Sicherheitserklärung

Stand 5. März 2024

Sicherheit auf einen Blick

Einführung

Dieses Dokument bietet Sicherheitsinformationen im Zusammenhang mit ISL Online-Software für den Desktop-Fernzugriff. Es dient dazu, den technischen Hintergrund und die implementierten Sicherheitsebenen in den ISL Online Produkten zu erläutern. Wir empfehlen, dieses Dokument an Kollegen, Partner oder Kunden zur Klärung eventueller Sicherheitsfragen zu verteilen.

Über uns

ISL Online gehört zu den Pionieren der Branche für Fernzugriffssoftware. Seit 2001 bieten wir Fernzugriffssoftware für IT-Profis und Support-Techniker von kleinen und mittleren Unternehmen bis hin zu Fortune 500-Unternehmen an. Die ISL ("Internet Services Layer") Software ist darauf ausgelegt, Fernsupport- und Fernzugriffssitzungen sicher und effizient zu gestalten.

ISL Online (XLAB) hat seinen Hauptsitz im Herzen Europas mit Büros in Deutschland, der Schweiz, Slowenien und dem Vereinigten Königreich. Zusammen mit autorisierten Partnern aus den Vereinigten Staaten, Asien/Pazifik, dem Nahen Osten, Afrika und Lateinamerika betreuen wir Kunden nahezu überall auf der Welt, wobei Japan derzeit unser stärkster Markt ist.

ISL Online Headquarters

XLAB d.o.o.
Pot za Brdom 100
SI-1000 Ljubljana
Slowenien
VAT ID: SI15779092
Reg. Number: 1639714
support@islonline.com
+386 1 2447760

Deutschland	Schweiz	Grossbritannien
ISL Online GmbH **Noetherstrasse 1** **D-69115 Heidelberg** **VAT ID: DE347105357** **Reg. Number: HRB 741430** verkauf@islonline.com **+49 (0)6221 321 4990**	ISL Online AG Aargauerstrasse 250 CH-8048 Zürich VAT ID: CHE-305.215.248 MWST Reg. Number: CHE-305.215.248 verkauf@islonline.com +41 (0)62 724 13 60	ISL Online Ltd. 22 Basepoint Business Centre Rivermead Drive, Westlea Swindon, Wiltshire SN5 7EX, UK VAT ID: GB942657990 Reg. Number: 06581089 sales@islonline.com +44 1793 608 7370

Eine Liste der authorisierten Partner weltweit befindet sich auf der Webseite:

https://www.islonline.com/company/contact-us.htm

Erwarten Sie maximale Sicherheit

Bei ISL Online nehmen wir die Sicherheit sehr ernst. Wir verwenden branchenübliche Sicherheitstechnologien, um Ihre Daten zu schützen und erfüllen die strengsten Sicherheitsstandards. Banken, Behörden und globale Unternehmen wählen ISL Online aufgrund unseres hohen Sicherheitsniveaus.

ISL Online bietet verschiedene Hosting-Optionen (Cloud, On-Premise, Private Cloud, sowie Managed Private Cloud). Einige in diesem Dokument beschriebenen Sicherheitsmaßnahmen gelten nur für bestimmte Hosting-Optionen. Für Details kontaktieren Sie uns bitte unter support@islonline.com.

Um sich mit den in diesem Dokument verwendeten Begriffen vertraut zu machen, besuchen Sie das ISL Online Glossar unter https://www.islonline.com/de/de/help/glossary.htm.

RSA oder ECDSA mit Diffie-Hellman-Schlüsselaustausch

ISL Online verwendet bei Beschreibung der Einrichtung von Fernsteuerungssitzungen folgende Terminologie:

- **Serververbindung** – die anfängliche TLS-Verbindung, die ISL Light mit einem ISL Conference Proxy-Server (ICP) herstellt.
- **Standardverbindung** – eine End-To-End verschlüsselte Verbindung (TLS) zwischen zwei ISL Light-Endpunkten, bei der Pakete durch einen ISL Conference Proxy (ICP) Server weitergeleitet werden. Sie besteht aus zwei logischen Komponenten: dem Steuerkanal und dem Datenstrom des Remote-Desktops.
- **Steuerkanal** – die Terminologie von ISL Online für die Komponente der Standardverbindung, die die Verbindung zwischen zwei Endpunkten aktiv hält. Der Datenstrom des Remote-Desktops ist nur möglich, solange der Steuerkanal aktiv ist.
- **Datenstrom des Remote-Desktops** – die Terminologie von ISL Online für die Komponente der **Standardverbindung**, welche verschlüsselte Datenpakete von einem Endpunkt zum anderen überträgt. **Der Datenstrom des Remote-Desktops** umfasst Bilder des Remote-Desktops, Dateien, die während der Sitzung zwischen den Endpunkten ausgetauscht werden, sowie Audio-/Videokommunikation zwischen dem Betreuer und dem Client, unter anderem Daten. Dieser absorbiert den Großteil der Bandbreite. Wenn möglich, wird der Datenstrom des Remote-Desktops auf eine **Direktverbindung** umgeleitet.
- **Direktverbindung** – eine End-To-End verschlüsselte Direktverbindung (TLS) zwischen zwei ISL Light-Endpunkten. In bestimmten Konfigurationen wird sie von einem TURN-Server weitergeleitet.

Um eine Fernzugriffssitzung vom lokalen Computer zu einem fernen Computer einzurichten, muss die ISL Light-Anwendung gestartet werden, die über den öffentlichen RSA 2048-Bit-Schlüssel des ISL Conference Proxy (ICP)-Servers verfügt. Die anfängliche TLS-Verbindung (**Serververbindung**) wird hergestellt, sobald die ISL Light-Anwendung bestätigt, dass sie sich unter Verwendung des bereitgestellten öffentlichen Schlüssels mit dem ISL Conference Proxy (ICP) Server verbindet.

Ist zwischen den beiden Endpunkten (Betreuer und Client) eine Serververbindung hergestellt, werden RSA-Schlüssel verwendet, um eine Standardverbindung zwischen den Endpunkten herzustellen. Dies wird erreicht, indem AES 256-Bit symmetrische Verschlüsselungsschlüssel unter Verwendung des Diffie-Hellman-Kryptografie-Algorithmus ausgehandelt werden.

Falls verfügbar, wird eine **Direktverbindung** zwischen den beiden Endpunkten eingerichtet, um die Inhalte der Sitzung direkt von einem Endpunkt zum anderen zu senden, ohne über den ISL Conference Proxy (ICP) Server geleitet zu werden. Die Direktverbindung wird unter Verwendung von Schlüsseln aus dem Elliptic Curve Digital Signature Algorithm (ECDSA P-256) hergestellt, um AES 256-Bit symmetrische Verschlüsselungsschlüssel des Diffie-Hellman-Kryptografie-Algorithmus auszuhandeln.

Die anfängliche **Standardverbindung** bleibt weiterhin aktiv, jedoch dient sie jetzt ausschließlich als Steuerkanal zur Verwaltung der Sitzungskonnektivität, ohne Informationen über den Inhalt des Datenstroms des Remote-Desktops zu enthalten.

AES 256-Bit Ende-zu-Ende-Verschlüsselung

Unabhängig vom Verbindungstyp (Standardverbindung oder Direktverbindung) wird der Inhalt des Datenstroms des Remote-Desktops zwischen dem lokalen und dem entfernten Computer zur Einhaltung höchster Sicherheitsstandards durch einen sicheren Tunnel, per symmetrischer AES 256-Bit End-To-End-Verschlüsselung geschützt, übertragen.

Standardverbindung

Bei Verwendung einer Standardverbindung wird der gesamte Datenverkehr, einschließlich des Steuerkanals und des Datenstroms des Remote-Desktops, über einen ISL Conference Proxy (ICP) Server geleitet. Der ICP kann den Inhalt der Sitzungen nicht entschlüsseln, sondern lediglich Pakete von einer Seite zur anderen übertragen.

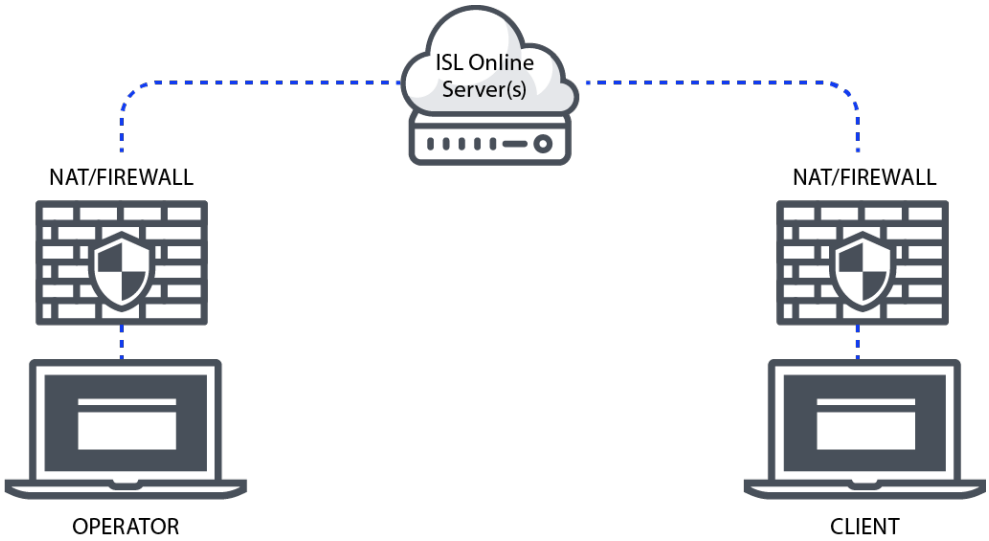

Diagramm der Standardverbindung unter Verwendung eines ISL Conference Proxy (ICP) Servers zur Verwaltung des Steuerkanals und des Datenstroms des Remote-Desktops.

Direktverbindung

In bestimmten Fällen wird eine Direktverbindung genutzt, was bedeutet, dass der Datenstrom den ISL Conference Proxy Server (ICP) umgeht und direkt zwischen dem Betreuer und dem Client hergestellt wird. Der ISL Conference Proxy Server (ICP) übernimmt dann lediglich die Handhabung des Steuerkanals.

Wenn beide Möglichkeiten verfügbar sind, vergleicht ISL Light, welche Verbindungsoption eine bessere Sitzungsgeschwindigkeit und -Qualität bietet. Zur Erkundung einer verfügbaren Direktverbindung führt ISL Light ICE (Interactive Connectivity Establishment) Kandidatenprüfungen durch, sobald der Steuerkanal hergestellt ist.

ICE (Interactive Connectivity Establishment) Kandidaten sind potenzielle Netzwerkadressen, die ein Gerät verwenden kann, um einen Kommunikationskanal mit einem anderen Gerät zu etablieren. ICE-Kandidaten umfassen verschiedene Arten von Adressen, deren Aufgabe es ist, Geräte bei der Bestimmung des optimalen

Kommunikationsweges zu unterstützen, insbesondere bei Network-Address-Translation (NAT) und Firewalls. Die ursprüngliche Verbindung zum ISL Conference Proxy Server (Steuerkanal, unter Verwendung von Multiplexing (MUX) Transport) bleibt für die Übermittlung von Metadaten bestehen, während der Datenstrom des Remote-Desktops auf eine Direktverbindung umgeleitet wird, sofern verfügbar.

Während des ICE-Prozesses tauschen die Geräte ihre Kandidatenlisten aus, und es werden Konnektivität-Prüfungen durchgeführt, um den optimalen Weg für die Kommunikation zu bestimmen. Die Verhandlung und Auswahl der Kandidaten sind Teil des ICE-Protokolls, das es den Geräten ermöglicht, sich an verschiedene Netzwerkumgebungen anzupassen und einen zuverlässigen Kommunikationskanal einzurichten. ISL Light bewertet die Qualität des MUX- (Multiplexing) Transports im Vergleich zum ICE-Transport. Diese Bewertung berücksichtigt Faktoren wie die Ping-Zeit, wobei die Qualität auf Basis der Latenz in der Kommunikation bestimmt wird. Das System wählt die Verbindung mit der geringeren Ping-Zeit, um eine optimale Leistung zu gewährleisten.

Die Haupttypen von ICE-Kandidaten sind:

- **Host-Kandidaten**
- **Server-Reflexive Kandidaten**
- **Relais-Kandidaten**

Host-Kandidaten

Dies sind die lokalen IP-Adressen des Geräts selbst. Host-Kandidaten repräsentieren die tatsächlichen Netzwerkschnittstellen des Geräts und werden für direkte Verbindungen verwendet, wenn sich beide Geräte im selben lokalen Netzwerk befinden.

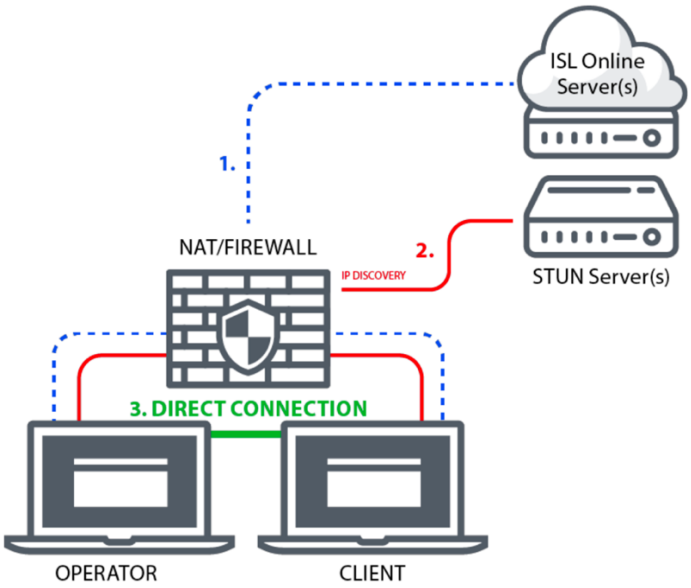

Diagramm der Direktverbindung über Host-Kandidaten in einem lokalen Netzwerk (LAN).

Für den Host-Kandidaten wird die Verbindung (blau dargestellte Linie repräsentiert den Steuerkanal) innerhalb des lokalen Netzwerks (LAN), ausgehend vom Computer des Betreuers, hergestellt. Sie durchquert die NAT/FIREWALL hin zum ISL Conference Proxy Server (ICP). Die Verbindung des Clients folgt einer vergleichbaren Route. Anschließend setzt sich die Verbindung (rote Linie) vom Computer des Betreuers und des Clients fort und durchquert die NAT/FIREWALL zu einem STUN-Server. Nach erfolgreicher Zuweisung wird eine direkte Verbindungssitzung (grüne Linie repräsentiert den Datenstrom des fernen Desktops) zwischen den Computern des Betreuers und des Clients hergestellt.

Server-Reflexive-Kandidaten

Server-reflexive Kandidaten werden durch STUN-Server (Session Traversal Utilities for NATs) zur Verfügung gestellt. STUN-Server reflektieren UDP-Pakete (User Datagram Protocol) zurück zum Gerät, was es ermöglicht, seine externe Adresse und den sichtbaren Port im Internet zu entdecken. Dies hilft bei der Herstellung von Kommunikation mit Geräten außerhalb des lokalen Netzwerks und überwindet NAT-Barrieren.

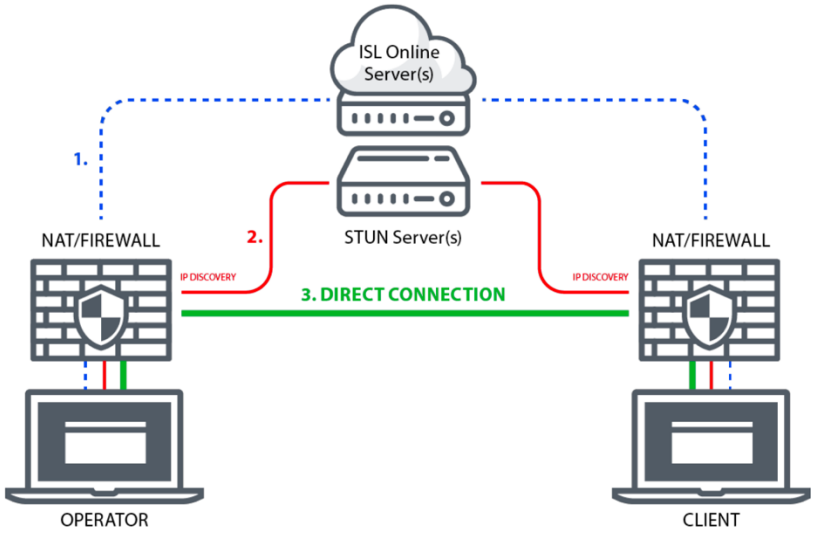

Diagramm der Direktverbindung über Server-Reflexive Kandidaten (STUN-Server).

Für den server-reflexiven Kandidaten Die Verbindung beginnt (blaue Linie – repräsentiert den Steuerkanal) vom Computer des Betreuers, geht durch die NAT und dann zum ISL Conference Proxy Server (ICP). Die Verbindung des Clients folgt einer vergleichbaren Route. Die Verbindung (rote Linie) führt vom Computer des Betreuers, durch die NAT/FIREWALL zu einem STUN-Server. Auf der Client-Seite erfolgt derselbe Prozess. Nach einer erfolgreichen Initiierung wird eine Direktverbindung (grüne Linie repräsentiert den Datenstrom des Remote-Desktops) zwischen Betreuer und Client hergestellt.

Relais-Kandidaten

Weitergegebene Kandidaten werden über einen TURN-Server (Traversal Using Relays around NAT) abgerufen. In Fällen, in denen eine direkte Kommunikation aufgrund restriktiver Firewalls oder symmetrischem NAT nicht möglich ist, können Geräte ein Relay Server nutzen, um ihre Daten über einen Drittanbieter-Server weiterzuleiten. TURN-Kandidaten helfen beim Aufbau der Kommunikation, wenn andere Methoden versagen.

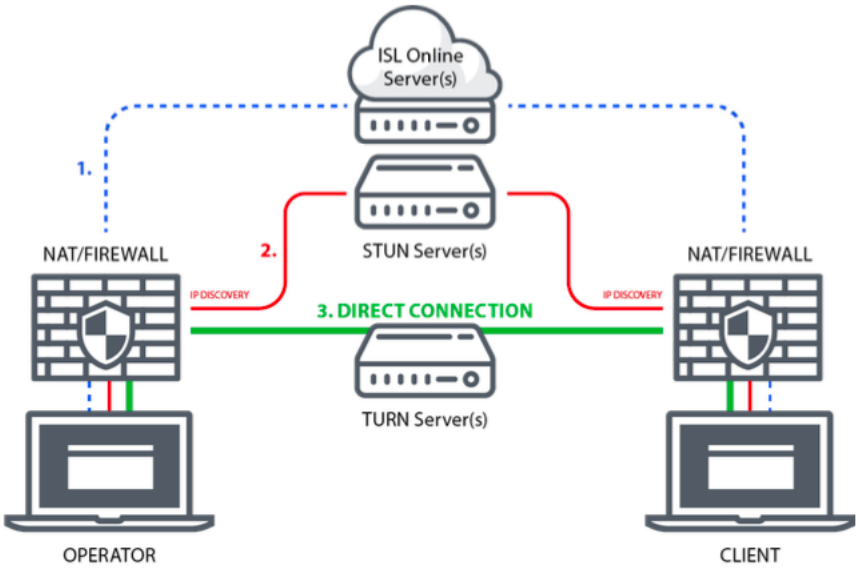

Diagram of Direct Connection via Relay Candidates (TURN Server(s)).

Bei Relais-Kandidaten beginnt die Verbindung (blaue Linie repräsentiert den Steuerkanal) am Computer des Betreuers, geht durch die NAT und danach zum ISL Conference-Proxy-Server (ICP). Die Client-Seite folgt derselben Route. Die Verbindung (rote Linie) führt weiter vom Computer des Betreuers und durchquert die NAT zu einem STUN-Server. Auf der Client-seite findet derselbe Prozess statt. Der wesentliche Unterschied zu den server-reflektierenden Kandidaten besteht darin, dass die Direktverbindung (grüne Linie repräsentiert den Datenstrom des Remote-Desktops) über einen TURN-Server zwischen dem Betreuer und dem Client hergestellt wird. Da die Sitzung End-To-End verschlüsselt ist, können die TURN-Server den Inhalt der Sitzungen nicht entschlüsseln; sie übertragen nur Datenpakete von einer Seite zur anderen.

Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung (2FA) ist eine zusätzliche Sicherheitsebene für Helpdesk-Techniker und IT-Profis. Mit aktivierter 2FA können sich Betreuer nur durch einen zweistufigen Verifizierungsprozess im ISL Online System anmelden, indem sie etwas angeben, das sie wissen (Passwort) und etwas, das sie besitzen (2FA-Token). Dieser zweite Faktor erhöht die Sicherheit und erschwert den unbefugten Zugriff erheblich.

Wir empfehlen die Verwendung der Zwei-Faktor-Authentifizierung, insbesondere bei hochsensiblen Systemen. ISL Online ermöglicht es, verschiedene Methoden für den zweiten Schritt der Verifizierung zu konfigurieren (E-Mail, Telefon, Authentifizierungs-App – TOTP, Sicherheitsschlüssel – Yubico-Schlüssel basierend auf dem FIDO U2F-Standard).

ISO/IEC 27001:2022 Zertifizierung (Informationssicherheitsmanagement)

Die ISO 27001:2022 ist international anerkannt und einer der am weitesten verbreiteten Standards für Informationssicherheit. Dieses Zertifikat legt die Anforderungen für ein umfassendes Informationssicherheitsmanagementsystem (ISMS) fest und definiert eine sichere Verwaltung und Behandlung von Informationen in Organisationen. Es wird nach einem gründlichen Auditprozess nur an Organisationen vergeben, die strenge Sicherheitspraktiken befolgen und einhalten.

Das Zertifikat ISO/IEC 27001:2022 bestätigt die Expertise von ISL Online im Management der Informationssicherheit und unser Engagement für das höchste Sicherheitsniveau im gesamten Unternehmen. Es ist ein weiterer Beweis dafür, dass die Daten bei ISL Online gut geschützt und sicher sind.

Neben der ISO 27001-Konformität werden die internen Handbücher und Sicherheitsrichtlinien von ISL Online regelmäßig anhand bester, von SSAE 16 (SOC 2) empfohlenen Praktiken überprüft.

Portfilterung

Mit ISL Online kann Ihre Firewall intakt bleiben, da ISL Light automatisch eine ausgehende Verbindung initiiert und versucht, über die Ports 7615, 80 oder 443 eine Verbindung herzustellen.

Größere Organisationen haben normalerweise jedoch eine Richtlinie zur Konfiguration ihrer Firewalls oder Proxies. Systemadministratoren möchten möglicherweise nur den Port 7615 öffnen, um den ISL Online-Datenverkehr direkt durchzulassen und den Rest weiter zu filtern. Es kann auch eine Ausnahme für DNS-Namen oder IP-Adressen konfiguriert werden.

Unabhängig von der Netzwerkkonfiguration analysieren die ISL Online-Apps automatisch verschiedene Ansätze, um einen funktionierenden Transport zu finden (Erkennung von Proxy-Einstellungen, Verwendung von WinINet, Erstellung eines Tunnels, Nutzung des Wildcard-DNS usw.).

Wenn eine Direktverbindung verwendet wird, muss die Firewall die für STUN- und TURN-Protokolle benötigten Ports zulassen. Meistens wird der Port 3478 verwendet, jedoch werden Relaisverbindungen auf beliebigen hohen Ports hergestellt.

Erlaubnis/Verweigerungs-Liste

Remote-Desktop-Software ist ein äußerst leistungsfähiges Werkzeug, das es ermöglicht, ferne Computer zu steuern. Daher ist zur Verhinderung von Missbrauch der Remote-Desktop-Software im Unternehmen die Verwendung von Erlaubnis- und Verweigerungs-Listen unerlässlich. Aus Sicherheitsgründen soll möglicherweise die Nutzung der ISL Online-Software innerhalb Ihrer Organisation eingeschränkt oder der Datenzugriff auf den ISL Conference Proxy-Server (ICP) basierend auf IP- und/oder MAC-Adressen begrenzt werden. Hierfür kann die „Erlaubnis“-Funktion dazu verwendet werden, um die Liste der IP-/MAC-Adressen zu spezifizieren, die eine Fernsupport-Sitzung starten oder auf einen unbeaufsichtigten Computer zugreifen dürfen. Die „Verweigerung“-Funktion kann wiederum zur Sperrung von IP-/MAC-Adressen aus der Verweigerungsliste verwendet werden. Diese Regeln können für einen bestimmten Benutzer oder die gesamte Domäne auf dem ISL Conference Proxy-Server (ICP) definiert werden. Beispielsweise kann Mitarbeitern erlaubt werden, Sitzungscodes für eine Fernsupport-Sitzung nur aus dem Büro (Bereich der IP-Adressen Ihres Unternehmens) zu generieren.

Geplante Sitzungen

Die Anfälligkeit für möglichen Missbrauch kann weiter einschränkt werden, indem der Zeitrahmen beschränkt wird, in dem Fernsupport-Sitzungen oder unbeaufsichtigte Zugriffe auf ferne Computer ausgeführt werden können. Beispielsweise können Fernsupport-Sitzungen ausschließlich für die Arbeitszeiten von 9 Uhr bis 17 Uhr festgelegt werden. Fernsupport-Sitzungen außerhalb dieses Zeitrahmens werden dementsprechend verhindert. Zudem werden alle aktiven Sitzungen bei Überschreitung des Zeitrahmens beendet.

Codesignierung

Die Codesignierung wird häufig verwendet, um Software, die über das Internet verteilt wird, zu schützen. Die Codesignierung ändert nichts an der Software, sondern fügt dem ausführbaren Code eine digitale Signatur hinzu. Diese digitale Signatur versichert den Anwendern, dass die Remote-Desktop-Software tatsächlich von einer vertrauenswürdigen Quelle stammt. Sie bietet genügend Informationen, um den Unterzeichner zu authentifizieren und sicherzustellen, dass der Code nachträglich nicht verändert wurde. ISL Online-Anwendungen sind mittels eines Codesignaturzertifikats digital signiert, welches ISL Online eindeutig als Softwareherausgeber identifiziert und garantiert, dass der Code seit der Signierung mit einer digitalen Signatur nicht verändert oder beschädigt wurde.

Externe Sicherheitsaudits und Penetrationstests

Regelmäßige systematische Sicherheitsaudits und gezielt durchgeführte Penetrationstests sind entscheidend für jeden Anbieter von Remote-Desktop-Software, der sich seiner Verantwortlichkeit für die Informationssicherheit bewusst ist. Sie ermöglichen es einem Unternehmen, potenzielle Schwächen und Sicherheitslücken zu erkennen und zu beheben. Unabhängige Sicherheitsaudits und Penetrationstests des ISL Online-Systems werden regelmäßig durchgeführt und belegen, dass ISL Online ein vertrauenswürdiger Dienst mit sehr hohem Maß an Sicherheit ist.

Funktionstransparenz (Kein Stealth-Modus)

Es ist wichtig, dass eine Remote-Desktop-Anwendung so gestaltet ist, dass sie niemals im Hintergrund laufen kann, ohne dass der ferne Anwender davon weiß. Die Funktionalität der Software sollte vollständig transparent sein, und der ferne Anwender sollte jederzeit in der Lage sein, dem Vorgehen des Helpdesk-Betreuers zu folgen. ISL Online ist darauf ausgelegt, Fernsupport über das Internet zu bieten, jedoch nur auf ausdrücklichen Wunsch des fernen Anwenders. Der ferne Anwender erlaubt einem Helpdesk-Betreuer, die Desktop-Freigabe zu starten, und kann die Sitzung jederzeit beenden. Wenn der Betreuer die vollständige Kontrolle über den Desktop des fernen Anwenders hat, kann letzterer die Kontrolle einfach an sich ziehen, indem er die Maus bewegt. Sobald die Sitzung beendet ist, kann der Helpdesk-Betreuer nicht mehr mit demselben Sitzungscode auf den fernen Computer zugreifen.

Anpassbare Kennwort-Richtlinie

Die Sicherheit Ihrer Daten hängt nicht nur von der Stärke des Verschlüsselungsverfahrens ab, sondern auch von der Komplexität des Anwenderkennworts, einschließlich Faktoren wie der Länge und Zusammensetzung des Kennworts sowie der angewandten Maßnahmen zur Sicherstellung, dass das Kennwort keinem Dritten offenbart wird.

Standardmäßig basiert die Kennwort-Sicherheitsrichtlinie von ISL Online auf den neuesten Spezifikationen des NIST (National Institute of Standards and Technology) – das Kennwort muss mindestens 8 Zeichen lang sein; führende und abschließende Leerzeichen werden entfernt; erlaubte Zeichen in den Kennwörtern sind alle druckbaren ASCII-Zeichen und Leerzeichen; das Kennwort wird gegen eine Blacklist der gängigsten und einfachsten Passwörter geprüft.

Zusätzlich bietet ISL Online die Möglichkeit, die angewandte Kennwortrichtlinie vollständig zu individualisieren, um global oder pro Anwender einen strengeren Sicherheitsstandard festzulegen.

ISL Online speichert Kennwörter nicht im Klartext, sondern verwendet Salted-Passwort-Hashing, um in Benutzerkontendatenbanken gespeicherte Passwörter zu schützen.

Schutz vor Brute-Force-Angriffen

Ein Brute-Force-Angriff ist eine Trial-and-Error-Methode, die jede mögliche Kombination berechnet, die ein Kennwort ausmachen oder eine verschlüsselte Datei entschlüsseln könnte. Bei einem Brute-Force-Angriff wird automatisierte Software verwendet, um eine große Anzahl aufeinanderfolgender Versuche zu generieren, bis der richtige Zugang gefunden wird. ISL Online hat eine Ratenbegrenzung für Anmelde- und Verbindungsversuche konfiguriert, um Brute-Force-Angriffe zu verhindern. ISL Conference Proxy-Server (ICP) verhindern Brute-Force-Angriffsversuche (Anmeldung), indem sie die maximale Anzahl fehlgeschlagener Anmeldeversuche für einen Benutzer oder für eine bestimmte Adresse in einem festgelegten Zeitraum begrenzen.

Intranet-Einrichtung (nur LAN)

Einige große Organisationen verwenden ISL Online nur für ihren internen Support über verschiedene geografische Standorte hinweg. In solchen Fällen muss die Remote-Desktop-Software das Einrichten von Remote-Desktop-Sitzungen innerhalb eines lokalen Netzwerks (LAN) ermöglichen. Wenn Sie ISL Online nur innerhalb Ihres LANs (Intranet) verwenden möchten, benötigen Sie keine öffentliche IP-Adresse. Sie benötigen nur eine private Adresse im Bereich der privaten Netzwerke (wie in RFC 1918 spezifiziert).

Unterstützung für Reverse Proxy

Ein Reverse Proxy kann die Topologie und die Eigenschaften von Backend-Servern verbergen, indem er die Notwendigkeit für direkten Internetzugang unnötig macht. Ein Reverse Proxy kann in einer dem Internet zugewandten DMZ platziert werden, aber die Webserver in einem privaten Subnetz verbergen. Dies verringert die Risiken eines unbefugten Zugriffs auf sensible Daten. ISL Online ermöglicht die Installation des Conference Proxy Servers hinter einem Reverse Proxy, um ersteren nicht direkt dem Internet auszusetzen, wobei das SSL auf dem Reverse Proxy endet.

Automatische Sitzungsaufzeichnung

Remote-Desktop-Software sollte nicht nur die Datenübertragung, sondern auch den Anbieter von Remote-Desktop-Support und den Kunden als Empfänger schützen. Die beste Methode hierfür ist die Sitzungsaufzeichnung. Dies gilt insbesondere für Unternehmen, die einem externen Dienstleistungsunternehmen die Computerwartung anvertraut haben, indem sie einen unbegrenzten Fernzugriff auf ihre Computer gewährt haben. ISL Online bietet die leistungsstarke Option, die Aufzeichnung automatisch zu Beginn jeder Fernzugriffssitzung zu starten, um die vollständige Kontrolle über die Fernzugriffsaktivitäten zu haben und mögliche Konflikte mit Kunden zu vermeiden. Die Aufzeichnung erfolgt lokal und nicht durch den Server, was bedeutet, dass die Sitzungsaufzeichnung die Ende-zu-Ende-Verschlüsselung der Sitzung nicht beeinträchtigt.

Zugriffsverwaltung

Wenn in einem Unternehmen die Remote-Desktop-Software nur von einer Person verwendet wird, ist das Einrichten von Zugriffsberechtigungen möglicherweise kein Anliegen, aber aus Sicherheitssicht wird diese Funktion sehr wichtig, sobald zahlreiche Benutzer die Software zur Verbindung mit fernen Computern verwenden. Mit ISL Online kann der Konto-Admin seinen Domänenbenutzern unterschiedliche Rechte und Einschränkungen zuweisen, einschließlich der Erlaubnis oder Sperrung des Zugriffs zu bestimmten Computern. Für jeden einzelnen Benutzer kann auch eine maximale Anzahl gleichzeitiger Sitzungen festgelegt, oder z.B.

das Recht für die Nutzung von Audio, Video, Remote-Drucken, Dateiübertragung oder Desktop-Freigabe deaktiviert werden.

Incident Management System (IMS)

Anbieter von Remote-Desktop-Software sollten über ein Incident Management System (IMS) verfügen, das eine schnelle Wiederherstellung des normalen Servicebetriebs nach einer ungeplanten Unterbrechung gewährleistet. ISL Online verwendet als IMS ein eigens entwickeltes Verfahrensbündel, um gemeldete Vorfälle zu behandeln. Jeder gemeldete Vorfall wird in unserem Ticketsystem verwaltet und umfasst normalerweise folgende Elemente:

- Zeitachse UTC (ein Protokoll der Ereignisse in chronologischer Reihenfolge in der UTC-Zeitzone)
- Zusammenfassung der Geschäftsleitung (kurze Beschreibung des Vorfalls)
- Ursache (Erklärung zur Vorfall-Ursache)
- Lösung und Wiederherstellung (Beschreibung des Prozesses zur Vorfall-Behandlung)
- Korrektive und präventive Maßnahmen (Ergriffene Maßnahmen zur künftigen Verhinderung solcher Vorfälle)
- Weitere relevante Informationen

IMS hilft uns, kontinuierliche Serviceniveaus aufrechtzuerhalten, die Verfügbarkeit von IT-Diensten zu messen, unerwünschte Ereignisse zu dokumentieren und deren Wiederauftreten zu reduzieren.

System- und Audit-Protokolle

Um den Vorschriften in den meisten Branchen zu entsprechen, sollte Remote-Desktop-Software Benutzern ermöglichen, Protokolle über Systemaktivitäten sowie Audit-Protokolle zu führen, die klare Verantwortlichkeiten aufzeigen.

ISL Online ermöglicht IT-Administratoren, Benutzer eindeutig zu identifizieren, Zugriffe auf Systeme anzuzeigen oder per Fernverbindung durchgeführte Aktionen mittels aktiver Sitzungsaufzeichnung nachzuvollziehen. Solche Aufzeichnungen können in jede einzelne Sitzung eintauchen und Informationen über einen Betreuer, einen Kunden, IP-Adressen usw. offenlegen. Das Protokollierungsniveau und Detaillierung der Systemprotokolle kann je nach Bedarf des Kunden angepasst werden.

Die in den Systemprotokollen enthaltenen Informationen entsprechen den Daten, die im Abschnitt „Datenminimierung“ zusammen mit zusätzlichen Informationen aufgeführt sind: „Aktion“ – das Ereignis, das dazu führte, dass das Protokoll geschrieben wurde. Darüber hinaus können clientseitige Debug-Protokolle aktiviert werden, die es ISL Online oder dem IT-Administrator des Kunden ermöglichen, die Ursache eines Problems zu untersuchen. Diese Protokolle sind sehr detailliert und können sensible Informationen enthalten (z. B. lokale Systempfade). Diese Protokolle erfordern sehr spezifische Anweisungen zur Aktivierung und werden nur auf lokalen Maschinen gespeichert. Sie müssen bei Bedarf manuell an ISL Online oder den IT-Administrator übertragen werden, wobei sichergestellt wird, dass der Kunde vollständig über deren Inhalt und darüber informiert ist, wer Zugang zu diesen Informationen hat.

Zusätzlich ist ein Audit-Protokoll verfügbar, das es dem Administrator ermöglicht, Konfigurationsänderungen und andere von Benutzern im System durchgeführte Aktionen zu überprüfen – Audit-Protokolle enthalten Informationen darüber, welcher Benutzer welche Aktion wann durchgeführt hat.

Eine Integration mit einer Drittanbieter-Lösung zur Protokollaggregation/Berichterstellung ist ebenfalls möglich.

Einschränkung von Funktionen

Remote-Desktop-Software ist ein universelles Werkzeug, das praktisch in allen Branchen eingesetzt wird. Entsprechend gibt es unzählige unterschiedliche Anwendungsfälle, die sehr flexible Lösungen erfordern. Daher kann die Software Funktionen enthalten, die in verschiedenen Sicherheitsstandards nicht benötigt oder genehmigt werden. ISL Online bietet vollständige Kontrolle der den Benutzern zur Verfügung stehenden Funktionen, indem einzelne, für den spezifischen Fall nicht benötigten Funktionen, eingeschränkt werden. Es kann beispielsweise komplett verhindert werden, dass der Betreuer die Kontrolle über den fernen Computer übernimmt, die Datenfreigabeoption oder Audio- oder Videokommunikation anwendet, sowie viele andere Optionen mehr. Beispiel einer wichtigen Einschränkung einer Funktion: Ein Bankmitarbeiter sollte in der Lage sein, den Bildschirm eines Kunden zu sehen, sollte jedoch niemals seinen eigenen Desktop offenlegen. In diesem Fall kann das Teilen des Desktops auf der Desk-Seite deaktiviert werden.

Externe Authentifizierung

Externe Authentifizierung ist eine Methode der Benutzerauthentifizierung, bei der ein externes System oder Dienst zur Überprüfung der Identität eines Anwenders während des Versuchs, auf ein System oder eine Anwendung zuzugreifen, angewandt wird. ISL Conference Proxy-Server (ICP) unterstützen zwei Haupttypen der externen Authentifizierung:

- **Typ 1** (Traditionelle Authentifizierung - LDAP, RADIUS): Der Anmeldeprozess bleibt vollständig von den ISL Conference Proxy-Servern (ICP) verwaltet, aber anstatt die eingegebenen Anmeldeinformationen gegen eine lokale Benutzerdatenbank zu verifizieren, kontaktiert das Authentifizierungsmodul ein externes System (z.B. LDAP, Active Directory, NetIQ eDirectory, RADIUS), versucht dort mit den bereitgestellten Anmeldeinformationen zu authentifizieren und erlaubt oder verweigert den Anmeldeversuch basierend auf der Antwort dieses externen Systems.
- **Typ 2** (Föderierte Authentifizierung - SAML 2.0): Der Anmeldeprozess ändert sich und die ISL Conference Proxy-Server (ICP) leiten den Benutzer zur Anmeldeseite des konfigurierten Identitätsanbieters weiter. Nach erfolgreicher Authentifizierung wird der Benutzer zurück zu den ISL Conference Proxy-Servern (ICP) geleitet und automatisch eingeloggt.

Für weitere Informationen zum SSO über das SAML 2.0-Protokoll siehe Punkt „Single Sign-On (SSO/SAML)“.

Single Sign-On (SSO/SAML)

Berechtigte Benutzer (Administratoren) können eine Single Sign-On (SSO)-Methode konfigurieren, die es Benutzern ihrer Organisationen ermöglicht, sich sicher zu authentifizieren und sich über Drittanbieter-SSO-Identitätsanbieter (z. B. Microsoft Entra ID, Okta usw.) mittels des sicheren SAML 2.0-Protokolls in ihre ISL Online-Konten einzuloggen. Wenn eine Organisation SSO konfiguriert, ändert sich der Anmeldefluss der Benutzer. Wenn ein Benutzer sich bei den Produkten und Dienstleistungen von ISL Online anmelden möchte, leiten die ISL Conference Proxy-Server (ICP) ihn zu einem externen Identity Provider (IdP) für die Benutzerauthentifizierung weiter. Ein Benutzer muss seine SSO-Anmeldeinformationen eingeben, die ihm von der Organisation zur Verfügung gestellt wurden.

Nach erfolgreicher Anmeldung verwendet der IdP das SAML 2.0-Protokoll, um den Benutzer zurückzuleiten und dem ISL Conference Proxy-Server (ICP) zu bestätigen, dass der Benutzer authentifiziert wurde und berechtigt ist, fortzufahren.

Zertifizierte Rechenzentren

Die Server von ISL Online (Public Cloud) werden weltweit in professionellen Rechenzentren gehostet. Wir wählen ausschließlich hochzuverlässige und in der Industrie bewährte Rechenzentren mit modernen Einrichtungen und Ausstattungen, wie redundante oder Notstromversorgungen, redundante Datenkommunikationsverbindungen, Umweltkontrollen (z. B. Klimaanlage, Brandschutz) und Sicherheitsvorrichtungen. Die Master-Server von ISL Online befinden sich innerhalb der Europäischen Union in nach ISO 27001 zertifizierten Rechenzentren. Die Server von ISL Online werden ausschließlich von unseren leitenden Systemadministratoren verwaltet, die strikten Richtlinien und Arbeitsabläufen folgen. Aufgrund der Sicherheitsrichtlinie der AES 256-Bit End-To-End-Verschlüsselung können selbst unsere Serveradministratoren nicht auf die Inhalte der Sitzungen zugreifen oder diese einsehen. Bei der Bereitstellung der Managed Private Cloud (MPC)-Lösung wird die Auswahl des Rechenzentrums vom Kunden spezifiziert und genehmigt, was bedeutet, dass der Kunde die vollständige Kontrolle darüber hat, wo die Server stehen.

Einhaltung von Vorschriften und Sicherheitsstandards

ISL Online ist ein Unternehmen mit Sitz in der Europäischen Union, was uns den weltweit strengsten Datenschutz- und Privatsphärenregulierungen unterwirft. Ausgehend von der Verordnung (EU) 2016/679 (DSGVO) hat ISL Online zahlreiche Sicherheitsmaßnahmen und Funktionen implementiert, die es unseren Nutzern ermöglichen, ihre Datenschutzrechte auszuüben und sicherzustellen, dass die Handhabung und Verarbeitung von Daten durch ISL Online gemäß den Grundsätzen der DSGVO erfolgt. Darüber hinaus ermöglicht ISL Online Fernzugriff, Fernunterstützung und Online-Kooperationstools auf höchstem Sicherheitsniveau, was durch die Zertifizierung nach dem ISO 27001 Sicherheitsstandard belegt ist. Die Software eignet sich auch für Unternehmen und Organisationen, die strenge HIPAA (Health Insurance Portability and Accountability Act) Anforderungen einhalten müssen und ihre Einhaltung prüfen. ISL Online integriert die ISO 27001-Praktiken auch in die Tools, die seinen Kunden zur Verfügung gestellt werden. Da die ISO 27001-Anforderungen die Anforderungen des HIPAA übertreffen, ermöglicht ISL Online seinen Kunden, HIPAA-konform zu bleiben oder zu werden. Ein spezielles Datenschutzteam kann Ihnen bei der Dokumentation und den Tests zum Nachweis der Einhaltung dieser Anforderungen helfen. Ähnlich, aufgrund der Überschneidungen zwischen ISO 27001 und SOC 2, ermöglicht ISL Online unseren Kunden, die Einhaltung der SOC-2-Vorschriften zu wahren. Der Umfang unserer ISO 27001-Zertifizierung umfasst:

Design, Entwicklung, Verkauf, Management und Support von IT-Produkten und -Dienstleistungen und sollte ausreichend die Bedürfnisse unserer Kunden abdecken, die versuchen, ihre Einhaltung des SOC 2-Standards nachzuweisen.

Bei weiteren Anfragen hierzu ist ein spezielles Datenschutzteam erreichbar unter: dataprotection@islonline.com

Datenminimierung

Die während der Remote-Desktop-Sitzungen zwischen Betreuern und Kunden übertragenen Daten (Sitzungsinhalte) werden NICHT auf den Servern von ISL Online gespeichert. Die Server speichern die Daten, die in der Metadatentabelle aufgeführt sind. ISL Online bemüht sich, nur die minimal erforderlichen Daten zu verarbeiten und zu speichern, die für den Betrieb unseres Dienstes und zur Bereitstellung der für die Geschäftsbedürfnisse unserer Kunden erforderlichen Sitzungsberichte und -historien notwendig sind. Es gilt zu beachten, dass die in diesem Kapitel aufgeführten Metadaten als Teil des Steuerkanals verwendet werden - was bedeutet, dass sie unabhängig vom für eine Fernsitzung verwendeten Verbindungstyp (Standardverbindung oder Direktverbindung), erstellt werden. Zusätzlich werden die in diesem Kapitel aufgeführten Metadaten nur auf den Servern von ISL Online gespeichert, wenn die Sitzung als Teil unseres gehosteten Dienstes erstellt wird. Für sicherheitssensiblere Organisationen wie Banken, nationale Agenturen, Unternehmensumgebungen... bieten wir die selbstgehosteten Modelle (Serverlizenz, Managed Private Cloud) an, bei denen das ISL Online-

System auf dedizierten Servern oder in privat betriebenen Rechenzentren installiert ist. In solchen Fällen bleiben alle Daten (einschließlich Sitzungs-Metadaten) in einer geschlossenen Umgebung.

Metadaten	**Beschreibung**
Datum	Timestamp - Datum und Uhrzeit des Sitzungsstarts durch den Betreuer
Sitzungscode	Eindeutiger Sitzungscode zur Herstellung einer Sitzung
Sitzungsname	Angepasster Sitzungsname (optional - wenn vom Betreuer eingegeben)
Anwendername	Anwendername des Betreuers
Client-E-Mail	E-Mail Adresse des Betreuten
Sitzungsdauer	Dauer der Sitzung in HH:MM:SS
Status	Zustandsbeschreibung der Sitzung (aktiv, angehalten, beendet.)
Sitzungstyp	Fernsupport (mit Gegenüber) oder Fernzugriff (ohne Gegenüber)
Sitzungsart	Timestamp - Datum und Uhrzeit bei Verbindung des Betreuers mit dem fernen Gerät
Bytes	Anzahl der transferierten Bytes während einer Sitzung
Server	ID des Host-Servers
Desk-Plattform	Betriebssystem des Hosts/Betreuers
Desk-Version	ISL Light / ISL Light Desk Version des Hosts/Betreuers
Desk-IP	IP-Adresse des Hosts/Betreuers
Client-Plattform	Betriebssystem des Clients
Client-Version	ISL Light / ISL Light Desk Version des Clients/Betreuten
Client-IP	IP-Adresse des Clients/Betreuten
Client-Rechnername	Rechnername des Clients/Betreuten
Client-Beschreibung	Host-Name des Client-Gerätes
Host-Rechnername	Angepasster Client-Rechnername (optional - wenn vom Betreuer eingegeben)
Client-Mac-Adresse	MAC-Adresse des Client-Computers
Host-Mac-Adresse	MAC-Adresse des Host-Computers
Verbrauchte PPU-Minuten	Während einer Sitzung verbrauchte Minuten eines Minutencoupons (sofern vorhanden und verfügbar)
Desk-Anmerkungen	Anmerkungen des Betreuers nach einer Sitzung in einem Sitzungsende-Dialog
Client-Anmerkungen	Anmerkungen des Betreuten nach einer Sitzung in einem Sitzungsende-Dialog
Chat-Mitschrift	Chat zwischen Betreuer und Betreuten während einer Sitzung. Standardmäßig ist dies deaktiviert. Bei Aktivierung des Sitzungsende-Dialogs wird auch die Chat-Mitschrift aktiviert
Bemerkungen	Bemerkungen zur Sitzung - sofern vom Betreuer eingegeben
Multi-Sitzungs-ID	HASH-Mac-Adressen des Gerätes
Desk-Netzwerkschnittstellen	Netzwerk-Schnittstellen auf der Host-Seite

Client-Netzwerkschnittstellen	Netzwerk-Schnittstellen auf der Client-Seite
Desk Transport	Angewandter Netzwerk-Transport auf Host-Seite
Client Transport	Angewandter Netzwerk-Transport auf Client-Seite
Desk Sprache	Sprache des Hosts
Client Sprache	Sprache des Clients
Systempfade	Lokale Systempfade, von welchen die ausführbare ISL Online Datei gestartet wurde.