imc
part of Scheer

Security Whitepaper

imc Learning Suite
Informationssicherheit

im-c.com

Security Whitepaper

imc Learning Suite
Informationssicherheit

Autor(en): Christoph Gast, Patrick Pekczynski
Datum: 21.03.2022

Dokument	Beschreibung
Version	14.12
Status (Entwurf / Überarbeitung/ Finalisierung)	Finalisierung
Kontaktperson(en)	Christoph Gast, Patrick Pekczynski

Historie	Status	Wer
13.12.2016	Entwurf	Christoph Gast
22.06.2021	Überarbeitung	Patrick Pekczynski
14.01.2022	Überarbeitung	Patrick Pekczynski
15.03.2022	Überarbeitung	Patrick Pekczynski
21.03.2022	Finalisierung	Dr. Peter Zönnchen

imc
information multimedia communication AG
Hauptsitz Saarbrücken
Scheer Tower, Uni-Campus Nord
D-66123 Saarbrücken
T. +49 681 9476-0 | Fax -530
info@im-c.com
im-c.com

Inhalt

1	**Informationssicherheit**	**4**
1.1	Vertraulichkeit	4
1.1.1	Bedrohung: Unbefugter Informationsgewinn	4
1.1.2	Gegenmaßnahmen: Verschlüsselung	5
1.2	Integrität	5
1.2.1	Bedrohung: Unbefugte Modifikation	5
1.2.2	Gegenmaßnahmen: Verschlüsselung und Redundanz	5
1.3	Authentizität	6
1.3.1	Bedrohung: Unbefugte Erzeugung	6
1.3.2	Gegenmaßnahmen: Sicherstellung der Identität	6
1.4	Verfügbarkeit	6
1.4.1	Bedrohung: Unbefugte Unterbrechung	6
1.4.2	Gegenmaßnahmen: Vermeiden des „Single Point of Failure“	7
1.5	Informationen zu Sicherheit und Sicherheitslücken	7
2	**Standards**	**8**
2.1	Transport Layer Security (TLS)	8
2.2	EV-SSL/TLS Zertifikate	9
2.3	Hashfunktionen der SHA-2-Familie	10
2.4	Verschlüsselungsstandards	10
2.4.1	Advanced Encryption Standard (AES)	10
2.5	Open Web Application Security Project (OWASP)	11
2.5.1	OWASP Top 10	11
3	**imc Learning Suite Sicherheitsmaßnahmen**	**12**
3.1	Berechtigungs- und Sichtbarkeitskonzepte	12
3.1.1	Profildaten	12
3.1.2	Organisationsmodell	13
3.1.3	Passwörter	14
3.1.4	Audit Log	15
4	**Penetrationstests**	**16**
5	**Quellenverzeichnis**	**17**

1 Informationssicherheit

Dieses Dokument gibt einen Überblick über das Thema imc Learning Suite und IT-Sicherheit.

1.1 Vertraulichkeit

Bei der elektronischen Abwicklung von Geschäften oder dem Austausch von Informationen ist es erwünscht, dass die Kommunikation zwischen Sender und Empfänger vertraulich bleibt und nur befugten Personen zugänglich ist.

1.1.1 Bedrohung: Unbefugter Informationsgewinn

Die Vertraulichkeit der Daten ist bedroht, wenn sich ein Dritter Zutritt zu den übermittelten oder gespeicherten Informationen verschafft. Dies kann beispielsweise durch das Abhören der Kommunikation oder direkten Zugang zu einem Computer zustande kommen.

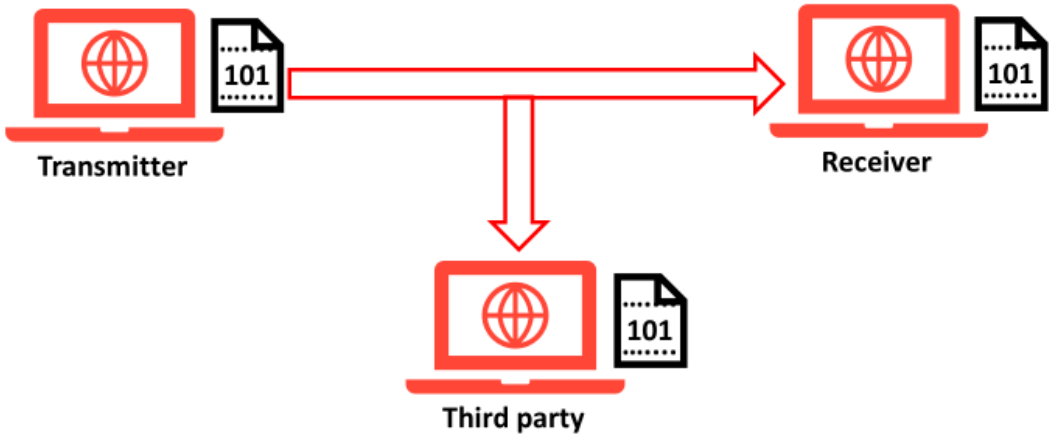

Abb. 1.1: Unbefugter Informationsgewinn

1.1.2 Gegenmaßnahmen: Verschlüsselung

Als Gegenmaßnahme werden Daten häufig verschlüsselt, um die enthaltene Information für Dritte unverständlich zu machen. imc Learning Suite ermöglicht eine sichere TLS-Verschlüsselung zwischen Client und Server und verhindert so das Abhören durch Dritte. Weitere Kommunikationswege können entsprechend den Sicherheitsbedürfnissen einzeln verschlüsselt werden. Der Zugang zu Rechnern kann außerdem durch gebäudetechnische Maßnahmen eingeschränkt werden.

1.2 Integrität

Integrität bedeutet, dass Informationen korrekt und unverändert sind. Der Empfänger einer Nachricht geht davon aus, dass ihn die Nachricht genauso erreicht, wie sie der Absender verfasst hat.

1.2.1 Bedrohung: Unbefugte Modifikation

Sobald ein Dritter Informationen unbefugt verändert, stellt dies einen Angriff auf die Integrität der Daten dar. Die Modifikation kann bei der Übertragung passieren oder auch direkt stattfinden, beispielsweise durch unbefugten Zutritt zu Computern.

Abb. 1.2: Unbefugte Modifikation

1.2.2 Gegenmaßnahmen: Verschlüsselung und Redundanz

Wenn Informationen verschlüsselt sind, kann der Angreifer keine sinnvollen Veränderungen vornehmen, da er den Inhalt nicht kennt. Eine weitere Möglichkeit ist der Einsatz von Redundanz. Durch Redundanz kann ein Empfänger erkennen, ob Daten verändert wurden. imc Learning Suite sichert die Kommunikation mit TLS-Verschlüsselung und nutzt darüber hinaus Tokenverfahren und ein gesichertes Sessionverfahren. Durch diese Verfahren wird die Kommunikation zwischen Client und Server zusätzlich geschützt und die Manipulation von Daten kann auf diese Weise erkannt und verhindert werden.

1.3 Authentizität

Authentizität ist die Gewissheit, dass Informationen von einer bestimmten Person stammen.

1.3.1 Bedrohung: Unbefugte Erzeugung

Wenn Daten so erzeugt werden, dass diese Daten einer falschen Person zugeordnet werden, stellt das einen Angriff auf die Authentizität dar. Beispielsweise können Überweisungen zu Lasten einer unbeteiligten Person ausgeführt werden, weil sich eine dritte Person als diese Person ausgegeben hat.

Abb. 1.3: Unbefugte Erzeugung

1.3.2 Gegenmaßnahmen: Sicherstellung der Identität

Es gibt viele Maßnahmen, welche die Identität einer Person sicherstellen sollen. Einige davon sind leichter zu knacken, beispielsweise die Authentifizierung mit Benutzername und Passwort, andere sind sicherer, wie z. B. eine digitale Signatur oder ein Fingerabdruck. imc Learning Suite setzt neben Verschlüsselung und sicheren Login-Daten auch auf Tokenverfahren, die eine Manipulation von Identitätsdaten verhindern und im Ernstfall erkennbar machen.

1.4 Verfügbarkeit

Verfügbarkeit bedeutet die Bereitstellung und die Funktionalität von Daten, Computern und Kommunikationsmitteln.

1.4.1 Bedrohung: Unbefugte Unterbrechung

Falls ein IT-System nicht oder nur teilweise läuft oder Informationen nicht zugänglich sind, kann dies schwerwiegende wirtschaftliche Folgen haben. Eine Denial-of-Service-Attacke (DoS) stellt beispielsweise eine unbefugte Unterbrechung dar. Hierbei werden Systeme absichtlich überlastet und sind nicht mehr oder nur noch eingeschränkt verfügbar.

Abb. 1.4: Unbefugte Unterbrechung

1.4.2 Gegenmaßnahmen: Vermeiden des „Single Point of Failure“

Systeme, die sich nicht durch einen Fehler an einer einzigen Stelle lahmlegen lassen (Single Point of Failure) sind besser vor unbefugter Unterbrechung geschützt. Erreicht werden kann dies durch hochverfügbare, redundante Systeme. Wenn ein System ausfällt, springt ein zweites, identisches System ein. imc Learning Suite unterstützt verschiedene Systemarchitekturen, die einen Single Point of Failure vermeiden. So kann eine hohe Verfügbarkeit des Systems beispielsweise durch Clustering erreicht werden. Clustering bedeutet, dass die einzelnen Systemkomponenten auf getrennte, untereinander vernetzte Server verlagert werden. Vorschläge für mögliche Systemarchitekturen sind im Technical Whitepaper für imc Learning Suite beschrieben.

1.5 Informationen zu Sicherheit und Sicherheitslücken

Weitere Informationen zu häufigen Sicherheitslücken in Softwareprodukten finden Sie unter den folgenden Links.

- Bundesamt für Sicherheit in der Informationstechnik (BSI):

  Umfassende Information zu Sicherheitslücken und Maßnahmen, wie man sich vor Sicherheitsrisiken schützen kann: http://www.bsi.de

- National Vulnerability Database (NVD):

  Datenbank mit konkreten Sicherheitslücken in Softwareprodukten: http://nvd.nist.gov/

2 Standards

2.1 Transport Layer Security (TLS)

Das Verschlüsselungsprotokoll *Transport Layer Security* (TLS) ist eine Weiterentwicklung des *Secure Sockets Layer* (SSL) Protokolls und ermöglicht die sichere Datenübertragung zwischen zwei Anwendungen (Vertraulichkeit und Integrität der Kommunikation).
Der Vorteil des TLS-Protokolls liegt vor allem darin, dass es unabhängig von Anwendungsprotokollen ist, sodass verschiedene Protokolle mit TLS abgesichert werden können. Ein Beispiel hierfür ist das *Hypertext Transfer Protocol* (HTTP). Unterstützt eine Anwendung HTTP und bietet sie einen sicheren Kommunikationskanal zum Datenaustausch an, so ist sie unter dem URI-Schema „https“ verfügbar. Hierbei ist zu beachten, dass „https“ sowohl SSL- als auch TLS-Verschlüsselung bedeuten kann.
Die Empfehlung von BSI (TR-02102-2, 2021) und NIST (SP800-52, 2019) ist, TLS mindestens in Version 1.2 zu verwenden.
imc Learning Suite bietet die Möglichkeit, die Kommunikation zwischen Client und Server mit TLS zu verschlüsseln. Dabei können verschiedene Verschlüsselungsalgorithmen implementiert und die Zertifizierungsschlüssel dem Sicherheitsbedürfnis entsprechend gewählt werden.

Im Allgemeinen ermöglicht TLS

- Authentifizierung der Kommunikationspartner,
- Vertraulichkeit der Daten durch Verschlüsselung,
- Integrität der Daten durch Verwendung von Hashwerten als Prüfsumme.

2.2 EV-SSL/TLS Zertifikate

Darüber hinaus unterstützt imc Learning Suite sogenannte Extended-Validation-SSL/TLS-Zertifikate (EV-SSL/TLS). Für ein EV-SSL/TLS-Zertifikat muss sich der Antragsteller einer erweiterten Überprüfung durch eine Zertifizierungsstelle unterziehen. Geprüft werden unter anderem die Identität und Geschäftsadresse des Antragstellers. Webseiten mit einem EV-SSL/TLS-Zertifikat werden im Browser durch den grün hinterlegten Firmennamen in der Adresszeile gekennzeichnet.

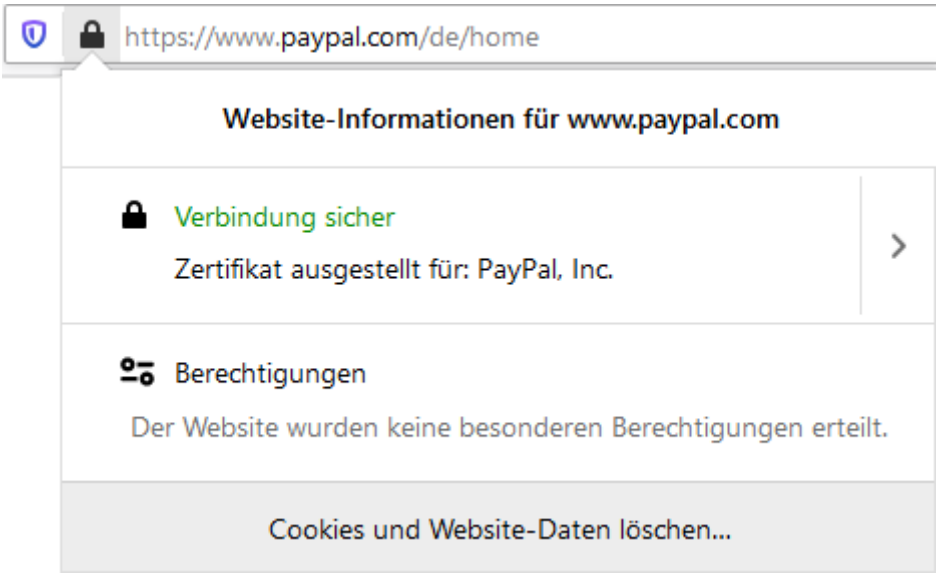

Abb. 2.1: Beispiel einer Website mit EV-SSL-Zertifikat

EV-Zertifikate werden beispielsweise im Online-Banking verwendet.

2.3 Hashfunktionen der SHA-2-Familie

Die SHA-2-Familie (von englisch secure hash algorithm, sicherer Hash-Algorithmus) ist der Oberbegriff für die vier kryptologischen Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512, die 2001 vom US-amerikanischen NIST als Nachfolger von SHA-1 standardisiert wurden. Zur Erzeugung des Hashwertes bei SHA-256 werden die Quelldaten in 512-Bit-Blöcke bzw. 16 32-Bit-Wörter aufgeteilt und iterativ mit 64 Konstanten und sechs logischen Funktionen verrechnet. Dabei wird mit einem Start-Hash aus acht 32-Bit-Wörtern begonnen. Dazu werden die ersten 32 Bits des Nachkommateils der Quadratwurzeln der ersten acht Primzahlen (2 bis 19) verwendet.

imc Learning Suite verwendet Hashfunktionen der SHA-2-Familie für Funktionalitäten, die einen sogenannten „digitalen Fingerabdruck" von Daten benötigen. Mit diesen Einwegfunktionen kann festgestellt werden, ob ein Benutzer im Besitz eines bestimmten zu Textes ist (z. B. Passwort). Bei der Passwortüberprüfung in imc Learning Suite werden also die Hashwerte des eingegebenen und des gespeicherten Passwortes miteinander verglichen. Das Verfahren wird durch eine mehrfache Nutzung von Sicherheitsmechanismen noch stärker gesichert.
Die zu verwendende Hashfunktion kann in imc Learning Suite konfiguriert werden. Der voreingestellt Wert ist SHA-256 und folgt Empfehlungen von BSI (TR-02102-2, 2021) und NIST (SP800-107, 2012).

2.4 Verschlüsselungsstandards

2.4.1 Advanced Encryption Standard (AES)

Der Advanced Encryption Standard (AES) ist ein FIPS[1]-geprüfter Verschlüsselungsstandard, der genutzt werden kann, um elektronische Daten zu schützen (FIPS-197 AES, 2001).
imc Learning Suite nutzt AES unter Anderem, um verschlüsselte URLs für den Abruf von Inhalten zu erzeugen („securedata"). Bei der AES-Konfiguration folgt imc Learning Suite den Empfehlungen von BSI (TR-02102-2, 2021) und NIST (SP800-38A , 2001) und setzt standardmäßig AES/CBC/PKCS5PADDING mit einer Schlüsselänge von 128-Bit ein.

[1] FIPS – Federal Information Processing Standard

2.5 Open Web Application Security Project (OWASP)

Das Open Web Application Security Project (OWASP, 2022) ist eine nicht-kommerzielle Organisation. Das Ziel von OWASP ist es, die Sicherheit von Software zu verbessern. OWASP macht auf häufige Sicherheitslücken aufmerksam und hilft dabei, diese Lücken zu bekämpfen. Weiterhin definiert OWASP Standards für die sichere Entwicklung und Anwendung von Software.

2.5.1 OWASP Top 10

Eine wichtige OWASP-Publikation ist die OWASP Top 10 der kritischsten Sicherheitsrisiken für Web-Anwendungen (OWASP Top 10, 2021).
imc folgt OWASP-Standards bei der Weiterentwicklung von imc Learning Suite. Die von OWASP empfohlenen Tools und Bibliotheken werden genutzt um die Sicherheit von imc Learning Suite an die geforderten Standards anzupassen.
imc unterzieht imc Learning Suite permanent neuen Tests und stellt somit sicher, dass das Sicherheitsniveau über alle Patch- und Release-Zyklen hinweg gehalten und durch ergänzende Sicherheitsmaßnahmen erhöht wird.

3 imc Learning Suite Sicherheitsmaßnahmen

Im Folgenden finden Sie eine Auswahl der in imc Learning Suite integrierten Sicherheitsmaßnahmen.
Tiefergreifende Konzepte für Sicherheitsexperten können im Rahmen eines Non-Disclosure-Agreements vorgestellt werden.

3.1 Berechtigungs- und Sichtbarkeitskonzepte

Die folgenden Kapitel beschreiben Maßnahmen, welche Anwender von imc Learning Suite selbst einstellen können oder welche mit Benutzereingaben in das System zu tun haben.

3.1.1 Profildaten

An verschiedenen Stellen von imc Learning Suite können Profildaten von Benutzern angezeigt werden, oder Benutzer können Daten eingeben. Profildaten enthalten die persönlichen Informationen einzelner Personen wie etwa Name oder E-Mailadresse. Beispielsweise kann ein Benutzer die Kontaktdaten von anderen Benutzern in sein Adressbuch aufnehmen, oder nach Personen suchen.
imc Learning Suite bietet die Möglichkeit, je nach Kontext und Benutzer unterschiedliche Daten anzuzeigen oder unterschiedliche Eingabefelder zur Verfügung zu stellen. Auf diese Weise können Sie genau bestimmen, welche personenbezogenen Daten in imc Learning Suite eingeben werden dürfen und welche dieser Profildaten für andere Benutzer sichtbar sind. Damit unterstützt imc Learning Suite unterschiedliche Stufen von Vertraulichkeit, die je nach Kontext flexibel anpassbar sind.

3.1.2 Organisationsmodell

Jede Organisation oder Firma, die imc Learning Suite einsetzt, hat ihre eigene interne Struktur. Diese Struktur kann über ein Mandanten-, Gruppen- und Freigabemanagement detailliert abgebildet werden.

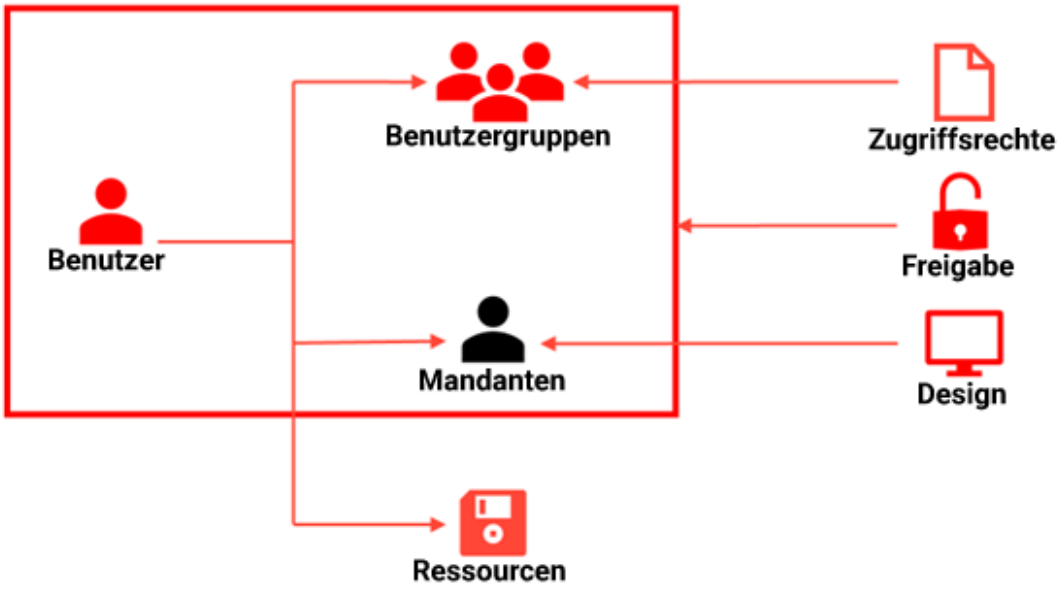

Abb. 3.1: Organisationsmodell

Mandanten

Mandanten dienen dazu, auf einem einzigen physischen System mehrere Teilsysteme zu betreiben. Die Teilsysteme können beispielsweise verschiedene Abteilungen innerhalb einer Organisation repräsentieren und sich im Design unterscheiden. Verschiedene Einstellungen in imc Learning Suite können mandantenspezifisch vorgenommen werden, wie etwa die Bestimmung eines Empfängerkreises für eine Benachrichtigung. Es können beliebig viele Mandanten angelegt werden.

Benutzergruppen

Einzelne Benutzer können in Benutzergruppen eingeteilt werden. Über die Benutzergruppen wird gesteuert, welche Funktionen den Mitgliedern einer Benutzergruppe zugänglich sind. Beispielsweise kann festgelegt werden, welche Navigationspunkte sichtbar sind und welche Funktionen die Gruppenmitglieder dort vorfinden. Es können beliebig viele Benutzergruppen und Untergruppen definiert werden.

Freigaben (ACL)

Über eine Access Control List (ACL) werden die Freigaben auf Objekte für Benutzer, Benutzergruppen und Mandanten festgelegt. Die Freigabe stellt ein Zugriffsrecht dar. Für jedes Objekt in imc Learning Suite (z. B. ein bestimmter Inhalt) kann festgelegt werden, welche Benutzer, Benutzergruppen oder Mandanten Zugriff auf dieses Objekt haben. Für jedes Objekt existieren

nur diejenigen spezifischen Berechtigungen, die zu seiner Verwaltung erforderlich sind, beispielsweise „Bearbeiten“, „Löschen“, oder „Freigeben“.

Organisationsmodell

Über die Kombination von Mandanten- und Gruppenzugehörigkeit sowie Freigaben lässt sich für jede Person genau festlegen, welche Inhalte diese Person zu sehen bekommt, wie die Inhalte dargestellt werden und auf welche Funktionen die Person Zugriff hat. Das Organisationsmodell von imc Learning Suite unterstützt somit optimal Vertraulichkeit und Integrität von Inhalten. Benutzer sehen nur die Inhalte, welche für sie bestimmt sind und können nur Änderungen vornehmen oder auf Funktionen zugreifen, wenn sie dazu befugt sind.

3.1.3 Passwörter

Autocomplete

Die Anmeldung an imc Learning Suite erfolgt mit einer eindeutigen Kombination aus Benutzername und Passwort. Je nachdem, wie der verwendete Browser eingestellt ist, werden diese Anmeldedaten eventuell im Browser gespeichert. Auf diese Weise muss der Anwender die Anmeldedaten nicht jedes Mal erneut eingeben, sondern der Browser füllt die Anmeldefelder automatisch aus (Autocomplete = Auto-Vervollständigung). Der Nachteil ist, dass Angreifer diese gespeicherten Anmeldedaten möglicherweise auslesen und missbrauchen können.
imc Learning Suite unterbindet das automatische Speichern der Anmeldedaten im Browser. Dabei ist es gleichgültig, ob der Anwender in seinem Browser die Autocomplete-Funktion aktiviert hat oder nicht. Die Passwörter anderer Internetseiten bleiben davon unberührt.

Identische Passwörter

Wenn ein Anwender ein Passwort für seinen imc Learning Suite-Zugang erstellt, wird der Hashwert des Passworts („digitaler Fingerabdruck“) in der imc Learning Suite-Datenbank gespeichert. Falls verschiedene Anwender zufällig identische Passwörter wählen, dann sind auch die Hashwerte dieser Passwörter identisch. So kann beispielsweise ein böswilliger Administrator, der Zugriff auf die imc Learning Suite-Datenbank hat, Passwort-Hashwerte vergleichen und daraus Rückschlüsse ziehen.
Um dem entgegenzuwirken, fügt imc Learning Suite jedem Passwort eine personenbezogene zufällige Zeichenfolge hinzu, die in der Kryptologie als „Salt“ bezeichnet wird. Diese Zeichenfolge wird zu dem Passwort hinzugefügt und bewirkt, dass die berechneten Passwort-Hashwerte niemals identisch sind, auch dann nicht, wenn die Passwörter im Klartext identisch sind.

Anmeldesperre

Die Anmeldung an imc Learning Suite erfolgt mit Benutzername und Passwort. Falls ein Anwender sein Passwort mehrmals hintereinander falsch eingibt, sperrt imc Learning Suite aus Sicherheitsgründen automatisch das Benutzerkonto (Anmeldesperre). Diese Anmeldesperre hat für den einzelnen Benutzer eine zeitweilige Einschränkung der Verfügbarkeit zur Folge. Wichtiger ist jedoch, dass das System mit dieser Anmeldesperre geschützt ist gegenüber Brute-Force-Angriffen auf die Passwörter. Brute-Force bedeutet hier, dass ein Angreifer solange Passwörter

ausprobiert, bis er eines der Passwörter geknackt hat und so potentiell großen Schaden anrichten kann. Die Anmeldesperre verhindert dies.
Die Anzahl der Anmeldeversuche bis zu einer Sperrung und die Dauer bis zu einer automatischen Entsperrung können frei konfiguriert werden.

3.1.4 Audit Log

Im Audit Log werden teilnehmerbezogene Daten wie zum Beispiel das Buchungsdatum oder der Buchungsstatus eines Kurses verwaltet und protokolliert. Änderungen, die durch den Kursteilnehmer verursacht wurden, werden ebenfalls im Audit Log protokolliert.
Der Audit Log ist üblicherweise nur geschulten Administratoren zugänglich. Mit dem Audit Log kann ein Administrator nachvollziehen, wann und wo von welcher Person Änderungen vorgenommen wurden. Falls diese Änderungen unerwünscht waren, beispielsweise wenn ein Teilnehmer einen Kurs versehentlich vorzeitig beendet hat, können diese Änderungen rückgängig gemacht werden.
Mit dem Audit Log stellt imc Learning Suite Administratoren ein wichtiges Tool zur Verfügung, mit welchem die Integrität der Daten sichergestellt werden kann.

4 Penetrationstests

Ein Penetrationstest, auch Pentest genannt, ist ein umfassender Sicherheitstest eines IT-Systems oder einer Software. Anhand von Methoden, die ein möglicher Angreifer anwenden würde, um in ein System einzudringen, werden systematisch potenzielle Sicherheitslücken aufgedeckt.

Die Ziele eines Penetrationstests sind:

- Aufdeckung von Schwachstellen,
- Aufdeckung von Fehlern, die durch fehlerhafte Bedienung auftreten können,
- Erhöhung der Sicherheit der Anwendung,
- Bestätigung der IT-Sicherheit durch unabhängige Dritte.

imc lässt regelmäßig Penetrationstests für imc Learning Suite durchführen. Die Ergebnisse der Tests fließen in neue Patches, Service Packs und Releases von imc Learning Suite ein.

5 Quellenverzeichnis

BSI Bundesamt für Sicherheit in der Informationstechnik. (12. März 2021). Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. (Version 2021-01). Deutschland. Abgerufen am 22. 06 2021 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2

NIST National Institute of Standards and Technology. (26. 11 2001). FIPS 197 Announcing Advanced Encryption Standard (AES). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

NIST National Institute of Standards and Technology. (12 2001). Special Publication 800-38A Recommendation for Block Cipher Modes of Operation Methods and Techniques . (2001 Edition). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

NIST National Institute of Standards and Technology. (08 2012). Special Publication 800-107 Recommendation for Applications Using Approved Hash Algorithms. (Revision 1). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf

NIST National Institute of Standards and Technology. (08 2019). Special Publication 800-52 Guidelines for the Selection,Configuration, and Use of Transport Layer Security (TLS) Implementations. United States of America. doi:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Open Web Application Security Project (OWASP). (2021). *OWASP Top 10 - The Ten Most Critical Web Application Security Risks*. Abgerufen am 14. 01 2022 von https://owasp.org/Top10/

Open Web Application Security Project (OWASP). (2022). *Open Web Application Security Project*. Abgerufen am 14. 01 2022 von Open Web Application Security Project: https://owasp.org/