nicht gewinnorientierten Stiftung getragene Messengerdienst noch immer bei Whistleblowern, Dissidenten, Journalisten und auch politischen Amtsträgern sowie Militärs beliebt.

So beliebt, dass spätestens seit Ende 2024 Trickbetrüger offenbar systematisch solche Menschen um ihre Zugangsdaten zum Signal-Benutzerkonto erleichtern wollen. Um Nutzerinnen und Nutzer noch deutlicher als bisher vor den digitalen Enkeltricks zu warnen und für die Gefahren zu sensibilisieren, hat der Betreiber von Signal am Montag neue Funktionen für die App angekündigt. Wird man von nicht persönlich verifizierten Signal-Nutzern kontaktiert, sollen mehrere Warnungen eingeblendet werden. »Signal wird dir niemals eine Nachricht schicken und nach deinem Registriercode, PIN oder Wiederherstellungsschlüssel fragen«, lautet ein Hinweis. Darüber hinaus wird vor dem sogenannten Phishing (»password fishing«) oder anderen Betrugsmaschen gewarnt.

Russische Spuren

Um Kontakt mit Signal-Nutzern herzustellen, benötigt man die Mobilfunknummer oder den von der Zielperson selbstgewählten Benutzernamen bzw. QR-Code. Die Betrüger der jüngsten Angriffswelle geben sich als Signal-Support-Team aus und behaupten, das Opfer müsse Sicherheitscodes mitteilen, da das eigene Konto möglicherweise kompromittiert sei. Der in Berlin für Amnesty International tätige IT-Sicherheitsforscher Donncha Ó Cearbhaill machte einen solchen Betrugsversuch am 8. Mai auf X öffentlich. Im Januar war er demnach von einem angeblichen »Signal Security Support Chat-Bot« angeschrieben worden. In der Nachricht wird eine »verdächtige Aktivität auf Ihrem Gerät« behauptet. Auch behauptete der Absender, es seien Versuche bemerkt worden, Zugang zu »privaten Daten in Signal« zu erlangen – gefolgt von der Aufforderung, den persönlichen Verifikationscode zu verraten.

Ó Cearbhaill sei es gelungen, hinter die Kulissen zu blicken. So sei er das Angriffsziel Nummer 13.730 in der Datenbank der Täter gewesen. »Das automatisierte System, das die Kampagne steuert«, werde von den Betreibern »ApocalypseZ« genannt. »Der Quellcode und die Benutzeroberfläche sind ausschließlich in Russisch verfasst. Die Angreifer übersetzten zudem die Kommunikation mit den Opfern ins Russische.« Diese Zuordnung dürfte hiesigen »Sicherheitsbehörden« ins Kalter-Krieg-Konzept passen.

Am 6. Februar hatten das dem CSU-kontrollierten Innenministerium unterstellte Bundesamt für Sicherheit in der Informationstechnik (BSI) und das für Spionageabwehr zuständige Bundesamt für Verfassungsschutz einen Sicherheitshinweis zum »Phishing über Messengerdienste« veröffentlicht. Darin ist die Rede von einem »wahrscheinlich staatlich gesteuerten Cyberakteur«, der Angriffe über Apps wie Signal durchführe. »Die geringen technischen Hürden dieser Angriffskampagne« lassen demnach den Schluss zu, dass ebenso »nichtstaatliche Akteure, insbesondere von cyberkriminellen Gruppierungen« verantwortlich sein könnten. Die amtliche Bewertung endet jedoch mit dem Urteil: »Angesichts der hochkarätigen Zielfläche ist in den derzeit bekannten Fällen wahrscheinlich von einem staatlich gesteuerten Cyberakteur als Urheber auszugehen.«

Innerhalb der darauffolgenden Monate stand für reichweitenstarke Medien praktisch fest: Russland war’s. Am 9. März berichtete die Nachrichtenagentur *Reuters* über »von Russland unterstützte Hacker«. Das Medienhaus *Correctiv* berichtete am 29. April, dass »die digitalen Spuren der Kampagne tatsächlich nach Russland« führen würden. Genauer: zu »einer Gruppe, die IT-Sicherheitsexperten von Google als ›UNC5792‹ kategorisieren« – wobei das »UNC« für nicht eindeutig zugeordnete Akteure oder Angriffe stehe. *Correctiv* behauptete weiter, dass es »eine Verbindung zu früheren Phishingkampagnen gegen Ziele in der Ukraine und der Republik Moldau« habe herstellen können.

T-Online hatte einen Artikel vom 4. Mai mit »Russland bringt Deutschland in Verlegenheit« überschrieben. »So unverfroren agieren Putins Agenten in Deutschland«, hatte der *Spiegel* am 7. Mai getitelt. Dort war die Rede von »Russlands jüngster Cyberattacke«, die Teil »einer breit angelegten Angriffswelle« sei, »mit der Russland Europa überzieht«. Die Nachrichtenagentur *dpa* meldete schließlich am 8. Mai, dass »verschiedene Sicherheitsexperten« davon ausgehen, »dass Angreifer aus Russland hinter der Cyberattacke stecken« und auch die Bundesregierung »nach Angaben aus Regierungskreisen« Russland hinter den Angriffen auf Signal-Nutzer sehe.

Sorglos an höchster Stelle

Besondere Aufregung herrscht, seit der *Spiegel* darüber berichtete, dass der oft fälschlicherweise als »Hack« bezeichnete Phishingangriff nicht nur bei »NATO-Angehörigen«, sondern auch bei mehreren Mitgliedern der Bundesregierung und des Bundestags erfolgreich gewesen sei. Am 22. April hatte das Blatt berichtet, dass Bundestagspräsidentin Julia Klöckner (CDU) zu den Opfern gehöre. Der Inlandsgeheimdienst sei sogar beim Kanzler vorstellig geworden. »In praktisch allen Fraktionen« gebe es betroffene Abgeordnete. Nach Angaben der SPD-Fraktion gegenüber *Spiegel* seien es dort »einige wenige« gewesen. Ebenso bei der Linke-Fraktion. Die Unionsfraktion habe keine

entsprechenden Angaben machen wollen. Schließlich habe der Generalbundesanwalt beim Bundesgerichtshof Ermittlungen wegen des Verdachts auf geheimdienstliche Agententätigkeit aufgenommen. Später berichtete das Magazin, dass auch Bildungsministerin Karin Prien (CDU) und Bauministerin Verena Hubertz (SPD) den Betrügern auf den Leim gegangen sein sollen. Sollte dies zutreffen, dürften die Täter Zugriff auf diverse bundestags-, regierungs- und parteiinterne Chatgruppen erlangt haben.

In einem am 8. Mai online veröffentlichten *Spiegel*-Interview kritisierte die Präsidentin von Signal, Meredith Whittaker, dass die von der Phishingattacke betroffenen Politikerinnen und Politiker öffentlich für ihre mutmaßliche Inkompetenz verunglimpft worden seien. Whittaker mahnte angesichts der großen Verbreitung von Signal unter ranghohen Amts- und Geheimnisträgern eine bessere Finanzierung des Messengerdienstes an. Dieser lebe von Spenden. Rüstungsstartups wie Helsing bekämen »für ihre Versprechungen Milliarden«, kritisierte sie. »Wir betreiben mit Signal eine schon funktionierende kritische Infrastruktur und werden nicht entsprechend unterstützt.« Das sei »ein krasses Missverhältnis«. Wer Signal so intensiv nutze »wie offenbar NATO-Vertreter oder die Bundesregierung, könnte darüber nachdenken, wie er beitragen kann«, regte sie an.

Die Opfer jedenfalls seien durch sogenanntes Social Engineering manipuliert worden, um den Fehler zu begehen, ihre Sicherheitscodes preiszugeben. Dies könne in jedem Messengerdienst passieren, erklärte die Signal-Präsidentin. Auf die Forderung von Bundestagsvizepräsidentin Andrea Lindholz (CSU) nach einem Signal-Verbot angesprochen, reagierte Whittaker mit Unverständnis. »Alle Plattformen dieser Größenordnung sind anfällig.« Das Problem werde abwandernden Nutzern »auf sämtliche anderen Dienste folgen, und viele davon sind per se erheblich unsicherer«. Es sei »völlig sachfremd, jetzt das Verbot eines einzelnen sicheren Messengerdienstes zu fordern, während andere völlig unerwähnt bleiben«, kritisierte auch die Linke-Abgeordnete Donata Vogtschmidt am 29. April in einer gemeinsamen Mitteilung mit ihrer Fraktionskollegin Sonja Lemke. Der Verbotsvorschlag lenke »von dem eigentlichen Problem« ab. Lemke verwies auf unaufmerksames Verhalten von App-Nutzern, das »niemand ausschließen« könne.

Kommerzielle Konkurrenz

Lindholz habe zudem auch den vollständigen Umstieg auf Apps des Herstellers Wire gefordert. Ende April sei »über den Bundestag« bereits diese Software »gepusht« worden, teilten die Linke-Politikerinnen mit. »Aktuell ist es der einzige Messengerdienst, der sich einfach auf den Endgeräten des Bundestags installieren lässt«, erklärte Lemke. Das dahinterstehende Unternehmen lobbyiere »seit Jahren beim Bundestag«. Im Digitalausschuss sei zu hören gewesen, dass Wire eine Integration des eigenen Produkts in die sogenannte Deutschland-App anstrebe.

Das Portal *Heise Online* hatte am 28. April über ein Schreiben Klöckners berichtet, in dem die Bundestagspräsidentin allen Abgeordneten die Nutzung des Wire-Dienstes ans Herz gelegt habe. Der Bericht spricht von »einem dringlichen Appell«. Auch habe das BSI dem Produkt »Wire Bund« zu dem Zeitpunkt bereits die Freigabe für Daten der Geheimhaltungsstufe

»Verschlusssache – nur für den Dienstgebrauch« erteilt. Zuvor hatte der *Spiegel* am 24. April berichtet, dass die Unionsfraktion gegenüber ihren Abgeordneten bereits im Februar nach einem Warnschreiben des Verfassungsschutzes dafür geworben haben soll, den Messengerdienst Wire zu benutzen.

In Berlin betreibt der Softwareanbieter offenbar über seine Wire Germany GmbH die technische Entwicklung des Instant-Messengers. Für das Jahr 2023 verzeichnete sie einen Gewinn von rund 270.000 Euro, wie aus dem Jahresabschluss hervorgeht. Mit 298.956 Euro fiel der Gewinn im Vorjahr etwas höher aus. Die Firma ist zu 100 Prozent im Besitz der Wire Group Holdings GmbH. Deren Geschäftsführer Benjamin François Schilz wurde nach Unternehmensangaben vom 9. Februar 2024 als CEO an Bord geholt, um die »internationale Expansion von Wire« voranzutreiben. Schilz ist ebenfalls Geschäftsführer der Wire Swiss GmbH mit Sitz in Zug. Dorthin ist Wire gezogen, nachdem der Sitz in den USA vermutlich vor allem aus Imagegründen – US-Firmen sind gesetzlich zur Kooperation mit Geheimdiensten verpflichtet – problematisch wurde. Gegründet worden war Wire ursprünglich von früheren Mitarbeitern von Apple, Skype, Nokia und Microsoft.

Wire hatte am 11. April 2024 seine »strategische Partnerschaft« mit der Schwarz-Gruppe bekanntgegeben. Das Ziel: »sichere Kommunikation und Datensouveränität in Deutschland und Europa« vorantreiben. Zur Schwarz-Gruppe gehören die Einzelhandelsmarken Lidl und Kaufland. Die Digitalsparte ist in der Schwarz Digits KG gebündelt. Aus Handelsregistereinträgen geht hervor, dass mit Stand vom 21. Januar unter anderem die Schwarz New Ventures GmbH zu 26,4 Prozent, aber auch die Roland Berger Industries GmbH mit Sitz in München mit 3,3 Prozent an der Wire Group Holding beteiligt ist. Weitere 10,2 Prozent hält demnach die Zeta Holdings Luxembourg SA. Wire Germany firmierte vor dem 1. Januar 2025 noch unter Zeta Project Germany.

Die zwei Linke-Abgeordneten vermuten, dass der Wire-Vorstoß aus Unionskreisen »auch auf weiteren Lobbyismus der Schwarz-Gruppe zurückzuführen ist, die ihr Produkt plazieren will und die sich als Vorreiter digitaler Souveränität in Europa vermarktet«.

https://www.jungewelt.de/artikel/522657.kampagne-gegen-signal-app-den-köder-geschluckt.html