islonline

Sicherheitserklärung

Änderungsstand: 8. Mai 2018

Einführung

Dieses Dokument enthält Informationen über die Sicherheit für die Benutzer von ISL Online Remote-Desktop-Software. Es wurde erstellt, um den technischen Hintergrund und die Sicherheits-Standards zu beschreiben, die in den ISL Online-Produkten implementiert sind. Gerne kann dieses Dokument an Kollegen, Partner oder Kunden verteilt werden, um eventuell bestehende Sicherheitsfragen zu klären.

Über uns

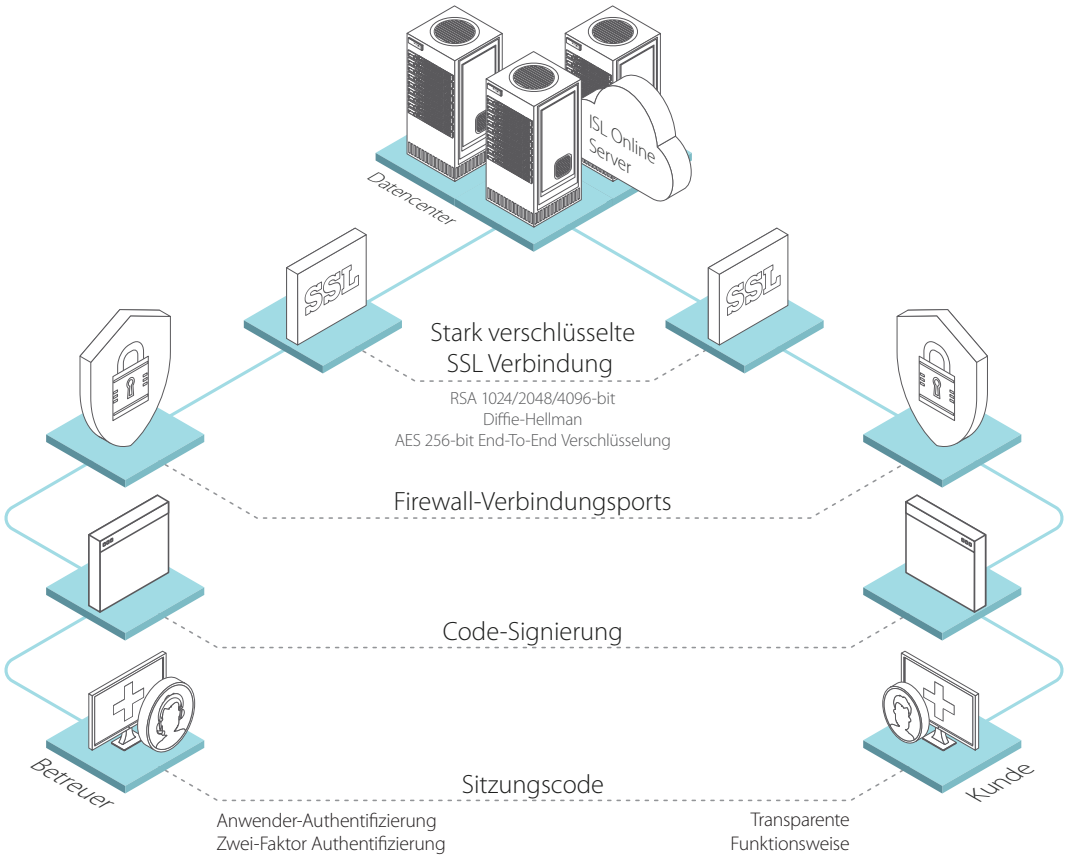
ISL Online ist ein Pionier in der Branche von Remote-Desktop-Support. Seit 2003 bietet ISL Online IT-Experten und Helpdesk-Technikern in mehr als 100 Ländern Fernsteuerungssoftware an, wobei Japan den stärksten Markt darstellt.

ISL Online kann über die Cloud oder per lokaler Eigeninstallation bereitgestellt werden und ermöglicht dem Benutzer, auf Windows-, Mac- oder Linux-Computer, sowie mobile Geräte zuzugreifen und diese zu steuern, um technischen Ad-Hoc-Support und Fernwartung bereitzustellen. Banken, Regierungsbehörden sowie globale Unternehmen setzen ISL Online aufgrund seines hohen Sicherheitsniveaus in der Remote-Support-Software-Industrie ein.

ISL Online wird von XLAB entwickelt, einer Softwareentwicklungsfirma mit Sitz in Slowenien und Niederlassungen in der Schweiz, Großbritannien und den USA. Wir arbeiten mit autorisierten Partnern in Europa, Asien / Pazifik, Nahost, Afrika und Lateinamerika zusammen und bedienen unsere Kunden praktisch weltweit. Besuchen Sie uns auf www.islonline.com .

Fordern Sie maximale Sicherheit

Bei ISL Online haben wir verstanden, dass bei der Ausführung von Verbindungen mit Remote-Computern für unsere Kunden die Informationssicherheit von größter Bedeutung ist. Daher wenden wir eine Reihe von Maßnahmen und Funktionen an, die ISL Online sicher machen und es ermöglichen, die strengen Sicherheitsstandards unserer Kunden zu erfüllen.



Zwei-Faktor Authentifizierung

Die Zwei-Faktor Authentifizierung bildet eine zusätzliche Sicherheitsebene beim Authentifizierungs-Prozess und macht einen unerlaubten Zugriff nahezu unmöglich.

Sitzungscode

Der Helpdesk-Betreuer übermittelt an seinen Kunden einen eindeutigen Sitzungscode, der sofort nach hergestellter Verbindung ungültig wird, und somit eine erneute Verbindung unter demselben Sitzungscode unmöglich macht.

Stärkste Verschlüsselung

Eine Remotedesktop-Supportverbindung mit einem Kunden wird über den RSA-2048/4096- Bit-Public-Private-Key-Austausch hergestellt. Bei einem erfolgreichen RSA-Schlüsselaustausch wird der gesamte Datenverkehr mit symmetrischen AES-256-Bit-Schlüsseln verschlüsselt.

Firewall-freundlich

ISL Online baut automatisch eine ausgehende Verbindung über die Ports 7615, 443 oder 80 auf, daher sollte die Funktion mit einer bestehenden Firewall ohne zusätzliche Konfiguration möglich sein.

Sicherheit auf einen Blick

RSA mit Diffie-Hellman Schlüsselaustausch	✓
AES 256-bit End-To-End Verschlüsselung	✓
Zwei-Faktor Authentifizierung (2FA)	✓
ISO 27001:2013 Zertifizierung (Informations-Sicherheitsmanagement)	✓
Port-Filtering	✓
Blacklisting / Whitelisting	✓
Code-Signierung	✓
Externe Sicherheits-Audits und Penetrations-Tests	✓
Funktions-Transparenz (Kein Stealth-Modus)	✓
Passwort-Verschlüsselung	✓
Schutz vor Brute-Force-Intrusion	✓
Intranet-Option (nur LAN)	✓
Reverse Proxy Support	✓
Option automatischer Sitzungsaufzeichnung	✓
Zugriffsverwaltung	✓
Incident Management System (IMS)	✓
Logs und Verantwortlichkeit	✓
Option der Funktionseinschränkung	✓
Externe Authentifizierung	✓
Datencenter & Metadaten	✓

Beachten Sie bitte:

ISL Online bietet verschiedene Hosting-Optionen (Cloud, Server-Lizenz, Private Cloud, Managed Private Cloud). Einige der in diesem Dokument beschriebenen Sicherheitsmaßnahmen sind nur für bestimmte Hosting-Optionen verfügbar. Bitte kontaktieren Sie uns für nähere Details (support@islonline.com).

RSA mit Diffie-Hellman Schlüsselaustausch

Um eine Remotedesktop-Supportverbindung mit einem Kunden herzustellen, muss der Helpdesk-Betreuer die ISL Light-Anwendung starten, die einen RSA 1024 Bit Public Key des ISL-Conference-Proxy Servers enthält. Eine erste Verbindung wird hergestellt, wenn der Public Key der ISL Light-Anwendung und Private Key des ISL-Konferenzproxyservers erfolgreich ausgetauscht und geprüft werden. Um die Authentizität der Übertragung zu gewährleisten, werden Industriestandard-X.509-Zertifikate verwendet. Diese PKI (Public Key Infrastructure) verhindert sogenannte „Man-in-the-Middle" Angriffe. Bei einem erfolgreichen Public / RSA 1024 Bit Private Key Austausch mit wird der kryptografische Algorithmus von Diffie-Hellman verwendet, um symmetrische AES-256-Bit-Schlüssel auszutauschen. Nach dem Austausch wird die gesamte nachfolgende Kommunikation zwischen der ISL Light-Anwendung und dem ISL Conference Proxy-Server mit symmetrischen AES 256-Bit-Schlüsseln verschlüsselt.

AES 256 Bit Ende-zu-Ende-Verschlüsselung

Wenn die Anwendungen ISL Light (Betreuer) und ISL Light Client (Kunde) auf dem ISL Conference Proxy-Server mit einem identischen eindeutigen Sitzungscode übereinstimmen, wird der neue SSL-Handshake gestartet, und ein AES 256-Bit-SSL-Tunnel mit verschlüsselter Datenübertragung hergestellt. Alle Informationen zwischen Betreuer und Kunden werden End-To-End verschlüsselt, sodass selbst der ISL Conference Proxy den Inhalt der Sitzung nicht entschlüsseln kann, sondern nur die Pakete von einer Seite auf eine andere überträgt.

Zwei-Faktor Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsebene für Helpdesk-Betreuer und IT-Experten. Bei aktivierter 2FA können sich Betreuer nur mit einem zweistufigen Verifizierungsprozess mittels Kennwort und einem 2FA-Token am ISL Online-System anmelden. Der zusätzliche zweite Faktor erhöht die Sicherheit und erschwert den Zugriff durch Unbefugte erheblich.

ISL Online empfiehlt grundsätzlich eine Zwei-Faktor-Authentifizierung, insbesondere auf hochsensiblen Systemen. Mit ISL Online können verschiedene Methoden für den zweiten Schritt der Verifizierung konfiguriert werden (E-Mail, Telefon, Authentifizierungs-App - TOTP, oder Sicherheitsschlüssel - Yubico-Schlüssel basierend auf FIDO U2F-Standard).

ISO / IEC 27001:2013 Zertifizierung (Informationssicherheit-Management)

Die ISO 27001:2013 ist international anerkannt und einer der am meisten anerkannten Standards für Informationssicherheit. Dieses Zertifikat legt die Anforderungen an ein umfassendes Informationssicherheits-Managementsystem (ISMS) fest und definiert, wie Organisationen Informationen sicher verwalten und handhaben müssen. Das Zertifikat wird nur an Organisationen vergeben, die einem strengen Audit-Prozess entsprechende Sicherheitspraktiken strikt befolgen.

Das ISO / IEC 27001:2013-Zertifikat bestätigt die Fachkenntnisse von ISL Online im Bereich Informationssicherheitsmanagement und dessen Bekenntnis zu höchster Sicherheit im gesamten Unternehmen.

Es ist ein weiterer Beweis dafür, dass mit ISL Online die Daten gut geschützt und sicher sind.
Neben der ISO 27001-Konformität werden bei ISL Online die internen Policen und Sicherheitsrichtlinien regelmäßig den von SSAE 16 (SOC 2) vorgeschlagenen „Best Practices“ angepasst.

Port-Filtering

Eine qualitative Remote-Desktop-Software kommt ohne zusätzliche Konfiguration der Firewall aus.
Mit ISL Online kann die bestehende Firewall unverändert bleiben, da ISL Light automatisch eine ausgehende Verbindung initiiert und versucht, eine Verbindung jeweils über die Ports 7615, 80 oder 443 herzustellen.

Größere Organisationen haben üblicherweise eigene Richtlinien für die Konfiguration ihrer Firewalls oder Proxies. Systemadministratoren können Port 7615 für den ISL Online Datenverkehr freischalten, wobei die restlichen Ports gefiltert werden, oder Ausnahmen bezüglich der DNS-Namen oder IP-Nummern konfigurieren.

Unabhängig von der Netzwerkkonfiguration wenden ISL Online-Anwendungen automatisch verschiedene Ansätze an, um einen funktionellen Transportweg zu finden (Erkennung von Proxy-Einstellungen, Verwendung von WinINet, Erstellung eines Tunnels, Nutzung des Wildcard-DNS usw.).

Blacklisting / Whitelisting

Remote-Desktop-Software ist ein sehr mächtiges Werkzeug, mit dem ferne Computer gesteuert werden können. Daher ist die Option für die Erstellung sogenannter „Whitelists" und „Blacklists" zur Verhinderung von Missbrauch der Remote-Desktop-Software in einem Unternehmen unerlässlich.

Zu diesem Zweck kann der Datenzugriff auf ISL Online-Server in ISL Online Anwendungen durch Einschränkungen der IP- und / oder MAC-Adressen eingeschränkt werden.
Mittels Funktion „allow" wird eine Liste von IP oder MAC-Adressen angelegt, die eine Remote-Support-Sitzung starten oder auf einen unbeaufsichtigten Computer zugreifen dürfen („Whitelist"). Im Gegenzug kann mit der Funktion „deny" eine Liste von IP oder MAC-Adressen erstellt werden, denen diese Aktionen untersagt werden („Blacklist"). Solche Regeln können für einen bestimmten Benutzer oder die gesamte Domäne auf einem ISL Online-Server definiert werden. Beispielsweise könnte Benutzern die Erlaubnis erteilt werden, Sitzungscodes für eine Remote-Support-Sitzung nur vom Büro aus zu generieren (IP-Adressbereich Ihres Unternehmens).

Code-Signierung

Die Code-Signierung wird häufig verwendet, um Software zu schützen, die über das Internet vertrieben wird. Die Code-Signierung nimmt keine Änderungen an der Software vor, sondern fügt dem ausführbaren Code lediglich eine digitale Signatur hinzu. Diese digitale Signatur garantiert dem Empfänger, dass die Remote-Desktop-Software tatsächlich von dem angegebenen Herausgeber stammt.
Es enthält genügend Informationen, um den Unterzeichner zu authentifizieren und sicherzustellen, dass der Code nicht nachträglich geändert wurde.

ISL Online-Anwendungen werden digital mit einem Code-Signierungs-Zertifikat signiert, das ISL Online als Software-Herausgeber zuverlässig identifiziert und garantiert, dass der Code seit seiner Unterzeichnung mit einer digitalen Signatur nicht verändert oder verfälscht wurde.

Externe Sicherheitsaudits und Penetrationstests

Regelmäßige systematische Sicherheitsaudits und eng fokussierte Penetrationstests sind für jeden, für die Informationssicherheit verantwortlichen Remote-Desktop-Softwareanbieter, von entscheidender Bedeutung. Sie ermöglichen es einem Unternehmen, potenzielle Schwachstellen und Sicherheitslücken rechtzeitig zu beheben.

Unabhängige Sicherheitsaudits und Penetrationstests an ISL Online-Anwendungen werden regelmäßig durchgeführt und zeigen, dass ISL Online ein vertrauenswürdiger Dienst ist, der ein sehr hohes Sicherheitsniveau bietet.

Funktions-Transparenz (kein Stealth-Modus)

Eine Remote-Desktop-Anwendung muss so konzipiert sein, dass diese niemals im Hintergrund und ohne Wissen des Kunden ausgeführt werden kann. Die Funktionalität der Software sollte vollständig transparent sein und der Kunde sollte in der Lage sein, die Aktionen des Helpdesk-Betreuers jederzeit verfolgen zu können.

ISL Online ist so konzipiert, dass eine Fernunterstützung über das Internet nur auf ausdrücklichen Wunsch des Kunden ausgeführt wird. Der Kunde erteilt dem Helpdesk-Betreuer die Freigabe zur Betrachtung und Kontrolle seines Computers und kann die Sitzung jederzeit auch beenden. Der Kunde kann dem Betreuer die Kontrolle seines Computers einfach entnehmen, indem er seine Maus bewegt. Nach beendeter Sitzung kann der Helpdesk-Betreuer nicht mehr mit demselben Sitzungscode auf den Computer des Kunden zugreifen.

Kennwortverschlüsselung

Die Sicherheit von Daten hängt nicht nur von der Stärke der Verschlüsselungsmethode ab, sondern auch von Faktoren wie Länge und Zusammensetzung des Kennworts, sowie angewandten Maßnahmen, die Kennwörter nicht in die Hände Dritter gelangen zu lassen.
Die ISL Online-Passwort-Sicherheitsrichtlinie basiert auf den neuesten NIST-Spezifikationen:
• Ein Kennwort muss mindestens 8 Zeichen lang sein;
• Alle führenden und nachgestellten Leerzeichen werden entfernt;
• Es sind alle druckbaren ASCII-Zeichen, sowie Leerzeichen zulässig.
Das Kennwort wird gegen eine „Blacklist", bestehend aus den gebräuchlichsten und einfachsten Passwörtern, die ein Sicherheitsrisiko darstellen könnten, geprüft.
ISL Online speichert Kennwörter nicht im Klartext, sondern verwendet fortschrittliche Kennwort-Hash-Methoden um die in Benutzerkontendatenbanken gespeicherten Passwörter zu schützen.

Schutz vor Brute-Force-Intrusion

Um unbefugten Zugriff zu verhindern, sollte auf der Remote-Desktop-Software ein Brute-Force-Schutz angewendet werden. Ein Brute-Force-Angriff ist eine Try&Error-Methode, bei der jede mögliche Kombination angewendet wird, um ein Kennwort oder eine verschlüsselte Datei zu entschlüsseln. Dabei wird automatisierte Software verwendet, die eine große Anzahl aufeinanderfolgender Versuche von Anmeldungen generiert, möglichst bis zum Erreichen einer erfolgreichen Anmeldung.

ISL Online hat eine Ratenbegrenzung für Anmelde- und Verbindungsversuche konfiguriert, um Brute-Force-Angriffe zu verhindern. ISL Online-Server verhindern Brute-Force-Intrusions- (Login-) Versuche, indem sie die maximale Anzahl fehlgeschlagener Anmeldeversuche für einen Benutzer oder für eine bestimmte Adresse im definierten Zeitraum begrenzen. Die Anmeldung kann auch zeitlich eingeschränkt werden, so dass diese nur in einem gegebenen Zeitraum zugelassen wird.

Intranet (nur LAN) Option

Einige große Organisationen verwenden ISL Online exklusiv für deren interne Unterstützung über verschiedene geografische Standorte hinweg. In solchen Fällen muss eine Remote-Desktop-Software das Einrichten von Remotedesktopsitzungen in einem lokalen Netzwerk (LAN) ermöglichen. Bei strikter Verwendung der ISL Online Anwendungen im LAN (Intranet) ist eine öffentliche IP-Adresse nicht erforderlich. Es wird lediglich eine private Adresse im Bereich privater Netzwerke benötigt (wie in RFC 1918 spezifiziert).

Reverse-Proxy-Unterstützung

Ein Reverse-Proxy macht einen direkten Internetzugriff auf Back-End-Server überflüssig, und verbirgt damit der Außenwelt die Topologie und Eigenschaften eines internen Netzwerkes. Man kann den Reverse-Proxy in eine mit dem Internet verbundene DMZ platzieren, aber gleichzeitig die Webserver in einem privaten Subnetz „verstecken". Dadurch wird das Risiko eines unbefugten Zugriffs auf sensible Daten verringert. ISL Online ermöglicht es, den Conference-Proxy-Server hinter einem Reverse-Proxy zu installieren, ohne diesen direkt dem Internet auszusetzen und SSL nur bis zum Reverse-Proxy zuzulassen.

Automatische Sitzungsaufzeichnungsoption

Remote-Desktop-Software sollte nicht nur die Datenübertragung selbst, sondern auch die Betreuer sowie deren Kunden durch die Möglichkeit einer Sitzungsaufzeichnung schützen. Dies gilt insbesondere für jene Unternehmen, die einem Wartungsunternehmen als Drittanbieter die Computerwartung anvertraut haben, und ihnen einen uneingeschränkten Fernzugriff auf ihre Computer gewähren.

ISL Online bietet eine leistungsstarke Option, die Aufzeichnung automatisch zu Beginn jeder Fernzugriffssitzung zu starten, um die volle Kontrolle über die Fernzugriffsaktivität zu haben und mögliche Konflikte mit Kunden zu vermeiden.

Zugriffsverwaltung

Zugriffsberechtigungen stellen, sofern es sich um eine oder wenige Personen mit Zugriffsberechtigung handelt, kein großes Problem dar. Bei zahlreichen Personen mit Zugriff auf fremde Computer ist dies jedoch ein sehr wichtiges Thema.
Mit ISL Online kann ein Konten-Administrator seinen Domänenbenutzern verschiedene Rechte und Einschränkungen zuweisen, einschließlich Aktivierung oder Deaktivierung des Zugriffs auf bestimmte Computer. Für jeden einzelnen Benutzer kann ebenfalls eine maximale Anzahl gleichzeitiger Sitzungen festgelegt, oder Rechte für die Verwendung von Audio-, Video-, Remote-Druckfunktionen, Dateiübertragung und Desktopfreigabe vergeben werden.

Incident Management System (IMS)

Remote-Desktop-Softwareanbieter sollten über ein Incident-Management-System (IMS) verfügen, das nach einer ungeplanten Unterbrechung eine schnelle Wiederherstellung des normalen Service-Betriebs ermöglicht.
ISL Online verwendet ein eigenes IMS, eine Reihe von Verfahren, die von ISL Online entwickelt wurden, um die gemeldeten Vorfälle optimal betreuen zu können, und diese gleichzeitig zu minimieren. Bei Meldung eines Vorfalls wird dieser im Ticketing-System angelegt und kann dort bearbeitet und verwaltet werden.

Jeder Vorfall enthält normalerweise die folgenden Elemente:
• Timeline UTC (ein Protokoll der Ereignisse in chronologischer Reihenfolge in der UTC-Zeitzone)
• Zusammenfassung (eine kurze Beschreibung des Vorfalls)
• Ursache (eine Erklärung der Ursache des Vorfalls)
• Lösung und Wiederherstellung (eine Beschreibung des Vorfallminderungsprozesses)
• Korrektur- und Präventivmaßnahmen (eine Erklärung der Maßnahmen, die ergriffen wurden, um solche Vorfälle in Zukunft zu verhindern)
• Andere wichtige Informationen

IMS ermöglicht es ISL Online, kontinuierliche Service-Niveaus aufrechtzuerhalten, die Verfügbarkeit von IT-Services zu messen, unerwünschte Ereignisse zu dokumentieren und deren Wiederholung möglichst zu minimieren.

Protokolle und Verantwortlichkeit

Die Führung von Protokollen und eine klare Verantwortlichkeit ermöglichen es, den Vorschriften möglichst vielzähliger Branchen zu entsprechen.

Mit ISL Online können IT-Administratoren Benutzer eindeutig identifizieren und feststellen, mit welchen Systemen zu welcher Zeit einer eine Verbindung stattgefunden hat, sowie bei einer aktivierten Sitzungsaufzeichnung verfolgen, welche Aktivitäten über die Fernverbindung getätigt wurden. Die Aufzeichnungen können für jede einzelne Sitzung Informationen über den Betreuer, den Kunden, sowie dessen IP-Adressen usw., offenlegen.

Zudem können Log-Aggregationen / Reporting-Lösungen von Drittanbietern (wie z. B. Kibana) ohne weiteres integriert werden.

Optionen der Funktionseinschränkung

Eine Remote-Desktop-Software ist ein universelles Werkzeug, das praktisch in allen Branchen eingesetzt wird. Dementsprechend gibt es unzählige verschiedene Anwendungsfälle, die sehr flexible Lösungen erfordern, und dabei auch eine Beschränkung der Funktionen in Bezug auf bestimmte Sicherheitsstandards erlauben.

Mit ISL Online können Funktionen eingeschränkt werden, die innerhalb einer Sitzung verfügbar sind: Steuerung des Remote-Computers, Übertragung von Dateien zwischen Kunde und Betreuer sowie viele andere Funktionen.

Ein Beispiel dafür, wo eine Funktionseinschränkung zur Anwendung kommt: Ein Bankangestellter sollte den Bildschirm eines Kunden sehen, niemals aber seinen eigenen Bildschirm den Kunden zeigen können. In diesem Fall kann die Desktopfreigabe auf der Betreuerseite deaktiviert werden.

Externe Authentifizierung

In das ISL Online-System können Verschiedene Typen von Authentifizierungsschemata, wie OpenLDAP, Microsoft Active Directory, Novell eDirectory oder RADIUS integriert werden. Bei konfigurierter externer Authentifizierung werden die Zugriffsrechte und Berechtigungen der Benutzer zur Verwendung der ISL Online-Software von IT-Administratoren verwaltet, die ihre eigenen internen Benutzerverwaltungsverzeichnisse verwenden.

Rechenzentren und Metadaten

Die Server von ISL Online (Public Cloud) werden von professionellen Rechenzentren auf der ganzen Welt gehostet. Dabei kommen explizit nur hochzuverlässige und industrieerprobte Rechenzentren zum Einsatz, mit zeitgemäßen Einrichtungen und Geräten, redundanten oder Reserve-Stromversorgungen, redundanten Datenkommunikationsverbindungen, Umgebungssteuerungen (z. B. Klimatisierung, Brandschutz) sowie zeitgemäßen Sicherheitsvorrichtungen. Die Master-Server von ISL Online befinden sich innerhalb der Europäischen Union in ISO 27001-zertifizierten Rechenzentren.

ISL Online Server werden ausschließlich von unseren Systemadministratoren unter Einhaltung strikter Kennwort-Richtlinien verwaltet. Aufgrund der AES-Sicherheitsrichtlinie für 256-Bit-End-to-End-Verschlüsselung können selbst Administratoren des Netzwerks den Inhalt der Sitzungen nicht sehen.

Außer grundlegenden Sitzungsparametern (Metadaten) werden auf den ISL Online-Servern KEINE zwischen Betreuern und Kunden während der Fernsitzungen übertragenen Daten gespeichert.

Metadaten	Beschreibung
Datum	Timestamp – Datum und Zeit zur Sitzungseröffnung durch den Betreuer.
Sitzungscode	Eindeutiger Sitzungscode für die Herstellung der Sitzung
Sitzungsname	Name der Sitzung (optional)
Anwendername	Name des Betreuers
Kunden-E-Mail	E-Mail-Adresse des Kunden (optional)
Sitzungsdauer	Sitzungsdauer in HH:MM:SS
Status	Sitzungs-Status (z.B. aktiv, angehalten, beendet, etc.).
Sitzungsstart	Timestamp – Beginn der Sitzung (Zustandekommen der Verbindung zwischen Betreuer und Kunden)
Bytes	Übertragene Anzahl an Bytes zwischen Betreuer und Kunde während der Sitzung
Server	ID des Servers, über den die Sitzung übertragen wurde
Plattform Betreuer	Betriebssystem des Betreuers
Version Betreuer	Vom Betreuer verwendete Version von ISL Light oder ISL Light Desk
IP Betreuer	IP Adresse des Betreuers
Kunden-Plattform	Betriebssystem des Kunden
Kunden-Version	Vom Kunden verwendete Version von ISL Light Client
Kunden-IP	IP Adresse des Kunden
Verbrauchte PPU Minuten	Anzahl der verbrauchten PPU-Minuten (optional)
Anmerkungen	Während der Sitzung notierte Anmerkungen (optional)
Multi-Sitzungs-ID	MAC Adresse des Gerätes, das für die Multi-Sitzungs-Option verwendet wurde (optional)
Netzwerk-Schnittstellen Betreuer	Netzwerk-Schnittstellen auf der Betreuer-Seite
Netzwerk-Schnittstellen Kunde	Netzwerk-Schnittstellen auf der Kunden-Seite
Übertragung Betreuer	Verwendete Übertragungsart vom Betreuer
Übertragung Kunde	Verwendete Übertragungsart vom Kunden
Sprache Betreuer	Verwendete Sprache des Betreuers
Sprache Kunde	Verwendete Sprache des Kunden

Für Organisationen mit sensiblen Daten wie Banken, nationale Behörden, oder ähnliche Unternehmensumgebungen bieten wir das Self-Hosted-Modell (Serverlizenz, Private Cloud) an, in denen das ISL Online System auf einem Server innerhalb der Organisation installiert ist. In diesem Fall werden alle Sitzungsverbindungen über den Server in der eigenen Organisation hergestellt. Da es sich bei der selbst gehosteten Installation um ein eigenständiges System handelt, ist das Unternehmen allein für die Administration des Servers verantwortlich. In diesem Fall verbleiben alle Daten (einschließlich Metadaten) in einer geschlossenen Unternehmensumgebung.