IT-Sicherheit im Corporate Learning durch LMS

von Annette Bouzo

Die Bedeutung eines Learning Management System (LMS) für die Sicherheit im Unternehmen wird mitunter unterschätzt. Dabei handelt es sich um ein unternehmenskritisches System. Als solches muss es entsprechend klug geschützt werden. Wie alle Software-Anwendungen muss es den Anforderungen von IT-Sicherheit und Datenschutz genügen. Doch die IT-Abteilung schützt vorwiegend vor Systemausfällen und Bedrohungen von außen wie Hacker-Angriffen, Viren und Schadsoftware. Wo liegen die speziellen zusätzlichen Sicherheitsaspekte für ein LMS und wie trägt ein zukunftssicheres LMS nun zu Datenschutz und Datensicherheit bei?

Schützenswertes LMS

Neben der unbestrittenen Notwendigkeit, personenbezogene Daten vor Missbrauch und unbefugtem Zugriff zu schützen, sind auch die Inhalte von Produktschulungen, insbesondere WBTs und Testergebnisse schützenswert. Produktschulungen beispielsweise geben mitunter auch Aufschluss über die Bauart von Produkten. Dabei werden insbesondere auch Schwachstellen thematisiert und konkrete Abhilfen aufgezeigt, was auch für den Mitbewerber interessant sein dürfte. WBTs und Tests dürfen weder inhaltlich noch bei ihren Einsatzergebnissen manipulierbar sein.

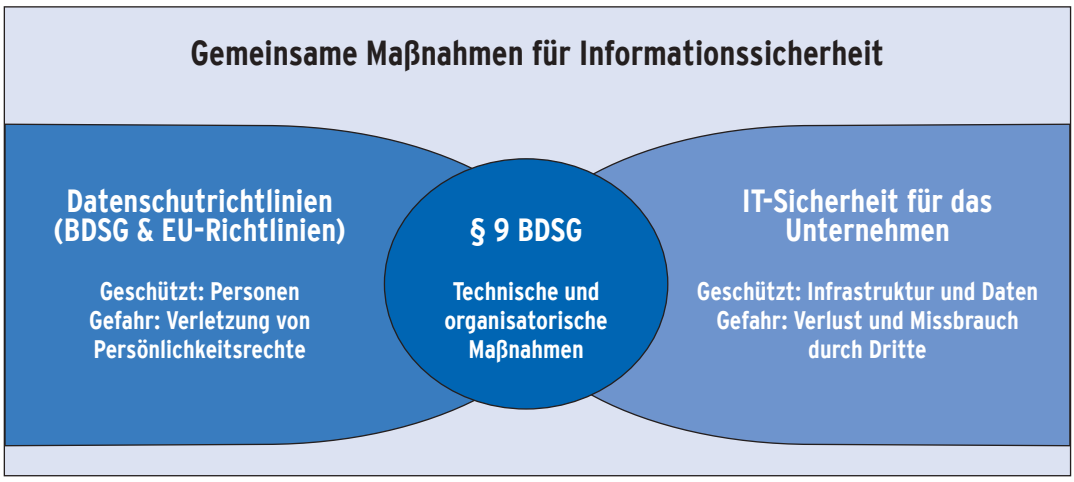
In Zeiten des Wandels und strategischer Neupositionierung ist das Learning Management System das führende Tool für den Know-how-Transfer. Inhalte, Volumen und Frequenz von Schulungen können dabei dem Wettbewerber nicht nur geplante strategische Neuausrichtungen, beispielsweise Vertriebs- / Service-Offensiven oder die zukünftige Verwendung neuer Technologien verraten. In Zeiten des Fachkräftemangels kann ein Sicherheitsleck auch die gezielte - mit den Kenntnissen über Mitarbeiterwissen unterlegte - Abwerbung von teuer qualifiziertem Fach- und Führungspersonal in sensiblen Bereichen vereinfachen.

Aufschluss über diese Details gibt nicht nur der Trainingskatalog, die Personaldatenbank oder die Historie des Learning Management Systems. Ein gezielter Zugriff der Datenklaue auf die Reporting-Einheit des LMS oder gar Inhalte von WBTs und Tests kann Unbefugten nicht nur Informationen zentral und bequem zur Weiterverarbeitung zur Verfügung stellen, sondern ganze Schulungsprogramme entwerten.

Daher ist das LMS für Unternehmen eine erfolgskritische Komponente und muss im eigenen Interesse geschützt werden. Der Betreiber eines LMS, im Regelfall also die eigene IT-Abteilung ist hier ein wichtiger Ansprechpartner.

IT-Sicherheit & Corporate Learning

Um die Gefahr von Hackerangriffen und Schadsoftware minimieren zu können, orientieren sich IT-Abteilungen und Softwarehersteller häufig an OWASP (The Open Web Application Security Project), einem Gremium, das jährlich eine relevante priorisierte Liste der gefährlichsten Angriffsflächen für Software-Anwendungen im Netz herausgibt (OWASP Foundation, 2016). Daraus leiten professionelle Softwarehersteller und IT-Abteilungen Maßnahmen ab, um das LMS gegen Bedrohungen wie z.B. SQL-Injektion oder Cross-Site Scripting (XSS) zu schützen. Dabei sind nicht nur passwort-geschützte Bereiche wie Trainingsportale zu sichern. Auch Webseiten, auf denen beispielsweise Trainingskataloge veröffentlicht werden und die nicht an eine Systemlandschaft angebunden sind, bieten



Informationssicherheit lässt sich inhaltlich in die zwei Bereiche Datenschutz und IT-Sicherheit teilen.

Angriffsflächen. Die Anforderungen an die IT-Abteilungen sind entsprechend hoch.

Datenschutz ist ein gesetzlich tief verankertes Grundrecht. Nicht nur das Bundesdatenschutzgesetz §9 (BDSG), sondern auch das Grundgesetz für die Bundesrepublik Deutschland (Art1I, 2I, GG), die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) sowie die Charta der Grundrechte der Europäischen Union (GRC) und die

Anlage §9 BDSG	Beispiele für konkrete Maßnahmen
Zutrittskontrolle: Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren	Sicherheitskonzept vor Ort, codierte Personalkarten/-Ausweise beim Betreten von Räumlichkeiten, Trennung der Räumlichkeiten von externem und internem Personal und / oder Aufsicht von Externen durch interne Personen
Zugangskontrolle: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können	Passwortroutinen, Nutzerkennungen, BIOS SecureID-Tokens oder VC, Verschlüsselungsverfahren
Zugriffskontrolle: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können	Benutzerkennung, Passwortsicherheit, Nutzer-historie, Rollen- und Rechtesystem, Anonymisierung von Auswertungen, gesicherte Terminalverbindungen (CITRIX), SOPs (Standard Operation Procedures), Unterweisung und Schulung der Mitarbeiter, Datenschutzbeauftragter
Weitergabekontrolle: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist	Nutzerhistorie, Verschlüsselung mit Standard-DRM (Microsoft AD RMS, S/MIME, open FT mit RSY/AES bzw. HTTPS
Eingabekontrolle: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind	Nutzerhistorie basierend auf Rollen und Rechtekonzept
Auftragskontrolle: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können	Möglichkeit der Anonymisierung beim Reporting. Bei Cloud- und SaaS-Dienstleistern ist entsprechend der physischen Serverstandort relevant. Bei Vertragsabschluss obliegt in Deutschland dem Kunden, von einem ausländischen Softwaredienstleister die Auftragsdatenverarbeitung nach deutschen Maßstäben einzufordern. Verstößt der Geschäftspartner, also beispielsweise der SaaS- oder Cloudprovider, gegen das BDSG wird der Auftraggeber rechtlich belangt. Dabei kann der Auftraggeber eine zyklische Kontrolle der BDSG-Belange vereinbaren und den Auftraggeber zur Kontrolle und Schulung seiner Angestellten verpflichten.
Verfügbarkeitskontrolle: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	IT-Sicherheitskonzept, Back-ups, Spiegelungen, Ausfallsicherungen und redundante Services
Datentrennung: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Beispielsweise logische Trennung von Test-/Integrations- und Produktivumgebungen oder Trennung über Codierung von Geschäftseinheiten auf Applikationsebene

Datenschutzrichtlinie der EU zeugen von dem Wert der Vertraulichkeit personenbezogener Daten.

Der Oberbegriff Informationssicherheit lässt sich inhaltlich in die zwei Bereiche Datenschutz und IT-Sicherheit teilen. Relevant für Unternehmen jeder Art sind die technischen und organisatorischen Maßnahmen, die nach der Anlage zu §9 daraus abgeleitet werden müssen.

In der Anlage von §9 BDSG heißt es: „Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird." Es sind also entsprechend angemessene Maßnahmen zu ergreifen. Dabei sollen dem Stand der Technik entsprechende Schutz- und Verschlüsselungsverfahren eingesetzt werden.

Viele Sicherheits- und Schutzmaßnahmen wie Zutritts- und Zugangskontrollen sollten unabhängig vom Aufgabenbereich in der gesamten Organisation umgesetzt werden. Im Folgenden soll aber vor allem auf Maßnahmen eingegangen werden, die beim LMS „greifen".

Interdisziplinäre Zugriffsrechte

Etablierte LMS haben rein vertikale oder horizontale Limitierungen aufgelöst. Zugriffsrechte werden nicht allein nach Abteilungsgrenzen (Vertrieb / Marketing) oder der Hierarchie (Direkter Vorgesetzter / Mitarbeiter) definiert, sondern vergeben Rollen nach faktischen Aufgabenbereichen. Dabei darf nicht übersehen werden, dass Personen auch mehr als eine Rolle innehaben können. So kann ein Mitarbeiter der Trainingsplanung gleichzeitig auch Vorgesetzter sein, eine Urlaubsvertretung eines Kollegen in einem anderen Bereich übernehmen oder als Trainer agieren. Ein LMS, das eine entsprechende Flexibilität bei der Definition von Gruppen-Zugriffsberechtigungen erlaubt, spart den sonst erforderlichen Zusatzaufwand, etwa von „Funktionslogins". Dadurch wird der leider mitunter gängigen Praxis vorgebeugt, sich gegenseitig Passwörter von Mitarbeiterkonten zu „leihen".

Daher haben sich für sichere LMS mit hoher Zukunftsorientierung bestimmte Standards beim Rollen- und Rechtemanagement etabliert. Solche LMS bieten ein äußerst differenziertes Rollen- und Rechtekonzept für Trainingsadministratoren, das neben hoher Prozessorientierung auch parallele Rollen und Vertretungsregelungen berücksichtigt. Dabei wird tatsächlich auf Datenebene zwischen Lese-/Bearbeitungs- und Löschrechten differenziert, ebenso sind explizite positive oder negative Ausnahmen definierbar. Eine Routine prüft dabei Widersprüche in den Zugriffsrechten. Relevante Dateneingaben und -änderungen lassen sich über die Nutzerhistorie nachvollziehen, Auswertungen können anonymisiert werden. So wird auch dem berechtigten Anliegen des Betriebsrates entsprochen.

Den gebuchten Schulungsteilnehmern werden Online-Zugänge aus dem Internet/Intranet angeboten, die den Zugriff auf die eigenen Buchungsdaten, anstehende Schulungen und Bildungshistorie erlauben. Handelt es sich um die Buchungsberechtigung für Dritte oder Teilnehmergruppen, darf nicht nur wie oben geschildert auf horizontal oder vertikaler Ebene agiert werden, da dies oft nicht der Organisationsrealität entspricht. Ein modernes LMS sollte deshalb prinzipiell beliebig flexibel konfigurierbare Zugriffe erlauben, die auf sicheren Selektionsalgorithmen basieren.

Bei der Definition von Rollen- und Rechten stehen dabei aber nicht nur die Prozesse und Aufgaben im Fokus. Ebenso muss zwischen kritischen und unkritischen Informationen unterschieden werden. Die ISO 27001 schreibt vor, dass eine Information ‚Anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung zu klassifizieren ist (DIN ISO/EC27001). Diese Vorschrift kann eine zusätzliche Entscheidungsgrundlage bei einer (Neu-) Konzipierung von Zugriffsrechten darstellen.

Learning Trends

Social Media, vor ein paar Jahren noch als Web 2.0 „gehypt", hat sich weiterentwickelt. Die aktualisierte Version in Corporate Learning-Zusammenhängen nennt sich ‚Informelles Lernen' und stellt den Dialog der Lernenden in den Mittelpunkt. Mitarbeiter, die sich auf modernen Lernplattformen bewegen, werden für Ihre Weiterbildungen gerne mit incentivierenden Symbolen belohnt. Manchmal sind diese Batches in Foren neben dem Profilbild oder Avatar sichtbar.

Sie demonstrieren nicht nur eine bestimmte Qualifikation, sondern sollen ebenfalls spielerisch zum Weiterbildungs-Wettbewerb anregen. Doch muss der Mitarbeiter aus Datenschutzgründen selbstständig steuern können, welche der einzelnen Batches in seinem Profil angezeigt werden dürfen. Besonders plakativ lässt sich dies an Inhalten zu sensiblen Themenbereichen, wie etwa aus dem Gesundheits- und Präventionsbereich illustrieren.

Auch das Thema Mobile Learning hat starken Einfluss auf die Sicherheitspolitik eines Unternehmens. Zielgruppenspezifisch sind durchsetzbare Geräte- und Nutzer-Richtlinien zu entwerfen. Ob wirklich alle Inhalte auf allen Gerätetypen verfügbar gemacht werden müssen, ist eine der vielen Fragen, die unternehmensindividuell beantwortet werden muss. Der Zugang zum LMS muss ebenso wie bei andere Anwendungen allen IT-Sicherheitsrichtlinien entsprechen. Dafür muss die Sicherheits-Software jeden mobilen Geräts mit den richtigen Sicherheitszertifikaten ausgerüstet sein und kontinuierlich aktualisiert werden. Insbesondere dürfen Lerninhalte auch auf mobilen Plattformen nicht manipulierbar sein.

Automatisierung & Vernetzung

Der Automatisierungsgrad bestimmt die Effizienz eines Unternehmens und hat deshalb einen großen Einfluss auf den Unternehmenserfolg. Eine durchgehende Systemintegration und automatisierte Prozessunterstützung erhöht die Daten- und Prozessqualität. Durch automatisierte Prozessunterstützung werden System- und Medienbrüche reduziert, wodurch das Volumen potentieller Fehlerquellen deutlich minimiert wird. Durch wegfallende Doppelarbeiten können Ressourcen effizienter eingesetzt werden. Auswertungen und Daten sind aktueller, verfügbarer und lassen durch ihre höhere Qualität sichere Entscheidungen zu. 60% der deutschen Mittelständler sehen im Bereich Digitalisierung und Vernetzung mit Partnern und Kunden Nachholbedarf (ak, 2015). Auch die Audits des Deutschen Bildungspreis sehen im Kernbereich IT-Infrastruktur noch große Defizite. Prozessunterstützung durch Automatisierung kann den Bereich Bildungs- und Talentmanagement nachhaltig stärken. (Dreyer, 2015)

Schnittstellen zu anderen Systemen oder die Zugriffsmöglichkeit über das Internet erhöhen die Priorität des Sicherheitsthemas, im Gegensatz zu einem in sich geschlossenen System. Das Anlegen der Benutzeraccounts mit Passwörtern und die entsprechend verschlüsselte Kommunikation der Zugangsdaten sind erste Schritte zu mehr Sicherheit.

INFO

TCmanager® LMS für Bildungsmanagement und Seminarverwaltung

Als sicheres LMS mit hoher Zukunftsorientierung hat sich TCmanager® LMS seit Jahren etabliert. Erfolgreiche Unternehmen unterschiedlichster Branchen wie SIEMENS, HypoVereinsbank oder KYOCERA Document Solutions, bei denen die Latte für IT-Sicherheit sehr hoch liegt, setzen TCmanager für ihre Bildungsprozesse ein. Das liegt neben anderen Highlights auch an den folgenden Eigenschaften von TCmanager®, die den hohen Sicherheitsansprüchen entsprechen:

Differenziertes Rollen – und Rechtekonzept

TCmanager® LMS bietet ein äußerst differenziertes Rollen- und Rechtekonzept für Trainingsadministratoren, das neben hoher Prozessorientierung auch parallele Rollen und Vertretungsregelungen berücksichtigt. Dabei wird tatsächlich auf Datenebene zwischen Lese-/ Bearbeitungs- und Löschrechten differenziert, ebenso sind explizite positive oder negative Ausnahmen definierbar.

Eine Routine prüft dabei Widersprüche in den Zugriffsrechten. Relevante Dateneingaben und -änderungen lassen sich über die Nutzerhistorie nachvollziehen, Auswertungen können anonymisiert werden. So wird auch den Anliegen des Betriebsrates entsprochen. Das praxiserprobte Rechte- und Rollenkonzept kann von entsprechend berechtigten und geschulten Anwendern selbstständig konfiguriert werden.

Zielgruppenoptimierte Trainingsportale

Den gebuchten Schulungsteilnehmern werden Online-Zugänge aus dem Internet/Intranet angeboten, die den Zugriff auf die eigenen Buchungsdaten, anstehende Schulungen und Bildungshistorie erlauben. Handelt es sich um die Buchungsberechtigung für Dritte oder Teilnehmergruppen, darf nicht nur wie oben geschildert auf horizontal oder vertikaler Ebene agiert werden, da dies oft nicht der Organisationsrealität entspricht. MyTCmanager Zugänge erlauben prinzipiell beliebig flexibel konfigurierbare Zugriffe, die auf sicheren Selektionsalgorithmen basieren.

TCmanager® Trainingsportale werden über eine zentrale Webportalverwaltung administriert, damit automatisiert die richtigen Kataloge, Preise, und AGBs individuell passend für die richtigen Zielgruppen ausgespielt werden. Inhalte von WBTs und Tests werden mit spezifischen Zugängen in die Repositories hochgeladen. Damit sind sie nicht über eine öffentliche URL ansteuerbar, sondern nur nach einer Buchung über das TCmanager® Trainingsportal - und damit nur im Lesezugriff - zugänglich. Die Legitimierung des Zugriffs wird durch SCORM-Tracking unterstützt, welches den Lernfortschritt immer einer konkreten Buchung zuordnet. So wird sichere Personalentwicklung effizient.

Eindrucksvolle Referenzen

Die Liste der Unternehmen, die TCmanager® LMS für Personalentwicklung, Akademiemanagement und Seminarverwaltung einsetzen, ist eindrucksvoll. Nicht nur große DAX-Unternehmen, Versicherungen und Banken, sondern auch erfolgreiche Mittelständler nutzen seit Jahren das breite Funktionsportfolio für Ihren Trainingsbereich. Auf www.softdecc.com findet sich nicht nur eine eindrucksvolle Liste der Referenzunternehmen, sondern auch persönliche Statements begeisterter Kunden.

Testinstallation

SoftDeCC bietet interessierten Unternehmen die Möglichkeit TCmanager® im eigenen Hause ausgiebig zu prüfen. Eine derartige Testinstallation wird gemäß den Anforderungen des Kunden konfiguriert. Das Pilotteam testet in einem vereinbarten Zeitraum nach einer sorgfältigen Schulung TCmanager® mit eigenen Daten. Bei Kauf der Software ist dieser Service kostenfrei.

Für mehr Information, Präsentationstermin und Beratung steht Ihnen Frau Susanne Ziegler unter der Telefonnummer: 089 / 890 678 30 oder info@softdecc.com zur Verfügung.

Beispiele für komplexere Anwendungen kann der Zugriff auf Lerninhalte verteilter elearning-Repositories sein, müssen hier doch auch die Urheber-/ Nutzungsrechte geschützt, manipulatorische Zugriffe ausgeschlossen und die Nutzung gegebenenfalls verrechnet werden.

Der Kreis der Stakeholder reicht jedoch inzwischen oft über das eigene Unternehmen heraus. Nicht nur Trainer, sondern auch externe Techniker, Servicekräfte, Handelspartner und Branchenverbände können gegebenenfalls über Trainingsportale und Lernplattform das LMS nutzen. Dies bedeutet aber nicht nur höhere Sicherheitsmaßnahmen in Bezug auf den Datentransfer und die Vielfalt der (mobilen) Endgeräte mit denen die IT-Abteilung zurechtkommen muss. Es bedeutet auch weitere Personendaten, die geschützt werden müssen.

Je komplexer und vernetzter die IT-Landschaft also ist, desto höher sind die Anforderungen an IT-Sicherheit und Datenschutz zu bewerten. Wie bei einem dreidimensionalen Gegenstand erweitert sich die Angriffsfläche bei steigendem Volumen. Da man die Sicherheitsthematik mit dem richtigen Konzept jedoch gut in Griff bekommen kann, übersteigt der Mehrwert professioneller Learning Management Systeme die potentielle Gefahr um ein Vielfaches.

Mitarbeiter als Leistungsträger - und Sicherheitsproblem

Erschreckend ist, dass in Studien als größtes Sicherheitsrisiko im Unternehmen ausgerechnet der Mitarbeiter genannt wird. Im Rahmen der InfoSecurity Europe 2014 wurde von App River, einem Anbieter für Web-Security-Lösungen, eine entsprechende Befragung durchgeführt. „70% der Befragten sehen den Faktor Mensch also schwächste Glied im Hinblick auf Sicherheitsrisiken im Unternehme. Weitere 44% machten Unkenntnis der Mitarbeiter als Schadensverursacher verantwortlich“ (www.it-sicherheit.de, 2014).

Neben deren Aufklärung über datenschutzrechtliche Belange ist also auch die Schulung der Mitarbeiter von großer Bedeutung. Auf dem Bildungsmarkt gibt es daher neben WBTs für Fachabteilungen auch vielerlei standardisierte und individualisierbare WBTs zum Thema Datenschutz, Passwort- und IT-Sicherheit. Es ist wichtig darauf zu achten, dass diese Einheiten SCORM-fähig sind, damit die Schulung auch in Einzelschritten nachvollziehbar erfolgt. Ein sicheres LMS kann natürlich nachweissicher schulen: Daher werden Schulungen mit WBTs und Tests wie Präsenztrainings gebucht und Einzelschritte mit Tages- und Zeitangaben in einer Historie mitgeschrieben, so dass der erreichte Status jederzeit nachvollzogen werden kann.

Viele Schulungen müssen je nach Aufgabenbereich zyklisch aktualisiert werden. Ein modernes LMS sollte deshalb die Gültigkeitsfristen überwachen und rechtzeitig signalisieren, wenn eine Neuzertifizierung ansteht. Sollte die notwendige Schulung nicht erfolgen, so kann in der Konsequenz der betroffene Mitarbeiter seine Tätigkeit nicht qualifiziert ausführen; bei manchen Tätigkeitsfeldern dürfen Mitarbeiter ohne nachgewiesene Erneuerung bestimmter Qualifikationen nicht eingesetzt werden und fallen dann als Leistungsträger zeitweilig aus. Diese Information wird in einer integrierten Systemlandschaft mit der Personaleinsatzplanung (PEP) abgestimmt, während Vorgesetzter und Personalabteilung gegebenenfalls informiert werden.

Der Gesetzgeber schreibt Unternehmen in §4 des BDSG die Benennung eines Datenschutzbeauftragten zwingend vor, wenn mehr als neun Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind oder Zugriff darauf haben. Dies ist im Trainings- und Schulungsbereich, aber auch im Vertrieb schnell gegeben. Die Person des Datenschutzbeauftragten darf aber nicht als lästiger Aufpasser eingeführt werden, sondern soll für Mitarbeiter und Management gleichermaßen als Ansprechpartner und Unterstützer bei Fragen und Problemen zur Verfügung stehen. Dazu muss die Person entsprechend geschult worden sein, die Bedeutung des Themas kommunizieren und die Einhaltung von Maßnahmen auf unterschiedlichen Hierarchieebenen durchsetzen können.

LMS-Hersteller im Fokus

Neben der internen IT ist auch der LMS-Hersteller über den ganzen Produktlebenszyklus gefragt. Professionelle LMS-Hersteller führen auch bei Patches und Sicherheits-Updates der Software ganzheitliche Testszenarien durch. Ganzheitlich bedeutet in diesem Fall, dass der Hersteller nicht nur einzelne Module programmiert und implementiert, sondern das nahtlose Zusammenspiel aller Elemente prüft. Schließlich haftet der Hersteller für sein Produkt und entwickelt

es im eigenen Interesse entlang der geltenden Sicherheitsstandards. Dabei helfen Anwenderberichte und Best Practice-Cases sowie optimalerweise auch der persönliche Austausch mit den angegebenen Referenzkunden.

Fazit

Ein LMS ist eine unternehmenskritische Einrichtung, die professionell geschützt werden muss. Anders als beim Schutz einfacher persönlicher Daten wie Adressen oder beruflichen Stationen werden in einem LMS oft komplette Bildungslebensläufe verwaltet. Ein effizientes LMS ist also keine Insellösung. Für einen maximal effizienten Einsatz muss es beispielsweise zur Vermeidung doppelter Datenhaltungen hochintegriert betrieben werden. Das LMS ist ein noch zu oft unterschätzter Stellhebel zur Erfolgssicherung des Unternehmens, was in der Konkurrenzsituation während der allgemein steigenden Digitalisierung (Industrie 4.0) auch eine Existenzfrage bedeuten kann.

Manchmal gibt es im Trainingsbereich Entwicklungen, die konzeptuell oder didaktisch als wertvoll gesehen werden, aber im Sicherheitsbereich Konsequenzen nach sich ziehen. Dafür müssen gemeinsame Konzepte erarbeitet werden, die dann im LMS flexibel umgesetzt werden müssen. Daten müssen von ihrer Erhebung, bei ihrer Übertragung und Verarbeitung bis zur Archivierung geschützt werden. Dabei müssen verschiedenste Aspekte beachtet werden: Serverstandort, Verschlüsselungs-, Zugangs- und Freigabelimitierungen und eine anpassungsfähige Software, die flexibel an Länder- oder betriebsratsspezifische Datenschutz-Vorgaben angepasst werden kann. Informationssicherheit ist planbar und mit den entsprechenden Tools auch umsetzbar.

Generell ist der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten. Der notwendige Bereich Bildungscontrolling ist hiervon natürlich betroffen. Lösung ist in höheren Abstrahierungsebenen und Anonymisierung personenbezogener Daten zu suchen.

Bei der Entscheidung für ein LMS muss nicht nur das Produkt mit seiner Integrationsfähigkeit, der Vielseitigkeit und Flexibilität seiner Funktionen, Zugänge und Schutzvorkehrungen bewertet werden. Ein nicht zu unterschätzender Faktor ist auch der Hersteller und dessen Softwaretest-, Entwicklungs- und Sicherheitsstandards sowie seine Erfahrung mit der Erfüllung von IT-Sicherheits-Standards.

Dies ist für Außenstehende oft nicht leicht zu beurteilen. Ein Indikator ist ein detailliertes Rollen- und Rechtekonzept, welches nicht bei vertikalen oder horizontalen Zugriffslimitierungen stehen bleibt, sondern aufgabenorientiert - etwa für besondere Schulungskampagnen - anpassbar ist. Gute und verlässliche Indikatoren sind beispielsweise auch Referenzkunden, die ihrerseits auf höchste Sicherheitsanforderungen Wert legen, wie zum Beispiel Banken, Medizintechnik oder führende DAX-Unternehmen.

Quellennachweis

ak. (8/9 2015): Mittelständler müssen ihre Geschäftssoftware modernisieren. (www.godesys.de/, Hrsg.) digitalbusiness Cloud & IoT , S. 12.

Dreyer, A. (2015): Bildungs- und Talentmanagement 2015. München: Deutscher Bildungspreis.

OWASP Foundation (1.2.2016): www.owasp.org. Abgerufen am 11. 03 2016 von https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

www.it-sicherheit.de (22.7.2014): Abgerufen am 04. 03 2016 von https://www.it-sicherheit.de/startseite/news/mitarbeiter-als-groesstes-sicherheitsrisiko-fuer-u/

KONTAKT

SoftDeCC Software GmbH

Ansprechpartner:
Susanne Ziegler
Vertrieb / Kundenbetreuung

Kapuzinerstr. 9 C
D-80337 München
Tel.: +49 (0) 89 / 89 06 78 30
Fax: +49 (0) 89 / 89 06 78 33

s.ziegler@softdecc.com
www.softdecc.com