2023/22 Ausland

https://www.jungle.world/artikel/2023/22/dubioser-download

Die chinesische App Tiktok soll in den USA verboten werden

Dubioser Download

Von **Elke Wittich Boris Mayer**

Montana hat die Nutzung von Tiktok verboten, die chinesische App gilt demokratischen wie republikanischen Politikern in den USA als Bedrohung. Doch die Datensicherung ist technisch schwer umzusetzen.

Trotz allen politischen Zwists sind sich Demokraten und Republikaner in den USA in einem Punkt weitgehend einig: Beide Parteien halten die beliebte chinesische App Tiktok für gefährlich und befürchten, sie könne von China für Spionage genutzt werden.

Dass Hacker in staatlichem Auftrag für China tätig sind, gilt seit dem Solarwinds-Hack 2020 als weitgehend gesichert. Damals hatte sich eine Gruppe mutmaßlich chinesischer Hacker mittels eines gekaperten und von ihnen dann manipulierten Updates einer Software des in Texas ansässigen Software-Unternehmens Solarwinds weltweit Zugang zu kritischer Infrastruktur in Behörden, Firmen, Ministerien und Organisationen verschafft.

Am 7. Dezember 2022 verbot Greg Abbott, der republikanische Gouverneur von Texas, allen Stellen seines Bundesstaats, auf regierungseigenen Geräten Tiktok zu nutzen. Ein entsprechender Gesetzentwurf namens HB 3289 wurde im Februar eingebracht,er verbietet den Download der Tiktok-App auf staatliche Rechner und Smartphones. Eine Ausnahme gibt es einzig für Ermittlungen gegen Straftäter und -täterinnen, allerdings muss die texanische Regierung dann umgehend darüber informiert werden, dass und warum die App dafür genutzt werden muss.

»Im Besitz einer chinesischen Firma, die Mitglieder der chinesischen Kommunistischen Partei beschäftigt, sammelt Tiktok signifikante Datenmengen von user devices, inklusive Daten über die Internetaktivitäten eines Users«, so hatte Greg Abbott die Notwendigkeit des Gesetzes im Februar begründet.

Am 17. Mai wurde Montana der erste US-Bundesstaat, in dem Tiktok de facto komplett verboten ist. Das Herunterladen der App ist generell nicht mehr zulässig. Jeder sie zum Download anbietenden entity, also beispielsweise App Stores oder dem Unternehmen selbst, droht nun eine Geldstrafe von 10 000 Dollar pro Tag, an dem die Download-Möglichkeit bestand. User und Userinnen sollen hingegen straffrei bleiben.

> Gegner des neuen Gesetzes machten umgehend klar, dass in Montana Ansässige das Verbot ganz einfach durch die Nutzung eines VPN umgehen könnten.

Sogenanntes Geofencing, also der Ausschluss von Nutzern aus bestimmten Ländern oder Regionen von einem Internetangebot, könnte Einwohnern von Montana der Zugriff auf Tiktok unmöglich machen, sagten Politiker des Bundesstaats. Sie verwiesen darauf, dass diese Technologie beispielsweise in Bundesstaaten, in denen Online-Sportwetten illegal sind, erfolgreich eingesetzt werde. Gegner des neuen Gesetzes machten allerdings umgehend klar, dass in Montana Ansässige das Verbot ganz einfach durch Nutzung eines VPN (virtual private network) umgehen könnten.

Nur wenige Tage nachdem das Tiktok-Verbot in Montana in Kraft getreten war, klagten die ersten User vor Gericht dagegen. Eine Gruppe von fünf Personen, die angeben, die App dazu zu benutzen, von ihnen erschaffenen Content zu posten, sieht ihre Redefreiheit bedroht – und steht mit dieser Sicht der Dinge nicht allein. Die im Jahr 1920 gegründete Bürgerrechtsorganisation American Civil Liberties Union (ACLU) nannte das in Montana erlassene Gesetz eine »verfassungswidrige Einschränkung der Redefreiheit«. Gegen ein Tiktok-Verbot wenden sich in den USA unter anderem Inhaber und Inhaberinnen kleiner Geschäfte, die eigenem Bekunden nach nicht auf die Nutzung der App verzichten wollen, weil sie einfache Möglichkeiten biete, mit Kunden in Kontakt zu bleiben oder neue Kundschaft hinzuzugewinnen.

Tiktok hatte bereits Ende vorigen Jahres angekündigt, das sich damals bereits abzeichnende Verbot nicht kampflos hinzunehmen, und initiierte das »Projekt Texas«, das vorsieht, alle US-Nutzerdaten auf Oracle-Servern in Texas zu verwalten. Seit Oktober 2022 werden alle neuen US-Nutzerdaten innerhalb des Landes verarbeitet und verwaltet. Die Migrierung alter Accounts wird allerdings mehrere Monate in Anspruch nehmen; im März begann das Unternehmen damit, alte, inaktive Accounts zu löschen. Medienberichten zufolge willigte Tiktok Ende Mai ein, dass Oracle-Techniker den Quellcode der App sowie die Algorithmen auf Schadcodes untersuchen können.

> Selbst wenn Daten und Server abgesichert sind und geregelt ist, dass keinerlei Abflüsse stattfinden können, gibt es keine hundertprozentige Sicherheit.

Im März reiste der CEO von Tiktok, Shou Zi Chew, persönlich nach Washington, D.C., um sich beim Energy and Commerce Committee des Repräsentantenhauses, vor das er vorgeladen war, den Fragen der Abgeordneten zu stellen. Es gelang ihm jedoch nicht, die Bedenken der Mitglieder des Komitees zu entkräften. Chew gab immer wieder ausweichende Antworten, vor allem als es um die im vorigen Jahr bekannt gewordene Überwachung zweier US-Journalisten und ihrer Kontaktpersonen ging. Im Dezember hatte Tiktok vier Mitarbeiter entlassen, die auf der Suche nach firmeninternen Leaks die entsprechenden Daten ausspioniert hatten. Dass ein offenbar vor der öffentlichen Bekanntgabe des Anhörungstermins auf TikTok gepostetes Video auftauchte, das ein Komiteemitglied namentlich nennt und das Nachladen einer Pistole zeigt, verbesserte die Stimmung nicht.

Gleichwohl wirft der von Politikern als Erfolg angesehene demonstrative Umzug auf die Oracle-Server einige Fragen auf – nicht zuletzt für private User, denen es mehrheitlich egal sein dürfte, wem die Server gehören, auf denen ihre Daten ausgewertet werden. Dass Daten auf Oracle-Servern in Texas liegen, sagt zudem nichts darüber aus, wer auf sie Zugriff hat oder in Zukunft Zugriff haben wird. Dazu kommt noch, dass Beschäftigte eines Unternehmens zuallererst eben das sind, nämlich Beschäftigte eines Unternehmens, egal ob der Sitz in China oder Texas liegt.

Selbst wenn Daten und Server abgesichert sind und geregelt ist, dass keinerlei Abflüsse stattfinden können, gibt es keine hundertprozentige Sicherheit. Denn jedes System kann gehackt werden – wie einfach das geht, hat nicht zuletzt der Fall Solarwinds gezeigt. Der zeigte allerdings auch, dass Spionage nach wie vor auf Stellen abzielt, an denen es interessante und zumindest vertrauliche Informationen zu holen gibt, die nicht genauso gut durch gezielte Beobachtungen an Ort und Stelle beschafft werden können.