ispring

Serviços da Web da iSpring: Visão geral dos processos de segurança

Data da revisão: setembro de 2022

Notificação

Índice

Introdução

Ajudar a proteger a confidencialidade, integridade e disponibilidade dos dados de nossos clientes é da maior importância para a iSpring, assim como manter a confiança do cliente. O objetivo deste documento é responder à pergunta "Como a iSpring me ajuda a proteger meus dados?" Especificamente, os processos de segurança física e operacional do iSpring são descritos para infraestrutura de rede e servidor sob controle do iSpring, bem como implementações de segurança específicas de serviço.

Visão geral dos serviços da web da iSpring

A iSpring presta os seguintes serviços da web:

1. **iSpring Learn** é um Sistema de Gestão de Aprendizagem (LMS - Learning Management System) hospedado para ensinar e avaliar funcionários ou alunos online.

2. **iSpring Space** é um serviço web para armazenar cursos de e-learning e colaborar com a equipe.

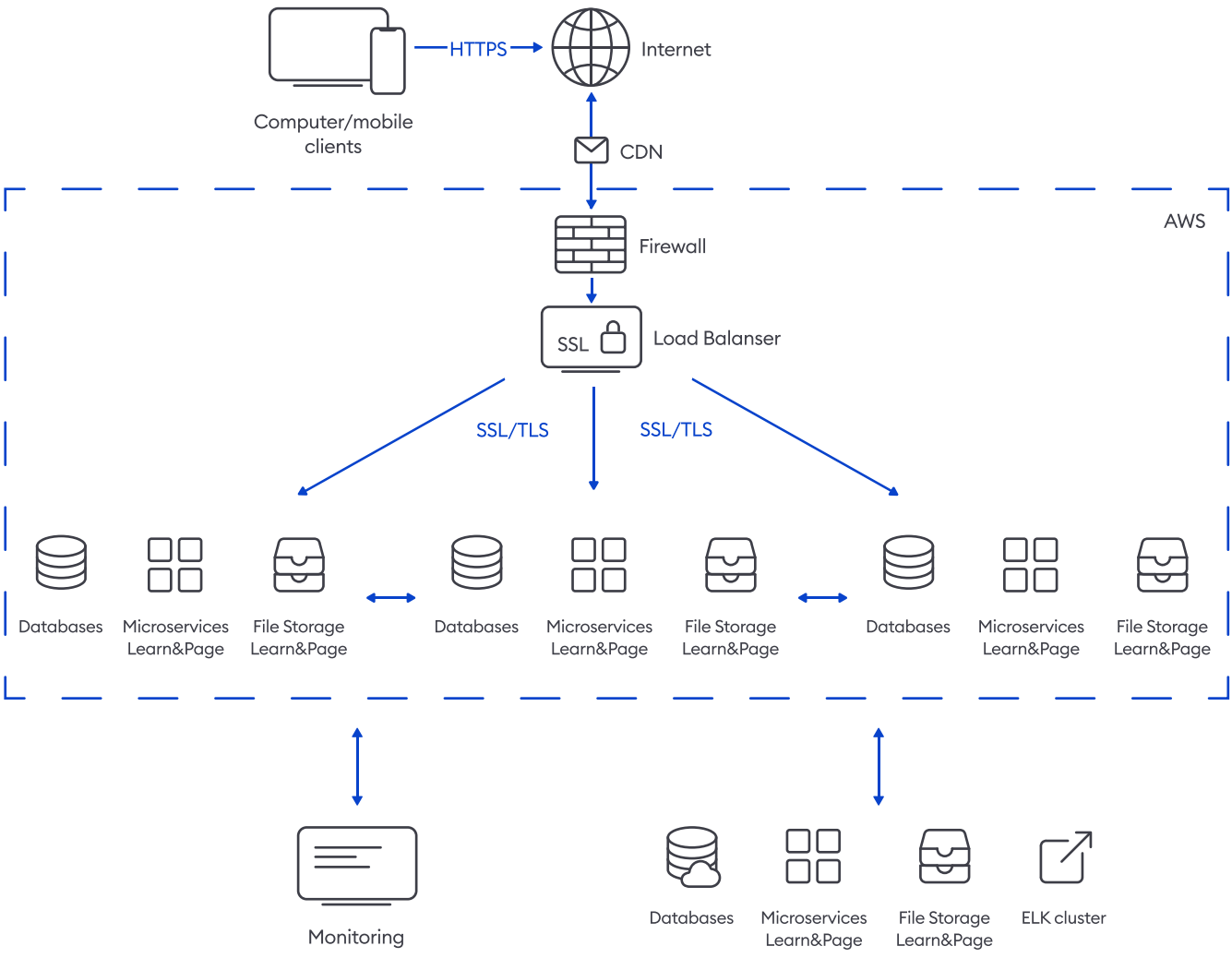
3. **iSpring Market** é uma plataforma baseada em nuvem para venda online de cursos.

Ambos os serviços da web estão totalmente integrados ao iSpring Suite, uma ferramenta de criação de cursos de e-learning, e aos aplicativos móveis da iSpring.

Princípios de design seguro

Os serviços da web da iSpring foram projetados para oferecer hospedagem segura de dados pessoais dos usuários e entrega de conteúdo, bancos de dados e análises dos usuários em uma rede não confiável. Durante o desenvolvimento do software, as considerações de segurança prevaleceram sobre as preocupações de usabilidade.

Diagrama de rede



Instalações seguras

A iSpring usa provedores de hospedagem confiáveis com altos padrões de segurança para executar componentes e serviços dos serviços da web da iSpring. A iSpring não depende de um único provedor de hospedagem; portanto, é possível alternar a operação de um provedor de hospedagem primário para um secundário no caso de qualquer problema inesperado.

Usamos os seguintes provedores de hospedagem para serviços da web da iSpring:

- **Liquid Web** (verifique as certificações Liquid Web)
- **Amazon Web Services** (verifique o Programa de conformidade AWS) (com certificação ISO 27001)
- **FirstColo** (com certificação ISO 27001)
- **Leaseweb** (com certificação ISO 27001)

Nossos provedores de hospedagem restringem o acesso físico aos seus servidores de acordo com as normas SSAE 16 e ISO 27001.

Rede segura

A iSpring usa firewalls de software (nível de sistema operacional) que são configurados para evitar negação de serviço (ataques DoS) e registrar conexões negadas. Todos os firewalls são configurados em modo de negação por padrão com algumas portas abertas para permitir o tráfego de entrada.

Plataforma segura

Os servidores de serviços da web da iSpring são executados no Debian Linux com os patches de segurança mais recentes instalados. Testes de penetração foram realizados para todos os servidores e os logs do sistema são auditados constantemente para identificar atividades suspeitas.

O Secure Shell (SSH) oferece suporte ao acesso remoto autenticado e criptografado de login pela equipe do iSpring. Quaisquer tentativas de acesso não autorizado aos servidores (por exemplo, ataques de dicionário) são monitoradas e bloqueadas automaticamente pelo sistema de prevenção de intrusão.

Monitoramento

A iSpring utiliza um sistema de monitoramento automatizado para oferecer um alto nível de desempenho e disponibilidade de serviço. O sistema de monitoramento interno faz verificações periódicas dos componentes e serviços dos serviços da web da iSpring para monitorar suas principais métricas operacionais. Os alarmes são configurados para notificar a equipe da iSpring por e-mail, mensagens instantâneas (Jabber) e SMS quando os limites de alerta antecipado das principais métricas operacionais são ultrapassados. Uma agenda de plantão é usada para garantir que a equipe esteja sempre disponível para responder aos problemasoperacionais. A documentação é mantida para ajudar e informar a equipe sobre como lidar com incidentes ou problemas. Os engenheiros de suporte técnico estão disponíveis 24/7/365.

Armazenamento e backup

A iSpring usa proteção contínua de dados em vez de backups regulares nos serviços da web da iSpring para evitar perda de dados e interrupção do serviço em caso de problemas de hardware. Todos os dados dos serviços da web da iSpring são armazenados de forma redundante em vários locais físicos. Funciona tanto para arquivos enviados por clientes quanto para respectivos dados armazenados em bancos de dados. No entanto, os bancos de dados dos clientes também passam por backup diariamente.

Acesso de funcionários

A iSpring exige que os funcionários com potencial acesso aos dados do cliente passem por uma extensa verificação de antecedentes (conforme permitido por lei), dependendo de seu cargo e nível de acesso aos dados.

A iSpring fornece acesso aos servidores do iSpring Learn ou ao seu console de administração apenas para funcionários da iSpring que tenham necessidades comerciais legítimas de tais privilégios. Quando um funcionário não precisa mais desses privilégios, seu acesso é imediatamente revogado, mesmo que ele continue sendo um funcionário da iSpring. Todo o acesso aos servidores iSpring Learn por funcionários da iSpring é registrado e auditado rotineiramente

Gestão de continuidade de negócios

Os serviços da web da iSpring foram projetados para tolerar falhas de sistema ou hardware com impacto mínimo no cliente. Todos os serviços da web da iSpring são implantados na configuração 1+1, para que, em caso de falha no data center primário, haja a opção de redirecionar o tráfego para um data center secundário. Usamos o serviço DNS dinâmico com um recurso de failover ativo para redirecionar automaticamente o tráfego de um servidor temporariamente indisponível para um servidor de backup.

Criptografia de dados

Os serviços da web da iSpring usam conexão segura (criptografada) sempre que possível e não afetam o desempenho geral dos usuários finais

Os seguintes tipos de conexões de usuários para serviços da web da iSpring são protegidos usando uma criptografia SSL/TLS de 256 bits:

- Todos os dados confidenciais, como senhas, informações de contato e cobrança, são sempre transferidos por SSL. As informações não confidenciais são transferidas por HTTP simples sem criptografia. Se a segurança do conteúdo estiver em questão, é possível ativar a opção **Forçar HTTPS** que torna criptografadas todas as conexões por SSL.

Somente conexões criptografadas são usadas para transferir dados entre servidores iSpring:

- Todas as mensagens de e-mail dos serviços da web da iSpring são enviadas por TLS.
- A replicação de banco de dados entre servidores de banco de dados é realizada por SSL.
- Todas as transferências de arquivos entre servidores de armazenamento são realizadas por SSL e SFTP.

Política de senha

Os serviços da web da iSpring exigem que cada senha tenha pelo menos seis caracteres, contenha pelo menos uma letra maiúscula e pelo menos um número. Esse requisito ajuda a evitar que as contas sejam configuradas com senhas curtas e comuns, facilmente comprometidas com um ataque de dicionário.

Tempos limite de inatividade

Um usuário pode sair de um PC público sem fazer logout e deixar um PC doméstico sem supervisão. Os serviços da web da iSpring abordam esse tipo de ameaça aplicando tempos limite de inatividade. Os usuários são automaticamente desconectados dos serviços da web da iSpring se sua conexão ficar inativa por vários minutos.

Compatibilidade do firewall

Os serviços da web da iSpring são compatíveis com firewall. A ferramenta de criação de cursos iSpring Suite se comunica com o iSpring Learn LMS por meio de uma conexão HTTP regular (porta 80) e HTTPS segura (porta 443). O iSpring Suite gera apenas tráfego HTTP e HTTPS de saída para as portas 80 e 443. Como a maioria dos firewalls já está configurada para permitir o tráfego de saída da web, os usuários não precisam configurar seu firewall manualmente.

Desativação do dispositivo de armazenamento

A política iSpring implica um processo de desativação para mídia removível e dispositivos de armazenamento. Esse processo foi desenvolvido para evitar que os dados do cliente sejam expostos a indivíduos não autorizados. Quando um dispositivo de armazenamento chega ao fim de sua vida operacional, um funcionário da iSpring especialmente treinado inicia um processo de desativação para ele. A iSpring usa as técnicas descritas no DoD 5220.22-M (“Manual Operacional do Programa Nacional de Segurança Industrial”) ou NIST 800-88 (“Diretrizes para Sanitização de Mídia”) para destruir dados como parte do processo de desativação. Se um dispositivo de hardware não puder ser desativado, ele será desmagnetizado ou fisicamente destruído de acordo com as práticas padrão do setor.

Protegendo a privacidade do cliente

A iSpring entende que todas as empresas que terceirizam a prestação de serviços estão preocupadas com a privacidade. A iSpring tem uma forte política de privacidade que proíbe a divulgação não autorizada de informações pessoais ou corporativas a terceiros.

Divulgação das informações do usuário

Para prestar serviços da web, a iSpring deve coletar determinadas informações pessoais do usuário, incluindo nome/sobrenome, endereço de e-mail e senhas no nível da conta. A iSpring não divulgará essas informações confidenciais a terceiros ou usará essas informações de qualquer maneira que não seja para prestar serviços acordados por todos os meios. Com o consentimento de seus clientes, a iSpring envia mensagens de atualização de serviço para usuários de serviços da web da iSpring para endereços de e-mail fornecidos durante o registro. Mais informações sobre a Política de Privacidade da iSpring estão disponíveis em https://www.ispringpro.com.br/politica-de-privacidade.

Conclusão

Os serviços da web da iSpring são soluções confiáveis para criação de e-learning, distribuição segura, rastreamento e compartilhamento de conteúdo. Os processos de segurança iSpring protegem todas as informações confidenciais contra divulgação não autorizada a terceiros. Proteção de dados contínua, monitoramento extensivo e balanceamento de carga garantem operação ininterrupta. O uso de criptografia de última geração mantém as informações confidenciais seguras. O fato de os serviços da web da iSpring serem compatíveis com firewall permite integrar esta solução perfeitamente com a rede e infraestrutura de segurança existente de qualquer empresa.