Social Enterprise: Cloud-Security im »Next Generation Workplace«

Social Collaboration unsicher?

Bild: © tan11/shutterstock.com

Das Management definiert die Strategie und selbstorganisierende Teams agieren in Eigenverantwortung entlang dieser Richtschnur. Dazu bedarf es einer neuen Organisationsstruktur im Sinne des Social Enterprise und der Hinwendung zur sozialen Zusammenarbeit. Dabei ist es besonders notwendig, unternehmensinterne Informationen zu schützen.

Durch soziale Netzwerke und sinkende Informationslaufzeiten, gepaart mit der wachsenden Mobilität der IT, ist es für Unternehmen mittelfristig überlebensnotwendig, neben der stetig wachsenden Produktivität eine hohe Reaktions- und Innovationsfähigkeit zu entwickeln. Hierfür bedarf es kreativer und vor allem engagierter Mitarbeiter. Zusätzlich steigt hinsichtlich der wechselnden Anforderungen und Rahmenbedingungen die Komplexität, sodass rein hierarchisch aufgebaute Unternehmen bereits aufgrund der über viele Stufen laufenden Kommunikationswege nicht mehr am Markt mithalten können.

Selbstorganisierende Teams, die in Eigenverantwortung einer vom Management definierten Strategie folgen und diese auch mit ihrer Erfahrung beeinflussen können, werden ein wesentlicher Baustein zum Erfolg sein. Dabei ist es besonders notwendig, unternehmensinterne Informationen zu schützen. Die im privaten Umfeld genutzten IT-Werkzeuge, welche nicht diesen hohen Sicherheitsanspruch haben, können im beruflichen Umfeld für die Kommunikation daher nur begrenzt eingesetzt werden.

Die fünf typischen Bedenken gegenüber Social Enterprise:

- Angst vor Einflussverlust: Ich möchte nichts teilen. Mein Wissen bedeutet Macht!
- Festhalten an Altbewährtem: Meine Führungskräfte denken, Social Enterprise sei Zeitverschwendung.
- Ignoranz digitaler Chancen: Kein IT-Werkzeug kann das alles, deswegen warten wir noch.
- Fehlendes digitales Konzept: Mit Social Enterprise ist Arbeitskontrolle möglich. Das geht nicht.
- Risiko-Aversion: Soziale Netzwerke aus der Cloud – sind dann vertrauliche Daten öffentlich?

Obwohl in vielen Unternehmen diese Vorurteile gegenüber neuen Kommunikationswerkzeugen bestehen, haben bereits einige Unternehmen damit begonnen, diese aufgrund der erkannten Notwendigkeit einzuführen und Erfahrungen mit der Beseitigung der genannten Barrieren gemacht. Laut einer Altimeter-Studie aus dem Jahr 2014 haben die befragten Unternehmen eine Steigerung der Kundenzufriedenheit und deutlich höhere Innovationskraft durch höheres Mitarbeiter-Engagement durch die Einführung von Social-Enterprise-Plattformen erreicht. Der Einfluss des Managements wurde dadurch sogar gesteigert und der Vorwurf der Zeitverschwendung widerlegt.

Die verschiedenen IT-Werkzeuge decken unterschiedliche Kommunikationsdimensionen und Anwendungsfälle ab. Durch Vorleben in der Nutzung können damit die digitalen Chancen auch heute schon zielgerichtet genutzt werden.

Die Einführung einer Social-Enterprise-Plattform benötigt ein »digitales Konzept«. Es sollte nie als Pilot erfolgen, da ein Pilot immer ein definiertes

Collaboration-Werkzeuge

Quelle: AppSphere AG

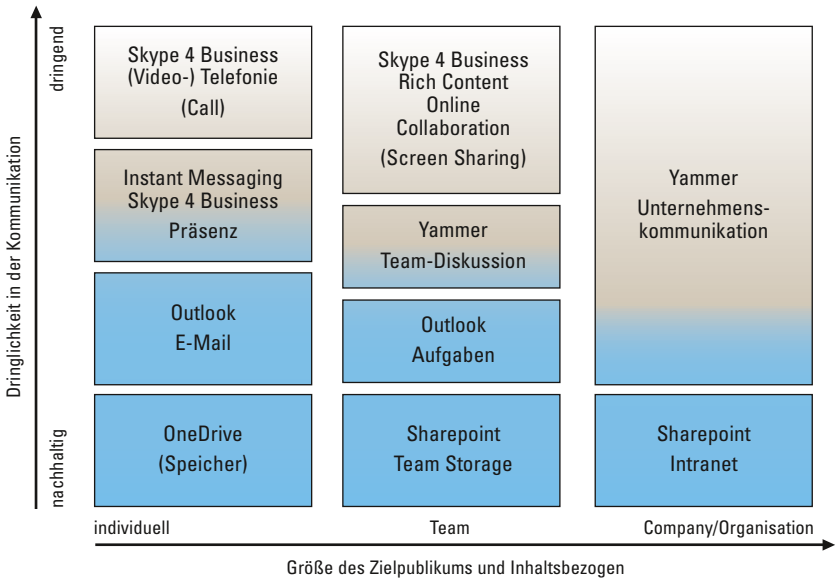

Abbildung 1: Einordnung der Collaboration-Werkzeuge mit Beispielen aus Microsoft Office 365.

Einführung einer Social-Enterprise-Plattform

Quelle: AppSphere AG

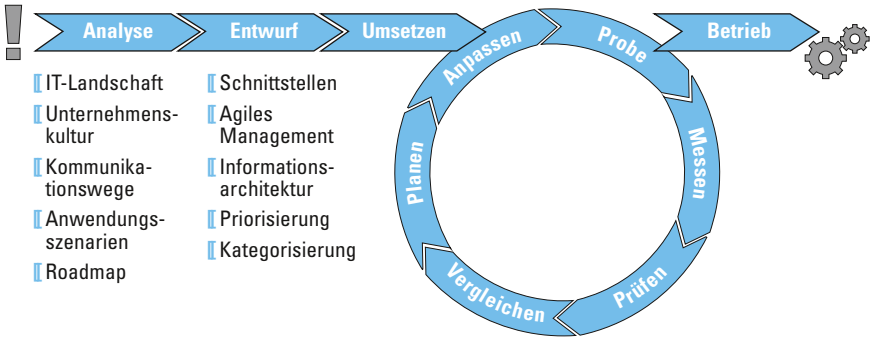

Abbildung 2: Phasenplan für die Einführung einer Social-Enterprise-Plattform nach SCM (School for Communication and Management)-Methode.

Rechtemanagement

Quelle: AppSphere AG

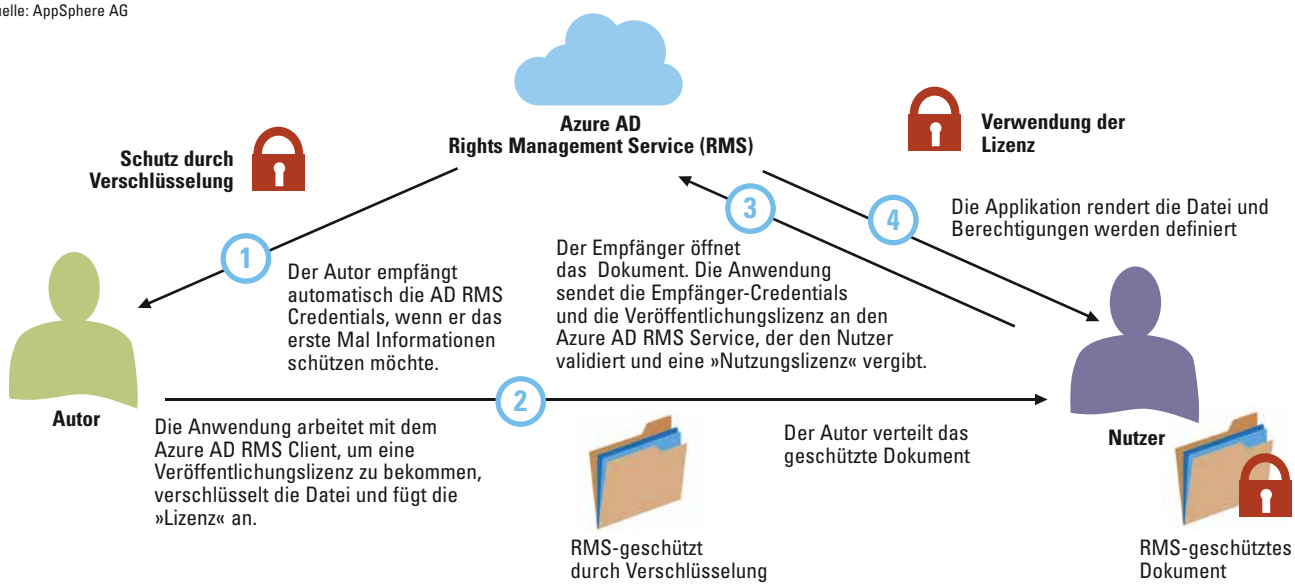

Abbildung 3: Dokumentenzentriertes Rechtemanagement für verteiltes Arbeiten am Beispiel von Microsoft.

Ende und damit auch eine potenzielle Abschaltung zur Folge haben kann. Ein Pilot bedeutet also immer eine Limitierung der Skalierung und des Umfangs der Möglichkeiten und damit auch eine Begrenzung des Business Cases einer Social-Enterprise-Plattform. Gerade diese Plattformen leben davon, dass sich alle im Unternehmen beteiligen und darauf verlassen können, dass die einmal eingegebenen Informationen von anderen und ihnen selbst wiedergefunden und genutzt werden können.

Es wird empfohlen, statt eines zeitlich begrenzten Piloten eine phasenorientierte Einführung mit Vision auf mobile Nutzung durchzuführen, damit die volle Produktivitätssteigerung entfaltet werden kann und zudem die Aussicht auf eine Weiterführung des Projekts hervorhebt. Erst durch übergreifende Kommunikation werden etablierte Wege verlassen und neue, unerwartete Ideen und Lösungen können entstehen.

Eine Arbeitskontrolle ist mit einer Social-Enterprise-Plattform nicht möglich. Die Status sagen nichts über die tatsächliche Anwesenheit oder Beschäftigung aus. Allerdings ist es ein Führungskulturthema, hier mehr Freiräume zu schaffen. Eine Unternehmenskultur kann nicht durch Regeln erfolgen. Es bedarf vielmehr an Führungskräften, welche die »Schnelligkeit durch Vertrauen« verstehen und sich von der Eigensicherung durch Säulendenken verabschieden.

Social Collaboration sicher möglich. Es greifen auch bei diesen Plattformen die bekannten Methoden aus der IT-Security: Authentifizierung, Autorisierung, Nichtabstreitbarkeit und Vertraulichkeit. Das bedeutet, dass die in den Unternehmen vorgegebenen Sicherheitsrichtlinien auch Social-Enterprise-Plattformen betreffen. Die Authentifizierung kann heute direkt mit einer Zwei-Faktor-Authentifizierung durch mobile Endgeräte erfolgen. Kombiniert mit der eindeutigen Identitätsfeststellung, führt ein entsprechendes Logging aller Aktivitäten auch zur Nichtabstreitbarkeit publizierter Informationen. Jegliche Publikation ist mit dem eigenen Namen verbunden. Zusätzlich ist es sinnvoll, neben einer Datenklassifizierung ein Rechte- und Filterungsmanagement im IT-Security-Konzept zu berücksichtigen, um die Anwender im »Next Generation Workplace«, der sich aus mobilen, integrierten Arbeits- und Kommunikationswerkzeugen zusammensetzt, vor versehentlichem Veröffentlichen geheimer Informationen zu schützen. Google hat diesen Schutz organisatorisch durch Umgangsregeln gelöst.

Eine Dokumentenklassifizierung sollte mindestens drei Klassen beinhalten: öffentlich, unternehmensintern, managementintern. Als öffentlich klassifizierte Informationen dürfen vom Mitarbeiter auch in öffentlichen Netzwerken verwendet und verbreitet werden. Unternehmensinterne Informationen dürfen nur innerhalb des Unternehmens verbreitet und managementinterne Informationen nur im Managementkreis verwendet werden. Durch das automatische Erzeugen der Dateieigenschaften beim Erstellen von Dokumenten und durch ein integriertes Rechtemanagement kann eine Klassifizierung auch schrittweise erfolgen, wenn alle nicht-klassifizierten Dokumente per Regel vom Publizieren ausgeschlossen sind.

Die meisten Social-Enterprise-Plattformen bieten ein solches Rechtemanagement. Es gibt bereits Anbieter, etwa Microsoft mit Office 365 RMS, die zusätzlich zu sozialen Netzwerken auch die Berechtigung auf Dokumente, das Sehen, Lesen, Weiterleiten, Ändern beziehungsweise Bear-

beiten und Löschen von Inhalten oder Dokumenten zeitlich, örtlich sowie personengebunden steuern. Dabei werden die Berechtigungen für den Zugriff dem verschlüsselten Inhalt im Dokument hinzugefügt und somit technisch der Abfluss von Informationen größtmöglich verhindert.

Zertifizierte Anbieter von Social-Enterprise-Plattformen halten strenge Normen ein. Die nutzenden Unternehmen können diese unabhängig erstellten Gutachten einfordern und verifizieren. Durch die Zertifizierungen ist eine technische Vertraulichkeit gewährleistet. Neben der Vertraulichkeit kann durch die schnelle Skalierbarkeit in der Cloud auch eine deutlich höhere Verfügbarkeit ohne ein Informationsabfluss gewährleistet werden.

Datenschutz im Social Enterprise gewährleistet. Es existieren in Deutschland neben dem oft zitierten Bundesdatenschutzgesetz auch unterschiedliche Landesdatenschutzgesetze, die Datenschutzgesetze der Kirchen, das Telemediengesetz (§§ 11 bis 15a TMG), den Sozialdatenschutz (§§ 67 bis 85a SGB X) sowie die gültige Europäische Datenschutzrichtlinie (95/46/EG). Diese Richtlinie beschreibt den Mindeststandard für den Datenschutz, der in allen EU-Mitgliedstaaten durch das nationale Gesetz

» **Zertifizierte Anbieter von Social-Enterprise-Plattformen** halten strenge Normen ein. «

sichergestellt sein muss. Zusätzlich gibt es in Deutschland noch den §203 Strafgesetzbuch (StGB), nach dem bestimmte Berufsgruppen bei Offenbarung von Geheimnissen mit bis zu zwei Jahren Freiheitsstrafe oder einer Geldstrafe belegt werden können.

Die voraussichtlich im Laufe dieses Jahres kommende EU-Datenschutz-Grundverordnung, welche die gültige EU-Datenschutzrichtlinie 95/46/EG ersetzen soll, wird ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedsstaaten gelten.

Für den berechtigten Umgang mit Daten wurden Instrumente entwickelt, etwa mittels Vertrag zur Auftragsdatenverarbeitung (§11 BDSG) oder Schweigepflichtentbindungserklärung (§03 StGB). Durch diese Instrumente ist es möglich, Daten innerhalb einer Social-Enterprise-Plattform in der Cloud zu verarbeiten.

Die Rechenzentren in der EU sind alle datenschutzrechtlich gleichgestellt. Aus Datenschutzsicht ist es demnach unerheblich, in welchem Mitgliedsland der EU sich das Rechenzentrum des Betreibers der Cloud-Lösung befindet. Als Nutzer einer Cloud-basierten Social-Enterprise-Plattform sind die Unternehmen verpflichtet, die technischen und organisatorischen Maßnahmen (TOM) zum Schutz personenbezogener Daten und deren Einhaltung beim Anbieter zu prüfen. Dieser Pflicht kann nachgekommen werden, indem regelmäßig ein Zertifikat nach ISO 27018 eines unabhängigen Gutachters vom Anbieter eingefordert wird.

Fazit. Mit Hilfe der genannten Sicherheitsmaßnahmen ist ein sicherer »Next Generation Workplace« schon heute möglich. Die große Anzahl möglicher Systeme bedingt eine für den Einsatzzweck spezifische Auswahl, bei der sich das beschriebene phasenorientierte Vorgehen bereits mehrfach im praktischen Einsatz bewährt hat.

Dr.-Ing. Jan Wörner

Dr.-Ing. Jan Wörner,
Solutions Architect,
AppSphere AG