LOGITECH SYNC

WHITEPAPER OVER BEVEILIGING EN PRIVACY

logitech®

INLEIDING

Logitech® Sync maakt het beheer van vergaderruimtes en Logitech-apparaten eenvoudig en intuïtief. Sync is gebaseerd op een veilig netwerk in de cloud en u kunt hiermee op schaal videovergaderingen implementeren en beheren. In deze whitepaper wordt uitgelegd hoe Logitech Sync omgaat met de beveiliging en privacy van klantgegevens, firmware-releases en de ontwikkeling van software.

Logitech is een wereldleider in het ontwikkelen van oplossingen voor hardware, software en services. Bovendien verbindt Logitech mensen met de digitale ervaringen die zij belangrijk vinden. We bieden een reeks eenvoudig te gebruiken samenwerkingstools. Verder leveren we eenvoudig te gebruiken software zodat u uw oplossingen voor videosamenwerking kunt contoleren, beheren en er inzichten over ontvangt. Op deze manier kunnen virtuele teams effectiever werken.

Logitech Sync is een integraal onderdeel van onze oplossingen voor videosamenwerking. Sync is een cloudgebaseerd platform voor apparaatbeheer waarmee de IT-afdeling Logitech-apparaten in vergaderruimtes op schaal kan beheren en controleren. Het werkt in combinatie met de Logitech Sync-app die werkt op een computer of een video-apparaat in de vergaderruimte.

Sync verwerkt gegevens en informatie van hardware-apparaten en biedt IT-beheerders concrete gegevens met betrekking tot controle, beheer en ruimte-inzichten. Sync-gebruikers kunnen zich eenvoudig aanmelden bij het speciale webportal op sync.logitech.com om hun Logitech-apparaten te beheren.

Deze nieuwe aanpak van externe bewaking en apparaatbeheer vereenvoudigt taken zoals firmware-updates en functie-implementatie, terwijl een API en toekomstgerichte architectuur een robuuste basis vormen voor nieuwe inzichten en integraties.

IT-managers maken zich natuurlijk zorgen over de beveiliging en privacy als het gaat om het verwerken van gegevens en software-updates. Om dit onderwerp aan te pakken, hebben we de volgende whitepaper opgesteld. Hierin wordt besproken hoe Logitech Sync omgaat met persoonlijke gegevens en firmware-releases. We gebruiken dergelijke gegevens op een manier die in overeenstemming is met het Privacybeleid van Logitech en de Servicevoorwaarden.

Opmerking: De meest recente versie van deze whitepaper is te vinden op de Logitech-website.

VEILIGHEIDSBEHEER BIJ LOGITECH

Klanten kunnen erop vertrouwen dat Logitech best-practice beveiligingsprocessen voor informatie vaststelt en implementeert. Alle beveiligingsprotocollen die voor de ontwikkeling van videosamenwerkingssoftware worden gebruikt, hanteren NIST 800-53 en ISO/IEC 27001:2013 als richtlijnen. Onze beveiligingsprocessen worden beheerd door een diverse groep belanghebbenden bij het product, variërend van productbeheer tot techniek. Zij passen deze beveiligingsnormen toe in onze Secure Software Development Lifecycle (SSDLC), als kernprincipes van het bedrijf.

CONTINUE INTEGRATIE EN LEVERING

Logitech implementeert Continue integratie en levering (CI/CD), een gevestigde pijplijn die strikte technische eisen oplegt om de kwaliteit van de software te waarborgen voordat nieuwe wijzigingen in productie worden doorgevoerd. Het proces stroomlijnt de kwaliteitsbewaking, waaronder (maar niet beperkt tot) functionele tests, beveiligingstests, integratietests en de goedkeuring van wijzigingen door alle belanghebbenden. Met ons implementatieproces kan een nieuwe release van de software naadloos worden geïmplementeerd zonder de beschikbaarheid van de service te beïnvloeden.

BEVEILIGING VAN DE TOEPASSING TESTEN

Logitech laat externe beveiligingsconsultants beveiligingstests uitvoeren om kwetsbaarheden te identificeren. Dergelijke statische applicatiebeveiligingstests (SAST), dynamische applicatiebeveiligingstest (DAST) en configuratiebeheer van clouddiensten richten zich op (maar beperken zich niet tot) veel voorkomende zwakke punten in de beveiliging, zoals in het Open Web Application Security Project (OWASP) en de Common Weakness Enumeration (CWE) van MITRE staat beschreven. Mochten er tijdens het testen kwetsbaarheden worden vastgesteld, dan zal Logitech alle beveiligingsproblemen verhelpen die door de leverancier zijn geïdentificeerd. Ondanks dat de beveiligingsbeoordeling bij grote releases door derden wordt verricht, voert Logitech tijdens ontwikkelingscycli intern ook SAST en DAST uit.

VERIFICATIE EN AUTORISATIE VAN DE GEBRUIKER

Wanneer de Sync-gebruikers zich bij het webportal aanmelden om hun Logitech-apparaten te beheren, gebruikt de Sync Portal toegangsmechanismen op basis van tokens en rollen om hen te verifiëren en de mate van toegang te autoriseren. Gebruikers bekijken of wijzigen gegevens op basis van hun toegewezen rol in het systeem. Verder is elke beveiligingstoken gebaseerd op een sessie en maar gedurende een bepaalde tijd geldig. Zodra de token vervalt, moeten gebruikers om het systeem beveiligd te houden de toegang vernieuwen door opnieuw hun aanmeldgegevens in te voeren.

INTEGRATIES VOOR EENMALIGE AANMELDING

De authenticatiedienst van Logitech Sync Portal ondersteunt eenmalige aanmelding (SSO) en kan worden geïntegreerd met standaard SAML2.0 identiteitsproviders (IdP), zoals Azure Active Directory en Okta. Met deze providers kan de Sync Portal gebruikers met behulp van hun aanmeldgegevens authenticeren, zonder aparte aanmeldgegevens te beheren, terwijl ze zich op het Sync-platform bevinden.

GEGEVENS IN TRANSIT

Logitech Sync bestaat uit twee delen, namelijk de Sync-applicatie voor desktops (die op uw hardware in de vergaderruimte werkt) en de Sync Portal in de cloud. Uw Sync-toepassing staat na de installatie en authenticatie direct in verbinding met Sync Portal, om beheer op afstand, controlemogelijkheden en diverse inzichten met betrekking tot het gebruik en de prestaties van de ruimte mogelijk te maken.

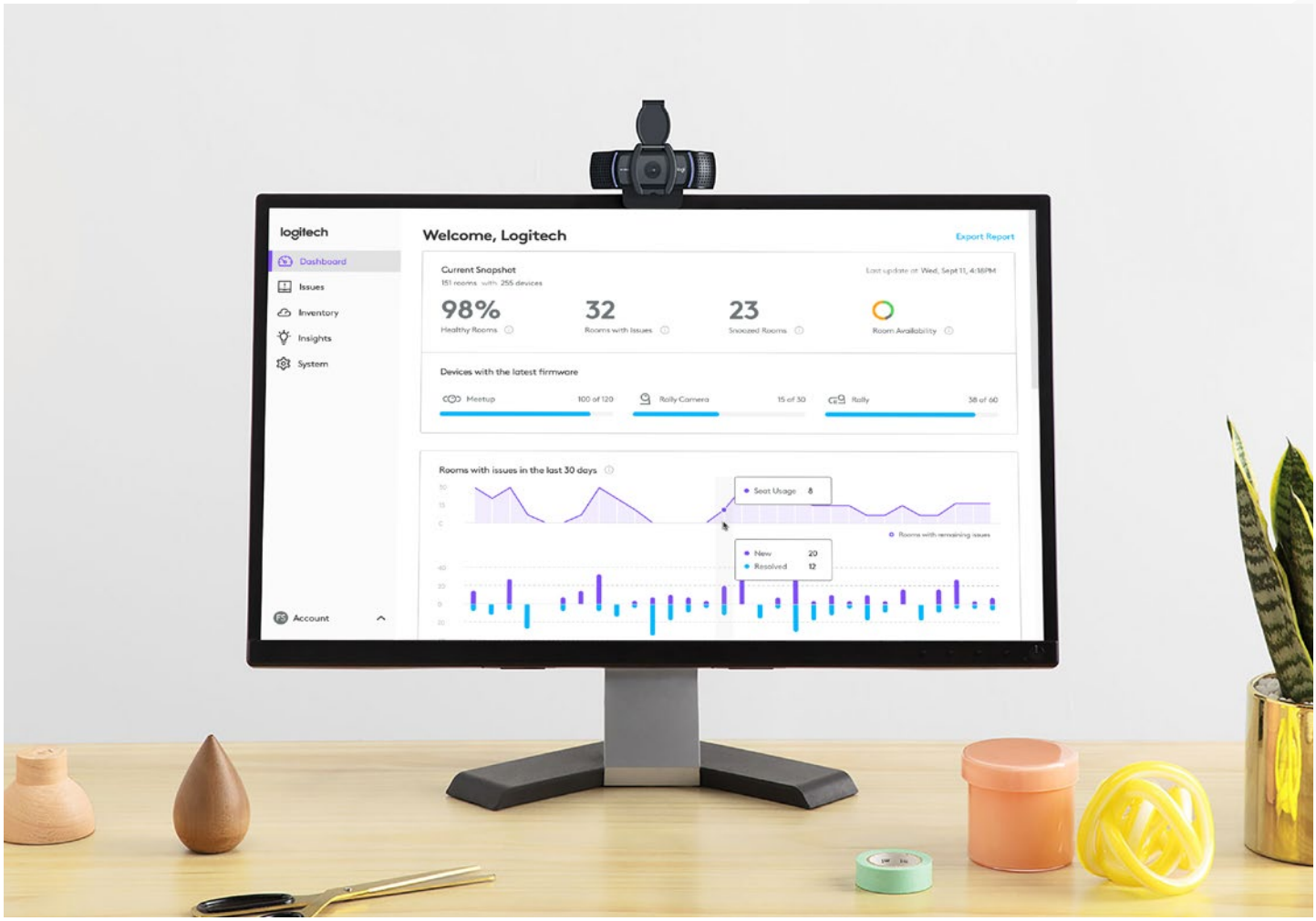
Alle communicatie[1] tussen de Logitech Sync Portal in de cloud en uw Sync-toepassing verloopt via de netwerkprotocollen HTTPS en MQTT. Het verkeer van beide protocollen wordt geauthenticeerd en versleuteld met behulp van Transport Level Security (TLS) versie 1.2 of hoger. Daarnaast wordt het ondersteund door een reeks AES-128/256-bit vercijferingen, om de vertrouwelijkheid en de integriteit van de gegevens over het internet te waarborgen.

ONGEBRUIKTE GEGEVENS

Om de klantgegevens in de backend-service van Sync te beschermen, wordt er binnen de database de sterkste standaard AES-256-bit versleutelingen gebruikt. Bovendien worden klantgegevens beschermd tegen datalekken door de cryptografische sleutels verder te versleutelen en deze door de gegevensservices van AWS centraal te laten beheren.

BESCHIKBAARHEID VAN DE SERVICE EN NOODHERSTEL

Dankzij een fault-tolerant ontwerp voor softwarearchitectuur en infrastructuur, kan de Logitech Sync-service dag en nacht worden gewaarborgd. Hoge beschikbaarheid (HA) kan pas worden bereikt als de schaalbaarheid van de computerapparatuur hoog is en de belasting wordt verdeeld. Actuele gegevens worden op servers aan de westkust van de VS gehost. Van deze gegevens wordt voortdurend een back-up gemaakt binnen het datacentrum. In geval van nood kan Logitech Sync op elk punt van de afgelopen 35 dagen en in elke regio worden hersteld, zonder dat de service onderbroken hoeft te worden.



GEGEVENSVERZAMELING EN PRIVACY

Het privacy- en beveiligingsbeleid beschrijft welke soorten gegevens Logitech verzamelt, hoe we deze gebruiken en hoe we persoonlijke informatie beschermen die is verzameld door onze producten, services, apps en software. Logitech bestaat uit een groep bedrijven die onder het moederbedrijf Logitech International S.A. vallen. Welk Logitech-bedrijf uw gegevens beheert, is afhankelijk van uw relatie met ons (klant, partner, contractant of andere relevante relatie). We nemen in de vergaderruimte geen geluid, video of statische beelden op en slaan deze nooit op in de cloud. In diagram 1.1 hieronder geven we een volledig overzicht van de gegevens die we verzamelen en waarvoor deze gegevens worden gebruikt.

Bron van gegevensverzameling	Verzamelde gegevenstypen	Doel van gegevensverzameling	Opslag van gegevens
Sync Portal (registratie en aanmaken van accounts)	• E-mailadres • Wachtwoord • Voornaam • Achternaam • Naam van de organisatie	Autorisatie van de gebruiker en aanmaken van accounts voor personen.	AWS
Aanvullende informatie in Sync Portal, verstrekt door de gebruiker	• Naam van de ruimte • Aantal zitplaatsen • Groepsnamen	Ruimtes groeperen en identificeren binnen Sync. Het aantal zitplaatsen wordt gebruikt om het gebruik van de zitplaatsen te berekenen, in combinatie met de metagegevens over de ruimtebezetting.	AWS
Sync-app (geïnstalleerd op de pc of appliance in de vergaderruimte, zoals de Logitech Rally Bar)	• Naam van het apparaat • Unieke ID van het apparaat • Firmwareversie van het apparaat • Serienummer van het apparaat • Versie van de Sync-app • OS-type van de computer • OS-versie van de computer • IP/MAC-adres • Metagegevens computerspecificaties • Bezetting vergaderruimtes (alleen metagegevens)	De informatie wordt gebruikt om functies zoals controle, beheer en analytische vaardigheden aan te kunnen bieden via Sync Portal.	AWS

TOEGANG TOT KLANT- EN SERVICEGEGEVENS

Logitech heeft voor het hosten van onze softwarediensten en gebruikersgegevens een contract afgesloten met de platformen van AWS. AWS past strikte bedrijfsrichtlijnen, beschermingslagen en bewaking toe om ervoor te zorgen dat de datacentra alleen voor goedgekeurde werknemers toegankelijk zijn.

Binnen Logitech worden de klantendatabase en de service-instellingen alleen toegankelijk gemaakt voor een kleine groep goedgekeurde personen. Dit zijn personen die verantwoordelijk zijn voor het onderhoud en de ondersteuning van de service.

BEWARING EN VERWIJDERING VAN GEGEVENS

Zodra een klant zich aanmeldt voor Logitech Sync, worden alle gebruikers- en apparaatgegevens die regelmatig zijn verzameld binnen de service bewaard, totdat de klant zich voor de service besluit af te melden. Om de service te beëindigen, moeten klanten hun verzoek indienen door het webformulier op support.logitech.com/response-center in te vullen. Logitech zal het verwijderingsproces vervolgens samen met de klant doorlopen. Zodra het account als 'verwijderd' is aangemerkt, worden alle klantgegevens (behalve de productlogs) onmiddellijk permanent verwijderd.

REACTIE OP VEILIGHEIDSINCIDENTEN

Logitech zet zich in om veilige producten en services te leveren aan onze klanten en ziet rapporten van onafhankelijke onderzoekers, brancheorganisaties, leveranciers, klanten en andere bronnen die zich bezighouden met beveiliging graag tegemoet. Logitech definieert een beveiligingslek als een onbedoelde zwakke plek in een product die een aanvaller de mogelijkheid kan geven om de integriteit, beschikbaarheid of vertrouwelijkheid van een product, software of service in gevaar te brengen.

Logitech Security zet verschillende statistieken in om de vertraging in het verkeer, drempelwaarden en foutpercentages te controleren op verdachte activiteiten. Daarnaast worden er door externe leveranciers regelmatig veiligheidstests uitgevoerd op belangrijke releases, om ervoor te zorgen dat het product veilig is. Eventuele kwetsbaarheden worden op gepaste wijze aangepakt.

Indien u een probleem tegenkomt, onderzoekt het productteam, in samenwerking met Logitech Security, onmiddellijk de gemelde abnormaliteiten en schendingen van de beveiliging binnen de gehele onderneming. U kunt uw zorgen over de beveiliging of schendingen van de Logitech-beveiliging kenbaar maken via onze pagina over de openbaarmaking van kwetsbaarheden of onze pagina over het Bug Bounty-programma.

logitech

Neem contact op met uw wederverkoper of met ons via www.logitech.com/vcsales

Logitech Americas
7700 Gateway Blvd.
Newark, CA 94560
Verenigde Staten

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] In 2021 zal een firmware-update voor Logitech Meetup, Rally, Rally Cam, Tap en Swytch plaatsvinden. Met deze update zal de volledige versleuteling voor deze nieuwere apparaten worden geconfigureerd.

Gepubliceerd in juni 2021