ispring

Servizi Web iSpring: Panoramica dei processi di sicurezza

Data di revisione: settembre 2022

Attenzione

Il presente documento è fornito solo a scopo informativo. Descrive le pratiche correnti di protezione dei dati dei clienti di iSpring a partire dalla data di rilascio del documento stesso; tali pratiche sono soggette a modifiche senza preavviso. Il presente documento non genera alcuna garanzia, né dichiarazioni, impegni contrattuali, condizioni o rassicurazioni da parte di iSpring, delle sue affiliate, dei suoi fornitori o licenzianti.

Sommario

Introduzione

Aiutare a proteggere la riservatezza, l'integrità e la disponibilità dei dati dei nostri clienti è della massima importanza per iSpring, così come lo è mantenere la fiducia e a stima dei clienti. Lo scopo del presente documento è rispondere alla domanda “In che modo iSpring può aiutarmi a proteggere i miei dati?”. Nello specifico, sono descritti i processi di sicurezza fisica e operativa di iSpring relativamente all'infrastruttura di rete e del server sotto controllo di iSpring e alle implementazioni della sicurezza specifica del servizio.

Panoramica dei Servizi Web iSpring

iSpring offre i seguenti Servizi Web:

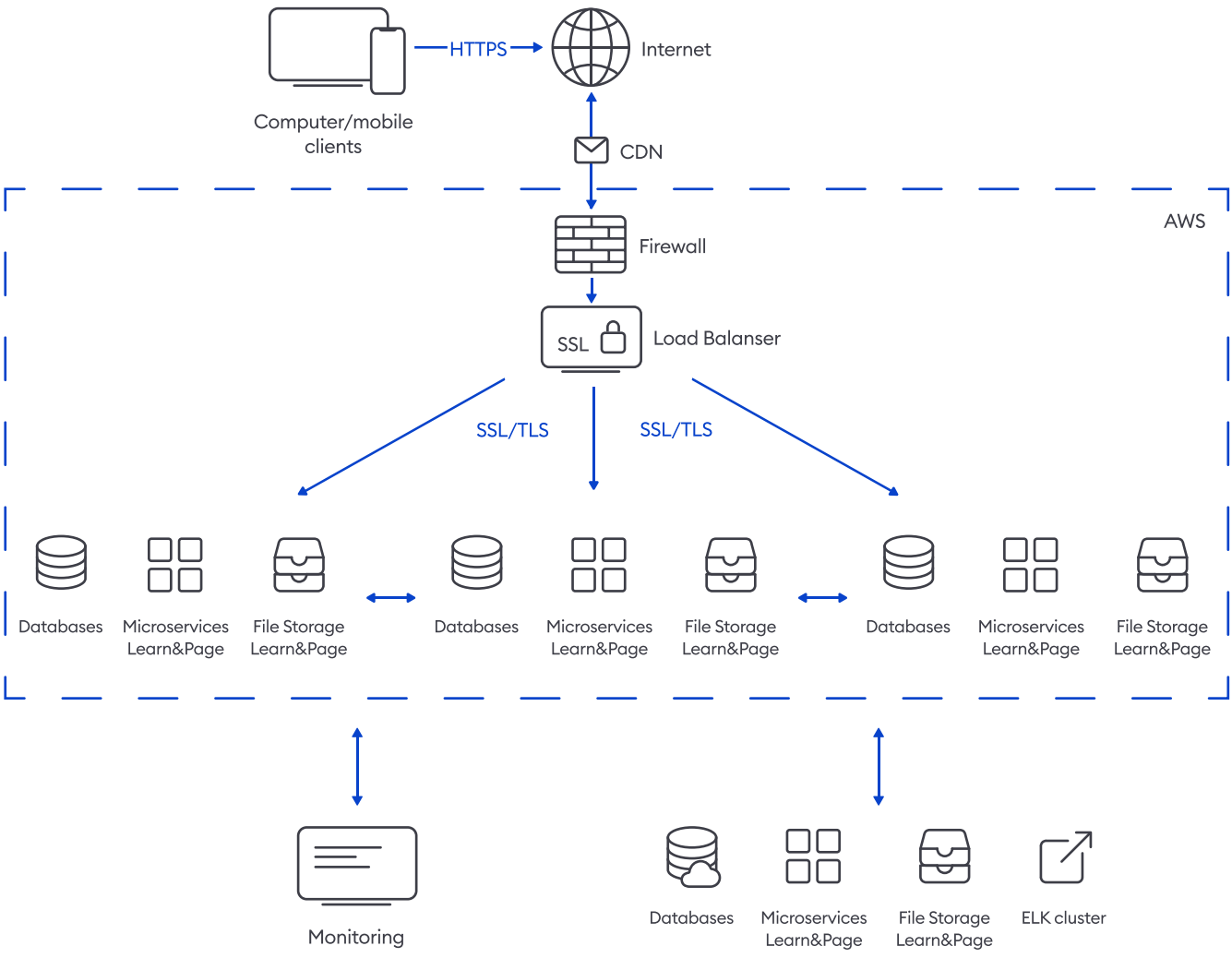
1. **iSpring Learn** è un Learning management system (LMS) ospitato per la formazione e la valutazione dei dipendenti o degli studenti online.
2. **iSpring Space** è un servizio Web per l'archiviazione dei corsi eLearning e per la collaborazione con il proprio team.
3. **iSpring Market** è una piattaforma basata su cloud per la vendita di corsi online.

Entrambi i servizi Web sono strettamente integrati in iSpring Suite, uno strumento di authoring per l'eLearning, e nelle applicazioni iSpring per dispositivi mobili.

Principi di progettazione sicura

I Servizi Web iSpring sono progettati per fornire un hosting sicuro dei dati personali degli utenti e per la distribuzione di contenuti, database e statistiche degli utenti su una rete non sicura. Durante la fase di sviluppo del software, le considerazioni di sicurezza sono state sempre prevalenti rispetto ai problemi di fruibilità.

Schema di rete



Infrastrutture sicure

iSpring utilizza fornitori di hosting attendibili che rispettano elevati standard di sicurezza per eseguire componenti e servizi dei Servizi Web iSpring. iSpring non si affida a un singolo fornitore di hosting, pertanto è possibile spostare un'operazione da un fornitore di hosting principale a uno secondario, nel caso di eventuali problemi imprevisti.

Per i Servizi Web iSpring usiamo i seguenti fornitori di hosting:

- **Liquid Web** (verifica le certificazioni di Liquid Web)
- **Amazon Web Services** (verifica il programma per la conformità di AWS) (certificazione ISO 27001)
- **FirstColo** (certificazione ISO 27001)
- **Leaseweb** (certificazione ISO 27001)

I nostri fornitori di hosting limitano l'accesso fisico ai loro server secondo quanto previsto dagli standard SSAE 16 e ISO 27001.

Rete sicura

iSpring usa firewall software (a livello di sistema operativo) che sono configurati per prevenire interruzioni di servizio (attacchi DoS) e registrare le connessioni negate. Per impostazione predefinita, tutti i firewall sono configurati in modalità negazione con alcune porte aperte per consentire il traffico in entrata.

Piattaforma sicura

I server dei Servizi Web iSpring girano su Debian Linux con le più recenti patch di sicurezza installate. I test di penetrazione sono stati eseguiti su tutti i server e i registri di sistema sono costantemente controllati per identificare le attività sospette.

Il protocollo Secure Shell (SSH) supporta l'accesso da remoto autenticato e crittografato da parte dello staff iSpring. Ogni tentativo di accesso non autorizzato ai server (ad es., attacchi dizionario) è monitorato e automaticamente bloccato dal sistema di prevenzione delle intrusioni.

Monitoraggio

iSpring utilizza un sistema di monitoraggio automatizzato per fornire un alto livello di performance e disponibilità del servizio. Il sistema di monitoraggio interno esegue controlli periodici dei componenti e dei Servizi Web iSpring per monitorare le relative metriche operative chiave. Vengono configurati dei sistemi d'allarme per l'invio allo staff di iSpring di notifiche via e-mail, di messaggi istantanei (Jabber) e di SMS quando vengono superate le soglie di allerta prestabilite delle metriche operative chiave. Per garantire che il personale sia sempre disponibile a rispondere ai problemi operativi è utilizzato un programma di reperibilità. La documentazione viene conservata per supportare e informare il personale relativamente alla gestione di incidenti o problemi. O tecnici del supporto tecnico sono in servizio 24 ore su 24, 7 giorni su 7 e 365 giorni l'anno.

Archiviazione e backup

iSpring utilizza la protezione continua dei dati anziché backup periodici presso i Servizi Web iSpring per evitare la perdita di dati e l'interruzione del servizio in caso di problemi hardware. Tutti i dati dei Servizi Web iSpring sono archiviati in modo ridondante in diversi luoghi fisici. Funziona così sia per i file caricati dai clienti sia per i relativi dati conservati nei database. In ogni caso, i database dei clienti sono oggetto di backup con cadenza quotidiana.

Accesso dei dipendenti

iSpring richiede allo staff con potenziale accesso ai dati dei clienti di sottoporsi a un controllo approfondito del background (ai termini di legge), variabile secondo la loro posizione e il livello di accesso ai dati.

iSpring fornisce l'accesso ai server iSpring Learn o alla relativa console di amministrazione solo ai dipendenti iSpring che abbiano legittime esigenze di lavoro per tali privilegi. Qualora un dipendente non abbia più legittime esigenze di lavoro per questi privilegi, il suo accesso viene immediatamente revocato, anche se lo stesso dipendente continua a essere un dipendente di iSpring. Ogni accesso ai server iSpring Learn da parte dei dipendenti iSpring è registrato e verificato regolarmente.

Gestione della continuità operativa

I Servizi Web iSpring sono progettati per tollerare errori di sistema o hardware con un minimo impatto sui clienti. Tutti i Servizi Web iSpring sono erogati in configurazione 1+1, cosicché, in caso di errore nel data center principale, ci sia l'opzione di reindirizzare il traffico in un data center secondario. Usiamo un servizio di DNS dinamico con una funzionalità failover attiva per reindirizzare automaticamente il traffico da un server temporaneamente non disponibile a un server di backup.

Crittografia dei dati

I Servizi Web iSpring utilizzano una connessione sicura (crittografata), quando possibile, senza influire sulla performance complessiva per gli utenti finali.

I seguenti tipi di connessione da parte degli utenti dei Servizi Web iSpring sono protetti mediante una crittografia SSL/TLS a 256 bit:

- Tutti i dati sensibili, come le password, le informazioni di contatto e di fatturazione sono sempre trasferiti su tecnologie SSL. Le informazioni non sensibili sono trasferite su una piattaforma HTTP senza crittografia. Se la sicurezza dei contenuti è a rischio, è possibile attivare l'opzione **Forza HTTPS**, che rende tutte le connessioni crittografate tramite SSL.

Per trasferire i dati tra i server iSpring sono utilizzate solo le connessioni crittografate:

- Tutti i messaggi e-mail dai Servizi Web iSpring sono inviati su TLS.
- La replica del database tra server di database è eseguita su SSL.
- Tutti i trasferimenti di file tra server di archiviazione sono eseguiti su SSL e SFTP.

Informativa sulla password

I Servizi Web iSpring richiedono che ogni password abbia una lunghezza minima di sei caratteri, contenga almeno un carattere maiuscolo e almeno un numero. Queste richieste aiutano ad evitare che gli account siano configurati con password brevi e comuni, le quali sono facilmente compromesse da un attacco dizionario.

Timeout di inattività

Un utente potrà allontanarsi da un PC pubblico senza disconnettersi e lasciare un PC privato incustodito. I Servizi Web iSpring affrontano questo tipo di minaccia applicando timeout di inattività. Gli utenti sono automaticamente disconnessi dai Servizi Web iSpring se la loro connessione rimane inattiva per diversi minuti.

Compatibilità del firewall

I Servizi Web iSpring sono compatibili con i firewall. Lo strumento di authoring di iSpring Suite comunica con iSpring Learn LMS su una connessione regolare HTTP (porta 80) e sicura HTTPS (porta 443). iSpring Suite genera solo traffico in uscita HTTP e HTTPS sulle porte 80 e 443. Poiché la maggior parte dei firewall è già configurata per consentire traffico Web in uscita, gli utenti non hanno bisogno di configurare manualmente il proprio firewall.

Disattivazione del dispositivo di archiviazione

La politica di iSpring prevede un processo di disattivazione per i supporti rimovibili e per i dispositivi di archiviazione. Questo processo è pensato per evitare che i dati dei clienti siano accessibili a persone non autorizzate. Quando un dispositivo di archiviazione raggiunge la fine della propria vita operativa, un dipendente di iSpring espressamente formato inizia il suo processo di disattivazione. iSpring utilizza le tecniche descritte nel DoD 5220.22-M (“National Industrial Security Program Operating Manual” – “Manuale operativo del programma nazionale per la sicurezza industriale”) o nel NIST 800-88 (“Guidelines for Media Sanitization” – “Linee guida per la sanificazione dei media”) per distruggere i dati nell'ambito del processo di disattivazione. Se un dispositivo hardware non può essere disattivato, esso sarà smagnetizzato o fisicamente distrutto, in conformità con le pratiche standard del settore.

Protezione della privacy dei clienti

iSpring comprende il fatto che tutte le aziende che esternalizzano la fornitura di servizi siano preoccupate per la privacy. iSpring ha una forte politica sulla privacy che proibisce la divulgazione non autorizzata delle informazioni personali o aziendali a qualsiasi terza parte.

Divulgazione delle informazioni dei clienti

Per fornire Servizi Web, iSpring deve raccogliere alcune informazioni personali degli utenti, inclusi nome e cognome, indirizzo e-mail e password del livello di account. iSpring non diffonderà queste informazioni riservate a nessuna terza parte, né le utilizzerà in nessuna maniera diversa dal fornire servizi concordati con tutti i mezzi. Con il consenso dei propri clienti, iSpring invia messaggi di aggiornamento del servizio agli utenti dei Servizi Web iSpring agli indirizzi e-mail forniti in fase di registrazione. Maggiori informazioni sull'informativa sulla privacy di iSpring sono disponibili su www.ispring.it/informativa-privacy.

Conclusioni

I Servizi Web iSpring sono soluzioni affidabili per la creazione di corsi eLearning, la distribuzione sicura, il monitoraggio e la condivisione dei contenuti. I processi di sicurezza di iSpring proteggono tutte le informazioni riservate dalla divulgazione non autorizzata a terzi. La protezione continua dei dati, il monitoraggio esteso e il bilanciamento del carico assicurano un'operatività ininterrotta. L'utilizzo di crittografia all'avanguardia mantiene al sicuro le informazioni riservate. Il fatto che i Servizi Web di iSpring siano compatibili con i firewall consente di integrare perfettamente questa soluzione con la rete esistente e l'infrastruttura di sicurezza di qualsiasi azienda.