GoToMeeting, GoToWebinar, GoToTraining und GoToStage

Betriebliche Datenschutz- und Datensicherheitskontrollen

LogMeIn GoToMeeting, GoToWebinar, GoToTraining und GoToStage – Betriebliche Datenschutz- und Datensicherheitskontrollen

Datum der Veröffentlichung: 18.3.2019

---

1 Produkte und Services

Dieses Dokument umfasst die Datenschutz- und Datensicherheitskontrollen für LogMeIn GoToMeeting, GoToWebinar, GoToTraining und GoToStage (gemeinsam als „GoTo-Dienste“ bezeichnet).

Bei den GoTo-Diensten handelt es sich um Online-Kommunikationsdienste, die es Einzelpersonen und Organisationen ermöglichen, je nach Dienstangebot mit zahlreichen Funktionen zu interagieren. Dazu gehören Bildschirmfreigabe, Videokonferenzen und integriertes Audio. Die GoTo-Dienste werden mit Hilfe eines Webbrowsers oder eines Client-Programms über ein global verteiltes Netzwerk proprietärer Hardware und Software bereitgestellt.

- GoToMeeting ermöglicht es Benutzern, Sitzungen über die GoToMeeting-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren.
- GoToWebinar ermöglicht es Unternehmen, über das Internet Events und Präsentationen für ein größeres lokales oder globales Publikum durchzuführen. Webinare werden über die GoToWebinar-Website und/oder die Client-Software geplant, einberufen und moderiert.
- GoToTraining ermöglicht es Benutzern, Schulungssitzungen über die GoToTraining-Website bzw. über Client-Software zu planen, einzuberufen und zu moderieren. Es bietet spezielle Funktionen für webbasierte Schulungen wie Online-Zugang zu Tests und Schulungsmaterialien und ein gehostetes Kursverzeichnis.
- GoToStage ist ein Online-Portal, in dem GoToWebinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoToStage-Homepage vorgestellt. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoToWebinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoToStage-Umgebung gelöscht werden.

2 Produktarchitektur

Die Bildschirmübertragung zwischen den Teilnehmern in Sitzungen der GoTo-Dienste erfolgt über einen Overlay-Netzwerkstapel, der logisch über dem konventionellen TCP/IP-Stapel auf den Computern der einzelnen Benutzer angeordnet ist (siehe Abbildung 1).

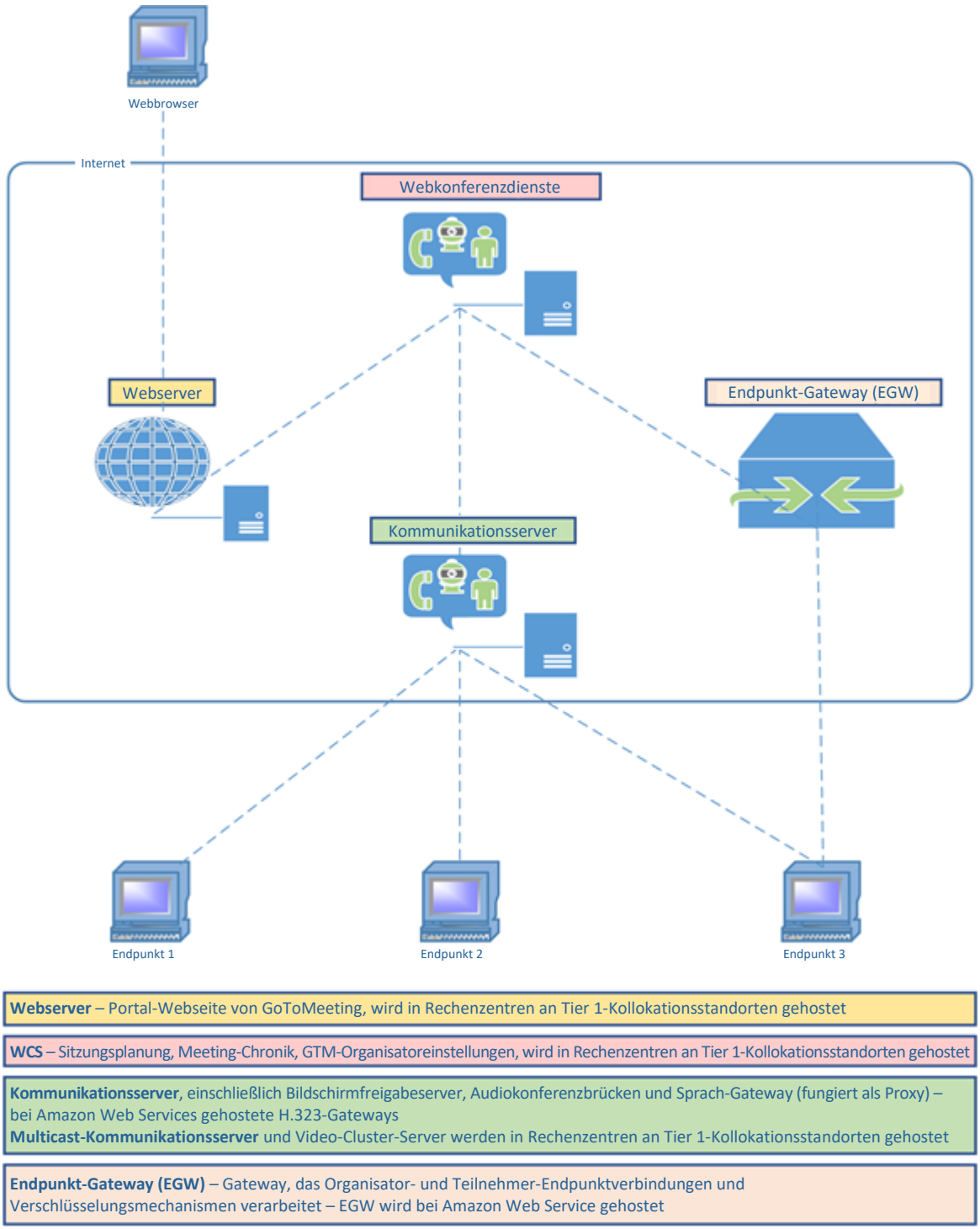

Abbildung 1 – Architektur von LogMeIn GoToMeeting, GoToWebinar, GoToTraining & GoToStage

Die Teilnehmer (Sitzungsendpunkte) verwenden ausgehende TCP/IP-Verbindungen über den Port 443, um mit den Kommunikationsservern und Gateways der Infrastruktur zu kommunizieren. Dabei können sich die Teilnehmer überall im Internet befinden. Clients kommunizieren in der Regel über das Endpunkt-Gateway mit den GoTo-Diensten. Neue Clients kommunizieren jedoch direkt mit Hilfe von REST-Aufrufen (Representational State Transfer) über Lastenausgleiche mit den Backend-Diensten. Die Dienstinfrastruktur ermöglicht es Benutzern des öffentlichen Telefonnetzes („PSTN“), sich in Meeting einzuwählen.

Die GoTo-Dienste verwenden ein ASP-Modell (Application Service Provider), das einen sicheren Betrieb gewährleistet und sich dabei in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines Unternehmens einfügt.

Die Architektur ist für eine hohe Leistung, Zuverlässigkeit und Skalierbarkeit konzipiert und wird auf Hochleistungs-Servern betrieben, auf denen die entsprechenden Sicherheits-Patches kontinuierlich installiert werden. Redundante Switches und Router sind so konzipiert, dass „Single Points of Failure“ ausgeschlossen werden. Geclusterte Server und Backup-Systeme stellen selbst bei hoher Auslastung oder einem Systemausfall sicher, dass die Anwendungsprozesse funktionieren. Broker verteilen die Last der Client-/Server-Sitzungen auf geografisch verteilte Kommunikationsserver, um die Leistung und eine angemessene Latenz sicherzustellen.

Die Dienstinfrastruktur wird hauptsächlich in Rechenzentren an Top Tier Kollokationsrechenzentren gehostet, wobei einige Komponentendienste bei Public Cloud-Anbietern gehostet werden. Die Audiokonferenzbrückendienste werden vollständig von Public Cloud-Anbietern gehostet und auch einige der Produkt-Broker-Dienste und der serviceorientierten Architekturdienste (SOA) werden von Public Cloud-Anbietern gehostet. Die Daten, die mit einem von einem Public Cloud-Anbieter gehosteten Dienst verbunden sind, werden auch bei diesem Anbieter gespeichert.

Der physische Zugang und Zugriff auf an Kollokationsrechenzentren gehosteten Servern ist eingeschränkt und wird kontinuierlich überwacht. Alle Standorte verfügen über redundante Stromversorgungen und entsprechende Einrichtungen zur Kontrolle der Umgebungsbedingungen. Die privaten Netzwerke und Backend-Server von LogMeIn sind durch Firewalls, Router und VPN-basierte Zugangskontrollen gesichert. Die Sicherheit der Infrastruktur wird kontinuierlich überwacht. Interne Mitarbeiter und externe Prüfer führen regelmäßige Tests auf Schwachstellen durch.

Weitere Informationen finden Sie im Whitepaper zur Sicherheit von GoToMeeting [1].

3 Technische Sicherheitskontrollen für GoTo-Dienste

LogMeIn nutzt technische Kontrollen nach Branchenstandard gemäß der Art und Weise und des Umfangs der Dienste (gemäß Definition des Begriffs in den Nutzungsbedingungen [2]). Diese Kontrollen wurden zum Schutz der Dienstinfrastruktur und der darin enthaltenen Daten entwickelt.

3.1 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen und einen Datenverlust in Unternehmens- und Produktionsumgebungen zu verhindern oder zu minimieren. Mitarbeiter erhalten bei Bedarf minimalen (oder „Least Privilege“-) Zugriff auf angegebene LogMeIn-Systeme, -Anwendungen, -Netzwerke und -Geräte. Zudem sind Benutzerrechte basierend auf der funktionalen Rolle und Umgebung voneinander getrennt.

3.2 Perimeterschutz

LogMeIn setzt Standard-Tools, -Techniken und -Dienste für den Perimeterschutz ein, die verhindern sollen, dass nicht autorisierter Netzwerkdatenverkehr in die Produktinfrastruktur gelangt. Das LogMeIn-Netzwerk enthält nach außen gerichtete Firewalls und eine interne Netzwerksegmentierung. Cloud-Ressourcen nutzen auch Host-basierte Firewalls. Außerdem wird ein Cloud-basierter DDoS-Schutzdienst (Distributed Denial of Service) eines Drittanbieters zum Schutz vor umfangreichen DDoS-Angriffen verwendet. Dieser Dienst wird mindestens einmal pro Jahr getestet. Wichtige Systemdateien werden vor böswilliger oder unbeabsichtigter Infizierung oder Zerstörung geschützt.

3.3 Datentrennung

LogMeIn nutzt eine mehrinstanzenfähige Architektur, die basierend auf dem LogMeIn-Konto eines Benutzers oder einer Organisation logisch auf Datenbankebene getrennt ist. Nur authentifizierten Parteien wird Zugriff auf die relevanten Konten gewährt.

3.4 Physische Sicherheit

Physische Rechenzentrumssicherheit

LogMeIn benutzt die Dienste von Kollokationsrechenzentren, um physische Sicherheit und umgebungsbezogene Sicherheitskontrollen für Serverräume mit Produktionsservern zu bieten. Zu diesen Kontrollen gehören:

- Videoüberwachung und Aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- Temperaturregelung von Heizung, Lüftung und Klimaanlage
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (USV)
- Zwischenböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen

- Schutz vor häufigen Naturkatastrophen und vom Menschen verursachten Katastrophen entsprechend der Geografie und des Standorts des jeweiligen Rechenzentrums
- Geplante Wartung und Validierung aller wichtigen Sicherheits- und umgebungsbezogenen Sicherheitskontrollen

LogMeIn beschränkt den physischen Zugang zu Kollokationsrechenzentren nur auf autorisierte Einzelpersonen. Für den Zugang zu einer Hosting-Einrichtung ist die Einreichung eines Antrags über das entsprechende Ticketing-System und die Genehmigung des jeweiligen Managers sowie eine Überprüfung und Genehmigung der Technikabteilung erforderlich. Die LogMeIn-Verwaltung überprüft die Protokolle für den physischen Zugang zu Rechenzentren und Serverräumen mindestens auf vierteljährlicher Basis. Im Fall einer Kündigung von zuvor autorisiertem Personal wird der physische Zugang zu Rechenzentren entfernt.

3.5 Datensicherung, Notfallwiederherstellung und Verfügbarkeit

Die Architektur von LogMeIn wurde im Allgemeinen so konzipiert, dass die Replikation zu geografisch verteilten Standorten nahezu in Echtzeit erfolgt. Datenbanken werden mit Hilfe einer rollierenden inkrementellen Backup-Strategie gesichert. Im Falle eines Notfalls oder eines Totalausfalls eines der vielen aktiven Standorte können die übrigen Standorte die Anwendungslast ausgleichen. Notfallwiederherstellung der Systeme wird regelmäßig getestet.

3.6 Malware-Schutz

Malware-Schutzsoftware mit Überwachungsprotokollen wird auf allen Servern der GoTo-Dienste eingesetzt. Warnmeldungen über Anomalien, einschließlich möglicher böswilliger Aktivität, werden an die Sicherheitsabteilung gesendet.

3.7 Verschlüsselung

LogMeIn implementiert einen kryptographischen Standard, der sich nach Empfehlungen von Industrievereinigungen, Empfehlungen von öffentlichen Ämtern für Sicherheit und Datenschutz und anderen für Standards relevanten Gruppen richtet. Der kryptografische Standard wird regelmäßig überprüft und ausgewählte Technologien und Verschlüsselungen werden in Einklang mit dem bewerteten Risiko und der Marktakzeptanz neuer Standards aktualisiert.

3.7.1 Verschlüsselung während der Übertragung

GoToMeeting, GoToWebinar und GoToTraining bieten End-to-End-Sicherheitsmaßnahmen für Daten. Daten über die Bildschirmfreigabe, Steuerungsdaten von Tastatur/Maus und Chat-Informationen sind auf Kommunikationsservern oder während der Übertragung über öffentliche oder private Netzwerke nie in unverschlüsselter Form verfügbar.

In zwei Schichten sind Kommunikationssicherheitskontrollen auf Basis starker Verschlüsselung implementiert: der Anwendungsprotokollschicht und der Multicast-Paket-Sicherheitsschicht (MPSL).

Sicherheit der Anwendungsprotokollschicht

Die Kommunikation zwischen Endpunkten wird durch in TLS-Protokollen (Transport Layer Security) nach IETF-Standard (Internet Engineering Task Force) geschützt.

LogMeIn empfiehlt Kunden zu ihrer eigenen Sicherheit, ihre Browser so zu konfigurieren, dass sie nach Möglichkeit standardmäßig eine starke Verschlüsselung verwenden und sicherstellen, dass die Sicherheitspatches für ihr Betriebssystem und ihre Browser aktuell sind.

Beim Herstellen einer TLS-Verbindung zur Website sowie zwischen den GoToMeeting-, GoToWebinar- oder GoToTraining-Komponenten authentifizieren sich die LogMeIn-Server mit Hilfe von Public-Key-Zertifikaten bei den Clients. Als zusätzlicher Schutz vor Infrastrukturattacken erfolgt eine gegenseitige zertifikatbasierte Authentifizierung bei allen Server-zu-Server-Verbindungen (z.B. MCS zu MCS oder MCS zu Broker).

Sicherheit der Multicast-Paketschicht

Zusätzliche Funktionen bieten unabhängig von den durch TLS bereitgestellten Funktionen eine vollständige End-to-End-Sicherheit für Multicast-Paketdaten. Insbesondere werden sämtliche Multicast-Sitzungsdaten durch End-to-End-Verschlüsselung und Integritätsmechanismen geschützt, die jeden mit Zugriff auf die Kommunikationsserver – egal ob Freund oder Feind – daran hindern sollen, eine Sitzung abzuhören oder Daten unerkannt zu manipulieren. Die MPSL bietet eine zusätzliche Ebene der Vertraulichkeit und Integrität der Kommunikation, die es nur bei LogMeIn-Produkten gibt.

Die Erstellung der MPSL-Schlüssel erfolgt mittels eines zufällig generierten 128-Bit-Seed-Werts, der vom Service Broker ausgewählt und über TLS an alle Endpunkte verteilt wird. Er dient als Eingabe für eine vom NIST bestätigte HMAC-SHA1-basierte Schlüsselableitungsfunktion. Am Ende der Sitzung wird der Seed-Wert aus dem Speicher des GoToMeeting Service Brokers gelöscht.

Des Weiteren schützt die MPSL Multicast-Paketdaten vor Abhörversuchen mit Hilfe einer 128-Bit-AES-Verschlüsselung im Counter-Mode. Klar-Text-Daten werden vor der Verschlüsselung zwecks Optimierung der Bandbreite mit proprietären Hochleistungstechniken komprimiert. Der Schutz der Datenintegrität wird durch Einschluss eines Integritätskontrollwerts erreicht.

Schutz bei Tonübertragungen

GoToMeeting, GoToWebinar und GoToTraining unterstützen integrierte Audiokonferenzen sowohl über das herkömmliche Telefonnetz als auch über VoIP (Internettelefonie). Das herkömmliche Telefonnetz gewährleistet von vornherein die Vertraulichkeit und Integrität der Sprachkommunikation. Bei VoIP-Verbindungen zwischen den Endpunkten und den Telefonkonferenzservern kommt sowohl über UDP als auch TCP ein SRTP (Secure Real-Time Transport Protocol) zum Einsatz. Client und Server tauschen die Schlüssel über die hergestellte TLS-geschützte HTTPS-Verbindung aus. Bei Video-Verbindungen von den Endpunkten zu den Video-Servern wird ein SRTP verwendet. Client und Server tauschen die Schlüssel über die hergestellte TLS-geschützte HTTPS-Verbindung aus.

GoToWebinar-Übertragung

GoToWebinar-Medien werden über das HTTP-Live-Streaming-Protokoll (HLS) übertragen, während die Broadcast-Gateways die Daten mischen und in andere Bitraten transkodieren, um die Inhalte auch für Clients mit suboptimalen Netzwerkverbindungen anzupassen. Die Gateways übertragen die Output-Medienstreams über RTP (Real-Time Transport Protocol) und HTTP an das Content Delivery Network (CDN), welches die Streams dann über HTTPS mit Hilfe von TSL-Schutzmechanismen an die Teilnehmer sendet.

GoToStage

GoToStage ist ein Online-Portal, in dem GoToWebinar-Organisatoren anpassbare Kanäle erstellen und ihre aufgezeichneten Webinare veröffentlichen können. Veröffentlichte Aufzeichnungen werden von uns in einer Reihe geschäftlicher Kategorien auf der GoToStage-Homepage vorgestellt. Ein auf GoToStage veröffentlichtes Video ist über die GoToStage-Homepage und über Suchmaschinen auffindbar, sofern der Organisator die Auffindbarkeit nicht mit Hilfe der Administrator-einstellungen auf seiner Kanalseite eingeschränkt. Andernfalls können alle bei GoToStage registrierten Personen mit einem direkten Link zum Kanal oder zur individuellen „Watch Now"-Seite des Videos die Aufzeichnung ansehen. Besucher registrieren sich mit ihrem Namen und ihrer E-Mail-Adresse bei GoToStage oder stellen über Konten in sozialen Netzwerken wie LinkedIn, Facebook und Gmail eine Verbindung her. Nach der Registrierung erfolgt die Wiedergabe des aufgezeichneten Webinars über eine signierte S3-URL mit einer festgelegten TTL. Organisatoren können die Veröffentlichung ihrer Aufzeichnungen über GoToWebinar jederzeit rückgängig machen, wodurch die Videos von ihrer Kanalseite und aus der GoToStage-Umgebung gelöscht werden. Zum Schutz der GoToStage-Administrationsfunktionen werden Passwörter verwendet, und alle Verbindungen im GoToStage-Portal sind mittels TLS geschützt.

3.8 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden monatlich auf Schwachstellen überprüft. Es werden auch regelmäßig Schwachstellenprüfungen dynamischer und statischer Anwendungen vorgenommen und Penetrationstestaktivitäten für bestimmte Umgebungen ausgeführt. Für die Ergebnisse dieser Überprüfungen und Tests werden in Netzwerk-überwachungstools Berichte erstellt und wo dies basierend auf der Wichtigkeit der identifizierten Schwachstellen erforderlich ist, werden Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den Technikteams sowie der Betriebsführung zur Verfügung gestellt werden.

3.9 Protokollierung und Warnmeldungen

LogMeIn erfasst identifizierten anomalen oder verdächtigen Datenverkehr in entsprechenden Sicherheitsprotokollen in den jeweiligen Produktionssystemen.

4 Organisatorische Kontrollen

LogMeIn setzt eine breite Palette an organisatorischen und administrativen Kontrollen ein, um die Sicherheits- und Datenschutzbestimmungen von GoToMeeting, GoToWebinar, GoToTraining, and GoToStage einzuhalten.

4.1 Sicherheitsrichtlinien und -verfahren

LogMeIn pflegt und implementiert umfangreiche Sicherheitsrichtlinien und -verfahren, die an Geschäftszielen, Compliance-Programmen und der allgemeinen Unternehmensführung ausgerichtet sind. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um die Einhaltung von Vorschriften stets sicherzustellen.

4.2 Einhaltung der Standards

Als Aktiengesellschaft hält LogMeIn geltende rechtliche, finanzielle, datenschutzrechtliche und regulatorische Anforderungen ein und erfüllt die folgenden Konformitätszertifikate und externen Audit-Berichte:

- SOC (Service Organization Control) II Typ-1-Berichte des amerikanischen Instituts der Wirtschaftsprüfer (American Institute of Certified Public Accountants, AICPA) für die GoToMeeting-, GoToWebinar- und GoToTraining-Dienste
- Sarbanes-Oxley-Gesetz (SOX)
- Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) bei den E-Commerce- und Zahlungsumgebungen von LogMeIn
- TRUSTe-Datenschutzzertifizierung für Unternehmen

4.3 Sicherheitsvorgänge und Incident-Management

Das Security Operations Center (SOC) von LogMeIn ist mit dem Security Operations-Team besetzt und ist für das Erkennen von und Reagieren auf Sicherheitsereignisse verantwortlich. Das SOC verwendet Sicherheits- und Analysesysteme, um mögliche Probleme zu identifizieren und hat einen Vorfallsreaktionsplan („Security Incident Response Plan“) entwickelt, der die entsprechenden Reaktionen vorgibt.

Der Vorfallsreaktionsplan ist auf die wichtigen Kommunikationsprozesse, die Incident-Management-Richtlinie für Informationssicherheit sowie standardmäßige Betriebsvorgänge ausgerichtet. Es wurde entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Diensten, einschließlich der GoTo-Dienste, zu verwalten, zu identifizieren und zu beheben. Laut Vorfalls-reaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicherheit von Informationen identifizieren und alle vermuteten oder bestätigten Ereignisse gegebenenfalls mit dem Management eskalieren. Mitarbeiter können Sicherheitsvorfälle gemäß des auf der Intranet-Seite von LogMeIn dokumentierten Prozesses per E-Mail, Telefon und/oder Ticket melden. Alle identifizierten oder vermuteten Ereignisse werden über standardisierte Ereignistickets dokumentiert, eskaliert und je nach Wichtigkeit selektiert.

4.4 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von LogMeIn basiert auf dem Microsoft Security Development Lifecycle (SDL) für einen sicheren Produktcode. Zu den Hauptelementen dieses Programms gehören manuelle Codeüberprüfungen, Bedrohungsmodellierung („Threat Modeling“), statische Codeanalysen, dynamische Analysen und Systemhärtung.

4.5 Personalsicherheit

Überprüfungen der Mitarbeiter – soweit dies nach geltendem Recht zulässig und für die Position angemessen ist – werden weltweit bei neuen Mitarbeitern vor dem Datum ihrer Einstellung vorgenommen. Die Ergebnisse werden im Personalstammblatt des Mitarbeiters hinterlegt. Die Kriterien der Mitarbeiterüberprüfung variieren in Abhängigkeit der Gesetze, der Arbeitsverantwortung und dem Führungsniveau des potenziellen Mitarbeiters und unterliegen den üblichen und zulässigen Praktiken des jeweiligen Lands.

4.6 Sicherheitsbewusstsein und Schulungsprogramme

Neueingestellte Mitarbeiter werden zur Orientierung über die Sicherheitsrichtlinien und den Verhaltenskodex und Geschäftsethik von LogMeIn informiert. Diese obligatorische jährliche Schulung zu Sicherheit und Datenschutz wird für die entsprechenden Mitarbeiter durch das Talentförderungsteam und mit Unterstützung des Sicherheitsteams durchgeführt.

Die Mitarbeiter und Zeitarbeiter von LogMeIn werden regelmäßig über die Anweisungen, Verfahren, Richtlinien und Standards zu Sicherheit und Datenschutz informiert. Dazu werden verschiedene Medien wie Einarbeitungsunterlagen für Neueingestellte, Aufklärungskampagnen, Webinare mit dem CISO, ein Sicherheits-Champion-Programm und der Aushang von Plakaten oder anderes Begleitmaterial genutzt, die mindestens halbjährlich ausgetauscht werden und Methoden zum Schutz von Daten, Geräten und Anlagen veranschaulichen.

5 Datenschutzpraktiken

LogMeIn nimmt den Schutz der Daten seiner Kunden und Endbenutzer sehr ernst und verpflichtet sich, entsprechende Praktiken zur Verarbeitung und Verwaltung von Daten offen und transparent preiszugeben.

5.1 Datenschutzrichtlinie

LogMeIn veröffentlicht die Arten von Informationen, die es sammelt und verwendet, um seine Dienste bereitzustellen, aufrechtzuerhalten, zu verbessern und zu sichern, in seiner Datenschutzerklärung auf der öffentlichen Website [3]. Das Unternehmen kann seine Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen an seinen Informationspraktiken und/oder Änderungen geltender Gesetze zu berücksichtigen, weist aber auf seiner Website auf jegliche Materialänderungen hin, bevor diese wirksam werden.

5.2 DSGVO

In dem Umfang, in dem LogMeIn personenbezogene Daten [wie im Datenverarbeitungsnachtrag (DPA) von LogMeIn im Ressourcen-Center unter www.logmeininc.com/gdpr definiert] im Namen des Kunden durch die Zurverfügungstellung von GoTo-Diensten verarbeitet, erfolgt dies im Einklang mit den Vorgaben der Datenschutz-Grundverordnung (DSGVO), die auf LogMeIn bei der Bereitstellung ihrer Dienstleistungen direkt anwendbar sind.

5.3 EU-US und Schweizer Datenschutzschild

LogMeIn, Inc. und ihre US-amerikanischen verbundenen Unternehmen nehmen an dem EU-US-Datenschutzschild („Privacy Shield“) und dem Schweizer Datenschutzschild hinsichtlich der Erhebung, Nutzung und Speicherung personenbezogener Daten aus den Mitgliedsstaaten der Europäischen Union und der Schweiz teil [4]. Die Zertifizierung wird jährlich durch TRUSTe überprüft, und alle Erkenntnisse werden unmittelbar durch LogMeIn umgesetzt.

5.4 Rückgabe und Löschung von Kundeninhalt

GoToWebinar- und GoToTraining-Kunden können ihre Aufzeichnungen innerhalb ihrer Dienstumgebung löschen. Außerdem können Kunden der GoTo-Dienste jederzeit die Rückgabe oder Löschung ihres Inhalts über standardisierte Schnittstellen anfordern. Wenn diese Schnittstellen nicht verfügbar sind, ergreift LogMeIn andernfalls wirtschaftlich zumutbare Maßnahmen, um den Kunden im Rahmen der technischen Möglichkeiten beim Abrufen oder Löschen seines Inhalts zu unterstützen. Zudem wird der Kundeninhalt innerhalb von dreißig (30) Tagen nach der Anfrage des Kunden gelöscht.

Nach Ablauf oder Beendigung eines zahlungspflichtigen Abonnements für GoToMeeting werden die Konten des Kunden in ein kostenloses Konto umgewandelt. Kostenlose GoToMeeting-Konten werden nach zwei (2) Jahren Inaktivität des Benutzers (z. B. keine Anmeldungen) automatisch gelöscht. Zur Berücksichtigung eines saisonalen Benutzerstamms werden GoToWebinar- und GoToTraining-Konten zwei (2) Jahre nach Ablauf oder Beendigung der jeweiligen Endlaufzeit gelöscht. GoToStage-Benutzer können ihre veröffentlichten Webinare während eines aktiven GoToWebinar-Abonnements jederzeit per Self-Service über die GoToWebinar-Dienstumgebung und/oder durch Einreichen einer Supportanfrage bei LogMeIn entfernen oder die Veröffentlichung rückgängig machen. Auf schriftliche Anfrage wird LogMeIn die Löschung des betreffenden Kontos und der Inhalte bestätigen.

5.5 Sensible Daten

Es ist das Ziel von LogMeIn, den gesamten Kundeninhalt zu schützen, und regulatorische und vertragliche Beschränkungen verlangen, dass die Verwendung von GoToMeeting, GoToWebinar, GoToTraining und GoToStage für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von LogMeIn hat, dürfen die folgenden Daten nicht in GoToMeeting, GoToWebinar, GoToTraining und GoToStage hochgeladen oder dort generiert werden:

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.

- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, die im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) und damit verbundenen Gesetzen und Vorschriften festgelegt sind.
- Informationen über Finanzkonten und Zahlungsinstrumente, einschließlich, aber nicht beschränkt auf Kreditkartendaten. Die einzige allgemeine Ausnahme von dieser Bestimmung betrifft ausdrücklich gekennzeichnete Zahlungsformulare und Seiten, die von LogMeIn verwendet werden, um Zahlungen für GoToMeeting, GoToTraining, GoToWebinar und GoToStage zu erheben.
- Alle Informationen, die besonders durch geltende Gesetze und Vorschriften geschützt sind, insbesondere Informationen über die Rasse, die ethnische Zugehörigkeit, religiöse oder politische Überzeugungen, organisatorische Mitgliedschaften der Person usw.

5.6 Nachverfolgung und Analysen

LogMeIn verbessert kontinuierlich seine Websites und Produkte mit Hilfe verschiedener Webanalysetools von Drittanbietern, die LogMeIn helfen zu verstehen, wie Besucher die Websites, Desktop-Tools und mobilen Anwendungen nutzen, was sie mögen und was sie nicht mögen und wo sie gegebenenfalls Probleme haben. Weitere Einzelheiten finden Sie in der Datenschutzrichtlinie [3]

6 Drittanbieter

6.1 Nutzung von Drittanbietern

Im Rahmen der internen Bewertung und der Prozesse im Zusammenhang mit Anbietern und Dritten können Anbieterbewertungen je nach Relevanz und Anwendbarkeit von mehreren Teams vorgenommen werden. Das Sicherheitsteam bewertet Anbieter von Diensten, die auf Informationssicherheit basieren, und nimmt auch die Bewertung der Hosting-Einrichtungen von Drittanbietern vor. Das Team für Recht und Beschaffung kann bei Bedarf nach internen Prozessen Verträge, Leistungsbeschreibungen und Dienstleistungsvereinbarungen bewerten. Angemessene Konformitätsdokumente oder -berichte können mindestens einmal jährlich eingeholt und bewertet werden, sofern dies für angemessen erachtet wird, um sicherzustellen, dass die Kontrollumgebung ordnungsgemäß funktioniert und alle erforderlichen benutzerbezogenen Kontrollen durchgeführt werden. Zudem müssen Drittanbieter, die sensible oder vertrauliche Daten hosten oder von LogMeIn Zugriff darauf erhalten haben, einen schriftlichen Vertrag zu unterzeichnen, in dem die relevanten Anforderungen für den Zugriff auf die Informationen sowie deren Speicherung oder Verarbeitung (sofern zutreffend) festgelegt sind.

6.2 Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Geschäftsprozessen und Datenverarbeitung durch Drittanbieter getroffen werden, überprüft LogMeIn die jeweiligen Nutzungsbedingungen von Drittanbietern und nutzt entweder von LogMeIn genehmigte Beschaffungsvorlagen oder verhandelt die Bedingungen dieser Drittanbieter, wenn dies als notwendig erachtet wird.

7 Kontakt zu LogMeIn

Kunden können sich bei allgemeinen Anfragen unter https://support.logmeininc.com/ oder bei Fragen zum Datenschutz unter privacy@logmein.com an LogMeIn wenden.

8 Referenzen

[1] LogMeIn, Inc., „GoToMeeting Security White Paper," 2017. [Online]. Available: https://assets.cdngetgo.com/35/6e/90b973b84e4f8a164fcbacc028f4/gotomeeting-security-white-paper-286395.pdf. [Zugriff am 2 April 2018].

[2] LogMeIn, Inc., „LastPass Technical Whitepaper," LogMeIn, Inc., January 2018. [Online]. Available: https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper_Jan-2018.pdf.

[3] LogMeIn, Inc., „LogMeIn Privacy Policy," LogMeIn, Inc., January 2018. [Online]. Available: https://secure.logmein.com/policies/privacy.aspx.

[4] LogMeIn, Inc., „LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., November 2017. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.

[5] LogMeIn, Inc., „Terms of Service for LogMeIn and Goto Services," LogMeIn, Inc., February 2018. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[6] LogMeIn, Inc, „Logmein Privacy Policy," [Online]. Available: https://secure.logmein.com/policies/privacy.aspx. [Zugriff am 2 April 2018].