ispring

iSpring Webdienste: Überblick über die Sicherheitsprozesse

Datum der Überprüfung: August 2022

Hinweis

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt die aktuellen Praktiken von iSpring zum Schutz der Daten von Kund*innen zum Zeitpunkt der Veröffentlichung dieses Dokuments dar, die sich ohne vorherige Ankündigung ändern können. Dieses Dokument begründet keine Garantien, Zusicherungen, vertraglichen Verpflichtungen, Bedingungen oder Zusagen von iSpring, ihren verbundenen Unternehmen, Lieferanten oder Lizenzgebern.

Inhaltsverzeichnis

Einführung

Der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten unserer Kund*innen ist für iSpring von größter Bedeutung, ebenso wie die Erhaltung des Vertrauens unserer Kund*innen. Der Zweck dieses Dokuments ist es, die Frage zu beantworten: „Wie hilft mir iSpring, meine Daten zu schützen?“ Konkret werden die physischen und betrieblichen Sicherheitsprozesse von iSpring für die von iSpring kontrollierte Netzwerk- und Serverinfrastruktur sowie die dienstespezifischen Sicherheitsimplementierungen beschrieben.

Überblick über die iSpring-Webdienste

iSpring bietet die folgenden Webdienste an:

1. **iSpring Learn** ist ein gehostetes Lernmanagementsystem (LMS) für den Online-Unterricht und die Beurteilung von Mitarbeiter*innen oder Student*innen.

2. **iSpring Space** ist ein Portal zum Speichern von E-Learning-Kursen und zur Zusammenarbeit mit dem Team.

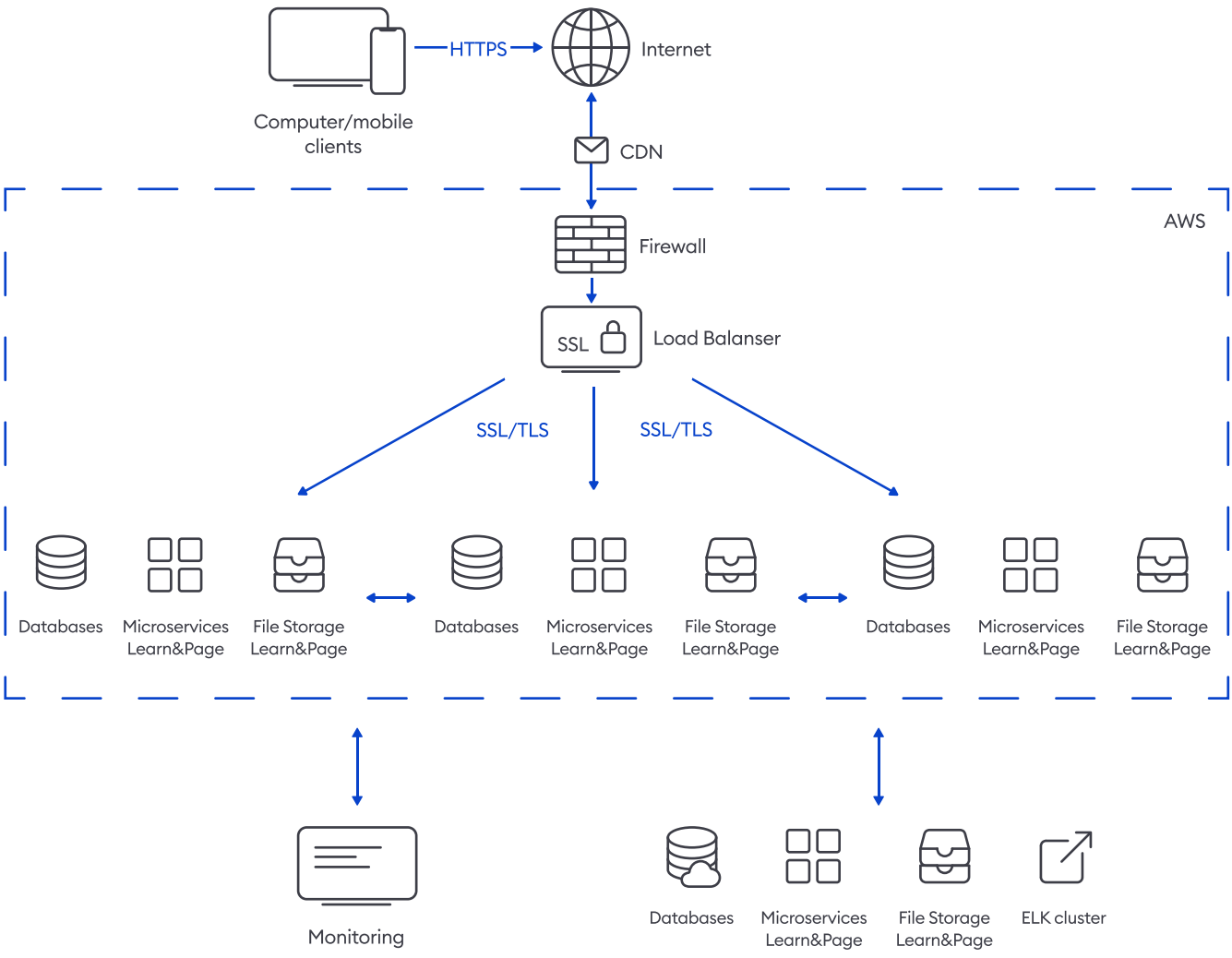
3. **iSpring Market** ist eine Cloud-basierte Plattform für den Online-Verkauf von Kursen.

Beide Webdienste sind eng mit der iSpring Suite, einem Autorentool für E-Learning, und den mobilen Anwendungen von iSpring integriert.

Sichere Designprinzipien

Die iSpring-Webdienste wurden entwickelt, um die persönlichen Daten der Benutzer*innen sicher zu hosten und die Inhalte, Datenbanken und Analysen der Benutzer*innen über ein nicht vertrauenswürdiges Netzwerk bereitzustellen. Bei der Entwicklung der Software hatten Sicherheitsüberlegungen Vorrang vor Fragen der Benutzer*innenfreundlichkeit.

Netzwerk-Diagramm



Sichere Einrichtungen

iSpring nutzt zuverlässige Hosting-Provider mit hohen Sicherheitsstandards, um die Komponenten und Dienste von iSpring Learn LMS und iSpring Space zu betreiben. iSpring verlässt sich nicht auf einen einzigen Hosting-Provider, sodass es möglich ist, den Betrieb von einem primären auf einen sekundären Hosting-Provider umzustellen, falls unerwartete Probleme auftreten.

Wir verwenden die folgenden Hosting-Anbieter für iSpring-Webdienste:

- **Liquid Web** (überprüfen Sie die Liquid-Web-Zertifizierungen)
- **Amazon Web Services** (überprüfen Sie das AWS-Konformitätsprogramm) (ISO-27001-zertifiziert)
- **FirstColo** (ISO-27001-zertifiziert)
- **Leaseweb** (ISO-27001-zertifiziert)

Unsere Hosting-Anbieter beschränken den physischen Zugang zu ihren Servern gemäß den Standards SSAE 16 und ISO 27001.

Sicheres Netzwerk

iSpring verwendet Software-Firewalls (auf Betriebssystemebene), die so konfiguriert sind, dass sie Denial-of-Service-Angriffe (DoS) verhindern und verweigerte Verbindungen protokollieren. Alle Firewalls sind standardmäßig im Verweigerungsmodus konfiguriert, wobei einige wenige Ports geöffnet sind, um eingehenden Datenverkehr zuzulassen.

Sichere Plattform

Die iSpring-Server laufen unter Debian Linux und sind mit den neuesten Sicherheitspatches ausgestattet. Für alle Server wurden Penetrationstests durchgeführt und die Systemprotokolle werden ständig überprüft, um verdächtige Aktivitäten zu erkennen.

Secure Shell (SSH) unterstützt den authentifizierten und verschlüsselten Remote-Login-Zugriff durch iSpring-Mitarbeiter*innen. Alle Versuche, sich unbefugt Zugang zu den Servern zu verschaffen (z. B. Wörterbuchangriffe), werden vom Intrusion Prevention System überwacht und automatisch blockiert.

Überwachung

iSpring verwendet ein automatisches Überwachungssystem, um ein hohes Maß an Serviceleistung und Verfügbarkeit zu gewährleisten. Das interne Überwachungssystem führt regelmäßige Überprüfungen der Komponenten und Dienste von iSpring Learn und iSpring Space durch, um ihre wichtigsten Betriebskennzahlen zu überwachen. Alarme sind so konfiguriert, dass iSpring-Mitarbeiter*innen per E-Mail, Instant Messaging (Jabber) und SMS benachrichtigt werden, wenn Frühwarnschwellen für wichtige Betriebskennzahlen überschritten werden. Ein Bereitschaftsplan garantiert, dass die Mitarbeiter*innen immer verfügbar sind, um auf betriebliche Probleme zu reagieren. Es wird eine Dokumentation geführt, die das Personal bei der Behandlung von Vorfällen und Problemen unterstützt und informiert. Die Ingenieur*innen des technischen Supports sind 24/7/365 im Einsatz.

Speicherung und Sicherung

iSpring verwendet Continuous Data Protection anstelle regelmäßiger Backups bei iSpring Learn LMS und iSpring Space, um Datenverluste und Serviceunterbrechungen im Falle von Hardwareproblemen zu vermeiden. Alle Daten von iSpring Learn und iSpring Space werden redundant an mehreren physischen Standorten gespeichert. Dies gilt sowohl für die von Kund*innen hochgeladenen Dateien als auch für ihre in Datenbanken gespeicherten Daten. Aber auch die Datenbanken der Kund*innen werden täglich gesichert.

Zugang für Mitarbeiter*innen

iSpring verlangt, dass Mitarbeiter*innen mit potenziellem Zugang zu Kund*innendaten je nach Position und Grad des Datenzugriffs einer umfassenden Hintergrundprüfung unterzogen werden (soweit gesetzlich zulässig).

iSpring gewährt den Zugang zu den iSpring-Learn-Servern oder seiner Verwaltungskonsole nur denjenigen iSpring-Mitarbeiter*innen, die einen legitimen geschäftlichen Bedarf für diese Privilegien haben. Wenn ein*e Mitarbeiter*in keinen geschäftlichen Bedarf mehr für diese Privilegien hat, wird ihm*ihr der Zugang sofort entzogen, auch wenn er*sie weiterhin ein*e Mitarbeiter*in von iSpring ist. Alle Zugriffe von iSpring-Mitarbeiter*innen auf die iSpring-Learn-Server werden protokolliert und routinemäßig überprüft.

Betriebskontinuitätsmanagement

Die iSpring-Webdienste wurden so konzipiert, dass sie System- oder Hardwareausfälle mit minimalen Auswirkungen auf den*die Kund*in verkraften. Alle iSpring-Webdienste werden in einer 1+1-Konfiguration bereitgestellt, sodass im Falle eines Ausfalls des primären Rechenzentrums die Möglichkeit besteht, den Datenverkehr auf ein sekundäres Rechenzentrum umzuleiten. Wir verwenden einen dynamischen DNS-Dienst mit einer aktiven Failover-Funktion, um den Datenverkehr von einem vorübergehend nicht verfügbaren Server automatisch auf einen Backup-Server umzuleiten.

Datenverschlüsselung

iSpring-Webdienste verwenden eine sichere (verschlüsselte) Verbindung, wo dies möglich ist und die Gesamtleistung für Endbenutzer*innen nicht beeinträchtigt.

Die folgenden Arten von Benutzer*innenverbindungen zu iSpring-Webdiensten werden durch eine 256-Bit-SSL/TLS-Verschlüsselung geschützt:

- Alle sensiblen Daten wie Passwörter, Kontakt- und Rechnungsinformationen werden immer über SSL übertragen. Nicht-sensible Daten werden über einfaches HTTP ohne Verschlüsselung übertragen. Wenn Sie sich Sorgen um die Sicherheit Ihrer Inhalte machen, können Sie die Option **HTTPS erzwingen aktivieren,** wodurch alle Verbindungen SSL-verschlüsselt werden.

Für die Datenübertragung zwischen iSpring-Servern werden nur verschlüsselte Verbindungen verwendet:

- Alle E-Mail-Nachrichten von iSpring-Webdiensten werden über TLS gesendet.

- Die Datenbankreplikation zwischen Datenbankservern wird über SSL durchgeführt.
- Alle Dateiübertragungen zwischen Storage-Servern werden über SSL und SFTP durchgeführt.

Passwortrichtlinie

Die iSpring-Webdienste verlangen, dass jedes Passwort mindestens sechs Zeichen lang ist, mindestens einen Großbuchstaben und mindestens eine Zahl enthält. Diese Anforderung hilft zu verhindern, dass Konten mit kurzen, allgemeinen Passwörtern konfiguriert werden, die leicht mit einem Wörterbuchangriff kompromittiert werden können.

Inaktivitätstimeout

Ein*e Benutzer*in kann einen öffentlichen PC verlassen, ohne sich abzumelden, und seinen*ihren PC zu Hause unbeaufsichtigt lassen. iSpring-Webdienste begegnet dieser Art von Bedrohung durch die Anwendung von Inaktivitätstimeouts. Benutzer*innen werden automatisch von den iSpring-Webdiensten abgemeldet, wenn ihre Verbindung mehrere Minuten lang inaktiv ist.

Firewall-Kompatibilität

Die iSpring-Webdienste sind Firewall-freundlich. Das Autorentool iSpring Suite kommuniziert mit iSpring Learn LMS über eine reguläre HTTP (Port 80)-Verbindung und eine sichere HTTPS (Port 443)-Verbindung.

iSpring Suite erzeugt nur ausgehenden HTTP- und HTTPS-Datenverkehr zu den Ports 80 und 443. Da die meisten Firewalls bereits so konfiguriert sind, dass sie ausgehenden Webverkehr zulassen, müssen Benutzer*innen ihre Firewall nicht manuell konfigurieren.

Außerbetriebnahme von Speichergeräten

Die iSpring-Richtlinie sieht einen Außerbetriebnahmeprozess für Wechseldatenträger und Speichergeräte vor. Dieser Prozess soll verhindern, dass Kund*innendaten in die Hände Unbefugter gelangen. Wenn ein Speichermedium das Ende seiner Lebensdauer erreicht, leitet ein*e speziell geschulte*r iSpring-Mitarbeiter*in einen Außerbetriebnahmeprozess für das Gerät ein. iSpring schult die Techniken, die im DoD 5220.22-M („National Industrial Security Program Operating Manual“) oder den NIST 800-88 („Guidelines for Media Sanitization“) beschrieben sind, um Daten im Rahmen des Außerbetriebnahmeprozesses zu vernichten.

Wenn ein Hardware-Gerät nicht außer Betrieb genommen werden kann, wird es entmagnetisiert oder gemäß dem Industriestandard physisch zerstört.

Schutz der Kund*innenprivatsphäre

iSpring ist sich darüber im Klaren, dass alle Unternehmen, die ihre Dienstleistungen auslagern, um den Datenschutz besorgt sind. iSpring verfügt über eine strenge Datenschutzpolitik, die die unbefugte Weitergabe von persönlichen oder Unternehmensdaten an Dritte untersagt.

Offenbarung von Benutzer*inneninformationen

Um Webdienste bereitstellen zu können, muss iSpring bestimmte persönliche Benutzer*inneninformationen erfassen, einschließlich Vor- und Nachname, E-Mail-Adresse und Passwörter auf Kontoebene. iSpring wird diese vertraulichen Informationen nicht an Dritte weitergeben oder diese Informationen in irgendeiner anderen Weise nutzen, als um die vereinbarten Dienste mit allen Mitteln bereitzustellen. Mit dem Einverständnis ihrer Kund*innen sendet iSpring Aktualisierungsnachrichten an Benutzer*innen von iSpring-Webdiensten an die von ihnen bei der Registrierung angegebenen E-Mail-Adressen. Weitere Informationen über die iSpring-Datenschutzrichtlinie finden Sie unter https://www.ispringlearn.de/datenschutz.

Fazit

iSpring-Webdienste sind zuverlässige Lösungen für E-Learning-Authoring, sichere Bereitstellung, Nachverfolgung und gemeinsame Nutzung von Inhalten. iSpring-Sicherheitsprozesse schützen alle vertraulichen Informationen vor unbefugter Weitergabe an Dritte. Continuous Data Protection, umfassende Überwachung und Lastausgleich sorgen für einen unterbrechungsfreien Betrieb. Die Nutzung modernster Verschlüsselungsverfahren sorgt für die Sicherheit vertraulicher Informationen. Da die iSpring-Webdienste Firewall-freundlich sind, lässt sich diese Lösung nahtlos in die bestehende Netzwerk- und Sicherheitsinfrastruktur eines jeden Unternehmens integrieren.