LOGITECH SYNC

WHITEPAPER SICHERHEIT UND DATENSCHUTZ

logitech®

EINLEITUNG

Logitech® Sync macht die Verwaltung von Konferenzräumen und Logitech-Geräten einfach und intuitiv. Sync besteht aus einer sicheren, cloudbasierten Architektur und unterstützt Sie dabei, Videokonferenzen im großen Umfang einzusetzen und zu verwalten. Dieses Whitepaper erklärt, wie Logitech Sync die Sicherheit und den Datenschutz von Kundendaten, Firmware-Versionen und Software-Entwicklung handhabt.

Logitech ist weltweit führend in der Entwicklung von Lösungen für Hardware, Software und Services und verbindet Menschen mit den für sie wichtigen digitalen Erfahrungen. Wir bieten eine Reihe von Tools für die Zusammenarbeit, die einfach zu bedienen sind. Außerdem unterstützen wir Sie mit einer einfach zu bedienenden Software bei der Überwachung und Verwaltung Ihrer Videokonferenz-Lösungen, damit virtuelle Teams effektiver arbeiten können.

Logitech Sync ist ein integraler Bestandteil unserer Videokonferenz-Lösungen. Sync ist eine cloudbasierte Plattform zur Geräteverwaltung, mit der die IT-Abteilung die Geräte von Logitech für Konferenzräume skalierbar verwalten und überwachen kann. Sync funktioniert in Verbindung mit der Logitech Sync App, die auf einem Computer oder einem Videogerät im Konferenzraum läuft.

Sync verarbeitet Daten und Informationen, die von Hardware-Geräten übermittelt werden und stellt IT-Administratoren verwertbare Daten zur Überwachung, Verwaltung und Raumübersicht zur Verfügung. Sync-Benutzer können sich einfach bei dem speziellen Webportal unter sync.logitech.com anmelden, um ihre Logitech-Geräte zu verwalten.

Dieser neue Ansatz für die Remote-Überwachung und die Geräteverwaltung vereinfacht Aufgaben wie Firmware-Updates und Funktionsaktivierung. Eine API (Programmierschnittstelle) und eine zukunftsweisende Architektur bilden die solide Grundlage für Weiterentwicklungen und Integrationen.

Natürlich sind IT-Verantwortliche über die Sicherheit und den Datenschutz im Umgang mit Daten und Software-Updates besorgt. Um dieses Thema aufzugreifen, haben wir das folgende Whitepaper erstellt, in dem der Umgang von Logitech Sync mit persönlichen Daten und die Bereitstellung von Firmware-Versionen erläutert wird. Wir verwenden diese Daten in Übereinstimmung mit den Datenschutzrichtlinien und Nutzungsbedingungen von Logitech.

Hinweis: Die aktuellste Version dieses Whitepapers finden Sie auf der Website von Logitech.

SECURITY GOVERNANCE BEI LOGITECH

Kunden können sich darauf verlassen, dass Logitech Best Practices für die Informationssicherheit etabliert und implementiert. Alle Sicherheitsprotokolle für die Entwicklung von Software für Videokonferenzen basieren auf NIST 800-53 und ISO/IEC 27001:2013. Unsere Sicherheitsprozesse werden von einer Vielzahl von Produkt-Stakeholdern verwaltet, vom Produktmanagement bis hin zur Entwicklung, die diese Sicherheitsstandards als operative Grundprinzipien in unserem Secure Software Development Lifecycle (SSDLC) anwenden.

KONTINUIERLICHE INTEGRATION UND BEREITSTELLUNG

Logitech implementiert eine bewährte Pipeline für die kontinuierliche Integration und Auslieferung (Continuous Integration and Delivery, CI/CD), die strenge technische Anforderungen durchsetzt, um die Qualität der Software sicherzustellen, bevor neue Änderungen in die Produktion gelangen. Der Prozess optimiert die Qualitätssicherung einschließlich aber nicht beschränkt auf Funktionstests, Sicherheitstests, Integrationstests und Änderungsgenehmigungen durch alle Stakeholder. Unser Bereitstellungsprozess stellt sicher, dass das neue Software-Release nahtlos bereitgestellt wird, ohne die Servicebereitschaft zu beeinträchtigen.

TESTS DER ANWENDUNGSSICHERHEIT

Logitech führt Sicherheitstests durch externe Sicherheitsberater durch, um Schwachstellen zu identifizieren. Die Tests berücksichtigen allgemeine Sicherheitsschwächen, wie sie im Open Web Application Security Project (OWASP) und in der Common Weakness Enumeration (CWE) von MITRE beschrieben werden, sind aber nicht darauf beschränkt. Unter anderem umfassen sie: Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) und die Bewertung der Cloud-Service-Konfiguration. Sollten im Rahmen der Tests Schwachstellen entdeckt werden, wird Logitech alle vom Anbieter identifizierten Sicherheitsprobleme beheben. Die Sicherheitsbewertung von Drittanbietern wird bei größeren Versionen durchgeführt, aber Logitech führt auch während der Entwicklungszyklen internes SAST und DAST durch.

BENUTZERAUTHENTIFIZIERUNG UND -AUTORISIERUNG

Wenn sich die Benutzer von Sync beim Webportal anmelden, um ihre Logitech-Geräte zu verwalten, verwendet das Sync Portal Token-basierte und rollenbasierte Zugriffsmechanismen, um sie zu authentifizieren und den Zugriffsbereich zu autorisieren. Benutzer können Daten je nach zugewiesener Rolle im System anzeigen oder ändern. Jedes Sicherheitstoken ist außerdem sitzungsbasiert und für eine bestimmte Zeit gültig. Sobald das Token abläuft, muss der Benutzer den Zugriff durch erneute Eingabe seiner Anmeldedaten aktualisieren, um die Sicherheit des Systems zu gewährleisten.

SINGLE SIGN-ON (SSO)-INTEGRATIONEN

Der Authentifizierungsdienst des Logitech Sync Portals unterstützt Single Sign-On (SSO) und kann mit Standard-SAML 2.0 Identity Providers (IdP) wie Azure Active Directory und Okta integriert werden. Diese Provider ermöglichen es dem Sync Portal, Benutzer mit den Anmeldeinformationen ihres Unternehmens zu authentifizieren, ohne separate Anmeldeinformationen zu verwalten, während sie die Sync-Plattform nutzen.

DATA-IN-TRANSIT

Logitech Sync besteht aus zwei Teilen: der Desktopanwendung Sync, die auf Ihrer Hardware im Raum läuft, und dem cloudbasierten Sync Portal. Nach der Installation und Authentifizierung kommuniziert die Sync-Anwendung direkt mit dem Sync Portal, um die Fernverwaltung, Überwachungsfunktionen und verschiedene Informationen zur Raumnutzung und -leistung zu aktivieren.

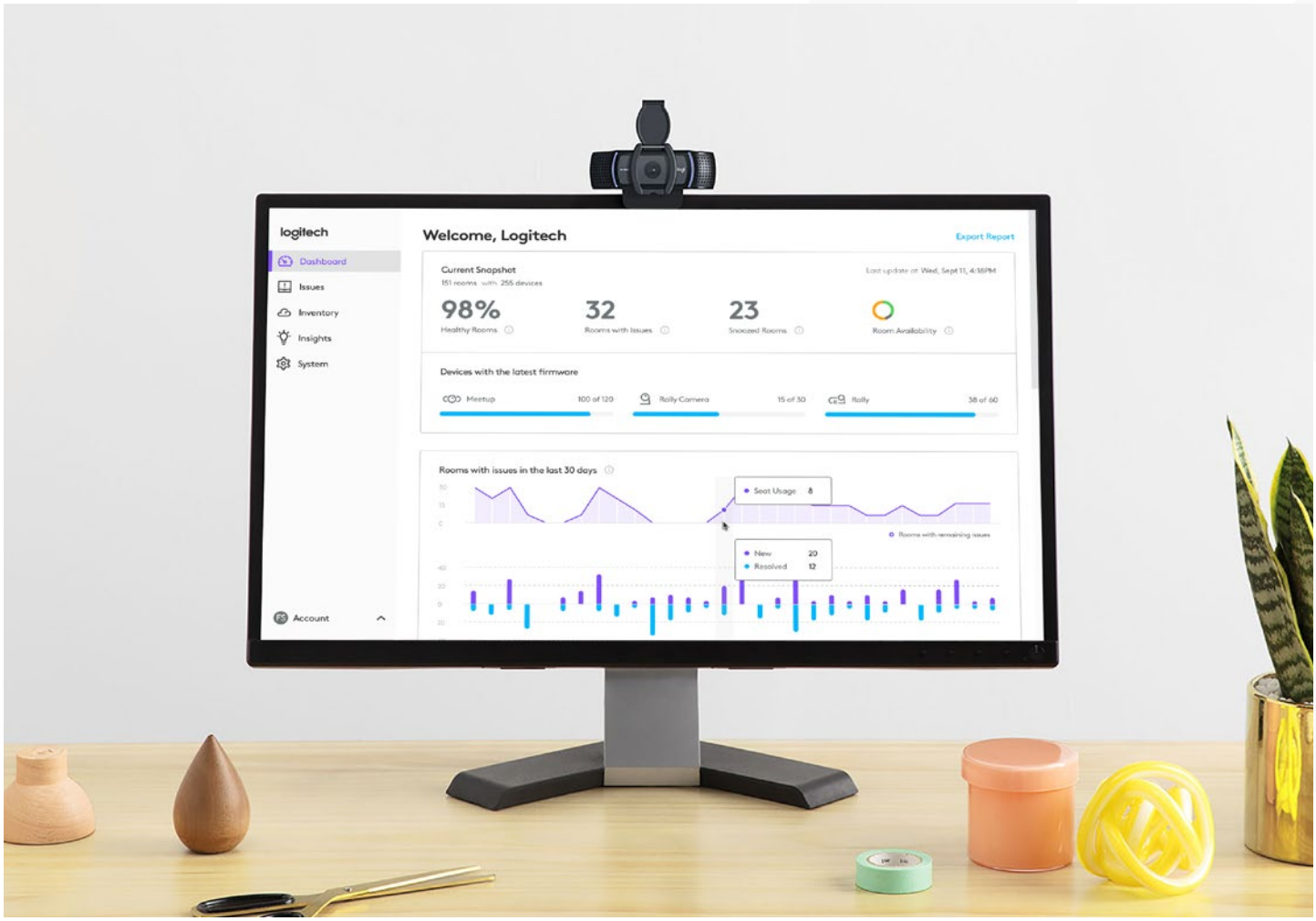
Die gesamte Kommunikation[1] zwischen dem cloudbasierten Logitech Sync Portal und Ihrer Sync-Anwendung erfolgt über die Netzwerkprotokolle HTTPS und MQTT. Der Datenverkehr beider Protokolle wird mittels Transport Level Security (TLS) Version 1.2 oder höher mit Unterstützung von AES-128/256-Bit-Chiffre-Suiten authentifiziert und verschlüsselt, um die Vertraulichkeit und Datenintegrität im Internet zu gewährleisten.

DATA-AT-REST

Die Kundendaten im Backend-Service von Sync werden innerhalb der Datenbank mit der stärksten Verschlüsselung des Standards AES-256 Bit geschützt. Außerdem werden die Verschlüsselungscodes zusätzlich verschlüsselt und zentral von den AWS-Datenservices verwaltet, um die Kundendaten vor Datenschutzverletzungen zu schützen.

SERVICEVERFÜGBARKEIT UND DISASTER RECOVERY

Um einen Service rund um die Uhr zu gewährleisten, wurde Logitech Sync mit einer fehlertoleranten Softwarearchitektur und -infrastruktur für einen hochverfügbaren Service entwickelt. Um Hochverfügbarkeit zu erreichen, sind die Rechenressourcen stark skalierbar und lastverteilt. Die aktuellen Daten werden auf Servern an der US-Westküste gehostet und die Daten werden kontinuierlich im Rechenzentrum gesichert. Im Notfall kann Logitech Sync jederzeit und in jeder Region wiederhergestellt werden, ohne Unterbrechung des Dienstes innerhalb der letzten 35 Tage.



DATENERFASSUNG UND DATENSCHUTZ

Die Datenschutz- und Sicherheitsrichtlinien beschreiben, welche Daten Logitech erfasst, wie wir sie verwenden und wie wir persönliche Informationen schützen, die durch unsere Produkte, Services, Apps und Software erfasst werden. Logitech ist eine Unternehmensgruppe, die unter ihrer Muttergesellschaft, der Logitech International S.A., arbeitet. Das Unternehmen von Logitech, das Ihre Daten verwaltet, hängt von Ihrer Beziehung zu uns ab (sei es als Kunde, Partner, Auftragnehmer oder eine andere relevante Beziehung). Wir nehmen zu keinem Zeitpunkt Ton, Video oder statische Bilder aus einem Konferenzraum in die Cloud auf oder speichern diese. In der folgenden Tabelle 1.1 finden Sie eine vollständige Auflistung der von uns erfassten Daten und deren Verwendung.

Quelle der Datenerfassung	Art der erfassten Daten	Zweck der Datenerfassung	Daten-speicher
Sync Portal (Registrierung und Kontoerstellung)	• E-Mail-Adresse • Kennwort • Vorname • Nachname • Name des Unternehmens	Benutzerauthentifizierung und Kontoerstellung für Einzelpersonen.	AWS
Sync Portal (zusätzliche, vom Benutzer bereitgestellte Informationen)	• Raumname • Anzahl der Plätze • Gruppennamen	Identifizierung und Gruppierung von Räumen innerhalb von Sync. Die Anzahl der Plätze wird zur Berechnung der Nutzung der Plätze in Kombination mit den Metadaten zur Raumbelegung verwendet.	AWS
Sync App (installiert auf dem PC im Konferenzraum oder auf einem Gerät, z. B. Logitech Rally Bar)	• Gerätename • Eindeutige Geräteidentifikation • Firmware-Version • Seriennummer des Geräts • Sync App-Version • Betriebssystem des Computers • Betriebssystem-Version des Computers • IP/MAC-Adresse • Metadaten-Spezifikationen des Computers • Belegung des Konferenzraums (nur Metadaten)	Die Informationen werden verwendet, um Funktionen zur Überwachung, Verwaltung und Analyse über das Sync Portal bereitzustellen.	AWS

DATENSCHUTZ

ZUGRIFF AUF SERVICE- UND KUNDENDATEN

Logitech schließt Verträge mit AWS-Plattformen ab, um unsere Software-Services und die Benutzerdaten zu hosten. AWS implementiert strenge Betriebsrichtlinien, Schutzschichten und Überwachungen, um sicherzustellen, dass nur zugelassene Mitarbeiter Zugang zu den Rechenzentren haben.

Bei Logitech ist der Zugriff auf die Kundendatenbank und die Service-Einstellungen auf eine kleine Gruppe zugelassener Personen beschränkt, die für die Wartung und den Support des Services verantwortlich sind.

DATENSPEICHERUNG UND -LÖSCHUNG

Sobald sich ein Kunde für Logitech Sync anmeldet, werden alle regelmäßig erfassten Benutzer- und Gerätedaten innerhalb des Services gespeichert, bis der Kunde sich entscheidet, den Service zu deaktivieren. Um den Service zu deaktivieren, sollten Kunden ihre Anfrage über das Webformular unter support.logitech.com/response-center stellen. Logitech wird dann den Löschvorgang mit dem Kunden durchgehen. Sobald das Konto als gelöscht markiert wurde, werden alle Kundendaten außer den Produktprotokollen sofort dauerhaft gelöscht.

REAKTION BEI VORFÄLLEN

Logitech ist bestrebt, seinen Kunden sichere Produkte und Services zu bieten und begrüßt Berichte von unabhängigen Forschern, Branchenorganisationen, Anbietern, Kunden und anderen Quellen, die sich mit dem Thema Sicherheit befassen. Logitech definiert eine Sicherheitslücke als eine unbeabsichtigte Schwachstelle in einem Produkt, die es einem Angreifer ermöglichen könnte, die Integrität, Verfügbarkeit oder Vertraulichkeit eines Produkts, einer Software oder eines Services zu gefährden.

Logitech Security setzt verschiedene Metriken ein, um Latenzzeiten, Schwellenwerte und Fehlerquoten des Datenverkehrs auf verdächtige Aktivitäten zu überwachen. Außerdem werden regelmäßig Sicherheitstests von Drittanbietern bei größeren Releases durchgeführt, um die Sicherheit des Produkts zu gewährleisten. Etwaige Schwachstellen werden entsprechend behoben.

Sollten Sie auf einen Fehler stoßen, untersucht das Produktteam in Zusammenarbeit mit Logitech Security umgehend unternehmensweit die gemeldeten Auffälligkeiten und vermuteten Sicherheitslücken. Sie können Ihre Sicherheitsanliegen oder Sicherheitslücken bei Logitech über unsere Seite zur Offenlegung von Sicherheitslücken oder über die Seite des Bug Bounty-Programms melden.

logitech

Wenden Sie sich an Ihren Händler oder kontaktieren Sie uns unter www.logitech.com/vcsales

Logitech Americas
7700 Gateway Blvd.
Newark, CA 94560, USA

Logitech Europe S.A.
EPFL – Quartier de l'Innovation
Daniel Borel Innovation Center
CH - 1015 Lausanne

Logitech Asia Pacific Ltd.
Tel: 852-2821-5900
Fax: 852-2520-2230

[1] 2021 wird es ein Firmware-Update für Logitech Meetup, Rally, Rally Cam, Tap und Swytch geben, um die vollständige Verschlüsselung für diese neueren Geräte zu konfigurieren.

Veröffentlicht im Juni 2021