imc
part of Scheer

ILS Security Whitepaper

Informationssicherheit mit imc Learning Suite

im-c.com

ILS Security Whitepaper

Informationssicherheit mit imc Learning Suite

Autor(en): Christoph Gast
Datum: 02.10.2020

Dokument	Beschreibung
Version	14.7
Status (Entwurf / Überprüfung / Finalisierung)	Finalisierung
Kontaktperson(en)	Dr. Julia Scheller, Dr. Peter Zönnchen

Historie	Status	Wer
13.12.2016	Entwurf	Christoph Gast
02.10.2020	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

Dieses Dokument gibt einen Überblick über das Thema imc Learning Suite und IT-Sicherheit. Dabei wird es um einzelne Computer, vernetzte Computer und das Internet gehen. Sie erfahren, welche Sicherheitsprobleme dort existieren und welchen Lösungsbeitrag imc Learning Suite liefert.

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.

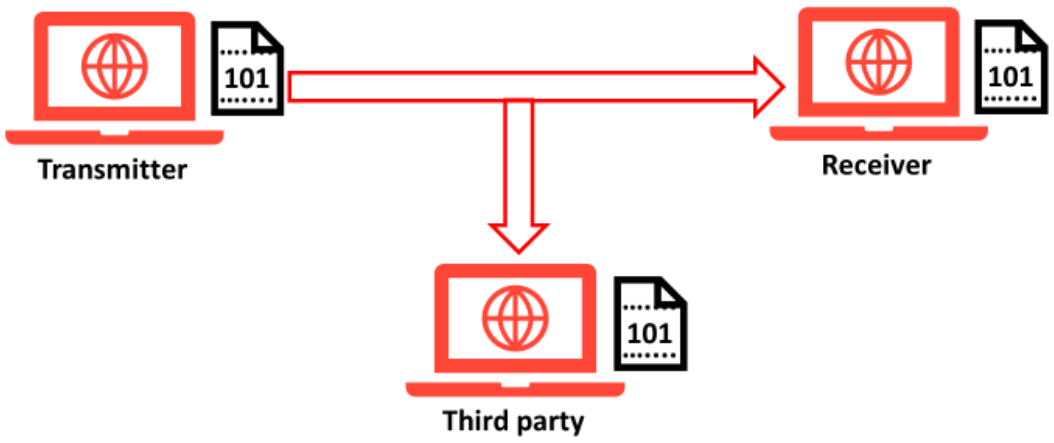

Abb. 1.1: Unbefugter Informationsgewinn

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 SSL-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 SSL-Verschlüsselung und nutzt darüber hinaus Tokenverfahren und ein gesichertes Sessionverfahren. Durch diese Verfahren wird die Kommunikation zwischen Client und Server zusätzlich geschützt; die Manipulation von Daten kann auf diese Weise erkannt und durch passende Gegenmaßnahmen 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 das Vorhandensein 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 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: Umfassende Information zu Sicherheitslücken und Maßnahmen, wie man sich vor Sicherheitsrisiken schützen kann: http://www.bsi.de
- National Vulnerability Database: Datenbank mit konkreten Sicherheitslücken in Softwareprodukten: http://nvd.nist.gov/
- The Open Source Vulnerability Database: Datenbank mit Sicherheitslücken in Open-Source-Softwareprodukten: http://osvdb.org/

2 Standards

2.1 SSL/TLS

Transport Layer Security (TLS) ist besser bekannt unter der Bezeichnung Secure Sockets Layer (SSL). Seit Version 3 wird SSL unter dem Namen TLS weiterentwickelt. TLS ist ein Verschlüsselungsprotokoll, welches die sichere Datenübertragung zwischen zwei Hosts ermöglicht.
Der Vorteil des SSL-Protokolls liegt vor allem darin, dass jedes Protokoll auf Basis des SSL-Protokolls implementiert werden kann. Ein Beispiel hierfür ist das HyperText Transfer Protocol Secure (HTTPS), welches identisch ist mit HTTP, mit dem Unterschied, dass die übertragenen Daten mit TLS verschlüsselt werden. Das HTTPS-Protokoll wird im Internet zur Authentifizierung und zur Verschlüsselung der Kommunikation zwischen Browser und Webserver verwendet.
imc Learning Suite bietet die Möglichkeit, die Kommunikation zwischen Client und Server mit SSL zu verschlüsseln. Dabei können verschiedene Verschlüsselungsalgorithmen implementiert und die Zertifizierungsschlüssel dem Sicherheitsbedürfnis entsprechend gewählt werden. Darüber hinaus unterstützt imc Learning Suite sogenannte Extended-Validation-SSL-Zertifikate (EV-SSL). Für ein EV-SSL-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-Zertifikat werden im Browser durch den grün hinterlegten Firmennamen in der Adresszeile gekennzeichnet. EV-Zertifikate werden beispielsweise im Online-Banking verwendet.

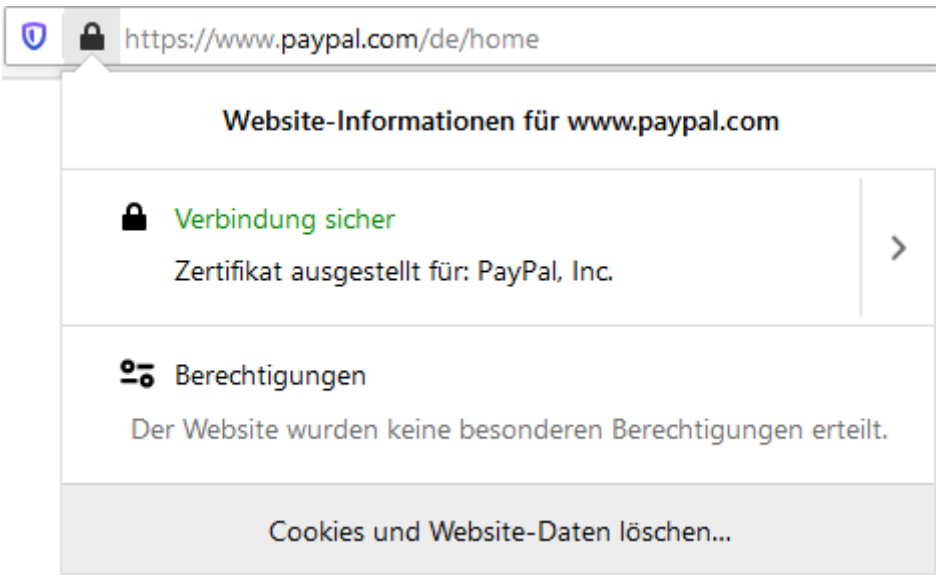

Abb. 2.1: Beispiel einer Website mit EV-SSL-Zertifikat

Im Allgemeinen ermöglicht SSL

- Authentifizierung der Kommunikationspartner,
- Vertraulichkeit der Daten durch Verschlüsselung,
- Integrität der Daten durch Überprüfung von Hashwerten (Hashwert = Prüfsumme).

2.2 MD5/SHA2

Message-Digest Algorithm 5 (MD5) ist eine populäre und schnelle kryptographische Hash-funktion. Hashfunktionen bilden eine Zeichenfolge beliebiger Länge auf eine Zeichenfolge mit fester Länge ab. MD5 generiert Hashwerte von 128 bit. Die 128 bit langen Hashwerte werden normalerweise als 32-stellige Hexadezimalzahlen ausgegeben.
Beispiel: 4eff7d0e702050df5fc72e2b8946ab41.
SHA-2 (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 Hash-Wertes 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 das MD5/SHA2-Verfahren für Funktionen, die eine Einwegverschlüsselung benötigen. Bei der Einwegverschlüsselung wird ein Text lediglich verschlüsselt, aber nicht mehr entschlüsselt. Auf diese Weise kann festgestellt werden, ob ein Benutzer im Besitz eines bestimmten zu verschlüsselnden Textes ist (z. B. Passwort). Bei der Passwortüberprüfung in imc Learning Suite werden also die verschlüsselten Hash-Werte des eingegebenen und des gespeicherten Passwortes miteinander verglichen. Das Verfahren wird durch eine mehrfache Nutzung von Sicherheitsmechanismen noch stärker gesichert.
Die Hashfunktion kann in imc Learning Suite über die Konfigurationsdatei clix.conf eingestellt werden (Abschnitt "security", "passwordHashAlgorithm"). Mögliche Werte sind dort MD5 und SHA-256.

2.3 DES

Der Data Encryption Standard (DES) ist ein weit verbreiteter Verschlüsselungs-Standard. Die Schlüssellänge beträgt 56 bit, kann aber durch Mehrfachanwendung verlängert werden. DES wird beispielsweise für die Sprachverschlüsselung verwendet. In Deutschland nutzen die Verfas-sungsschutzbehörden des Bundes und der Länder den DES-Standard.
imc Learning Suite nutzt DES für den sicheren Datenaustausch. Daten werden von imc Learning Suite mit Hilfe des DES-Standards verschlüsselt bevor sie übermittelt werden.

2.4 OWASP

Das Open Web Application Security Project (OWASP) ist eine nicht-kommerzielle Organisation. Das Ziel von OWASP ist es, die Sicherheit von Software zu verbessern. OWASP macht auf häufige Sicherheitslücken aufmerksam und ermöglicht es damit, diese Lücken zu bekämpfen. Weiterhin definiert OWASP Standards für die sichere Entwicklung und Anwendung von Software. Eine wichtige OWASP-Publikation ist die Top 10 der gravierendsten Sicherheitsmängel von Web-Anwendungen.
imc berücksichtigt die 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

höchste Standards erfüllt werden können. 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.

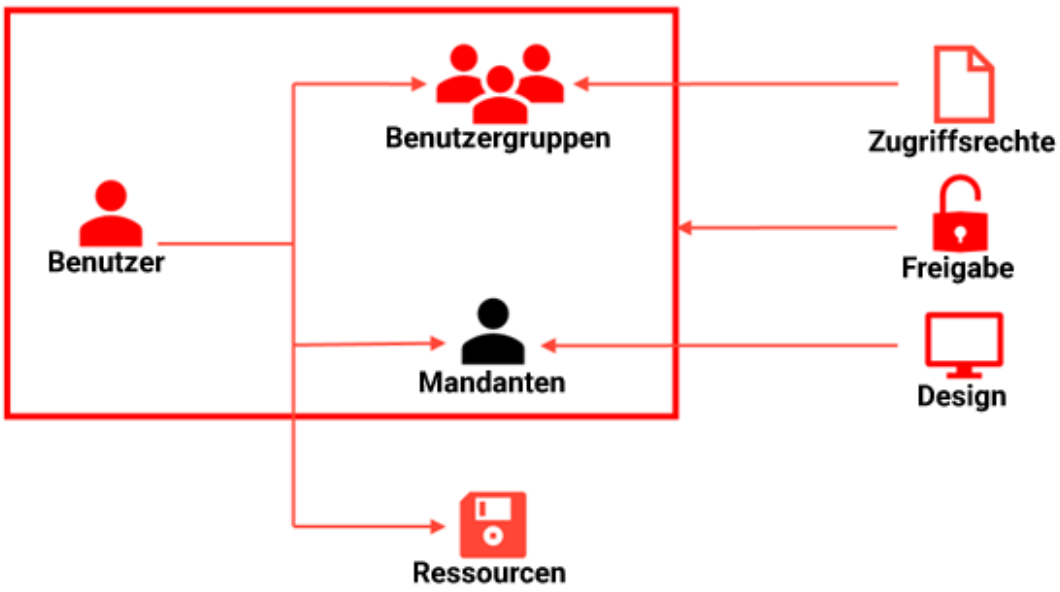

Abb. 3.1: Organisationsmodell

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 das Passwort verschlüsselt in der imc Learning Suite-Datenbank gespeichert (als sogenannter Hash-Wert). Falls verschiedene Anwender zufällig identische Passwörter wählen, dann wären normalerweise auch die verschlüsselten Versionen dieser Passwörter identisch. So könnte beispielsweise ein Administrator, der Zugriff auf die imc Learning Suite-Datenbank hat, verschlüsselte Passwörter vergleichen und daraus Rückschlüsse ziehen.
Um dem entgegenzuwirken fügt imc Learning Suite jedem Passwort einen personenbezogenen „Salt“ hinzu. Als Salt bezeichnet man in der Computerkryptographie eine zufällige Zeichenfolge. Diese Zeichenfolge wird an das Passwort angehängt und bewirkt, dass die verschlüsselt abgelegten Passwörter niemals identisch sind, auch dann nicht, wenn die Passwörter im Klartext identisch sein sollten.

Denial of Service (DoS)

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 (Denial of Service). Diese Anmeldesperre hat zwar 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-Aktionen gegen die Passwörter. Brute Force bedeutet hier, dass ein angreifender Server solange Passwörter ausprobiert, bis er eventuell 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 Pen Test 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,
- Bestätigung der IT-Sicherheit durch 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.