PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 5059 di Martedì 30 novembre 2021

Le componenti chiave della sicurezza di una piattaforma LMS

Quali sono i fattori da considerare nella scelta di un LMS per garantire la sicurezza dei dati e delle informazioni in esso contenute?

Sia che tu stia utilizzando il tuo **LMS** per la formazione aziendale interna sia per vendere corsi online ai tuoi clienti, la sicurezza della tua piattaforma LMS dovrebbe essere una priorità.

Un LMS è infatti uno dei principali archivi di **dati e informazioni sensibili aziendali**: può contenere i dati dei dipendenti (se usi la piattaforma per la formazione aziendale) o dei tuoi clienti (se sei un rivenditore di corsi online), informazioni sulle politiche aziendali, dettagli riservati su prodotti o strategie, etc.

Una violazione della sicurezza della piattaforma potrebbe portare al furto di questi dati o all'interruzione del funzionamento della piattaforma, con conseguenti danni economici e d'immagine.

Per proteggere la tua azienda da queste eventualità, è quindi fondamentale che la piattaforma LMS rispetti elevati **livelli di sicurezza**. Ma quali sono le funzionalità necessarie per tenere i dati del tuo LMS al sicuro? Scopriamole insieme.

Gestione autenticazione e password

Per prima cosa, assicurati che il **sistema di gestione delle autenticazioni e degli accessi in piattaforma** offra un robusto livello di protezione. L'autenticazione è la capacità di verificare l'identità di un utente e determinare se ha diritto ad accedere in piattaforma. Normalmente, l'accesso ad un LMS avviene mediante delle credenziali di accesso (username e password), ma uno dei problemi più comuni (che è anche causa di molti attacchi informatici) riguarda proprio la gestione delle password degli utenti. Eccoti, quindi, alcuni suggerimenti per aumentare il livello di sicurezza delle autenticazioni.

Scadenza password
La maggior parte degli utenti ha una pessima gestione delle password: c'è chi utilizza la stessa password per più account e chi non cambia la password regolarmente. Fai in modo che il tuo LMS richieda agli utenti di **reimpostare la password regolarmente**: ad esempio, una volta al mese. Assicurati inoltre che il sistema non consenta loro di riutilizzare password già usate in precedenza, altrimenti i tuoi sforzi saranno del tutto vani.

Caratteristiche password
Un altro aspetto da non trascurare è che generalmente gli utenti scelgono password facili da ricordare che, in altre parole, sono assolutamente poco sicure. In questo caso, è molto importante che la piattaforma LMS ti consenta di impostare dei **requisiti minimi per le password**, ad esempio definendone la lunghezza minima, il numero di caratteri speciali o alfanumerici che devono contenere, etc.

Tentativi di accesso limitati
In molti casi, gli utenti malintenzionati continuano a provare ad accedere al sistema finché non ottengono la giusta combinazione di lettere, numeri e caratteri speciali. Ti consigliamo quindi di prevedere al **massimo tre tentativi di accesso**. Dopo il terzo tentativo consecutivo fallito, l'account dovrebbe essere bloccato fino all'intervento di un amministratore.

Verifica in due passaggi
La verifica in due passaggi è un metodo di accesso alla piattaforma che aggiunge un ulteriore livello di sicurezza al processo di login, richiedendo all'utente di indicare **due diverse forme di autenticazione**. La prima è quella normale, generalmente la password; la seconda, invece, può prevedere modalità differenti: inserire un codice ricevuto via SMS o via e-mail, rispondere ad una telefonata automatica, utilizzare un'app di autenticazione, etc.

Single Sign-ON (SSO)
Il Single Sign-ON (in acronimo SSO) è un processo di autenticazione che consente ad un utente di accedere a più applicazioni con un **unico set di credenziali** di accesso, con enormi vantaggi non solo per l'utente (che deve quindi ricordare una sola password per tutti i software aziendali), ma anche per l'azienda, che **centralizza il controllo dei propri account utente**. Come? Ad esempio, applicando le stesse politiche e restrizioni di sicurezza per tutte le piattaforme e i software usati in azienda (anche quelli in cloud di terze parti, come potrebbe essere una piattaforma LMS), nonché di aggiornare in massa tutti i propri account in caso di violazione.

Protocollo SSL

L'accesso all'LMS dovrebbe avvenire esclusivamente tramite una **connessione sicura**, al fine di garantire che tutti i dati scambiati tra il server e il computer dell'utente siano crittografati, impedendo ai criminali informatici di visualizzare o rubare le informazioni trasferite. Assicurati quindi che il fornitore LMS utilizzi un **protocollo SSL (Secure Sockets Layer)**, cioè il sistema di sicurezza che stabilisce una connessione crittografata tra il tuo sito web e il browser di un utente.

Backup e ripristino di emergenza

Sebbene tutti i livelli di sicurezza fin qui elencati siano fondamentali per difendere i tuoi dati, è estremamente importante che la piattaforma sia dotata anche di **sistemi di backup automatici** che ti consentano di salvare regolarmente le informazioni in essa contenute (non solo i dati sensibili ma, banalmente, anche i contenuti dei corsi, i materiali didattici, i dati di fruizione, gli attestati, etc.).

D'altronde, cosa succede ai dati archiviati se il server in cui sono conservati subisce un danno? Assicurati quindi che il tuo fornitore LMS sia dotato di idonei sistemi di backup e che disponga di **piani di ripristino** nel caso in cui i dati venissero compromessi.

Conformità alla normativa sulla privacy (GDPR)

Per non incorrere in pesanti sanzioni, assicurati che la tua piattaforma LMS metta in atto un sistema di **gestione e trattamento dei dati** conforme alla normativa in materia di privacy e garantisca che le informazioni siano trattate secondo i principi di riservatezza, integrità, riservatezza e disponibilità previsti dal GDPR (Regolamento generale sulla protezione dei dati UE).

Protezione dei dati: il caso DynDevice LMS

Come abbiamo visto, un LMS è a tutti gli effetti uno dei principali archivi di dati e informazioni aziendali. Di conseguenza, quando si sceglie una piattaforma LMS, risulta fondamentale affidarsi ad un fornitore che garantisca adeguati **livelli di sicurezza**.

In quest'ottica, **DynDevice LMS** offre la garanzia di un elevato standard tecnologico, della massima affidabilità del sistema e della sicurezza dei dati. Il sistema si appoggia su infrastrutture informatiche adeguatamente strutturate (continuità del servizio 24 ore su 24, idonei sistemi di back-up e di ripristino, connettività suppletive ed alternative in caso di cadute di linea o picchi di traffico) e, al tempo stesso, estremamente sicure per garantire la tutela e la riservatezza dei dati personali trattati.

Mega Italia Media, l'eLearning company bresciana che ha sviluppato DynDevice LMS, dispone inoltre di un **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)** certificato ISO27001 che costituisce parte integrante del Modello

Organizzativo 231 adottato dall'azienda.

www.puntosicuro.it