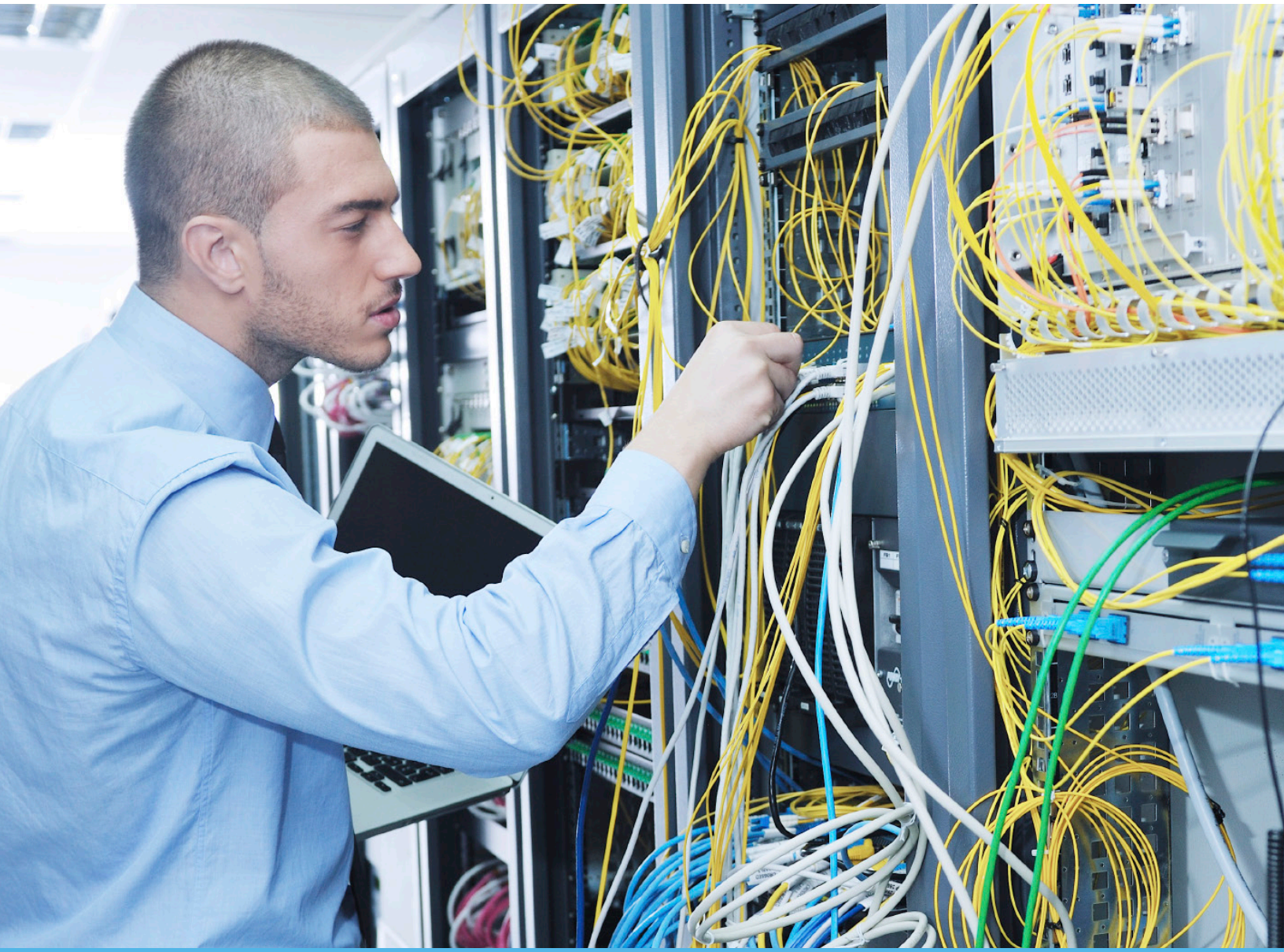
Rescue by LogMeIn

DIE ARCHITEKTUR UND SICHERHEIT VON LOGMEIN RESCUE

Übersichtsbroschüre



Inhalt

EINLEITUNG

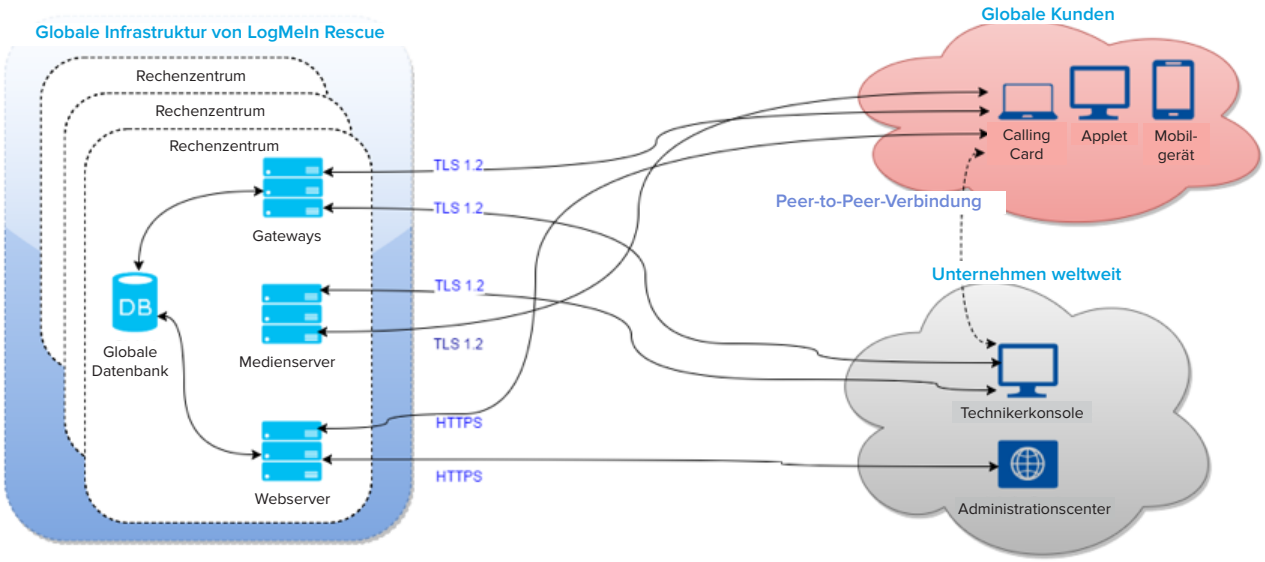
Skalierbarkeit, Sicherheit, Zuverlässigkeit, Benutzerfreundlichkeit. Diese vier Eigenschaften machen eine gute Fernsupportlösung aus; sie gehen jedoch nicht immer Hand in Hand. Fernsupportlösungen, die zwei oder drei dieser Eigenschaften besitzen, gibt es in Hülle und Fülle – aber eine Lösung, die alle vier Kriterien erfüllt, findet man selten. LogMeIn, Inc. hat mit LogMeIn Rescue genau so eine Lösung entwickelt.

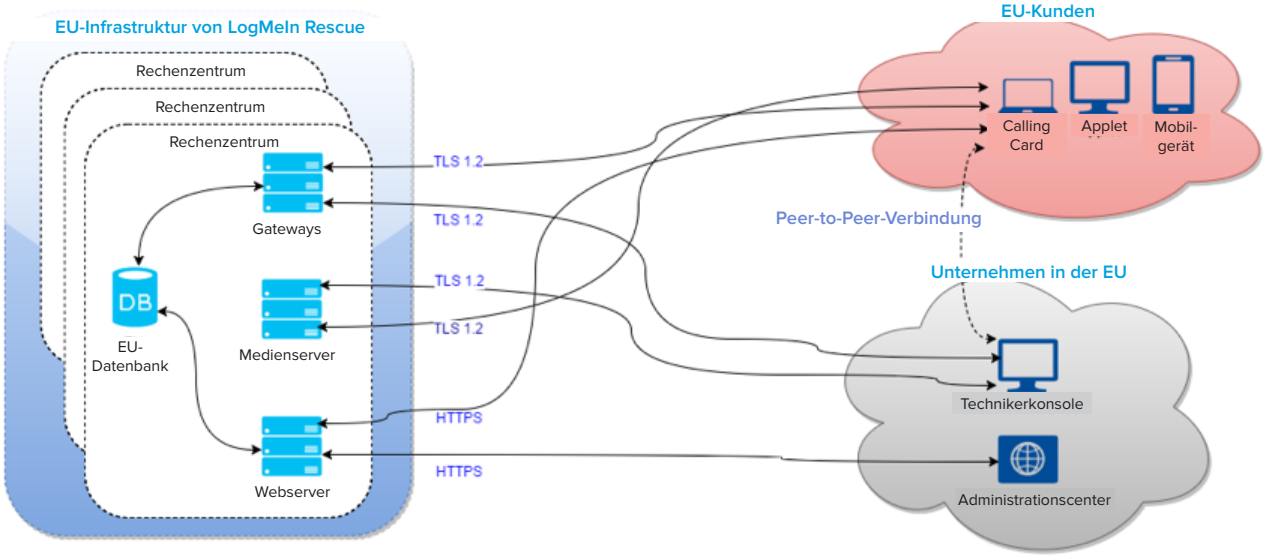
Skalierbarkeit. Egal, ob Sie nur einen Techniker beschäftigen oder ein Callcenter mit 10.000 Mitarbeitern betreiben – Rescue ist die Lösung für Sie, um Ihre Arbeit zu erledigen.

Sicherheit. Die Supportsitzungen werden mittels 256-Bit-AES- Verschlüsselung durchgängig zwischen Ausgangs- und Zielgerät geschützt. Alle Supportmaßnahmen müssen vom Endbenutzer genehmigt werden, bevor sie der Techniker ausführen kann. Die Sitzungsprotokolle werden für später verschlüsselt in einer Datenbank gespeichert und die Fernsteuerungssitzungen lassen sich als Videodatei aufzeichnen.

Zuverlässigkeit. LogMeIn Rescue wird in sechs Carrier-Grade-Rechenzentren mit vollständig redundanter Infrastruktur gehostet.

Benutzerfreundlichkeit. Das System lässt sich von Ihren Technikern innerhalb weniger Stunden in Betrieb nehmen. Die von Ihnen betreuten Endbenutzer können mit nur wenigen Klicks Support anfordern. Es muss weder auf Techniker- noch auf Endbenutzerseite Software installiert werden.





VERTRAULICHKEIT DER DATEN

Sicherheit wird oft mit Datenvertraulichkeit gleichgesetzt, und die Datenvertraulichkeit wiederum mit Verschlüsselung. Die Verschlüsselung wird dann anhand des verwendeten symmetrischen Kryptosystems und der Länge des Schlüssels charakterisiert. Diese falsche Auffassung führt häufig zu Fehlbezeichnungen wie etwa „256-Bit AES Secure". Dies ist natürlich irreführend.

Ein sicheres Online-System muss folgende Kriterien erfüllen:

- Authentifizierung der kommunizierenden Parteien
- sichere Aushandlung der verwendeten Schlüssel, ohne dass sie von Dritten abgefangen werden können
- vertraulicher Nachrichtenaustausch
- Möglichkeit zur Erkennung von Nachrichten, die während der Übertragung modifiziert wurden

Die Verschlüsselungsprotokolle SSL bzw. TLS (Secure Sockets Layer und Transport Layer Security) wurden speziell für diese Verfahren und Zwecke entwickelt. Sie wurden erstmals Mitte der 90er von der Netscape Communications Corporation veröffentlicht und haben sich mittlerweile als Industriestandard für die sichere Kommunikation über das Internet etabliert. SSL/TLS wird unter anderem von Visa, MasterCard und American Express eingesetzt.

Die von LogMeIn Rescue genutzte SSL-Implementierung ist OpenSSL (http://www.openssl.org). LogMeIn setzt immer die neueste verfügbare Version ein. Zum Zeitpunkt der Veröffentlichung arbeitete Rescue mit Version 1.0.2j.

SCHLÜSSELVEREINBARUNG

Zum Beginn einer Supportsitzung, wenn die Verbindung zwischen dem Endbenutzer und dem Techniker hergestellt wird, müssen sich ihre Computer auf einen Verschlüsselungsalgorithmus und den dazugehörigen Schlüssel einigen, der für die gesamte Dauer der Sitzung verwendet wird. Die Bedeutung dieses Schrittes wird oft unterschätzt – aus relativ verständlichen Gründen: Die Schlüsselvereinbarung klingt nach einer simplen Angelegenheit, die sich einfach und schnell erledigen lässt.

Es ist allerdings ganz und gar nicht einfach: Um so genannte Man-in-the-Middle-Angriffe zu verhindern, bei denen sich ein Computer C zwischen die Computer A und B schaltet und sich sowohl A als auch B gegenüber als der jeweils andere Teilnehmer ausgibt, müssen Zertifikate verwendet werden. Da weder der Techniker noch der Endbenutzer auf ihrem Computer Serversoftware und ein SSL-Zertifikat installiert haben, wenden sich beide an einen LogMeIn-Rescue-Server, um die erste Phase der Schlüsselvereinbarung mit diesem Computer abzuwickeln. Das Zertifikat wird sowohl von der Technikerkonsole als auch dem Applet des Endbenutzers überprüft, um sicherzustellen, dass der Vermittler garantiert ein Rescue-Server ist.

NACHRICHTENAUSTAUSCH

Das TLS-Protokoll ist mit einer großen Anzahl von Verschlüsselungssammlungen kompatibel, und die kommunizierenden Teilnehmer können sich auf ein Verschlüsselungsverfahren einigen, das von beiden unterstützt wird. Dies erfüllt vor allem zwei Hauptzwecke: Erstens lässt sich das Protokoll um neue Verschlüsselungssammlungen erweitern, ohne die Abwärtskompatibilität zu beeinträchtigen, und zweitens können Sammlungen, bei denen kryptographische Schwächen erkannt wurden, in neueren Ausführungen weggelassen werden.

Da alle drei Komponenten des Kommunikationssystems von LogMeIn Rescue der Kontrolle LogMeIns unterliegen, wird immer dieselbe Verschlüsselungssammlung eingesetzt: AES256-SHA im CBC-Modus (Cipher Block Chaining) mit RSA-Schlüsselvereinbarung. Das bedeutet:

- Die Verschlüsselungsschlüssel werden wie im vorigen Abschnitt beschrieben über aus privaten und öffentlichen RSA-Schlüsseln bestehende Schlüsselpaare ausgetauscht.
- Als Ver-/Entschlüsselungsalgorithmus kommt das Kryptosystem AES (Advanced Encryption Standard) zum Einsatz.
- Der Verschlüsselungsschlüssel hat eine Länge von 256 Bit.
- Als Grundlage für die Nachrichtenauthentifizierungscodes (MACs) wird SHA-2 verwendet. Ein MAC ist ein kurzer Datensatz, der zur Authentifizierung einer Nachricht dient. Der MAC-Wert schützt sowohl die Integrität einer Nachricht als auch ihre Authentizität, da die kommunizierenden Teilnehmer anhand dieses Codes erkennen können, ob die Nachricht auf irgendeine Weise modifiziert wurde.

- Der CBC-Modus sorgt dafür, dass jeder Chiffretextblock von allen vorangegangenen Klartextblöcken abhängt, und dass ähnliche Nachrichten im Netzwerk nicht als solche erkennbar sind.

Auf diese Weise wird sichergestellt, dass die zwischen dem Endbenutzer und dem Techniker übertragenen Daten durchgängig verschlüsselt sind und nur die betreffenden Teilnehmer Zugriff auf die im Nachrichtenstrom enthaltenen Daten haben.

AUTHENTIFIZIERUNG UND AUTORISIERUNG

Bei der Authentifizierung und Autorisierung in LogMeIn Rescue handelt es sich um zwei verschiedene Prozesse mit unterschiedlichen Zielen.

Die Authentifizierung stellt sicher, dass der Techniker bzw. Administrator, der sich beim Rescue-System anmeldet, tatsächlich die Person ist, für die er sich ausgibt. Bei Rescue erfolgt die Authentifizierung relativ unkompliziert: Dem Techniker wird von seinem Administrator eine Login-ID (normalerweise seine E-Mail-Adresse) samt Passwort zugewiesen. Zu Beginn seines Arbeitstages gibt der Techniker diese Zugangsdaten dann in das Anmeldeformular auf der LogMeIn-Rescue-Website ein.

Bei LogMeIn Rescue authentisiert sich zunächst das Rescue-System über sein Premium-SSL-Zertifikat mit 2048-Bit-RSA-Schlüssel dem Techniker (bzw. seinem Browser) gegenüber. Dies stellt sicher, dass der Techniker seinen Benutzernamen und sein Passwort auf der richtigen Website eingibt. Der Techniker meldet sich dann mit seinen Zugangsdaten beim System an.

LogMeIn Rescue speichert keine Passwörter, sondern generiert stattdessen mit Hilfe von scrypt Hashwerte aus den Passwörtern, die dann in der Rescue-Datenbank gespeichert werden. Die Hashwerte werden mit einem 24 Zeichen langen Salt versehen, welcher von einem kryptographisch sicheren Zufallszahlengenerator (CSPRNG) für jedes individuelle Passwort erstellt wird.

LogMeIn Rescue bietet den Administratoren die Möglichkeit, eine Reihe von Passwortrichtlinien durchzusetzen:

- Die Administratoren können eine Mindestanforderung an die Passwortqualität sowie ein maximales Passwortalter festlegen. Hierbei sehen die Administratoren und Techniker die Qualität des gewählten Passworts auf der integrierten Messanzeige.
- Die Techniker können dazu gezwungen werden, ihr Rescue-Passwort bei der nächsten Anmeldung zu ändern.
- Master-Administratoren können die Mitglieder ihrer Organisation dazu zwingen, bei der Rescue-Anmeldung die zweistufige Verifizierung zu verwenden.

LogMeIn Rescue ermöglicht es den Administratoren außerdem, eine SSO-Richtlinie für die Einmalanmeldung (Single Sign-On) umzusetzen. Dabei kommt die Security Assertion Markup Language (kurz SAML) zum Einsatz; ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen zwei Sicherheitsdomänen (zwischen einem Identitätsanbieter und einem Dienstanbieter). Die Techniker können dann nur auf bestimmte vordefinierte Anwendungen zugreifen und nutzen zur Anmeldung bei diesen Anwendungen eine einzige SSO-ID. Die SSO-ID eines Technikers lässt sich per Knopfdruck außer Kraft setzen.

Bei der zweistufigen Verifizierung werden Rescue-Konten mit Hilfe von LastPass Authenticator um eine zweite Schutzschicht erweitert. Die ausgewählten Mitglieder der Organisation müssen dabei eine zusätzliche Möglichkeit einrichten, ihre Identität zu bestätigen. Die Einrichtung der Authenticator-App wird in folgenden Fällen ausgelöst:

- Der ausgewählte Benutzer versucht, sich auf der sicheren Website bei seinem Rescue-Konto anzumelden.
- Der ausgewählte Benutzer versucht, sich bei der Computer-App der Technikerkonsole anzumelden.
- Der ausgewählte Benutzer versucht, sein Rescue-Passwort zu ändern.

Technisches Whitepaper von LastPass: https://enterprise.lastpass.com/wp-content/uploads/LastPass-Technical-Whitepaper-3.pdf

Eine Autorisierung wiederum findet sehr oft statt – mindestens einmal pro Fernsupportsitzung. Nachdem der Endbenutzer, für den Support geleistet werden soll, das Applet heruntergeladen und ausgeführt hat, nimmt ein Techniker Kontakt mit ihm auf. Der Techniker kann über das Applet mit dem Endbenutzer chatten, aber alle anderen Maßnahmen wie etwa das Senden einer Datei oder die Anzeige des Remotedesktops müssen vom Benutzer ausdrücklich genehmigt werden. Es kann auch eine „einzige Aufforderung“ für

alle Berechtigungen gesendet werden. Dies ist für langwierige Fernsupportsitzungen gedacht, wenn der Kunde unter Umständen nicht die ganze Zeit anwesend ist. Wenn diese Option für eine Technikergruppe aktiviert ist, können die Mitglieder dieser Gruppe vom jeweiligen Kunden eine „globale“ Berechtigung anfordern. Wird diese gewährt, so können sie beispielsweise die Systeminformationen anzeigen oder die Fernsteuerung starten, ohne dass eine weitere Genehmigung durch den Endbenutzer erforderlich ist.

Administratoren können ihren Technikern auch IP-Adressen-Beschränkungen auferlegen. Wenn diese Option aktiviert ist, lassen sich die verfügbaren IP-Adressen auf eine sehr kurze Liste beschränken. Techniker, denen eine bestimmte Aufgabe zugewiesen wurde, können dann nur von einer zuvor für diese Aufgabe genehmigten IP-Adresse auf Rescue zugreifen.

Der Administrator einer Technikergruppe kann außerdem im Administrationscenter bestimmte Funktionen deaktivieren. Er kann zum Beispiel verhindern, dass die Mitglieder einer Technikergruppe Dateien von den Endbenutzern empfangen können. Hier sehen Sie einige Berechtigungen, die der Administrator gewähren bzw. verweigern kann:

- Fernsteuerung starten
- Neustart
- Desktopansicht starten
- Sitzungen aufzeichnen
- Dateien senden und empfangen
- private Sitzungen starten
- Datei-Manager starten
- Windows-Anmeldeinformationen anfordern
- URLs senden
- Zwischenablage synchronisieren
- Systeminformationen anzeigen
- Skripte ausführen
- eine einzige Aufforderung für alle Berechtigungen verwenden
- Sitzungen übertragen
- Bildschirm für Kunden freigeben

Das Rescue-System authentisiert sich auch dem Endbenutzer gegenüber, für den Support geleistet wird. Das vom Benutzer heruntergeladene und ausgeführte Applet ist mit LogMeIns Codesignaturzertifikat (welches auf einem 2048-Bit-RSA-Schlüssel basiert) signiert. Diese Information wird dem Benutzer üblicherweise in seinem Webbrowser angezeigt, bevor er die Software ausführt.

Der Endbenutzer, der Support erhält, muss sich nicht authentisieren. Es liegt in der Verantwortung des Technikers, die Identität des Benutzers festzustellen – entweder per Chat oder telefonisch. Das Rescue-System verfügt über authentifizierungsähnliche Mechanismen wie etwa eindeutige PIN-Codes; diese sind jedoch zur Weiterleitung der Supportsitzungen an die korrekte private oder gemeinsame Warteschlange und nicht als Authentifizierungsmethode gedacht.

ÜBERWACHUNG UND PROTOKOLLIERUNG

Jeder Anbieter von Fernsupportlösungen muss großen Wert auf Fragen der Verantwortlichkeit und Rechenschaftspflicht legen. LogMeIn Rescue verfügt daher über zwei verschiedene Überwachungsfunktionen.

Zunächst einmal wird ein sogenanntes „Chatprotokoll“ in der Datenbank von Rescue gespeichert. Das Chatprotokoll wird von der Technikerkonsole in Echtzeit an die Rescue-Server übermittelt und enthält die Ereignisse sowie die Chatnachrichten einer bestimmten Supportsitzung. In der Protokolldatei wird beispielsweise aufgezeichnet, wann die Fernsteuerung gestartet bzw. beendet oder eine Datei vom Techniker an den Endbenutzer gesendet wurde. Dazugehörige Metadaten wie etwa der Name und der MD5-Hash-Fingerabdruck der übertragenen Datei werden gegebenenfalls ebenfalls im Protokoll vermerkt. Die Datenbank mit den Chatprotokollen lässt sich über das Administrationscenter abfragen. Zum Zeitpunkt der Veröffentlichung dieses Dokuments sahen LogMeIns Aufbewahrungsrichtlinien vor, dass die Inhalte der Chatprotokolle nach dem Ende einer Fernsupportsitzung zwei Jahre lang online und danach zwei Jahre lang im Archiv verfügbar sein mussten. Zur leichteren Anbindung an CRM-Systeme kann LogMeIn Rescue Sitzungsdaten auch an eine URL senden. Die Administratoren können dabei wählen, ob die Chatnachrichten in diese Daten einbezogen werden sollen. Die aufgezeichneten Chatnachrichten zwischen Techniker und Kunde können zudem auch automatisch aus den im Res-

cue-Datenzentrum gespeicherten Sitzungsdaten weggelassen werden.

Zweitens ermöglicht es LogMeIn Rescue den Technikern, während der Desktopansicht oder der Fernsteuerung aufgetretene Ereignisse als Videodatei zu speichern. Diese Funktion ist aus Gründen der Rechenschaftspflicht und Haftung von großer Bedeutung. Die Aufnahmen werden in einem vom Techniker gewählten Verzeichnis gespeichert. In großen Supporteinrichtungen sollte sich dieser Speicherort auf einem Netzwerkserver befinden. Der von diesen Aufnahmen beanspruchte Speicherplatz kann stark variieren und ist ausschließlich von den Inhalten auf dem Gerät des Endbenutzers und deren Komprimierbarkeit abhängig. Auswertungen von Millionen von Fernsteuerungssitzungen, die mit LogMeIn durchgeführt wurden, ergaben, dass der durchschnittliche Speicherplatzverbrauch einer Minute an Fernsteuerungsdaten zwischen 372 und 1024 kByte liegt. Die Aufnahmen werden entweder direkt im AVI-Format oder in einem LogMeIn-eigenen Zwischenformat gespeichert, das mit Hilfe des Tools „Rescue AVI Converter“ in eine gewöhnliche AVI-Datei umgewandelt werden kann. Der Konvertierer steht unter help.logmein.com zum Download zur Verfügung. Das proprietäre LogMeIn-Format, RCREC genannt, kann die Größe der Aufnahmen um rund zehn Prozent verringern.

ARCHITEKTUR DER RECHENZENTREN

LogMeIn Rescue wird in hochmodernen und sicheren Rechenzentren gehostet, die wie folgt ausgestattet sind:

- mehrstufige Sicherheitskontrollen, biometrische Zugangskontrollsysteme, Rund-um-die-Uhr-Videoüberwachung und Alarmüberwachung
- unterbrechungsfreie und redundante Stromversorgung (Gleich- und Wechselstrom), Notstromgeneratoren vor Ort
- redundante HLK-Konstruktion mit Unterbodenlüftung für ideale Temperaturregelung
- Rauchmelder über und unter dem Doppelboden; doppelt gesicherte, vorgesteuerte Trockensprinkleranlage

Die Infrastruktur von LogMeIn Rescue selbst ist äußerst sicher und zuverlässig:

- Redundanz auf Serverkomponentenebene: redundante Stromversorgung und Lüfter, RAID-1-gespiegelte Festplatten
- Redundanz auf Serverebene: je nach Rolle Aktiv/Passiv-Cluster oder Aktiv/Aktiv-Cluster
- Redundanz auf Rechenzentrumsebene: sechs Rechenzentren (US-Westküste, mittlerer Teil der USA, mittlerer südlicher Teil der USA, US-Ostküste, London (Großbritannien) und Frankfurt (Deutschland)) mit so gut wie verzögerungsfreier Ausfallsicherung
- doppelt redundante Firewalls, bei denen nur die Ports 80 und 443 geöffnet sind
- Aktiv/Passiv-Datenbankcluster
- redundanter Lastenausgleich inkl. SSL
- redundante Web- und Anwendungsservercluster mit Lastenausgleich
- redundante Gatewayservercluster mit Lastenausgleich

ÜBERBLICK ÜBER DEN ÜBERGABEPROZESS DES LOGMEIN-RESCUE-GATEWAYS

Beim Starten des digital signierten Rescue-Applets auf einem Computer geschieht Folgendes:

- Das Applet enthält einen GUID (Globally Unique Identifier) zur Sitzungsauthentifizierung, der beim Download von der Website als Ressource in die .exe-Datei eingebettet wurde.
- Daraufhin wird eine Liste der verfügbaren Gateways von secure.logmeinrescue.com heruntergeladen.
- Das Applet wählt ein Gateway aus der Liste aus und stellt mittels TLS eine Verbindung zu ihm her; das Gateway wird anhand seines SSL-Zertifikats vom Applet authentifiziert.
- Das Gateway authentifiziert das Applet mit dem GUID und verzeichnet in der Datenbank, dass der Benutzer auf einen Techniker wartet.

Beim Aufrufen einer Sitzung in der Rescue-Technikerkonsole geschieht Folgendes:

- Es wird eine Anfrage mit dem Sitzungsauthentifizierungs-GUID an das Gateway gesendet, um eine Re-

lay-Verbindung zwischen der Technikerkonsole und dem Kunden-Applet herzustellen.

- Das Gateway authentifiziert die Verbindung und beginnt mit der Datenübertragung über die Transportschicht (Relay-Daten werden nicht entschlüsselt).

Nach dem Aufbau einer Relay-Verbindung versuchen die Teilnehmer, eine Peer-to-Peer-Verbindung (P2P) herzustellen:

- Das Applet wartet nun auf eine TCP-Verbindung über einen von Windows zugewiesenen Port.
- Wenn innerhalb einer bestimmten Zeitdauer (zehn Sekunden) keine TCP-Verbindung aufgebaut werden kann, versucht das System, mit Hilfe des Gateways eine UDP-Verbindung herzustellen.
- Sobald eine TCP- oder UDP-Verbindung besteht, wird der P2P-Kanal (mit Hilfe des Sitzungsauthentifizierungs-GUIDs) von den Teilnehmern authentifiziert und der Datenverkehr von der Relay-Verbindung auf diesen Kanal übertragen.
- Im Falle einer UDP-Verbindung wird TCP mit Hilfe von XTCP, einem LogMeIn-eigenen Protokoll, das auf dem BSD-TCP-Stapel basiert, über den UDP-Datagrammen emuliert.

Alle Verbindungen werden durch das TLS-Protokoll gesichert (mittels AES-256-Bit-Verschlüsselung mit SHA-256-MACs). Beim GUID zur Sitzungsauthentifizierung handelt es sich um einen 128 Bit langen, kryptographisch zufälligen ganzzahligen Wert.

DATENBANK

- Alle Daten, die sensible Informationen enthalten, werden mittels 256-Bit-AES-Verschlüsselung geschützt (Chatprotokoll und benutzerdefinierte Felder).
- Die Rescue-Datenbank wird alle 24 Stunden automatisch gesichert. Die Backup-Datenbank wird mit derselben Verschlüsselung wie das Original im Rechenzentrum gespeichert.
- Die Data-Residency-Option von Rescue ermöglicht es Ihnen, den Speicherort der Endbenutzerdaten festzulegen: entweder innerhalb der Europäischen Union (Frankfurt, London) oder in den USA. LogMeIn garantiert jenen Nutzern, die die EU als Datenspeicherort wählen, dass sie ausschließlich mit Rechenzentren innerhalb der EU verbunden werden und dass die Kundendaten die gewählte Region nie verlassen. Es gibt keine Verbindung zwischen unseren EU- und US-basierten Rechenzentren.

DIE MEDIENARCHITEKTUR VON RESCUE

Beim Mediendienst von Rescue handelt es sich um einen eigenständigen Dienst, der auf WebRTC aufgebaut ist und das Videostreaming mit Rescue Lens möglich macht. Er wickelt für jene Rescue-Sitzungen, bei denen die Lens-Funktion zum Einsatz kommt, sogenannte „Konferenzen“ ab. Die Konferenzteilnehmer (Peers) treten den Konferenzen bei und verlassen sie, und die Clients senden Video- und Audiostreams, die dann von den anderen Teilnehmern empfangen werden. Lens überträgt die Videoinhalte in eine Richtung von der Lens-App an die Technikerkonsole.

Der Mediendienst besteht aus drei Hauptkomponenten: dem MediaSDK, dem Sitzungsmanager und dem Streamingserver. Diese Komponenten sind für das Erstellen/Löschen und das Beitreten/Verlassen von Konferenzen zuständig. Sie kommunizieren über die bestehenden sicheren Kommunikationskanäle zwischen der Technikerkonsole und der Rescue-Website sowie der Lens-App und der Website.

MediaSDK

Der Mediendienst ist auf WebRTC aufgebaut, und zwar in Form eines dünnen Wrappers über der WebRTC-Codebasis. Dieses sogenannte MediaSDK kommt in der Technikerkonsole und den Lens-Apps für mobile Endgeräte zum Einsatz.

Sitzungsmanager

Der Sitzungsmanager ist eine einfache Website mit Lastenausgleich, die eine REST-API zur Verwaltung der Konferenzen (Erstellen/Löschen/Beitreten/Verlassen) bereitstellt. Der Sitzungsmanager nimmt nur Anforderungen von der Rescue-Website an.

Streamingserver

Der Mediendienst nutzt Jitsi, eine Open-Source-Lösung für Streamingserver, um die Streams zwischen den Peers (der Technikerkonsole und der Lens-App) zu übertragen. Sowohl die Technikerkonsole als auch die Lens-App sind mit dem Streamingserver verbunden. Die Lens-App streamt

ihre Videoinhalte an den Streamingserver. Der Server streamt die Videoinhalte an die Technikerkonsole. Jitsi fungiert wie ein Relayserver zwischen den Peers. Eine Lens-Sitzung besteht aus zwei Streams (einer wird gesendet; der andere wird empfangen).

FÜR LOGMEIN RESCUE GELTENDE BRANCHEN-STANDARDS

SOC 2

LogMeIn Rescue ist für SOC 2 (Service Organization Control 2) zertifiziert, was Kunden die Gewissheit gibt, dass wir die richtigen Kontrollen zum Schutz ihrer wichtigen Daten einsetzen.

SOC 2 ist ein umfassendes Prüfverfahren, bei dem – aufbauend auf verschiedenen Prinzipien und Kriterien – die zur Datenverarbeitung verwendeten Steuerungsmechanismen sowie die Vertraulichkeit der von diesen Systemen verarbeiteten Informationen getestet werden. Um die SOC-2-Konformität aufrechtzuerhalten, muss sich LogMeIn jedes Jahr erneut einer Prüfung unterziehen. SOC 2 gilt US-weit in vielen Branchen als „Goldstandard" für Softwareanbieter, und der regelmäßige Erwerb der SOC-2-Bescheinigung ist ein weiterer Beweis für unser Engagement in Sachen Sicherheit und Datenschutz.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein Gesetz der Europäischen Union (EU) über den Schutz der Daten und der Privatsphäre aller Personen in der EU. Hauptziel der DSGVO ist es, den Bürgern und Einwohnern mehr Kontrolle über ihre personenbezogenen Daten zu geben und das regulatorische Umfeld innerhalb der EU zu vereinfachen. LogMeIn Rescue gibt seinen Benutzern die Kontrolle über die in ihrem Namen gespeicherten Daten („Inhalt", wie in den Nutzungsbedingungen definiert), damit sich diese auf ihr Kerngeschäft konzentrieren und gleichzeitig effizient auf die DSGVO vorbereiten können.

- Rescue-Benutzer sind in der Lage, ihre Daten über die Berichterstattungsfunktion des Administrationscenters oder die Rescue-APIs zu exportieren.
- Rescue-Benutzer können ihre auf LogMeIn-Rescue-Servern gespeicherten Daten löschen.
  - Es lassen sich alle Daten in Zusammenhang mit einem Supporttechniker löschen.
  - Es lassen sich alle Daten in Zusammenhang mit einer Supportsitzung löschen, darunter personenbezogene Daten, die sich auf Kunden beziehen bzw. an sie gebunden sind.

Auf diese Weise ermöglicht es LogMeIn Rescue seinen Benutzern, die Vorschriften und Anforderungen der DSGVO zu erfüllen.

Nähere Informationen zur DSGVO finden Sie auf der DSGVO-Website von LogMeIn.

HIPAA

LogMeIn hat zwar keine Kontrolle über die während einer Supportsitzung von den Benutzern ausgetauschten Inhalte, aber der LogMeIn-Rescue-Dienst ist so konzipiert, dass er selbst die strengsten Sicherheitsrichtlinien erfüllt und Einrichtungen, die den Datenschutzauflagen des amerikanischen Health Insurance Portability and Accountability Acts (HIPAA) unterliegen, bei der Einhaltung der entsprechenden regulatorischen Vorgaben hilft.

Möglichkeiten zur Zugriffskontrolle

- Berechtigungen lassen sich detailgenau zuweisen (bestimmte Techniker können z. B. den Bildschirm nur ansehen, das Remotegerät aber nicht steuern).
- Auf den Servern in LogMeIns Rechenzentren werden keine Daten von Remotegeräten gespeichert (sondern wie oben erwähnt nur Sitzungs- und Chatprotokolle). Die gesendeten Chatnachrichten können außerdem aus den aufgezeichneten Sitzungsdaten weggelassen werden.
- Berechtigungen lassen sich so festlegen, dass die Techniker keine Dateien übertragen und daher keine Dateien von Remotegeräten „entwenden" können.

- Der Endbenutzer muss am Remotegerät anwesend sein, um den Fernzugriff zu genehmigen.
- Der Endbenutzer behält stets die Kontrolle und kann die Sitzung jederzeit beenden.
- Die Nutzung bestimmter Funktionen kann den Technikern untersagt werden, bis sie der Endbenutzer ausdrücklich genehmigt hat (z. B. Fernsteuerung, Desktopansicht, Dateiübertragung, Abrufen der Systeminformationen, Neustart und Wiederherstellung der Verbindung).
- Die Zugriffsrechte werden nach Beendigung der Sitzung automatisch aufgehoben.
- Wenn der Techniker für eine zuvor festgelegte Zeitdauer inaktiv ist, wird er automatisch abgemeldet.
- Hosting in redundanten Carrier-Grade-Rechenzentren mit sicherem, beschränkten Zugang

Überwachungsmechanismen

- Option zur zwingenden Sitzungsaufzeichnung mit der Möglichkeit, die Protokolldateien in einem sicheren freigegebenen Netzwerk zu speichern
- Auf dem Hostcomputer wird zu Sicherheits- und Qualitätsprüfungszwecken ein Protokoll mit den Sitzungen und Aktivitäten der Techniker beim Fernzugriff erstellt (erfolgreiche Anmeldungen, fehlgeschlagene Anmeldungen, Start der Fernsteuerung, Ende der Fernsteuerung, Neustart initiiert, Abmeldung).
- Authentifizierung von Personen bzw. Einheiten
- Die Identität des Technikers wird über eine eindeutige E-Mail-Adresse oder eine SSO-ID definiert und der Techniker muss sich authentisieren.
- Bei übermäßig vielen fehlgeschlagenen Anmeldeversuchen wird das Konto gesperrt.
- Möglichkeit, den Technikern die Anmeldung nur von bestimmten IP-Adressen aus zu gestatten

Sicherheit der Datenübertragung

- durchgängige 256-Bit-AES-Verschlüsselung des gesamten Datenverkehrs zwischen Ausgangs- und Zielgerät
- MD5-Hash für eine bessere Rückverfolgbarkeit der übertragenen Dateien

SCHLUSSBEMERKUNG

Die Entscheidung für eine Fernsupportlösung wird häufig auf Basis ihrer Funktionen und ihres Preises getroffen. Da Sie dieses Dokument lesen, haben Sie wahrscheinlich bereits festgestellt, dass LogMeIn Rescue Ihre Bedürfnisse diesbezüglich erfüllt. Mit unseren Ausführungen oben konnten wir Sie hoffentlich davon überzeugen, dass die Architektur von Rescue das richtige Maß an Skalierbarkeit, Sicherheit, Zuverlässigkeit und Benutzerfreundlichkeit aufweist.