LOGITECH VIDEOKONFERENZ-LÖSUNGEN – SICHERHEIT & DATENSCHUTZ

EINLEITUNG

Cyber-Angriffe werden weltweit immer häufiger und ausgeklügelter. Sie stellen erhebliche Risiken für Unternehmen dar, die auf einen hybriden Arbeitsplatz setzen, der Tag für Tag verteilter und virtueller wird.

Cyberkriminalität kann heutzutage immer und überall stattfinden. Dabei nutzen Hacker Schwachstellen in der Software und Hardware aus, etwa Kameras, Headsets und andere Geräte.

In diesem Whitepaper erläutern wir unseren Ansatz bezüglich Sicherheit und Datenschutz für Geräte mit CollabOS. Dazu gehören derzeit Rally Bar, Rally Bar Mini, RoomMate, Tap Scheduler und Tap IP.

WAS IST COLLABOS?

CollabOS ist das einheitliche Betriebssystem für ausgewählte Videokonferenzgeräte von Logitech. Mit CollabOS arbeiten diese Geräte nahtlos zusammen, werden kontinuierlich optimiert und lassen sich einfacher als je zuvor implementieren und verwalten. So können Sie allen Beteiligten ein qualitativ hochwertiges und einheitliches Meetingerlebnis bieten.

CollabOS vereinfacht die Bereitstellung und Verwaltung von Videokonferenzen weiter, indem Logitech Hardware und Anwendungen sowie Planungsdienste von Drittanbietern (z. B. Microsoft Teams, Zoom und Robin) integriert werden.

CollabOS verbessert kontinuierlich die Benutzererfahrung von Teilnehmern an Videobesprechungen und verlängert gleichzeitig die Lebensdauer Ihrer Investitionen in Videokonferenzen. Firmware-Updates mit neuen Funktionen, Verbesserungen und Sicherheitsvorkehrungen werden automatisch und ohne zusätzliche Kosten im Over-the-Air-Verfahren an die Geräte ausgeliefert.

GERÄTE MIT COLLABOS

- **Rally Bar** und **Rally Bar Mini** sind erstklassige All-in-one-Videobars von Logitech für große, mittelgroße und kleine Konferenzräume. Sie sind mit einer einzigartigen optischen Kamera, simultanem Zwei-Wege-Audio und einer sekundären dedizierten KI-Kamera ausgestattet. Beide Videobars können im USB- oder Appliance-Modus bereitgestellt werden und zeichnen sich durch außergewöhnliche Flexibilität und Benutzerfreundlichkeit aus.

  Mehr über Rally Bar und Rally Bar Mini erfahren

- **RoomMate** ist eine Videokonferenz-Appliance für unterstützte Konferenzkameras und Peripheriegeräte, darunter das Rally System, MeetUp und Audiogeräte von Drittanbietern. RoomMate ermöglicht eine einfache Bereitstellung von Microsoft Teams® Rooms auf Android, Zoom Rooms Appliances und anderen führenden Videokonferenzdiensten.

  Mehr über RoomMate erfahren

- **Tap IP** ist ein Touch-Controller für das Netzwerk, der die einfache Teilnahme an Videokonferenzen über verschiedene Plattformen und Anwendungen hinweg ermöglicht. Mit einem großen 10,1-Zoll-Display, einem flachen Profil und einem Bewegungssensor für die sofortige Einsatzbereitschaft ermöglicht Tap IP das einfache Teilen von Inhalten und ein einheitliches Meeting-Erlebnis in allen Räumen.

  Mehr über Tap IP erfahren

- **Tap Scheduler** ist ein speziell entwickeltes Planungspanel für Konferenzräume, das den Arbeitsalltag erleichtert. Tap Scheduler macht es einfach, Besprechungsdetails einzusehen und einen Raum für Ad-hoc- oder zukünftige Besprechungen zu reservieren. Farbige LEDs lassen die Verfügbarkeit auch aus der Ferne erkennen, sodass Mitarbeiter schnell einen freien Raum finden.

  Mehr über Tap Scheduler erfahren

SICHERHEIT UND DATENSCHUTZ

Sicherheit und Datenschutz spielen bei der Entwicklung aller Videokonferenzprodukte von Logitech eine wichtige Rolle. CollabOS basiert auf Android 10, das Sicherheit, Datenschutz und Performance auf Spitzenniveau bietet.

Bei der Entwicklung von Logitech Produkten setzen wir auf einen sicheren Entwicklungslebenszyklus, in dessen Rahmen wir bei Produktdesign, -entwicklung und -einführung die Best Practices der Branche einhalten. Den Erwartungen an die Sicherheit werden wir gerecht und übertreffen sie mitunter sogar, indem wir die Sicherheit bereits in den frühesten Designphasen berücksichtigen.

Dies umfasst eine Prüfung des Produktdesigns durch einen Sicherheits-Untersuchungsausschuss mit Sicherheitsexperten aus dem gesamten Unternehmen. Bei der Entwicklung und beim Testen wird die Sicherheit von Systemen und Software nach strengen Kriterien geprüft. Außerdem nutzen wir das STRIDE-Modell, den Branchenstandard zur Klassifizierung von Sicherheitsrisiken.

Hinweis: Sofern nicht anders angegeben, gelten die in diesem Whitepaper beschriebenen Sicherheits- und Datenschutzmerkmale für alle fünf oben aufgeführten Geräte, die im vorliegenden Whitepaper als „CollabOS Geräte" bezeichnet werden.

INFORMATIONSSICHERHEIT

SICHERER ENTWICKLUNGSLEBENS-ZYKLUS (SECURE DEVELOPMENT LIFECYCLE, SDLC)

In jeder Phase der Systementwicklung für den SDLC von Logitech für CollabOS Geräte finden Sicherheitsüberprüfungen statt. Dies umfasst Design, Implementierung und Veröffentlichung. In der Designphase werden alle Designdokumente von internen und externen Sicherheitsexperten geprüft.

Die Implementierungsphase umfasst sowohl automatisierte als auch persönliche Prüfungen des Codes des Entwicklungsteams. Für sämtlichen Quellcode werden statische Analysen durchgeführt, in deren Rahmen Probleme identifiziert und vom Entwicklungsteam und von Sicherheitsexperten untersucht werden.

Bei der Entwicklung der Software für CollabOS Geräte werden Branchenstandards wie die folgenden angewendet (keine vollständige Liste):

- Android Secure Coding Standard
- SEI CERT Oracle Coding Standard for Java
- SEI CERT C Coding Standard
- SEI CERT C++ Coding Standard

Bevor Software veröffentlicht wird, wird sie einer Reihe von umfassenden Funktions- und Sicherheitstests unterzogen. Der SDLC wird auch bei Systemupdates und Neuveröffentlichungen angewendet. Außerdem wird die Software, die bereits im Einsatz ist, gepflegt und mit Sicherheitspatches aktualisiert, um Probleme zu beheben, die zwischen Hauptversionen erkannt werden.

SICHERHEIT UND DATENSCHUTZ VON ANFANG AN

Bei CollabOS Geräten sind Sicherheit und Datenschutz von Anfang an feste Bestandteile – vom Beginn der Produktentwicklung über die Implementierung und Veröffentlichung bis hin zu den Updates.

Im Folgenden finden Sie eine Auswahl der Maßnahmen, mit denen wir die Sicherheit dieser Geräte gewährleisten:

- **Mit einer starken Grundlage beginnen:** Die Plattform basiert auf Android 10, das Verbesserungen in den Bereichen Sicherheit und Stabilität mit sich bringt.
- **Universelle Standardkennwörter vermeiden:** Die CollabOS Geräte von Logitech entsprechen den Best Practices der Branche und den Gesetzen des US-Bundesstaats Kalifornien, die die Verwendung von universellen Standardkennwörtern verbieten. Die Geräte haben kein Standardkennwort.
- **Software auf dem neuesten Stand halten:** Mit Firmware-Updates nach dem Over-the-Air-Prinzip werden CollabOS Geräte ständig auf dem neuesten Stand gehalten.
- **Software-Integrität bewahren:** Alle Software-Images werden während der Produktion digital signiert und über sichere Verbindungen verteilt. CollabOS Geräte überprüfen die Signatur jedes Software-Images, bevor die Software installiert oder aktualisiert wird. So werden Integrität und Echtheit der Software bewahrt.
- **Sicher kommunizieren:** Ab CollabOS Version 1.7 werden für die gesamte Kommunikation zwischen CollabOS Geräten und der Cloud die Transport Level Security (TLS)-Versionen 1.2 und 1.3 verwendet. TLS 1.1 und 1.0 sind auf CollabOS Geräten deaktiviert und werden bei Sicherheitsscans nicht mehr angezeigt. Anwendungen, die auf der Plattform ausgeführt werden, können ähnliche oder zusätzliche Arten der Datenübertragung verwenden. Wir empfehlen Ihnen, Ihren App-Diensteanbieter zu fragen, welche Sicherheitsprotokolle unterstützt werden.
- **Persönliche Daten schützen:** Auch wenn auf CollabOS Geräten keine personenbezogenen Daten vorgehalten oder gespeichert werden, speichern Anbieter von Videodiensten unter Umständen solche Daten in ihren Apps. Wir empfehlen Ihnen, sich bei den Dienstanbietern über ihre Richtlinie zu personenbezogenen Daten zu informieren.

INFORMATIONSSICHERHEIT

SICHERHEIT DER APPS AUF DEN GERÄTEN

CollabOS Geräte enthalten mehrere Anwendungen, die für den alltäglichen Betrieb benötigt werden. Um die Sicherheit des Geräts sicherzustellen, achtet Logitech sorgfältig darauf, welche Anwendungen sich auf dem Gerät befinden dürfen.

Wir steuern mithilfe von Whitelists, welche Anwendungen genutzt werden können. Zum Sichern der Software vor der Auslieferung entfernen wir außerdem alle Apps, Dienste und Gerätetreiber, die nicht unbedingt erforderlich sind. Dadurch verringert sich die Angriffsfläche. Alle CollabOS Geräte greifen auf die integrierten SELinux-Richtlinien zurück, die ein Bestandteil des Android-Systems sind.

ANTI-ROLLBACK-FUNKTION

Die von CollabOS unterstützten Geräte verfügen über eine Funktion, die sicherstellt, dass ein aktualisiertes System nicht auf eine frühere (und möglicherweise weniger sichere) Software zurückgesetzt wird.

HARDWARESICHERHEIT

Alle von CollabOS unterstützten Geräte sind mit mehreren Merkmalen ausgestattet, die die Sicherheit des Geräts erhöhen. Erforderliche Geheimnisse und Schlüssel auf dem Gerät werden mithilfe einer vertrauenswürdigen Enklave geschützt. Für die Hardware wird ein sicheres Startverfahren genutzt, um sicherzustellen, dass die Boot-Software und die System-Firmware gültig sind (beide wurden bei der Produktion signiert).

PRÜFUNG DER SICHERHEIT

Für interne Qualitätssicherungsprozesse werden Tools zum Testen der Sicherheit der Softwarekomponenten eingesetzt, um jede Softwareversion auf Sicherheitsprobleme zu prüfen. Die Software kann nur veröffentlicht werden, wenn alle Tests bestanden werden.

FIREWALL-REGELN – PORTS FILTERN/ BLOCKIEREN

Alle CollabOS Geräte implementieren ihre eigenen Firewall-Regeln zum Filtern und Blockieren von Ports, sodass über das Netzwerk weniger Angriffsfläche geboten wird.

ANZEIGEN FÜR AUFNAHMEN UND DATENSCHUTZ AUF EXTERNEN GERÄTEN

Bei allen CollabOS Aufnahmegeräten, einschließlich Mikrofonen und Kameras, wird klar und deutlich angezeigt, wenn sie verwendet werden. Im Lieferumfang von Rally Bar und Rally Bar Mini sind Objektivabdeckungen für die Konferenzkameras enthalten.

Hinweis: Dies gilt nicht für Tap IP, Tap Scheduler oder RoomMate, die keine Kameras oder Mikrofone haben und weder Video noch Audio aufzeichnen können.

SANDBOXING-METHODE FÜR ANWENDUNGEN

Mithilfe einer integrierten Sandbox-Methode für Anwendungen wird verhindert, dass sich die Anwendungen auf der Plattform gegenseitig stören. Für jede Anwendung und die zugehörigen Daten gibt es einen eigenen Arbeitsbereich. Mithilfe dieser Bereiche wird auch verhindert, dass eine Anwendung mit anderen Anwendungen kommuniziert oder ihre Ausführung verhindert. Dazu zählt auch das Lesen und Schreiben von Daten, das nur in der jeweiligen Anwendungs-Sandbox möglich ist.

DATEN SICHERN – VERSCHLÜSSELTER SPEICHER

Bei von CollabOS unterstützten Geräten werden alle Daten in einem Speicher abgelegt, der auf Hardware-Ebene verschlüsselt ist.

DATENSICHERHEIT AUF DEM BACK-END

Die Kommunikation zwischen CollabOS Geräten und Logitech Back-End-Systemen, die diese unterstützen, erfolgt ausschließlich über verschlüsselte Kanäle mit Transport Layer Security (TLS). Das gilt auch für Over-the-Air-Updates. Dies ermöglicht sowohl die Verschlüsselung der Daten bei der Übertragung als auch die Authentifizierung des Systems, mit dem das Gerät kommuniziert.

Wir nutzen das IoT-Framework (Internet of Things) von Amazon und die zugehörige Infrastruktur, um die sichere Datenübertragung zwischen dem Gerät und dem Back-End zu ermöglichen und die Daten in der Cloud zu schützen.

SCHWACHSTELLEN- UND RISIKO-MANAGEMENT

Wir beobachten die Sicherheit unserer Produkte aktiv und stellen zeitnah Updates bereit, um bekannte Schwachstellen zu beheben.

REAKTION BEI VORFÄLLEN

Logitech freut sich, wenn Kunden oder Sicherheitsforscher Probleme melden, die sie in unseren Produkten finden, damit wir diese beheben können. Wir nehmen an einem öffentlichen Bug-Bounty-Programm teil, in dessen Rahmen Forscher einen Beitrag zur Sicherheit unserer Produkte leisten können, indem sie Probleme melden und für ihre Erkenntnisse gewürdigt werden. Logitech würdigt verantwortungsbewusste Melder von Sicherheitsvorfällen, die sich als korrekt und umsetzbar erweisen.

Außerdem werden Vorfälle erfasst und so schnell wie möglich behoben. Wir erwarten von den Personen, die Vorfälle melden, dass sie die akzeptierten Vorgehensweisen für eine verantwortungsbewusste Offenlegung einhalten.

WEITERE MATERIALIEN

Weitere Informationen zu den von CollabOS unterstützten Geräten, etwa Rally Bar, Rally Bar Mini, RoomMate, Tap IP und Tap Scheduler, finden Sie unter logitech.com/vc.

KONTAKT

Wenn Sie Bedenken im Hinblick auf die Sicherheit von Logitech Produkten haben, können Sie sich über die Seite logitech.com/security an uns wenden. Für Anfragen anderer Art rufen Sie bitte logitech.com/contact auf.

Logitech Inc.
7700 Gateway Blvd.
Newark, CA 94560, USA
Veröffentlicht im
November 2023