imc
part of Scheer

LMS-Einstellungen zu Datenschutz und Sicherheit

Projektleitfaden

imc Learning Suite

15. Oktober 2023

Informationen

Der Zweck dieses Leitfadens ist es, im Rahmen eines LMS-Einführungsprojekts unsere Kunden bei den Einstellungen zu Datenschutz und Sicherheit zu unterstützen. Dieser Leitfaden enthält die wichtigsten Informationen zu Einstellungsmöglichkeiten in diesen beiden Bereichen, welche im Rahmen des Einführungsprojekts betrachtet werden sollten.

Verwiesen wird hierbei auf die weiterführenden offiziellen Dokumente, die das Standardprodukt imc Learning Suite zur Verfügung stellt und welche für Kunden aufrufbar sind. Dieser Leitfaden stellt daher keine vollständige Dokumentation aller Möglichkeiten und Maßnahmen des Standardprodukts bereit. Vielmehr werden hier die wichtigsten Einstellungsoptionen behandelt, die im Rahmen eines Einführungsprojekts betrachtet werden müssen.

Im Rahmen des Projektabschlusses sollten zu allen Themen dieses Kunden-Leitfadens Entscheidungen und Einstellungen festgehalten werden. Folgende Bereiche werden in der Folge erläutert:

Datenschutzerklärung

Das LMS erlaubt die Verwendung einer Datenschutzerklärung im Rahmen des Anmeldeprozesses. Die Datenschutzerklärung kann (i.d.R. pro Mandanten) aktiviert werden oder deaktiviert werden.
Ist die Datenschutzerklärung aktiv, so muss der Nutzer beim ersten Anmeldevorgang die Datenschutzerklärung akzeptieren. Auch bei Änderungen am Text der Datenschutzerklärung muss der Lerner im Zuge des nächsten Anmeldevorgangs die Datenschutzerklärung nochmals akzeptieren. Eine Ablehnung der Datenschutzerklärung hat eine Passivierung des Nutzers zur Folge. Außerdem ist es möglich, dem Lerner im System die Möglichkeit zu geben, die Datenschutzerklärung aktiv zu widerrufen, was ebenfalls eine Deaktivierung seines Nutzeraccounts zur Folge hat.

Im Zuge des Einführungsprojekts ist zu definieren und zu konfigurieren, ob die Datenschutzerkläung verwendet wird und wenn ja, ob dann auch ein Widerruf im späteren Verlauf erlaubt ist.

Löschkonzept

Das LMS erlaubt das automatische Löschen (physisches Löschen oder Anonymisieren) von Nutzeraccounts, um z.B. Aufbewahrungsfristen abzubilden. Daneben ist das manuelle Löschen von Nutzerobjekten jederzeit durch einen Administrator möglich. Außerdem bietet das LMS die Option, dass Nutzer selbst ihren Account löschen können, was ebenfalls eine direkte physische Löschung oder Anonymisierung des Nutzerobjekts zur Folge hat. Als Alternative müssen Nutzer einen Löschauftrag per Mail und außerhalb des LMS an die Administration des LMS senden.

Im Zuge des Einführungsprojekts ist zu definieren und zu konfigurieren, ob Nutzer Ihren Account selbst löschen dürfen (oder ggf. nur einen Löschauftrag per Mail an die Administration senden

können) und ob es automatisierte Löschroutinen gibt, die Nutzerobjekte physisch löschen oder anonymisieren.

Sicherheitseinstellungen

Das LMS wird standardmäßig mit Sicherheitseinstellungen initialisiert (*Security by Default*). Es gibt jedoch fachliche Gründe, Sicherheitseinstellungen zu reduzieren:

- Sofern ein externer Katalog (Angebot vor Anmeldung eines Nutzers) verwendet wird, so muss hierzu die Einstellung „Anmeldung erzwingen" deaktiviert werden. Außerdem muss der Aufruf von Kursbeschreibungsseiten aktiviert werden, so dass auch vor der Anmeldung ein Aufruf von Objekten möglich ist, für die ein Zugriff des Portalmandanten erlaubt ist (Freigaben).
- Beim Speichern von Beschreibungsfeldern und Textfeldern werden standardmäßig HTML-Inhalte geprüft und entfernt. Dies kann dazu führen, dass Inhalte nach dem Speichern angepasst werden. Eine kurzzeitige Deaktivierung dieses Sicherheitsfeatures ist möglich, eine dauerhafte Deaktivierung sollte genauestens betrachtet werden.

Im Zuge des Einführungsprojekts ist zu definieren und zu konfigurieren, ob Sicherheitseinstellungen gegenüber dem Ansatz Security by Default angepasst wurden und zu welchem Zweck dies erfolgt ist.

Authentifizierung

Das LMS unterstützt verschiedene Authentifizierungsverfahren (u.a. lokale Anmeldung, SSO via SAML2 oder OIDC), welche pro Mandanten eingestellt werden können. Der Zugriff auf Mandanten-spezifische Portalseiten kann über eigene URLs oder über Parameter (*client*) umgesetzt werden. Für die lokale Anmeldung über das LMS können spezifische Passwortrichtlinien definiert werden, die von der Standardkonfiguration abweichen. Dies betrifft die Passwortkomplexität, die Dauer der Passwortgültigkeit, die Optionen zur Erzeugung von Passörtern sowie ggf. die Verwendung eines 2FA-Verfahrens.
Zusätzlich ist zu betrachten, ob Authentifizierungsverfahren Umgebungsspezifisch konfiguriert werden müssen. Insbesondere bei SSO-Verfahren ist dies nötig, da eine Produktiv-Umgebung und eine Test-Umgebung unterschiedliche Rücksprungpunkte für das SSO-Verfahren benötigen.

Im Zuge des Einführungsprojekts ist zu definieren und zu konfigurieren, welche Authentifizierungsverfahren (ggf. Mandanten-spezifisch und Umgebungs-spezifisch) eingerichtet sind und ob es Änderungen an den Passwortrichtlinien zur lokalen Anmeldung gab.

Anonymisierungsskripte

Sofern der Kunde neben der Produktiv-Umgebung weitere Umgebungen betreibt (Test, Stage, Dev oder ähnliches), so empfiehlt die imc von Zeit zu Zeit eine Spiegelung der Produktivdaten in die weiteren Umgebungen. Dies stellt sicher, dass der Datenstand vergleichbar ist und eine echte Testmöglichkeit erhalten bleibt. Die Spiegelung der Daten umfasst immer den kompletten Datenstand, d.h. die Datenbank inklusive der Objekte und der Konfiguration sowie der abgelegten Dateien im Datei-Verzeichnis des LMS. Eine Teil-Spiegelung ist nicht möglich.

Wird das LMS von der imc in der Cloud betrieben, so wird die imc eine Anonymisierung von Nutzerdaten vornehmen, um der EU-DSGV nachzukommen. Hierbei ist es möglich, Nutzer aus der Anonymisierung auszuschließen, um ein Testen in den nicht produktiven Umgebungen zu ermöglichen. Welche Nutzeraccounts von der Anonymisierung ausgeschlossen werden sollen, wird durch den Kunden im Projekt festgelegt. Hierzu empfiehlt es sich Gruppen im LMS anzulegen und deren Nutzer von der Anonymisierung auszuschließen.
Im Falle, dass der Kunde selbst den Betrieb des LMS durchführt (on-premise, im Gegensatz zum Cloud-Betrieb durch imc), ist es wichtig, im Rahmen des Einführungsprojekts die Bereitstellung einer ggf. anonymisierten Datenbank an imc zu Supportzwecken zu klären. Die Übermittlung der Datenbank sollte auf die gleiche Weise erfolgen wie imc neue Auslieferungspakete bereitstellt (per SFTP).

Im Zuge des Einführungsprojekts ist zu definieren und zu konfigurieren, welche Nutzer bzw. Nutzergruppen von der Anonymisierung ausgenommen werden sollen sofern neben der Produktiv-Umgebung der Betrieb weiterer Umgebungen (z.B. Test-Umgebung) erfolgt. Außerdem ist sicherzustellen, dass eine Übermittlung einer Datenbank an imc zu Supportzwecken im Falle des on-premise-Betriebs möglich ist.