Checkliste für die Werkzeugauswahl

So einfach geht sichere Zusammenarbeit

Die Evaluation und Einführung einer Collaboration-Lösung ist keine grosse Sache. Der Nutzen für das Unternehmen hingegen schon. **Von Gabriel Gabriel**

Wenn Mitarbeiter, Abteilungen und Unternehmen heute sicher zusammenarbeiten wollen, müssen vertrauliche Informationen geschützt und sicher verteilt werden. In der Praxis aber werden geschäftskritische Dokumente der Bequemlichkeit halber oft in Desktop-Anwendungen bearbeitet, gespeichert, verwaltet, vor allem aber auch sorglos verteilt. Hierzu zählen etwa Ausschreibungen, Kalkulationen für das Preismanagement, Konstruktionspläne, Kunden- und Finanzdaten oder sogar Vertragsunterlagen. Diese befinden sich auf lokalen Festplatten oder Servern, oft unverschlüsselt und frei zugänglich. Gängige Schutzmechanismen konzentrieren sich bestenfalls auf eingeschränkte Zugriffsrechte, persönliche Verzeichnisse und die Verschlüsselung von Datenträgern.

Erhöhte Gefahr droht bei ungeschützten E-Mails, populären Filesharing-Diensten und dem Einsatz mobiler Endgeräte. Dabei ist die sichere Zusammenarbeit und Verteilung von Dokumenten keine Hexerei, sondern mit einfachen organisatorischen und technischen Massnahmen zu bewerkstelligen: Die teilweise unterschiedliche Bedeutung der Dokumente für einen Schadensfall beantwortet mit einer groben Klassifizierung die Frage, welche Dokumente tatsächlich geschützt werden müssen.

Kein grosses Projekt nötig

Die Definition der einzelnen Klassifizierungsstufen sollte in eine unternehmensweit gültige Richtlinie für Informationssicherheit münden. Zu den organisatorischen Massnahmen zählt, Mitarbeiter zu sensibilisieren. Oft halten Unternehmen sie dazu an, Informationen manuell zu klassifizieren, um die nötige Sensibilität für vertrauliche Informationen zu erreichen – etwa per Dateimerkmalen oder Kopf- und Fusszeilen innerhalb des Dokuments. Für die Klassifizierung ist also kein umfangreiches Projekt nötig.

Vielmehr geht es darum, ein Verständnis dafür zu schaffen, Informationen entsprechend ihres Schutzniveaus zu behandeln. Hierfür müssen Voraussetzungen für eine möglichst einfache Kategorisierung greifen: Geschulte Mitarbeitende sollten Kategorisierungen wie «vertraulich» oder «streng vertraulich» für Dokumente ohne grosses Nachdenken mit minimalem Aufwand verteilen können. Für die Zuweisung von Rechten und Regeln sowie die Behandlung der Informationen ist der Business-Bereich verantwortlich. IT- und Compliance-Verantwortliche schaffen dafür den notwendigen Rahmen. Zu den technischen Massnahmen gehören neben der Verschlüsselung dedizierte Lösungen für die sichere Aufbewahrung und Zusammenarbeit. Bewährt haben sich hochsichere Dokumentenmanagement- und Collboration-Lösungen.

Was geschützt werden sollte

Vertrauliche Dokumente verbleiben dabei stets innerhalb einer geschützten, digitalen Arbeitsumgebung, können aber trotzdem sicher über Unternehmens- oder Abteilungsgrenzen hinweg verteilt werden. Idealerweise lässt sich eine Lösung an Geschäftsprozesse anpassen. Gleichzeitig muss die Plattform einfach zu bedienen sein, um Akzeptanz bei den Anwendern zu erreichen. Ihre vollen Stärken spielt eine solche Lösung beispielsweise in der Verwaltungsrats- und Geschäftsleitungskommunikation aus. Hier sind die Anforderungen

Wichtige Funktionsanforderungen

Worauf Unternehmen vor der Einführung von Collaboration-Tools achten sollten:

- Produktive und sichere Zusammenarbeit über Unternehmensgrenzen hinweg
- Sicherer, webbasierter Zugriff mit Passwort und SMS-TAN
- 256-Bit-Verschlüsselung auf Server und beim Versand sowie in allen Apps
- Ausgefeiltes Berechtigungskonzept
- Abschirmung von Betreiber und IT-Abteilung (Administrator- und Provider-Shielding)
- Versionierung
- Revisionssichere Protokollfunktion (Audit Trail)
- Integration von Information Rights Management Services
- Intuitive Benutzeroberfläche
- Sicheres Arbeiten mit zertifizierten mobilen Apps
- Betrieb auf dedizierten Servern in zertifizierten, sicheren Rechenzentren

und der Umfang in der Informationsbeschaffung und Kommunikation in den letzten Jahren kontinuierlich gestiegen. Ein verändertes Arbeitsumfeld mit schnellen Informationszyklen und gestiegene Haftungsrisiken zwingen Mitglieder von Kontrollgremien dazu, die Effektivität und Effizienz ihrer Überwachungsarbeit belegen zu können. Gleichzeitig müssen Entscheidungen schneller getroffen, vertrauliche Daten sicher ausgetauscht und Abstimmungen vertraulich durchgeführt werden. So erlaubt es eine Lösung für den sicheren Austausch von Informationen konkret, Dokumente wesentlich rascher anzufordern und schneller fundierte Entscheidungen zu treffen. Ebenso gilt es, die volle Einhaltung der Vertraulichkeit, Integrität und Authentizität von Informationen im Rahmen von Governance-Richtlinien zu gewährleisten.

Doch auch bei Unternehmensübernahmen, beim Know-how-Schutz, im Ein- und Verkauf, der Produktion, der Lieferanten- und Kundenkommunikation, mit Behörden oder im Rahmen interner Revisionen gilt es, höhere Sicherheitsanforderungen zu erfüllen. Unabhängig von Industriesegment und Unternehmensgrösse, Positionen und Zuständigkeiten steht fest: Um die Wettbewerbsfähigkeit zu erhalten, müssen sensible Geschäftsinformationen schnell, sicher und transparent mit internen oder externen Personen ausgetauscht werden können. Stets muss dabei eine Lösung verwendet werden, die vertrauliche Dokumente bei der Weiterleitung und Speicherung garantiert vor unerlaubtem Zugriff schützt. Darüber hinaus sollte die Plattform über Funktionen verfügen, mit denen sich individuelle Zugriffsrechte für Einzelpersonen oder Teams definieren lassen und die minutiös dokumentieren, wer wann auf welches Dokument zugegriffen hat. Hinzu kommen Anforderungen an individuelle Benutzerrechte, Unterstützung mobiler Endgeräte sowie eine möglichst anwenderfreundliche Benutzeroberfläche.

«Mitarbeitende sollten Kategorisierungen wie ‹vertraulich› oder ‹streng vertraulich› für Dokumente ohne grosses Nachdenken mit minimalem Aufwand verteilen können»

Gabriel Gabriel
Managing Director von Brainloop Schweiz

Worauf es ankommt

Zu den wesentlichen Sicherheitsmerkmalen zählt das Information Rights Management: Spezielle Sicherheitsrichtlinien für Dokumente, etwa beim Verändern, Drucken oder Weiterleiten an andere Nutzer, lassen sich zentral auf dem Server definieren. Erlischt eine Berechtigung für ein Dokument, weil sie vom Teilenden widerrufen wird, darf der Empfänger nicht mehr darauf zugreifen können. Das gilt auch, wenn eine Berechtigung zeitlich befristet ist. Ebenso zählen Sicherheits-Features wie digitale Wasserzeichen oder die Verwendung von Dokumenten-IDs zum Funktionsumfang. Ein weiterer zentraler Bestandteil einer Collaboration-Lösung ist die durchgängige Verschlüsselung. Daten sollten nicht erst im Rechenzentrum des Anbieters, sondern beim Speichern in der Cloud-basierten Umgebung, beim Transfer und auf mobilen Endgeräten verschlüsselt sein. Unumgänglich für den mobilen Einsatz ist eine Remote-Wipe-Funktion: Geht ein Gerät verloren, lassen sich die Informationen darauf per Fernzugriff löschen. Doch auch das automatische Löschen von Inhalten ohne Online-Anbindung lässt sich realisieren, wenn ein Passwort dreimal falsch eingegeben wurde. Unumgänglich ist eine Zugriffskontrolle, beispielsweise über Zwei-Faktor-Authentifizierung. Hinzu kommt, dass Berechtigungen für eine Datei in unterschiedlichen Stufen vorliegen müssen. Dazu gehören unter anderen das Lesen und Editieren. Eine Lösung muss ferner einen lückenlosen Nachweis darüber liefern, welcher Nutzer was mit den Daten getan und an wen wann ein Anwender welche Dateien mit welchen Berechtigungen verschickt hat. Auch für Administratoren sollten Sicherheitsvorkehrungen wie «Administrator-Shielding» gegeben sein. Damit lässt sich technisch festlegen, dass ein Administrator keinen Zugriff auf die Daten hat.

Weiter muss ein Zugriff vom Rechenzentrumsbetreiber und Lösungsanbieter auf die Daten des Unternehmens jederzeit ausgeschlossen sein. Essenziell ist es zudem, dass der Betrieb sowie das Rechenzentrum des Anbieters nach ISO 27001 zertifiziert ist. Weitere Bedeutung bei der Wahl einer Lösung kommt der Integrationsfähigkeit, den vorhandenen Collaboration-Features und der Benutzerfreundlichkeit zu. Ausserdem sollte die Lösung plattformunabhängig, also unabhängig von Geräten sein, auf denen sie eingesetzt wird. ■

Gabriel Gabriel
ist Managing Director von Brainloop Schweiz:
www.brainloop.ch