Sichere Zusammenarbeit ist keine Hexerei. Die Evaluation und Einführung einer Collaboration-Lösung ist keine grosse Sache. Der Nutzen für das Unternehmen hingegen schon.

VON GABRIEL GABRIEL*

Dass Mitarbeiter, Abteilungen und Unternehmen heute sicher zusammenarbeiten, ist branchenübergreifend zum Zünglein an der Waage für den Unternehmenserfolg geworden. Vertrauliche Informationen müssen geschützt und sicher verteilt werden können – in der Verwaltungsratskommunikation ebenso wie bei Mergers & Acquisitions oder Due-Diligence-Prüfungen. In der Praxis aber werden selbst geschäftskritische Dokumente wie Ausschreibungen, Kalkulationen für das Preismanagement, Konstruktionspläne, Kunden- und Finanzdaten oder sogar Vertragsunterlagen der Bequemlichkeit halber oft in gängigen Desktop-Anwendungen bearbeitet, gespeichert, verwaltet, vor allem aber auch sorglos verteilt. Sie 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 unter anderem 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 relativ einfachen organisatorischen und technischen Massnahmen zu bewerkstelligen: Die teilweise unterschiedliche Bedeutung der Dokumente für einen Schadenfall beantwortet mit einer groben Klassifizierung eine grundlegenden Frage: Welche Dokumente müssen tatsächlich geschützt werden?

Kein grosses Projekt nötig. Die Definition der einzelnen Klassifizierungsstufen sollte in eine unternehmensweit gültige Informationssicherheitsrichtlinie münden. Zu den organisatorischen Massnahmen gehört, Mitarbeiter zu sensibilisieren. Oft halten Unternehmen die Mitarbeitenden dazu an, Informationen manuell zu klassifizieren, um die nötige Sensibilität für vertrauliche Informationen zu erreichen – etwa per Dateimerkmalen oder Kopf- oder Fusszeilen innerhalb des Dokuments. Es ist also für die Klassifizierung kein umfangreiches Projekt nötig. Vielmehr geht es in diesem Zusammenhang darum, ein grundsätzliches Verständnis im Unternehmen dafür zu schaffen, dass Informationen entsprechend ihres Schutzniveaus behandelt werden müssen. Dennoch müssen Voraussetzungen greifen, um eine Kategorisierung möglichst einfach zu ermöglichen: Geschulte Mitarbeitende sollten in der Lage sein, Kategorisierungen wie «vertraulich» oder «streng vertraulich» für Dokumente ohne grosses Nachdenken mit minimalem Aufwand zu verteilen. Für die Zuweisung der entsprechenden Rechte und Regeln sowie die Behandlung der Informationen ist der Business-Bereich verantwortlich. IT- und Compliance-Verantwortliche schaffen dafür den notwendigen Rahmen.

Technische Massnahmen. Zu den technischen Massnahmen gehören neben einer Verschlüsselung dedizierte Lösungen für die sichere Aufbewahrung und Zusammenarbeit. Bewährt haben sich hochsichere Dokumentenmanagement- und Collboration-Lösungen. Das grundsätzliche Prinzip: Vertrauliche Dokumente verbleiben stets innerhalb einer geschützten, digitalen Arbeitsumgebung, können jedoch trotzdem sicher über Unternehmens- oder Abteilungsgrenzen hinweg verteilt werden. Idealerweise lässt sich eine Lösung an individuelle Geschäftsprozesse anpassen. Gleichzeitig muss die Plattform einfach zu bedienen sein, um eine Akzeptanz bei Anwendern zu erreichen und eine fehlerhafte Handhabung zu vermeiden.

Typische Prozesse und Bereiche mit Schutzbedarf. Ihre vollen Stärken spielt eine Lösung in der Verwaltungsrats- und Geschäftsleitungskommunikation aus. Hier sind die Anforderungen und der Umfang in der Informationsbeschaffung und Kommunikation in den letzten Jahren kontinuierlich gestiegen. Ein verändertes Arbeitsumfeld mit schnellen Informationszyklen, vor allem aber gestiegene Haftungsrisiken, zwin-

Bild: YB – Fotolia.com

Vertrauliche Informationen müssen geschützt und sicher verteilt werden können.

GABRIEL GABRIEL
ist Managing Director von Brainloop Schweiz,
www.brainloop.ch

gen Mitglieder von Kontrollgremien dazu, die Effektivität und Effizienz ihre Überwachungsarbeit belegen zu können. Gleichzeitig müssen Entscheidungen schneller getroffen und vertrauliche Daten sicher ausgetauscht und Abstimmungen vertraulich durchgeführt werden. So erlaubt es eine Lösung für den sicheren Austausch von Informationen Verwaltungsräten 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 im Zusammenhang von Unternehmensübernahmen, beim Know-how-Schutz, im Ein- und Verkauf, in der Produktion, der Lieferanten- und Kundenkommunikation, mit Behörden oder im Rahmen interner Revisionen gilt es, höhere Sicherheitsanforderungen zu erfüllen.

Anforderungen an eine Collaboration-Plattform. Unabhängig von Industriesegment und Unternehmensgrösse, von Positionen und Zuständigkeiten steht fest: Um die Wettbewerbsfähigkeit zu erhalten, müssen sensible Geschäftsinformationen heute schnell, sicher und transparent mit internen oder externen Personen ausgetauscht werden können. Immer muss dabei eine Lösung im Mittelpunkt stehen, die vertrauliche Dokumente bei der Weiterleitung und Speicherung garantiert vor unerlaubtem Zugriff schützt. Darüber hinaus sollte die Plattform über umfassende Funktionen verfügen, mit der sich individuelle Zugriffsrechte für unterschiedliche Einzelpersonen oder Teams definieren lassen und die minutiös dokumentiert, wer wann auf welches Dokument zugegriffen hat. Hinzu kommen die Anforderung an individuelle Benutzerrechte, die Unterstützung mobiler Endgeräte sowie eine möglichst anwenderfreundliche Benutzeroberfläche. Die wesentlichen Merkmale im Einzelnen:

Sicherheit. Zu den wesentlichen Sicherheitsmerkmalen zählt das Information Rights Management: Spezielle Sicherheitsrichtlinien für Dokumente, etwa beim Verändern, beim Drucken oder beim 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 etwa auch, wenn eine Berechtigung hinfällig wird, weil sie zeitlich befristet war. 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. Dabei sollten Daten nicht erst im Rechenzentrum des Service-Anbieters verschlüsselt werden. Vielmehr müssen Informationen beim Speichern in der Cloud-basierten Umgebung, beim Transfer und auf mobilen Endgeräten verschlüsselt sein. Unumgänglich für den mobilen Einsatz ist zudem eine Remote-Wipe-Funktion: Geht ein Gerät verloren, lassen sich die Informationen darauf per Fernzugriff durch einen Administrator löschen. Doch auch das Löschen von Inhalten ohne Online-Anbindung lässt sich realisieren. So können Informationen automatisch gelöscht werden, wenn ein Passwort drei Mal falsch eingegeben wurde.

Nachvollziehbarkeit. Unumgänglich ist eine Zugriffskontrolle, beispielsweise über eine 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 können, welcher Nutzer was mit welchen Daten getan hat. Ebenso muss unveränderbar nachgewiesen werden können, an wen und wann ein Anwender welche Dateien mit welchen Berechtigungen verschickt hat. Aber auch für Administratoren sollten entsprechende Sicherheitsvorkehrungen getroffen werden. So muss in diesem Zusammenhang die Möglichkeit des «Administrator-Shielding» gegeben sein. Damit lässt sich technisch festlegen, dass selbst ein Administrator keinen Zugriff auf die Daten selbst hat. Weiter muss ein Zugriff vom Rechenzentrumsbetreiber und Lösungsanbieter auf die Daten des Unternehmens jederzeit ausgeschlossen sein. Essenziell ist es für Organisationen zudem, dass der Betrieb sowie das Rechenzentrum des Serviceanbieters nach ISO 27001 zertifiziert worden ist. Weitere Bedeutung bei der Wahl einer Lösung kommt der Integrationsfähigkeit, den vorhandenen Collaboration-Features, Benutzerfreundlichkeit zu. Ausserdem sollte die Lösung plattformunabhängig, also unabhängig von den Geräten sein, auf denen sie eingesetzt werden.

Fazit: Ausgefeiltes Berechtigungskonzept. Vertrauliche Informationen müssen geschützt und sicher verteilt werden können – in der Verwaltungsratskommunikation ebenso wie bei Mergers & Acquisitions oder Due-Diligence-Prüfungen. Eine sichere Lösung umfasst neben der Einbindung in interne Geschäftsprozesse eine revisionssichere Dokumentation sowie ein ausgefeiltes Berechtigungskonzept, das regelt, welche Person Zugriff auf welches Dokument erhält. Mit der Lösung lässt sich auch eine Klassifizierung von Informationen einfach umsetzen. Der Einsatz setzt eine Sensibilisierung von Unternehmensführung und Mitarbeiter voraus.

COLLABORATION-LÖSUNG

Funktionsanforderungen bei der Evaluation einer sicheren Zusammenarbeitslösung:

- 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