CLOUD

Fürchten Sie sich weiter?

Cloud, neue Technologien per se, Mobilität sind eine fruchtbare Quelle für Misstrauen, Bedenken, unspezifische Widerstände und Blockaden jeder Art. Wen wundert es auch?

Dr. Tobias Höllwarth
Eurocloud Austria, Co-Autor
«Cloud Computing & Enterprise Mobility Management»

Unbekanntes ist generell nichts, womit vernünftige Menschen im Regelfall ganz frei und unbeschwert umgehen können. Das ist das Vorrecht der Jugend, aber mit zunehmender Erfahrung wird man eben auch umsichtiger. Relevant dabei ist es, die Balance zwischen unbedachter Unbeschwertheit und verbohrten Angstzuständen zu finden.

Cloud-Knowledge

Im Regelfall reduzieren sich Bedenken, wenn man das Unbekannte bekannter macht und selbst erkennen kann, was dahintersteckt und worum es geht. Genau Gleiches gilt für Technologien oder Cloud Services. Das Problem dabei ist, dass es recht kompliziert ist, sich dieses Bild zu machen. So einfach die Nutzung dieser neuen Services ist, so differenziert und thematisch vielseitig ist deren Beurteilung und Bewertung. Oder anders gesagt: Es braucht eine ordentliche Portion neuen Know-hows, um dies leisten zu können.

Selbst die erste Stufe – nämlich Transparenz zu erhalten, mit wem man denn überhaupt ins Geschäft kommt, wenn man einen Cloud-Service bezieht – ist eine Herausforderung. Weitere Fragen, wie: Wer erbringt das Service? Wo, in welcher Qualität, mit welchem Vertrag, in welchem Rechenzentrum, mit welchen Daten etc., sind nochmals komplexer zu beantworten.

Cloud-Check

Dem Laien hilft in allen solchen technologischen Fragen seit jeher das technische Zertifikat, das „Pickerl", weiter. Mit ihm auf der Windschutzscheibe des Autos vertrauen wir auf die Funktionsfähigkeit des Gefährts. Aber in Unternehmen muss es in Zukunft Mitarbeiter geben, die diese Dinge selbst prüfen und bewerten können. Vom Einkauf über Rechtsabteilung, Fachabteilung und IT – alle zusammen müssen letztlich ihr Okay geben und eine fundierte Aussage treffen können, ob ein Service das richtige ist oder nicht.

Das sind die 160.000 IT-SpezialistInnen, die laut Günther Oettinger in der EU jetzt schon fehlen. Und es werden noch mehr werden. Und diese MitarbeiterInnen werden gut bezahlt werden, denn sie sind rar. Know-how-Aufbau ist „Key" für jedes Unternehmen, das moderne Informations- und Kommunikationsmedien nutzen möchte. Statt selbst zu installieren und upzudaten, erhalten Qualitäts-, Schnittstellen- und Vertragsmanagement höhere Bedeutung. Wer es verabsäumt, dieses Know-how aufzubauen, wird sich weiterhin mit Unbekanntem konfrontiert sehen und weiter fürchten. ■

Datensicherheit maximieren!

Reinhard Travnicek
Branchenexperte und Co-Autor „Cloud Computing & Enterprise Mobility Management"

Heute ist es selbstverständlich auf Geschäftsdaten mobil zuzugreifen und diese an Partner, Kunden oder Kollegen zu verschicken. Im Regelfall ist man sich nicht bewusst, welche komplexen Abläufe man mit ganz einfach zu bedienenden Apps wie Mail oder Social Media startet. Selten weiß man, woher die Geschäftsdaten, die gerade geteilt werden, geholt wurden, wo sie zwischengespeichert werden, in welcher Form der Empfänger diese Daten dann erhält und wie er darüber verfügen kann.

Als Sicherheitsverantwortlicher in einem Unternehmen muss man sich aber schon die Frage stellen, ob ein Benutzer immer und überall die sicherheitsrelevanten Konsequenzen seines Handelns abschätzen kann. Es muss bewusst gemacht werden, wieweit man Benutzer mit technischen Maßnahmen daran hindern kann, grobe Sicherheitsfehler zu begehen und wieviel Schulung und Reglementierung notwendig ist.

Wo sollte man beginnen?

„Auch der längste Marsch beginnt mit dem ersten Schritt" (Laozi - Daodejing/ Tao Te King, Kapitel 64). Die Maximierung der Datensicherheit ist eher als zyklischer Prozess zu betrachten und daher ist es meist nebensächlich, in welchem Bereich man Maßnahmen setzt. In der Regel wird die Datensicherheit immer erhöht. Daher ist auch die Reihenfolge der folgenden Maßnahmen weder als vollständig, noch als vorgegebene sequentielle Ordnung zu verstehen.

Ziele der Benutzer-Schulung

Benutzer sind sich bewusst:

- dass einmal weitergegebene Daten nicht mehr im Einflussbereich des Unternehmens stehen
- dass Daten unterschiedlicher Sicherheitsstufen unterschiedlich behandelt werden müssen

Benutzer wissen:

- dass sie ungewöhnliche Anfragen / Vorkommnisse hinterfragen bzw. melden müssen
- dass sie den Diebstahl oder den Verlust eines mobilen Endgerätes umgehend melden müssen
- dass mobile Endgeräte am Ende des Lebenszyklus nicht ungelöscht der Wiederverwertung zugeführt werden dürfen

Ziele von Mobilem Datenmanagement

- Auf Firmendaten darf nur mittels vom Unternehmen freigegebener Apps zugegriffen werden.
- Geschäftsdaten müssen in Sicherheitscontainern auf den mobilen Endgeräten gespeichert werden (Data at rest).
- Der Zugriff auf Geschäftsdaten darf nur verschlüsselt erfolgen (Data in transit).
- Geschäftsdaten müssen auch in Zwischenspeichern immer verschlüsselt bleiben.
- Das Endgerät muss frei von Viren und Malware sein.
- Der Benutzer des Endgerätes muss eindeutig identifizierbar sein.
- Datenaustausch muss auch die Funktionen Digital Rights Management und Data Loss Prevention unterstützen.

Ziele von Datenklassifizierung

Die Wichtigkeit bzw. das Geheimhaltungsinteresse von Geschäftsdaten wird in der Regel in Stufen abgebildet und die Daten dann entsprechend gekennzeichnet, sortiert oder markiert. Typische Klassifizierungskategorien sind: streng vertraulich, vertraulich, intern, kundenbezogen, öffentlich.

Um weiterführende Informationen zum Thema Mobile Devices und Mobiles Datenmanagement zu erhalten, fordern Sie den Leitfaden Nummer 9 „Enterprise Mobility - Markt, Produkte und technische Herangehensweisen sowie relevante organisatorische und juristische Aspekte" der EuroCloud Österreich an ■