SICHERHEIT

Welche Einstellungen zum Datenschutz bietet ZOOM

Zugangsbeschränkungen zu Meetings durch:

- Passwortschutz
- Domainabgleich – Nutzer müssen über eine E-Mailadresse einer zugelassenen Domain besitzen
- Warteraum – Gastgeber kann Nutzer einzeln prüfen und dem Meeting hinzufügen

Tipps rund um die Sicherheit und Privatsphäre für Zoom-Benutzer

1. Schützen Sie Ihr Konto

Ein Zoom-Konto ist, wie der Name bereits sagt, ein Konto wie jedes andere. Bei der Einrichtung Ihres Kontos sollten Sie sich deshalb der Grundlagen des Kontoschutzes bewusst sein und diese effektiv anwenden. Verwenden Sie ein sicheres und eindeutiges Passwort und schützen Sie Ihr Konto mithilfe einer Zwei-Faktor-Authentifizierung, wodurch Ihr Konto schwieriger zu hacken ist und besser geschützt wird, selbst wenn Ihre Kontodaten verloren gehen (obwohl dies bisher noch nicht geschehen ist).
Es gibt mindestens einen weiteren Zoom-spezifischen Haken: Nach der Registrierung erhalten Sie zusätzlich zu Ihrem Login und Passwort eine persönliche Meeting-ID. Machen Sie diese nicht öffentlich. Und da Zoom die Option bietet, öffentliche Meetings mit Ihrer persönlichen Meeting-ID zu erstellen, ist es recht einfach, diese ID zu leaken. Wenn Sie dies tun, kann jeder, der Ihre PMI kennt, an jedem von Ihnen veranstalteten Meeting teilnehmen. Teilen Sie diese Informationen daher mit Bedacht.

2. Verwenden Sie Ihre Arbeits-E-Mail, um sich bei Zoom zu registrieren

Ein seltsamer Glitch in Zoom (der zum Zeitpunkt dieses Blogeintrags noch nicht behoben ist) führt dazu, dass der Dienst E-Mails mit derselben Domain einer Firmen-Adresse kennzeichnet und Kontaktinformationen mit jedem, der diese Domain besitzt, teilt. Bei gängigeren Domains wie @gmail.com oder @yahoo.com geschieht dies nicht. Bei Benutzern, die Zoom-Konten mithilfe von E-Mails registriert haben, die mit @yandex.kz enden, einem öffentlichen E-Mail-Dienst in Kasachstan, trat dieses Szenario jedoch häufiger auf. Das könnte möglicherweise auch bei E-Mail-Adressen, die zu kleineren öffentlichen E-Mail-Anbietern gehören, geschehen.
Benutzen Sie deshalb Ihre Firmen-Mail, um sich bei Zoom zu registrieren. Das Teilen Ihrer Firmen-Kontaktdaten mit Ihren echten Kollegen sollte keine große Sache sein. Wenn Sie keine geschäftliche E-Mail Adresse besitzen, verwenden Sie ein Wegwerfkonto mit einer bekannten öffentlichen Domain, um Ihre persönlichen Kontaktdaten privat zu halten.

3. Fallen Sie nicht auf gefälschte Zoom-Apps herein

Die Anzahl der schädlichen Dateien, deren Dateinamen die Namen beliebter Videokonferenzdienste (Webex, GoToMeeting, Zoom und andere) enthielten, hatte sich im März im Vergleich zu den monatlichen Daten des vorherigen Jahres ungefähr verdreifacht, stellte Danis Parinov, Sicherheitsexperte bei Kaspersky, fest. Dies bedeutet höchstwahrscheinlich, dass Übeltäter mehr Missetaten aufgrund der Beliebtheit von Zoom und anderen Apps dieser Art begehen und diese Malware als Videokonferenz-Clients zu tarnen versuchen.
Fallen Sie nicht darauf herein! Verwenden Sie die offizielle Website von Zoom (Zoom.us), um Zoom sicher für Mac und PC herunterzuladen. Nutzen Sie den App Store oder Google Play auf Ihren Mobilgeräten.

4 Verwenden Sie keine sozialen Netzwerke, um Konferenzlinks zu teilen

Leider sind zurzeit an vielen Orten Online-Veranstaltungen die einzige Art von öffentlicher Zusammenkunft, die erlaubt ist, sodass Zoom immer mehr Menschen anzieht. Aber selbst wenn Ihr Event wirklich für alle öffentlich zugänglich ist, sollten Sie es vermeiden, den Link in sozialen Netzwerken zu teilen.
Wenn Sie vor dem Lesen dieses Beitrags etwas über Zoom gewusst haben, haben Sie wahrscheinlich vom sogenannten Zoombombing gehört. Der von Techcrunch-Journalist Josh Constine geprägte Begriff beschreibt die Unterbrechung von Zoom-Meetings mit anstößigen Inhalten durch Trolle. Derzeit diskutieren mehrere Chats auf Discord und Threads auf 4Chan (beide bei Trollen beliebt) Ziele für ihre nächsten Raids. Woher bekommen Trolle Informationen über bevorstehende Ereignisse? Genau, sie finden sie in sozialen Netzwerken. Vermeiden Sie es daher, Links zu Zoom-Meetings zu veröffentlichen. Wenn Sie aus irgendeinem Grund den Link immer noch öffentlich posten möchten, stellen Sie sicher, dass Sie die Option *Persönliche Besprechungs-ID verwenden* nicht aktivieren .

5. Schützen Sie jedes Meeting mit einem Passwort

Die Verwendung eines Kennworts für Ihr Meeting ist nach wie vor das beste Mittel, um sicherzustellen, dass nur die Personen, die Sie in Ihrem Meeting haben möchten, daran teilnehmen können. Kürzlich hat Zoom den Passwortschutz standardmäßig aktiviert – ein guter Schritt. Verwechseln Sie das Passwort für das Meeting jedoch nicht mit Ihrem Kennwort für das Zoom-Konto. Und wie bei Meeting-Links sollten Meeting-Passwörter niemals in sozialen Netzwerken oder anderen öffentlichen Kanälen zugänglich gemacht werden, da sonst Ihre Bemühungen, Ihren Anruf vor Trollen zu schützen, vergeblich sind.

6. Aktivieren Sie den Warteraum
Eine weitere Einstellung, mit der Sie mehr Kontrolle über das Meeting haben. Der kürzlich standardmäßig aktivierte *Warteraum* lässt die Teilnehmer in einen virtuellen „Warteraum“ warten, bis der Gastgeber jeden einzelnen genehmigt. Auf diese Weise können Sie steuern, wer an Ihrem Meeting teilnimmt, auch wenn jemand, der nicht teilnehmen sollte, das Passwort dafür erhalten hat. Außerdem können Sie eine unerwünschte Person aus dem Meeting und in den Warteraum werfen. Wir empfehlen, dieses Kästchen aktiviert zu lassen.

7. Achten Sie auf die Bildschirmfreigabefunktion
Jede normale Videokonferenz-App bietet eine Funktion zur Bildschirmfreigabe, also die Fähigkeit eines Teilnehmers, seinen Bildschirm anderen anzuzeigen und Zoom ist keine Ausnahme. Hier einige Einstellungen, die man beachten sollte:
Beschränkung der Bildschirmfreigabefunktion auf den Leiter oder Ausdehnung auf alle Teilnehmer des Anrufs. Wenn keine andere Person diese Funktion benötigt, wissen Sie genau, welche Option Sie auswählen müssen.
· Gleichzeitige Bildschirmfreigebe für mehrere Teilnehmer. Wenn Sie nicht sofort erkennen können, warum Ihre Besprechungen diese Funktion benötigen sollte, werden Sie sie wahrscheinlich auch nie benötigen. Behalten Sie sie im Hinterkopf, falls Sie sie jemals aktivieren müssen.

8. Nutzen Sie wenn möglich den Webclient
Die verschiedenen Zoom-Apps haben eine Vielzahl an Schwachstellen und Fehlern. Einige Versionen erlauben Hackern den Zugriff auf Kamera und Mikrofon des Geräts, während andere das Hinzufügen von Nutzern in Videokonferenzen ohne deren Zustimmung möglich machte. Zoom hat die oben genannten und ähnliche Probleme bereits behoben und die Weitergabe von Benutzerdaten an Facebook und LinkedIn eingestellt. Angesichts einer fehlenden, ordnungsgemäßen Sicherheitsbewertung bleiben Zoom-Apps jedoch wahrscheinlich angreifbar und sie verwenden möglicherweise weiterhin zwielichtige Methoden, z. B. das Teilen von Daten mit Dritten.

Aus diesem Grund empfehlen wir, wenn möglich, die Weboberfläche von Zoom zu verwenden, anstatt die App auf Ihrem Gerät zu installieren. Die Webversion befindet sich in einer Sandbox im Browser und verfügt nicht über die Berechtigungen einer installierten App, wodurch der Schaden begrenzt wird, den sie möglicherweise verursachen kann.

In einigen Fällen kann es jedoch vorkommen, dass Zoom das Installationsprogramm schon heruntergeladen hat, selbst wenn Sie die Weboberfläche verwenden möchten oder wenn es keine weitere Möglichkeit gibt, als sich den Client herunterzuladen, um am Meeting teilnehmen zu können. In diesem Fall können Sie wenigstens die Anzahl der Geräte, auf denen Zoom installiert ist, auf ein Gerät beschränken. Verwenden Sie ein Zweitgerät wie ein zweites Smartphone oder ein Ersatz-Laptop. Wählen Sie ein Gerät ohne persönliche Informationen. Wir wissen, dass das etwas paranoid klingt, aber Vorsorge ist besser als Nachsorge.
Übrigens, wenn Ihr Unternehmen bereits Skype for Business (früher als Lync bekannt) verwendet, haben Sie eine andere Option. Skype for Business ist mit Zoom kompatibel und kann Zoom-Konferenzgespräche genauso gut verarbeiten – ohne die oben genannten Mängel.

9. Glauben Sie nicht an die von Zoom angekündigte Ende-zu-Ende-Verschlüsselung
Zoom gewann seinen Marktanteil nicht nur aufgrund seiner Preise und Funktionen, sondern auch, weil es Reklame für die End-to-End-Verschlüsselung des Produkts macht. Bei der Ende-zu-Ende-Verschlüsselung wird die gesamte Kommunikation zwischen Ihnen und den anrufenden Personen so verschlüsselt, dass nur Sie und die anrufenden Personen sie entschlüsseln können. Alle anderen Parteien, einschließlich der Dienstleister, können dies nicht.
Klingt cool, ist aber so gut wie unmöglich, wie Sicherheitsexperten hervorgehoben haben. Zoom müsste in dem Fall bestätigen, dass das andere *Ende*, also der Zoom-Server, verschlüsselt ist, was wiederum bedeutet, dass das Video wirklich verschlüsselt ist. Aber Zoom-Mitarbeiter und möglicherweise auch Strafverfolgungsbehörden haben Zugriff darauf. Der Text in Chats scheint jedoch wirklich durchgehend verschlüsselt zu sein. Die irreführende Verschlüsselung ist nicht unbedingt ein Grund, um Zoom endgültig aufzugeben, denn andere beliebte Videokonferenzdienste verfügen ebenfalls nicht über eine Ende-zu-Ende-Verschlüsselung. Sie sollten dies jedoch berücksichtigen und persönliche Gespräche oder geschäftliche Geheimnisse bei Zoom vermeiden.

10. Überlegen Sie, was Menschen sehen oder hören können
Dieser gilt für jeden Videokonferenzdienst, nicht nur für Zoom. Bevor Sie mit dem Anruf beginnen, nehmen Sie sich einen Moment Zeit, um zu überlegen, was die Leute sehen oder hören, wenn Sie sich dem Anruf zuschalten. Selbst wenn Sie alleine zu Hause sind, erwartet man von Ihnen, dass Sie vollständig angezogen sind. Grundlegende Pflege ist wahrscheinlich eine gute Idee.
Gleiches gilt für Ihren Bildschirm, wenn Sie ihn freigeben möchten. Schließen Sie alle Fenster, die andere lieber nicht sehen sollten, egal ob es sich um ein Überraschungsgeschenk handelt, das Sie online für eine