TECHNISCHE UND ORGANISATORISCHE DATENSICHERHEITSMAßNAHMEN

Inhalt

Einleitung

Die hier vorgestellten technischen und organisatorischen Datensicherheitsmaßnahmen wurden von LogMeIn, Inc. („LMI“) zur Unterstützung des Sicherheitsprogrammsimplementiert.

Technische und organisatorische Datensicherheitsmaßnahmen

LMI implementierte und pflegt ein Sicherheitsprogramm, das die ISO/IEC 27000-Serie von Kontrollstandards als Baseline nutzt.

Physische Zugangskontrolle der Verarbeitungsbereiche

Webanwendungen, die Kommunikationseinrichtungen infrastruktur und die Datenbankserver von LMI befinden sich in sicheren Datencentern. LMI hat geeignete Maßnahmen ergriffen, um die Datenverarbeitungssysteme (Telefone, Datenbank- und Anwendungsserver und verwandte Hardware), auf denen persönliche Daten verarbeitet bzw. verwendet werden, vor dem Zugriff unbefugter Personen zu schützen.

Dies wird durch Folgendes erreicht:

- Einrichtung von Sicherheitsbereichen.
- Schutz und Einschränkung der Zugangswege.
- Absicherung der Datenverarbeitungsgeräte und der PCs.
- Einrichtung von Zugangsautorisierungen für Mitarbeiter und Dritte, einschließlich der entsprechenden Dokumentation.
- Verordnungen/Einschränkungen bei Kartenschlüsseln.
- Beschränken des physischen Zugangs zu den Servern durch Verwendung elektronisch gesicherter Türen und separater Käfige an den Kollokationsstandorten.
- Der Zugang zum Datencenter, in dem persönliche Daten gespeichert sind, wird durch das Sicherheitspersonal mithilfe elektronischer Überwachung und CCTV-Videoüberwachung protokolliert, überwacht und aufgezeichnet.
- Datencenter, in denen sich persönliche Daten befinden, werden durch Sicherheitsalarmsysteme und weitere entsprechende Sicherheitsmaßnahmen geschützt, z. B. durch benutzerbezogene Authentifizierungsverfahren, darunter biometrische Authentifizierungsverfahren (z. B. Handgeometrie) und/oder elektronische Ausweise mit den Passfotos der Benutzer.

Zugriffssteuerung für Datenverarbeitungssysteme (logisch)

LMI hat geeignete Maßnahmen ergriffen, um seine Datenverarbeitungssysteme vor dem Zugriff unbefugter Personen zu schützen.

Dies wird durch Folgendes erreicht:

- Identifizierung des Terminals und/oder des Terminalbenutzers bei den LMI Systemen.
- Automatisches Timeout des Benutzerterminals bei Ruhezustand; zum erneuten Öffnen sind Identifizierung und Kennwort erforderlich.
- Automatische Sperre der Benutzer-ID, wenn mehrere falsche Kennwörter eingegeben werden. Events werden protokolliert und die Protokolle werden regelmäßig durchgesehen.

- Nutzung von Firewall, Router und VPN-basierten Zugangssteuerungen, um die privaten Service-Netze und Backend-Server zu schützen.
- Kontinuierliche Kontrolle der Infrastruktursicherheit.
- Regelmäßige Überprüfung der Sicherheitsrisiken durch interne Mitarbeiter und Prüfer von Drittfirmen.
- Ausstellen und Schutz der ID-Codes.
- Rollenbasierte Zugriffssteuerung, die so implementiert ist, dass sie dem Least-Privilege-Prinzip entspricht.
- Der Remotezugriff auf die LMI Infrastruktur, die die Dienste bereitstellt, wird durch Zwei-Faktor-Authentifizierungstoken abgesichert.
- Der Zugriff auf Hostserver, Anwendungen, Datenbanken, Router, Switches usw. wird protokolliert.
- Zugriffsanforderungen und Anforderungen zur Verwaltung von Benutzerkonten müssen interne Genehmigungssysteme durchlaufen.
- Der Zugriff muss von einer entsprechend autorisierten Stelle genehmigt werden. In den meisten Fällen sind für die Genehmigung einer Anforderung mindestens zwei Freigaben erforderlich: die des Vorgesetzten des Mitarbeiters und die des Freigabeberechtigten oder „Eigentümers“ des bestimmten Systems bzw. der internen Anwendung.
- Die Kennwörter müssen der LMI Kennwortrichtlinie entsprechen, die Anforderungen an Mindestlänge sowie Komplexität stellt und regelmäßige Zurücksetzungen vorschreibt.
- Das Zurücksetzen von Kennwörtern wird über das LMI Ticketsystem abgewickelt. Neue oder zurückgesetzte Kennwörter werden dem Mitarbeiter über das interne, sichere, verschlüsselte E-Mail-System oder anhand einer Voicemail zugestellt.

LMI beschäftigt Intrusion Detection-Systeme und nutzt auch kommerzielle und benutzerdefinierte Werkzeuge zu sammeln und zu untersuchen, ihre Anwendung und System-Logs für Anomalien.

Zugriffssteuerung für die Nutzung bestimmter Bereiche der Datenverarbeitungssysteme

Personen, die zur Nutzung des Datenverarbeitungssystems berechtigt sind, können nur auf persönliche Daten zugreifen, für die sie über die entsprechenden Zugriffsrechte verfügen (Autorisierung). Ohne entsprechende Autorisierung können persönliche Daten weder gelesen, kopiert, geändert noch entfernt werden.

Dies wird durch Folgendes erreicht:

- Mitarbeiterrichtlinien und Schulungen unter Berücksichtigung der Zugriffsrechte der einzelnen Mitarbeiter auf die persönlichen Daten.
- Benutzer haben eindeutige Anmeldedaten. Rollenbasierte Zugriffssteuerungssysteme dienen dem Beschränken des Zugriffs auf bestimmte Funktionen.
- Überwachung der Aktivitäten, mit denen persönliche Daten hinzugefügt, gelöscht oder geändert werden.
- Effektive und angemessene Disziplinarmaßnahmen gegen Personen, die ohne Autorisierung auf persönliche Daten zugreifen.

- Freigabe persönlicher Daten nur für autorisierte Personen.
- Steuerung des Zugriffs auf Kontodaten und persönliche Daten des Kunden über rollenbasierte Zugriffssteuerungssysteme (RBAC) gemäß dem Least-Privilege-Sicherheitsprinzip.
- Interne Segmentierung und logische Isolierung der LMI Mitarbeiter zur Umsetzung der Richtlinien, die dem Least-Privilege-Prinzip folgen.
- Anforderungsgesteuerte Definition des Autorisierungsschemas und der Zugriffsrechte sowie deren Überwachung und Protokollierung.
- Regelmäßige Überprüfung der Konten und Berechtigungen (für gewöhnlich alle 3-6 Monate, je nach System und Vertraulichkeit der Daten, auf die es Zugriff bietet).
- Kontrolle über die Dateien, kontrollierte und dokumentierte Vernichtung der Daten sowie Richtlinien, die die Aufbewahrungsfristen für Sicherungskopien festlegen.

Verfügbarkeitskontrolle

LMI hat geeignete Maßnahmen ergriffen, um sicherzustellen, dass persönliche Daten vor zufälliger Zerstörung oder unbeabsichtigtem Verlust geschützt sind.

Dies wird durch Folgendes erreicht:

- Globale und redundante Service-Infrastruktur, die mit kompletten Sites für die Notfallwiederherstellung eingerichtet ist.
- Ständige Bewertung unserer Datencenter und Internet Service Provider (ISP), um die Leistung für die Kunden hinsichtlich der Bandbreite, Latenz und Isolierung im Falle einer Notfallwiederherstellung zu optimieren.
- Einrichtung unserer Datencenter an sicheren Kollokationsstandorten, die ISP-Carrier-neutral sind und physische Sicherheit sowie redundante Stromversorgung und Infrastruktur bieten.
- Service Level Agreements mit ISP, um möglichst lange Betriebszeiten zu gewährleisten.
- Funktionalität für schnelles Failover.
- Aufrechterhaltung von Kapazitätserweiterungssystemen (DR) und jährlichen Testen von DR-Zentren durch Abschalten der Primärstandorte für mindestens 24 Stunden. Systeme und Prozesse zur Erkennung und Verteidigung von DDoS-Angriffen, sofern das Produkt nicht in aktiver / aktiver Konfiguration ausgeführt wird.

Kontrolle bei der Datenübertragung

LMI hat geeignete Maßnahmen implementiert, um zu verhindern, dass persönliche Daten während der Übertragung oder während des Transports der Datenträger von unbefugten Personen gelesen, kopiert, verändert oder gelöscht werden.

Dies wird durch Folgendes erreicht:

- Nutzung angemessener Firewall- und Verschlüsselungstechnologien zum Schutz der Gateways und Übertragungswege, über die die Daten transportiert werden.
- Vertrauliche persönliche Daten werden bei der Datenübertragung mithilfe aktueller TLS-Versionen oder anderer Sicherheitsprotokolle verschlüsselt, die starke Verschlüsselungsalgorithmen und -schlüssel verwenden.

- Bestimmte Typen vertraulicher persönlicher Daten von Kunden und sonstige vertrauliche Kundendaten (z. B. Kreditkartennummern) werden bei der Speicherung innerhalb des Systems verschlüsselt.
- Schutz des webbasierten Zugriffs von Mitarbeitern auf die Benutzeroberflächen der Kontoverwaltung durch die Verschlüsselung mit TLS.
- End-to-End-Verschlüsselung der Bildschirmübertragung für Remotezugriffe, Support und Kommunikation in Echtzeit.
- Nutzung von Integritätsprüfungen zum Überwachen der Vollständigkeit und Richtigkeit der übertragenen Daten.

Eingabekontrolle

LMI hat geeignete Maßnahmen implementiert, damit überprüft werden kann, ob und von wem persönliche Daten in das Datenverarbeitungssystem eingegeben oder daraus entfernt wurden.

Dies wird durch Folgendes erreicht:

- Authentifizierung des autorisierten Personals.
- Schutzmaßnahmen für die Eingabe persönlicher Daten in den Arbeitsspeicher sowie für das Lesen, Verändern und Löschen der gespeicherten persönlichen Daten, einschließlich der Dokumentation oder Protokollierung von wesentlichen Änderungen an Kontodaten und -einstellungen.
- Trennung und Schutz aller gespeicherten persönlichen Daten über Datenbankschemas, logische Zugriffssteuerung und/oder Verschlüsselung.
- Nutzung der Anmeldedaten für die Benutzeridentifizierung.
- Physische Sicherheit der Datenverarbeitungseinrichtungen.
- Automatischer Ablauf von Sitzungen.

Trennung der Verarbeitung von Daten für unterschiedliche Zwecke

LMI hat geeignete Maßnahmen ergriffen, damit persönliche Daten, die für unterschiedliche Zwecke erfasst wurden, separat verarbeitet werden können.

Dokumentation

LMI bewahrt die Dokumentation technischer und organisatorischer Maßnahmen für Audits und als Nachweise auf. LMI unternimmt angemessene Schritte, um sicherzustellen, das seine Mitarbeiter und andere Personen am Arbeitsplatz die technischen und organisatorischen Maßnahmen, die in diesem Dokument aufgeführt werden, kennen und einhalten. LMI kann in eigenem Ermessen nicht vertrauliche Teile der Audit-Berichte Kunden zur Verfügung stellen, um die Einhaltung der in diesem Programm dargelegten technischen und organisatorischen Maßnahmen zu verifizieren.

Überwachung

LMI greift nicht auf Kundendaten des Kunden zu, es sei denn, dem Kunden, der LMI verpflichtet ist, die Dienste durchzuführen, zu überwachen, zu analysieren und zu verbessern, zur Unterstützung der Kundenerfahrung, wie gesetzlich vorgeschrieben oder auf Verlangen des Kunden; LMI hat geeignete Maßnahmen implementiert, um die

Zugriffsbeschränkungen der LMI-Systemadministratoren zu überwachen und sicherzustellen, dass sie gemäß den erhaltenen Anweisungen handeln.

Dies wird durch Folgendes erreicht:

- Individuelle Ernennung der Systemadministratoren.
- Durchführung geeigneter Maßnahmen zum Aufzeichnen der Zugriffsprotokolle der Systemadministratoren bei der Infrastruktur und Sicherstellen, dass sie über einen angemessenen Zeitraum sicher, fehlerfrei und unverändet bleiben.
- Führen und Aktualisieren einer Liste der Identifizierungsmerkmale des Systemadministrators (z. B. Vorname, Nachname, Funktion oder Organisationsbereich) und Verantwortlichkeiten.

Definitionen

„LMI“ steht für LogMeIn, Inc. und alle seine direkten und indirekten Tochtergesellschaften.

„Kunde“ steht für einen Käufer eines LMI Angebots.

„Persönliche Daten“ sind Informationen, die sich direkt oder indirekt auf eine identifizierte oder identifizierbare natürliche Person beziehen.

„Security Framework“ bezieht sich auf die Sammlung an Richtlinien und Verfahren von LMI zur Informationssicherheit, darunter insbesondere Richtlinien, Schulungen, Bildung, Überwachung, Untersuchung und Umsetzung der Anstrengungen im Bereich der Datenverwaltung und der Sicherheit.

• Dokumenthistorie

Version	Überarbeitet am	Autor	Hinweise
1.0	30. Juni 2015	Stacey Simson	
2.0	20. Mai 2016	Lisa Hall	
3.0	1.October 2016	Kari Zeni	
4.0	1 February 2017	Margaret Granger	