Checkliste

Datenschutz und Informationssicherheit

Die vorliegende Checkliste fasst die wichtigsten Informationen rund um Datenschutz und Informationssicherheit zusammen. Sie dient als Anregung und Orientierung für Ihre eigenen Überlegungen. Die Checkliste soll Ihnen helfen, Softwarelösungen für E-Learning, Personalentwicklung und Weiterbildung unter Berücksichtigung des Datenschutzes und der Informationssicherheit erfolgreich einzuführen.

Datenschutz und **Informationssicherheit** sind bei IT-Projekten wie dem Outsourcing von IT-Leistungen, Lösungen für E-HRM (Electronic Human Resources Management) oder der Einbindung mobiler Endgeräte in Personalentwicklung und Weiterbildung unerlässlich. Das Bundesdatenschutzgesetz, interne IT-Sicherheitsvorgaben, die Anforderungen von Datenschutzbeauftragten und Betriebsrat stecken den Rahmen ab, innerhalb dessen sich Konzeption, Implementierung und Betrieb bewegen.

1. Konzepte und Begriffe

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Rahmen seines Konzeptes zum IT-Grundschutz **drei Grundwerte der Informationssicherheit** beschrieben:

Vertraulichkeit	Schutz der Informationen vor unbefugter Preisgabe
Verfügbarkeit	Alle Dienstleistungen und Informationen können zum geforderten Zeitpunkt genutzt werden.
Integrität	Daten bzw. Informationen bleiben vollständig und unverändert.

Weitere häufig benutzte Begriffe im Kontext von Datenschutz und Informationssicherheit sind:

Datenschutz	Der Schutz personenbezogener Daten vor dem Missbrauch durch Dritte, geregelt durch das Bundesdatenschutzgesetz (BDSG)
Informationssicherheit (auch: Datensicherheit)	Der Schutz von Daten im Hinblick auf die Anforderungen, die sich aus den Grundwerten Vertraulichkeit, Verfügbarkeit und Integrität ergeben.
Datensicherung (engl. Backup)	Das Erstellen von Sicherungskopien vorhandener Daten zum Schutz vor Datenverlust
Authentisierung	Die Prüfung und Verifizierung der Identität eines Nutzers bei der Anmeldung an einem System. Das gilt auch in Bezug auf die Identitätsprüfung von IT-Komponenten oder Anwendungen.

Der Schutzbedarf wird vom BSI in die drei Kategorien normal, hoch, sehr hoch eingeteilt:		
Schutzbedarf	Die Schadensauswirkungen sind begrenzt und überschaubar	*normal*
	... sind beträchtlich	*hoch*
	... sind katastrophal, existenziell bedrohlich	*sehr hoch*

Beispiel: Schutzbedarf in einem Lernmanagementsystem

*In Bezug auf die **Vertraulichkeit** ist der Schutzbedarf hoch. Personaldaten sind besonders schutzbedürftige personenbezogene Daten, deren Bekanntwerden die Betroffenen erheblich beeinträchtigen kann. Bezüglich der **Integrität der Daten** besteht ein normaler Schutzbedarf, da Fehler rasch erkannt werden und die Daten nachträglich korrigiert werden können. Auch die **Verfügbarkeit** ist lediglich in normalem Umfang zu schützen, denn Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.*

2. Datenschutz

Beim Datenschutz unterscheidet das BDSG zwischen **technischen** und **organisatorischen Maßnahmen:**

Technische Maßnahmen	▪ betreffen die Gebäude, Räume o.Ä. ▪ werden direkt in der Soft- und Hardware umgesetzt
Organisatorische Maßnahmen	▪ sind Handlungsanweisungen ▪ sind Verfahrens- und Vorgehensweisen

Im Rahmen des Datenschutzes sind durch technische und organisatorische Maßnahmen sicherzustellen: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot. Was das konkret für die Umsetzung bedeutet, zeigen wir beispielhaft an den folgenden vier Aspekten:

Zugangskontrolle	▪ Ist gewährleistet, dass Unbefugte keinen Zugang zu den Datenverarbeitungsanlagen haben?
Weitergabekontrolle	▪ Ist die sichere Weitergabe von Daten geregelt? ▪ Ist die sichere Verschlüsselung der Daten gewährleistet?
Eingabekontrolle	▪ Werden Eingabeänderungen bei der Datenverarbeitung protokolliert?
Auftragskontrolle	▪ Werden Auftragsänderungen bei der Datenverarbeitung protokolliert? ▪ Ist eine Vereinbarung zur Auftragsdatenverarbeitung durch externe Provider (SaaS) erforderlich? ▪ Sind alle internen Funktionen (Fachabteilung, Rechtsabteilung, Datenschutzbeauftragte/r) frühzeitig eingebunden, um eine termingerechte Vereinbarung zur Auftragsdatenverarbeitung sicherzustellen?

3. Informationssicherheit

Zum Schutz der Daten und ihrer Integrität sind folgende Punkte zu beachten:

Management	▪ Werden alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt? ▪ Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung regelt?
Sicherheit von IT-Systemen	▪ Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt? ▪ Sind allen Systembenutzern Rollen und Profile zugeordnet worden? ▪ Ist klar geregelt, welche Mitarbeiter auf welche Daten zugreifen dürfen?
Vernetzung und Internetanbindung	▪ Ist festgelegt, wie mit potenziell gefährlichen Zusatzprogrammen (Plug-Ins, z.B. bei Web Based Trainings) und aktiven Inhalten umgegangen wird? ▪ Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?
Beachtung von Sicherheitserfordernissen	▪ Werden vertrauliche Informationen sorgfältig aufbewahrt? ▪ Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?
Passwörter und Verschlüsselung	▪ Sind alle relevanten Sicherheitsmechanismen aktiviert? ▪ Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult? ▪ Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks, Tablet-PCs oder Smartphones ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt? (Stichwort: Mobile Learning)

Beispiel: Softwarelösungen im HR-Bereich

Typische Softwarelösungen im HR-Bereich *wie z.B. ein Lernmanagementsystem oder eine Seminarverwaltungssoftware sind heute oft Webanwendungen, d.h. browserbasiert. Webanwendungen werden sowohl in öffentlichen IT-Netzen (z.B. dem Internet) als auch in Firmennetzen (Intranet) zur Bereitstellung von Daten und Anwendungen eingesetzt. Dabei müssen Webanwendungen Sicherheitsmechanismen umsetzen, die den Schutz der Daten gewährleisten und Missbrauch verhindern.*

4. Informationssicherheit in der HR-Praxis

Die folgende Checkliste für Softwarelösungen, die im HR-Bereich zum Einsatz kommen, basiert auf dem **Konzept des IT-Grundschutzes**, den das BSI entwickelt hat.

Planung	▪ Existiert ein Anforderungskatalog für Standardsoftware? ▪ Sind Verantwortlichkeiten und Regelungen, z.B. von Zugriffsrechten und Passwortgebrauch, festgelegt?
Umsetzung	▪ Wie erfolgt die Authentisierung? ▪ Kann eine sichere Konfiguration gewährleistet werden? ▪ Wie erfolgt der Schutz vertraulicher Daten? ▪ Verläuft das Einbinden von Daten und Inhalten kontrolliert?
Betrieb	▪ Wie ist die Vergabe von Zugriffsrechten geregelt? ▪ Erfolgt eine Dokumentation der zugelassenen Benutzer und Rechteprofile? ▪ Ist eine Schulung zu Sicherheitsmaßnahmen geplant? ▪ Werden sicherheitsrelevante Ereignisse protokolliert?

Um eine **Softwarelösung für E-Learning, Personalentwicklung und Weiterbildung** erfolgreich einzuführen, sollten **Sicherheitsfragen** vor dem eigentlichen Projektstart gemeinsam mit den im Unternehmen verantwortlichen Ansprechpartnern sowie Auftragnehmern und Dienstleistern geklärt werden. Durch frühzeitige **Sicherheitsprüfung** wird das Risiko einer zeitlichen Verzögerung im Projektverlauf und bei der Inbetriebnahme minimiert. Dies gilt insbesondere dann, wenn das künftige System bei einem externen Anbieter und Provider (Software-as-a-Service / SaaS) betrieben werden soll.

Quellen und weiterführende Literatur finden Sie unter:

- *Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, S. 49 ff., www.bsi.bund.de/gshb*
- *Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Informationssicherheit. IT-Grundschutz kompakt, www.bsi.bund.de/grundschutz*
- *DatenschutzWIKI herausgegeben von der Bundesbeauftragen für den Datenschutz http://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Ma%C3%9Fnahmen*
- *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05021.html*
- *Bundesdatenschutzgesetz (BDSG), www.gesetze-im-internet.de/bdsg_1990*

Weitere Informationen / Beratung

time4you GmbH communication & learning, Karlsruhe
Fon +49 (0)721 83 01 60, info@time4you.de, www.time4you.de

time4you GmbH, gegründet 1999, ist führender Anbieter von Software und Lösungen für E-Learning, Personalentwicklung und Weiterbildung. Das innovative Karlsruher Unternehmen realisiert als Dienstleister und Software-Hersteller für nationale wie internationale Kunden maßgeschneiderte High-End-Lösungen.