ZEIT ONLINE

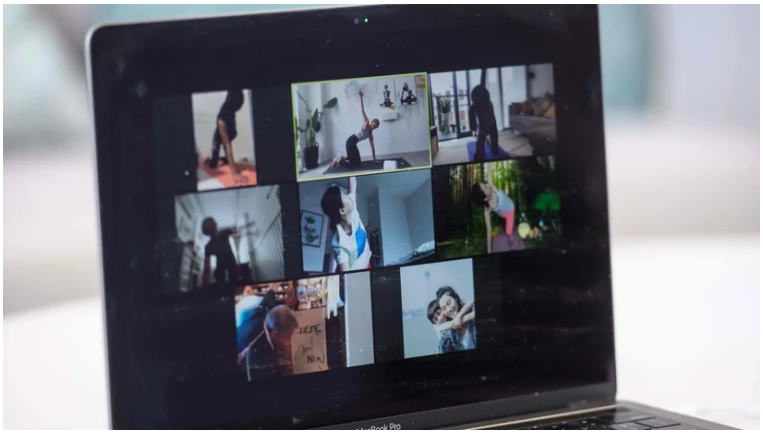
Zoom

Unter Beobachtung

Je populärer der Videodienst Zoom wird, umso mehr Sicherheitslücken finden IT-Experten. Nicht alle Fehler sind gleich gefährlich. Dennoch müssen Nutzer vorsichtig sein.

Von **Meike Laaff** und **Lisa Hegemann**

3. April 2020, 5:55 Uhr / 29 Kommentare



Yoga über Zoom: Wer den Dienst nutzt, sollte sehr entspannt mit seinen Daten sein. © Anthony Wallace/AFP/Getty Images

In Zeiten sozialer Isolation ist der Videokonferenzdienst Zoom für viele Menschen weltweit eine Rettung. Über Zoom kann man mit den Eltern telefonieren, mit den Kolleginnen konferieren – und sich einfach abends auf einen Tee oder einen Wein mit Freunden treffen. Das geht vergleichsweise leicht und funktioniert zumeist sogar ohne nervige Verbindungsprobleme, auch bei größeren Gruppen.

Je populärer der Dienst wird, desto intensiver interessieren sich allerdings auch Sicherheitsforscherinnen und -forscher für ihn. Und sie finden ständig neue Lücken, stoßen auf falsche Versprechungen oder beunruhigende technische Lösungen. Wie gefährlich sind die Schwachstellen von Zoom für Nutzerinnen und Nutzer?

Wir haben die Software schon mal für Sie installiert …

Schon im vergangenen Jahr wurde eine massive Sicherheitslücke [https://www.zeit.de/digital/2020-03/videokonferenzen-zoom-app-homeoffice-

quarantaene-coronavirus] öffentlich, die kriminellen Hackerinnen und Hackern Zugriff auf potenziell Millionen Kameras von Mac-Nutzern hätte ermöglichen können. Angreifer konnten Nutzerinnen und Nutzer auf eine präparierte Website locken, die den Videodienst startete – und so Menschen abhören oder ihnen heimlich zusehen. Unternehmensangaben zufolge war die Lücke entstanden, weil Zoom versucht, seinen Dienst besonders userfreundlich zu gestalten. Oder, um es deutlicher zu sagen: Für eine bessere Nutzbarkeit hat man offenbar die Sicherheit vernachlässigt. Eine Schwerpunktsetzung, die der Firma nun erneut Schwierigkeiten zu bereiten scheint.

So installiert sich die Software von Zoom auf Macs, bevor Nutzer dazu ihre Einwilligung erteilt haben. Teilweise über ein sogenanntes Preinstall-Script: Das ist eigentlich dazu gedacht, das Betriebssystem vor der Installation zu prüfen. Zoom nutzt es, um einfach eine Installation zu starten. Darauf machte der Mac-Entwickler Cabel Sasser [https://twitter.com/cabel/status/1244788176482258945] via Twitter aufmerksam.

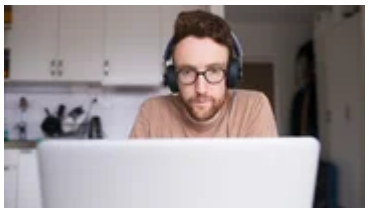
Der deutsche Sicherheitsforscher Felix Seele erklärte, ebenfalls auf Twitter [https://twitter.com/c1truz_/status/1244737672930824193], noch eine weitere technische Abkürzung, die sich Zoom erlaubt: Ist eine Userin nicht als Administratorin auf dem Mac eingeloggt und das System schon installiert, fragt Zoom den Benutzernamen und das Administrator-Passwort ab. Die Software gibt sich also als Betriebssystem aus, um damit Root-Rechte zu erlangen – weitreichende Zugriffsrechte, mit denen man Einstellungen am System ändern kann.

Das sei zwar nicht zwangsläufig ein bösartiges Vorgehen, aber schon "sehr dubios" und hinterlasse einen "bitteren Nachgeschmack" [https://twitter.com/c1truz_/status/1244737676990976001], so Seele. Auch Thorsten Holz, Professor für Systemsicherheit an der Ruhr-Universität Bochum, hält das Vorgehen für "nicht ganz in Ordnung". Die Software täusche vor, dass das Apple-Betriebssystem nach Administrator-Daten frage, frage aber eigentlich selbst danach. "Das ist ein Trick, den auch Schadsoftware verwendet", sagt Holz im Gespräch mit ZEIT ONLINE. Firmenchef Eric Yuan [https://twitter.com/ericsyuan/status/1245104758240632832] reagierte auf Twitter auf Seeles Kritik und versprach etwas vage, man werde sich weiter verbessern.

Mac Attacks!

Zusätzlich demonstrierte der einstige NSA-Hacker und heutige Sicherheitsforscher Patrick Wardle in einem Blogpost [https://objective-see.com/blog/blog_0x56.html] eine weitere Sicherheitslücke. Sie soll es möglich machen, sich den Zugriff auf Mikrofone und Webcams von Mac-Nutzern zu erschleichen. Gewöhnlich müssen Nutzerinnen und Nutzer zustimmen, wenn

KOMMUNIZIEREN IN DER PANDEMIE



Videokonferenzen

Ok, Zoomer

[https://www.zeit.de/digital/2020-03/videokonferenzen-zoom-app-homeoffice-quarantaene-coronavirus]

Videotelefonie

Haben Sie noch Ihr Skype-Passwort?

[https://www.zeit.de/digital/internet/2020-04/videotelefonie-videokonferenzen-coronavirus-online-tools-zoom-skype-facebook]

eine Software auf ihre Kamera oder ihr Mikrofon zugreifen will. Das müssen sie auch bei Zoom. Aber würde es kriminellen Angreifern gelingen, in die Zoom-Software Schadcode einzuschleusen, erlangten sie "automatisch" alle Zugriffsrechte, die Zoom eingeräumt wurden [https://techcrunch.com/2020/04/01/zoom-doom/], so Wardle. Sprich: Es wäre möglich, den Nutzer durch die Kamera und über das Mikrofon zu überwachen. Wardles Fazit: "Wenn du dich für deine Sicherheit und Privatsphäre interessierst, hör vielleicht auf, Zoom zu nutzen."

Der Bochumer Professor Holz hält diese Lücke für eher unkritisch. Es müsse schon vorher Schadsoftware auf dem Mac laufen, damit dieser Angriff funktionieren könne, sagt er. Habe ein krimineller Hacker eigenen Code auf dem Rechner des Opfers ausgeführt, könne er danach mit Hilfe von Zoom auch noch Zugriff auf Kamera oder Mikrofon bekommen. "Der eigentliche Schaden wäre also schon vorher passiert."

Entschuldigen Sie, dürfte ich kurz an Ihr Passwort?

Für Nutzerinnen und Nutzer, die Zoom auf ihren Windows-Rechnern laufen lassen, sah es offenbar nicht besser aus. Konkret problematisch soll die Chatfunktion von Zoom gewesen sein, über die man während einer Telefonkonferenz auch per Kurznachricht mit Teilnehmern kommunizieren kann. Angaben der Tech-Seite *Bleeping Computer* [https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/] zufolge soll es möglich gewesen sein, über im Chat von Zoom-Meetings verschickte und entsprechend präparierte Links das Windows-Passwort von Nutzern herauszufinden [https://arstechnica.com/information-technology/2020/04/unpatched-zoom-bug-lets-attackers-steal-windows-credentials-with-no-warning/].

Diese Links führen nicht auf Websites, sondern auf sogenannte UNC-Pfade. Vereinfacht ausgedrückt machen die es möglich, von anderen Rechnern aus auf Dateien eines Computers zuzugreifen, sie zum Beispiel herunterzuladen. Noch schlimmer: Wird ein UNC-Pfad ausgeführt, versendet Windows automatisch auch die Login-Daten für den Rechner – Nutzername und Passwort. Das Passwort ist zwar gewöhnlich verschlüsselt, also nicht im Klartext einsehbar, es kann aber laut *Bleeping Computer* einfach entschlüsselt werden. Zoom

erklärte laut der Technikwebseite *Ars Technica,* dass man sich dieses Problems bewusst sei und an einer Lösung arbeite.

Nutzerinnen und Nutzer müssen sich über diese Sicherheitslücke aber nicht allzu viele Gedanken machen, sagt Thorsten Holz. Denn erstens müsse man sich zunächst einmal in einem Videoanruf mit einer Person befinden, bevor die einen Link über den Chat verschicken kann. Dass jemand, den man kennt, bösartige Links verschickt, ist eher unwahrscheinlich. Und wenn man mit Fremden videokonferiert, sollte man ohnehin vorsichtig sein.

> **»Es handelt sich nicht um eine Möglichkeit, massenhaft Zoom-Nutzer unbemerkt auszuspionieren, sondern um eine gezielte Einzelattacke.«**
>
> *—Thorsten Holz, Professor für Systemsicherheit*

Zweitens müsste der Nutzer erst auf den Link klicken, bevor irgendetwas passiert. Das Programm startet nicht automatisch. Da die Links auch noch anders aussehen als gewöhnliche Weblinks, können aufmerksame Nutzer sie erkennen. "Es handelt sich dabei nicht um eine Möglichkeit, massenhaft Zoom-Nutzer unbemerkt auszuspionieren", sagt Holz, "sondern um eine gezielte Einzelattacke, für die man dann auch erst das Vertrauen des Nutzers gewinnen müsste." Holz hält die Diskussionen darüber daher für einen ziemlich aufgeblasenen Hype.

Die losen Enden der Verschlüsselung

Trotzdem gibt es einen Kritikpunkt, der alle Nutzerinnen und Nutzer betrifft, ob sie nun Windows- oder Mac-Rechner verwenden. Am Dienstag wurde bekannt, dass Zoom seine Videokonferenzen gar nicht so verschlüsselt, wie es bislang vom Unternehmen behauptet wurde. "Derzeit ist es nicht möglich, Ende-zu-Ende-Verschlüsselung für Zoom-Videomeetings zu ermöglichen", sagte eine Unternehmenssprecherin gegenüber der US-Rechercheplattform *The Intercept* [https://theintercept.com/2020/03/31/zoom-meeting-encryption/]. Bei dieser Form der Verschlüsselung wären die Daten nur für die Kommunikationspartner einsehbar, auf Firmenservern lägen sie lediglich verschlüsselt vor. Genau das hatte Zoom in seinem White Paper [https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf] versprochen. In solchen Veröffentlichungen erklären Unternehmen die Funktionsweise ihrer Software.

Stattdessen nutzt Zoom laut *The Intercept* ein Verschlüsselungsprotokoll namens *Transport Layer Security*, kurz TLS. Das verschlüsselt Daten zwar auch, aber, wie der Name schon verrät, nur während des Transports. Das bedeutet,

MEIKE LAAFF

Redakteurin im Ressort Digital, ZEIT ONLINE

LISA HEGEMANN

Redakteurin im Ressort Digital, ZEIT ONLINE

dass Zoom-Meetings zwar nicht von jemandem mitgehört werden können, der sich ins WLAN eingehackt hat, sehr wohl aber, theoretisch, von Zoom-Mitarbeitern. Denn auf den Rechnern von Zoom könnten diese Daten wieder entschlüsselt werden. Einzig Zoom-Chats dürften derzeit wirklich Ende-zu-Ende-verschlüsselt sein, so *The Intercept*.

Für zwei Personen sei eine Ende-zu-Ende-Verschlüsselung recht einfach herzustellen, sagt Wissenschaftler Holz. Doch gerade in Videokonferenzen mit mehreren Teilnehmerinnen und Teilnehmern werde es kompliziert: "Da kommen teils neue Menschen hinzu, teils verlassen andere das Meeting", sagt Holz. "Kryptografisch bekommen wir das nicht so einfach hin."

Gruppen-Videokonferenzen seien nicht leicht Ende-zu-Ende zu verschlüsseln, sagt auch der Computerwissenschaftler Matthew Green von der Johns-Hopkins-Universität gegenüber *The Intercept*. Apples FaceTime demonstriere aber: "Es ist möglich. Es ist nur eben nicht einfach."

Technisch etwas "sehr Gutes" gebaut, sicherheitstechnisch nicht so

In einem Blogpost [https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/] entschuldigte sich Zoom für das "Missverständnis", das man verursacht habe. Nutzten alle Teilnehmerinnen und Teilnehmer eines Meetings die Zoom-App, dann verschlüssele man alles – Video, Audio, Chat und Screensharing-Funktionen, mit denen man sehen kann, was auf anderen Rechnern läuft. In diesem Szenario "sind keine Nutzerinformationen während des Übertragungsprozesses auf Zoom-Rechnern oder für Zoom-Mitarbeiter verfügbar", schreibt Zoom. Verwende jemand die Software aber zum Beispiel über das Telefon oder andere Programme, könnten solche Sicherungsprozesse fehlen – auch wenn man sich bemühe, die Kommunikation trotzdem zu verschlüsseln.

Das Problem: Ist die Verbindung nicht verschlüsselt, können Angreifer möglicherweise mithören oder -sehen. Interessant dürfte das besonders für Nachrichtendienste sein. Denn aktuell nutzen auch Regierungen und Politiker, etwa der britische Premier Boris Johnson [https://www.spiegel.de/politik/ausland/grossbritannien-boris-johnson-gibt-sensible-daten-per-tweet-zu-videokonferenz-preis-a-5f299820-cc44-4f95-989e-c5f5225c8ce6], die Software. Zoom stellt allerdings klar: Man habe noch nie einen Mechanismus für Regierungsbehörden gebaut, mit dem man Livemeetings entschlüsseln

könne. Experte Holz sagt: Für vertrauliche Gespräche sei Zoom möglicherweise nicht geeignet. Dafür solle man eher auf Programme wie den verschlüsselten Messenger Signal zugreifen.

Zoom kündigte in einem weiteren Beitrag [https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/] außerdem an, dass die Sicherheitslücken, die Angriffe auf Mikros und Webcams bei Macs und auf Windows-Systeme erlauben könnten, geschlossen sind. Auf Kritik aus der Datenschutz- und Sicherheitscommunity reagieren – darin hat das Unternehmen so langsam Routine. Und darin will es in Zukunft noch besser werden: Ab sofort würden alle Entwickler auf die wichtigsten Vertrauens-, Sicherheits- und Datenschutzprobleme angesetzt, schreibt Firmenchef Yuan in dem Blogpost.

"Ich muss sagen, dass ich beeindruckt bin", sagte Seele, der einige der Probleme bei Mac-Rechern öffentlich gemacht hatte, dem US-Techmagazin *The Verge* [https://www.theverge.com/2020/4/2/21204648/zoom-macos-installer-update-privacy-security-concerns]. Zoom habe tatsächlich die Preinstall-Scripte entfernt, sodass sich Nutzerinnen und Nutzer wirklich durch den Installierungsprozess klicken müssen, bevor sich die Software herunterlädt.

Nasa und SpaceX zoomen nicht mehr

Der Schaden ist für Zoom aber schon angerichtet. Unternehmen wie SpaceX und die amerikanische Bundesbehörde Nasa haben angekündigt, die Software von Zoom nicht länger nutzen zu wollen – wegen erheblicher Datenschutz- und Sicherheitsbedenken. SpaceX-Verantwortliche schrieben in einer internen E-Mail, aus der die Nachrichtenagentur Reuters [https://de.reuters.com/article/usa-zoom-spacex-idDEKBN21K0HE] zitiert, dass ihre Mitarbeiterinnen und Mitarbeiter lieber "E-Mail, Text oder Telefon" verwenden sollten.

Selbst das FBI warnte Nutzerinnen und Nutzer: Sie sollten keine Besprechungen auf "öffentlich" stellen. Und IT-Experten haben schon wieder was gefunden, worum sich Zoom nun kümmern muss: Der Sicherheitsforscher Brian Krebs bastelte ein automatisiertes Tool, das öffentliche Zoom-Konferenzen findet, in dem es die Identifikationsnummern errät – womit diese Meetings also für jeden und jede auffindbar sind. Das schrieb er in einem Blogpost [https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/]. Und der IT-Sicherheitsforscher Thorsten Schröder hat Schwachstellen entdeckt, über die man schadhaften Code ausführen kann, wie die *Riffreporter* [https://www.riffreporter.de/vr-reporterin/dank-zoom-kann-dein-computer-zum-spionage-tool-werden/] berichten.

"Zoom hat sich offenbar auf die Funktionalität seiner Software konzentriert und die Sicherheit dabei vernachlässigt", sagt Holz. Er glaubt aber nicht, dass

Zoom damit allein ist: Auch in anderen Videokonferenztools würde man sicherlich solche Lücken finden, sähe man so genau hin wie bei Zoom. Für alle, die Zoom weiter verwenden wollen (oder berufsbedingt müssen), hat die amerikanische Organisation Electronic Frontier Foundation [https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls], die sich für digitale Privatsphäre einsetzt, nun eine Anleitung: Sie zeigt, wie man die eigenen Daten auf dem Videodienst schützen und es Angreifer möglichst schwer machen kann.

Von der Software abraten will auch Wissenschaftler Holz nicht. Das Unternehmen habe eine komplexe Anwendung und technisch etwas "sehr Gutes" gebaut, sagt er. Er selbst werde Zoom weiter nutzen, weil die Videoübertragung, anders als bei anderen Diensten, selbst bei größeren Gruppen stabil bleibe. Aber: "Ich verstehe auch, wenn Menschen aus Sicherheitsgründen lieber andere Dienste nutzen wollen."