90-Tage-Sicherheitsplan: Wichtige Aktualisierungen mit Stand vom 1. Juli 2020

Am 1. April 2020 **versprachen** wir, einige Verbesserungen im Bereich Sicherheit und Datenschutz vorzunehmen. Mit dem 90-Tage-Programm, das an diesem Tag angekündigt wurde, hat sich unser Unternehmen auf sieben Ziele eingeschworen, die Sicherheit und Datenschutz fest in der DNA von Zoom verankern. Im Folgenden informieren wir Sie über den aktuellen Stand der Umsetzung der jeweiligen Selbstverpflichtungen:

#1: Die Entwicklung weiterer Funktionen mit Wirkung vom 1. April einfrieren und unsere gesamten Ingenieursressourcen auf unsere größten Probleme hinsichtlich Vertrauen, Sicherheit und Datenschutz konzentrieren.

Status: Wir haben die Entwicklung von all den Funktionen, die nicht mit Datenschutz und Sicherheit zu tun haben, für 90 Tage auf Eis gelegt. Wir veröffentlichten **Zoom 5.0** mit AES 256 GCM-Verschlüsselung, dem Sicherheitssymbol und der Funktion „einen Benutzer melden". Außerdem bietet diese Version geänderte Standardeinstellungen für Meetings (standardmäßig aktivierte Kennwörter und Warteräume), schärfere Kontrollen bei Zoom Chat und mehr. Wir **übernahmen Keybase**, begannen mit dem Aufbau unseres End-to-End-Verschlüsselungsangebot für alle Benutzer (kostenlose und kostenpflichtige Konten) und führten eine nach geografischem Standort **angepasste Datenweiterleitung** ein.

#2: Eine umfassende Überprüfung mit Fachleuten von Drittparteien und repräsentativen Benutzern durchführen, um alle unsere neuen Fälle der Verbrauchernutzung zu verstehen und deren Sicherheit zu gewährleisten.

Status: Wir haben mit einer Gruppe von Experten von Drittparteien gearbeitet, um unsere Produkte, Methoden und Richtlinien zu überprüfen und zu verbessern. Darunter waren unser CISO-Rat, Luta Security, Bishop Fox, Trail of Bits, NCC Group, Praetorian, Crowdstrike, Center for Democracy and Technology und andere Organisationen in den Bereichen Datenschutz, Sicherheit und Inklusion.

#3: Einen Transparenzbericht erstellen, der detaillierte Informationen bezüglich dem Abfragen von Daten, Aufzeichnungen oder Inhalt liefert.

Status: Wir haben deutliche Fortschritte gemacht bei der Definition des Rahmens und Ansatzes für einen Transparenzbericht, der ausführliche Informationen zu an Zoom gerichtete Anfragen nach Daten, Aufzeichnungen oder Inhalten bietet. Wir freuen uns darauf, unsere Finanzdaten für das zweite Quartal in unserem im Laufe des Jahres erscheinenden ersten Bericht vorzulegen. Kürzlich haben wir einen **Leitfaden für Anfragen von Regierungsseite** veröffentlicht und auch unsere Datenschutzrichtlinien aktualisiert, in erste Linie, um sie leichter verständlich zu machen. Diese Dokumente finden Sie auf **https://zoom.us/de-de/privacy-and-legal.html**.

#4: Unser aktuelles Fehlerprämienprogramm verbessern.

Status: Wir haben ein zentrales Softwarefehler-Repository und entsprechende Workflowprozesse entwickelt. Dieses Repository nimmt Berichte zu Sicherheitsrisiken von HackerOne, Bugcrowd und **security@zoom.us** (letzteres erfordert keine Geheimhaltungsvereinbarung) auf, die durch Praetorian vorselektiert wurden. Wir haben einen fortlaufenden Überprüfungsprozess mit täglichen Meetings eingeführt und unsere Kommunikation mit Sicherheitsexperten und externen Gutachtern verbessert. Wir haben einen Head of Vulnerability and Bug Bounty und mehrere zusätzliche Ingenieure für Anwendungssicherheit eingestellt und sind dabei, weitere Sicherheitsingenieure, die sich alle speziell mit Sicherheitsrisiken beschäftigen werden, anzuwerben.

#5: Einen CISO-Rat in Partnerschaft mit führenden CISOs aus der ganzen Industrie ins Leben rufen, um einen laufenden Dialog über die besten Praktiken in den Bereichen Sicherheit und Datenschutz fördernd zu begleiten.

Status: Wir haben unseren CISO-Rat ins Leben gerufen, der von Gary Sorrentino, unserem Global Deputy CIO, geleitet wird und 36 CIOs von Unternehmen unterschiedlicher Branchen, einschließlich SentinelOne, Arizona State University, HSBC und Sanof, zu seinen Mitgliedern zählt. Dieser Rat ist in den letzten drei Monaten vier Mal zusammengetreten und hat uns in wichtigen Fragen wie der Auswahl regionaler Rechenzentren, Verschlüsselung, Authentifizierung von Meetings und wesentliche Sicherheitsfunktionen beraten.

#6: Eine Reihe von simultanen Whitebox Penetrationstests einsetzen, um weiterhin Probleme zu identifizieren und anzugehen.

Status: Zoom hat mehrere Firmen –Trail of Bits, NCC Group und Bishop Fox – mit der Überprüfung unser gesamten Plattform beauftragt. Zu ihrem Auftragsumfang gehörten die Produktionsumgebung, die Kern-Webanwendung und das Unternehmensnetzwerk von Zoom sowie die öffentlichen API für übliche Clients.

#7: Jeden Mittwoch ein wöchentliches Webinar veranstalten, um unsere Community bei Datenschutz und Sicherheit auf den neuesten Stand zu bringen.

Status: Seit dem 1. April haben wir jeweils mittwochs insgesamt 13 Webinare veranstaltet, bei der einige unserer Führungskräfte und Berater anwesend waren und live Fragen von den Teilnehmern beantworteten.

Andere wichtige Aktualisierungen:

- Seit 1. April haben wir mehrere neue Führungskräfte gewonnen oder personelle Veränderungen auf der obersten Führungsebene durchgeführt:
  - **Velchamy Sankarlingam** President of Product and Engineering
  - **Jason Lee**, Chief Information Security Officer
  - **Damien Hooper-Campbell**, Chief Diversity Officer
  - **H.R. McMaster** in den Zoom Vorstand berufen
  - **Josh Kallmer**, Global Head of Public Policy and Government Relations,
  - Head of Vulnerability and Bug Bounty, fängt am 13. Juli an
  - Andy Grant, Head of Offensive Security, fängt am 13. Juli an
- **Zoom Phone zu Zoom für Behörden hinzugefügt**, welches bereits nach dem U.S. Federal Risk and Authorization Management Program (FedRAMP) autorisiert ist
- Wir sind weiterhin fest entschlossen, unser Ingenieursteam in den USA deutlich zu vergrößern, um durch unsere **neuen Niederlassungen** in Phoenix, Arizona und Pittsburgh, Pennsylvania die verstärkte Nutzung von Zoom zu unterstützen