ELEARNINGNEWS ARTICLE

Year 5 - number 177 Wednesday 20 october 2021

The key components of LMS platform security

What factors should you consider when choosing an LMS to ensure the security of the data and information it contains?

Whether you're using your **LMS** for internal corporate training or to sell online courses to your customers, the security of your LMS platform should be a priority.

In fact, an LMS is one of the main repositories of sensitive **corporate data and information**: it can contain employee data (if you're using the platform for corporate training) or your customers' data (if you're an online course reseller), information about company policies, confidential details about products or strategies, etc.

A breach of platform security could lead to the theft of this data or the disruption of platform operations, resulting in financial and image damage.

To protect your business from these eventualities, it is therefore crucial that your LMS platform adheres to high **levels of security**. But what features are necessary to keep your LMS data safe? Let's find out together.

Authentication and password management

First, make sure that your in-platform **authentication and access management system** offers a robust level of protection. Authentication is the ability to verify a user's identity and determine if they are eligible for in-platform access. Normally, access to an LMS is through login credentials (username and password), but one of the most common problems (which is also the cause of many cyber attacks) is precisely the management of user passwords. Here are some suggestions to increase the security level of authentication.

Password Expiration

Most users have poor password management: some use the same password for multiple accounts and some don't change their passwords regularly. Have your LMS require users to **reset their passwords regularly**: for example, once a month. Also make sure that the system doesn't allow them to reuse previously used passwords, otherwise your efforts will be in vain.

Password characteristics

Another aspect that should not be overlooked is that users generally choose passwords that are easy to remember, which, in other words, are absolutely insecure. In this case, it is very important that the LMS platform allows you to set **minimum requirements for passwords**, such as defining their minimum length, the number of special or alphanumeric characters they must contain, etc.

Limited access attempts

In many cases, malicious users will keep trying to access the system until they get the right combination of letters, numbers and special characters. Therefore, we recommend that you allow a **maximum of three login attempts**. After the third consecutive failed attempt, the account should be locked until an administrator intervenes.

Two-Step Verification

Two-step verification is a platform access method that adds an extra layer of security to the login process by requiring the user to provide **two different forms of authentication**. The first one is the normal one, usually the password; the second one, instead, can involve different ways: entering a code received via SMS or email, answering an automated phone call, using an authentication app, etc.

Single Sign-On (SSO)

Single Sign-On (SSO) is an authentication process that allows a user to access multiple applications with a **single set of credentials**, with enormous advantages not only for the user (who has to remember a single password for all business software), but also for the company, which **centralizes control of its user accounts**. How? For example, by enforcing the same security policies and restrictions for all platforms and software used in the company (even those in the third-party cloud, such as an LMS platform might be), as well as mass updating all their accounts in the event of a breach.

SSL Protocol

Access to the LMS should only be via a **secure connection**, in order to ensure that all data exchanged between the server and the user's computer is encrypted, preventing cybercriminals from viewing or stealing the transferred information. Therefore, make sure that the LMS provider uses a **Secure Sockets Layer (SSL) protocol**, which is the security system that establishes an encrypted connection between your website and a user's browser.

Backup and disaster recovery

Although all the security levels listed so far are essential to defend your data, it is extremely important that the platform is also equipped with automatic **backup systems** that allow you to regularly save the information it contains (not only sensitive data but, trivially, also course content, teaching materials, usage data, certificates, etc.).

On the other hand, what happens to archived data if the server where it is stored suffers damage? Make sure that your LMS provider has appropriate backup systems in place and has **recovery plans** in place in case data is compromised.

Privacy compliance (GDPR)

To avoid incurring heavy penalties, make sure that your LMS platform puts in place a data **management and processing system** that complies with privacy regulations and ensures that information is treated according to the principles of confidentiality, integrity, privacy and availability as set out in the GDPR (EU General Data Protection Regulation).

Data protection: the case of DynDevice LMS

As we have seen, an LMS is to all intents and purposes one of the main repositories of business data and information. Consequently, when choosing an LMS platform, it is essential to rely on a supplier that guarantees adequate **levels of security**.

From this point of view, **DynDevice LMS** offers the guarantee of a high technological standard, maximum system reliability and data security. The system relies on computer infrastructure adequately structured (continuity of service 24 hours on 24, suitable back-up and recovery systems, additional and alternative connectivity in case of line failures or traffic peaks) and, at the same time, extremely safe to ensure the protection and confidentiality of personal data processed.

Mega Italia Media, the eLearning company from Brescia that has developed DynDevice LMS, also has an ISO27001 **certified Information Security Management System (SGSI)** that is an integral part of the 231 Organizational Model adopted by the company.

Translated with www.DeepL.com/Translator