

# Handlungsstrategien zur Informationssicherheit in KMU

**Statt von Datenschutz sollte besser von Massnahmen zur Informationssicherheit gesprochen werden. Diese betreffen nicht nur die Informatik, sondern finden ihren Niederschlag in allen Disziplinen der Unternehmensführung. Zweiter Teil eines Expertengesprächs am «runden Tisch».**

VON THOMAS BERNER

**T**echnisch, rechtlich, organisatorisch: Informationssicherheit muss umfassend angegangen werden. Darin sind sich die Gesprächspartner einig. Es geht um die sog. Compliance, also das Zusammenspiel der genannten Aspekte. Dieses ist so individuell wie die einzelnen Unternehmen, eine Standardlösung gibt es also nicht, so schön dies auch wäre. Dennoch können einige Dinge die Basis für eine unternehmensweite Informationssicherheit bilden. Darüber sprachen wir mit den drei Experten Jerry Krattiger (SOLVIS AG), Ursula Sury (Die Advokatur Sury GmbH) und Stephan Richard.

## Eine Frage der Organisation

Der Schutz von Information und die Prozesse zu ihrer Weitergabe sollten in von den Unternehmen festgelegten Abläufen folgen. Mit Fragen zur Sicherheit und Kontrollen im IT-Bereich beschäftigt sich auch Wirtschaftsprüfer Stephan Richard. «Meine Sicht ist darauf ausgerichtet, wie diese Prozesse innerhalb von Unternehmen zweckmässig, rechtmässig, aber auch wirtschaftlich organisiert werden. Häufig treffe ich die Situation an, dass die Kontrolle im IT-Bereich zwar funktioniert, aber nicht oder ungenügend dokumentiert ist. D.h. die technischen Vorkehrungen sind getroffen, die eigentlichen Prozesse aber nicht definiert», so beschreibt er die Situation, in denen sich viele KMU befinden.

## Prozesse dokumentieren

Dokumentation – dies klingt wohl für viele KMU gleich nach Papierkram und zusätzlichem administrativen Aufwand. Doch Stephan Richard relativiert: «Es geht nicht darum, ein komplexes Werk von 500 Seiten zu

kreieren. Für kleine und mittlere Unternehmen reicht in der Regel schon eine A4-Seite aus, um die wesentlichen Risiken festzuhalten, und eine halbe Seite für die Beurteilung der wesentlichen IT-Risiken.» Als Grundlage für den Zugriffsschutz kann z.B. bereits ein Firmenorganigramm dienen. «Dies ist oft schon der erste Schritt zur Festlegung aller Berechtigungen. Und wenn dann noch jeder weiss, was er zu tun hat, ist schon viel gewonnen. Deshalb machen Stellenbeschriebe eben immer noch Sinn», stellt Stephan Richard klar. In kleineren Betrieben mit weniger als zehn Mitarbeitenden kann dies natürlich etwas flexibler gehandhabt werden. Doch Stephan Richard wirft ein, dass auch solche Firmen wachsen und plötzlich über mehrere Abteilungen verfügen. «Und dann fängt's eigentlich richtig an.»

## Zugriffsrechte definieren

Nicht jeder Mitarbeitende muss auf alle Informationen in einem Unternehmen jederzeit zugreifen können. Für Jerry Krattiger ist eine saubere Zuteilung von Zugriffsrechten ein wesentliches Element. Doch er warnt auch vor falschem Vertrauen: «Häufig erhalten jene Stimmen im Unternehmen, welche am lautesten danach schreien, dann auch viele Rechte, die ihnen vielleicht gar nicht zustehen würden. Werden solche Rechte missbräuchlich benutzt, kann einer Firma riesiger Schaden entstehen, wie die jüngsten Beispiele aus der Finanzbranche gezeigt haben.» Und scheidet ein Mitarbeiter aus dem Unternehmen aus, müssen dessen Zugriffsrechte ebenso sauber gelöscht werden – eine Aufgabe für die Personalabteilung, Ein- und Ausstritte von Mitarbeitenden ordnungsgemäss zu managen.

## INFORMATIONSSICHERHEIT IN KMU

Informationssicherheit umfasst nicht nur die IT. Folgende Punkte sollten auch KMU ganzheitlich angehen:

- Mögliche Risiken für Datenverluste ermitteln und innerhalb des IKS festhalten
  - Prozesse und Zugriffsrechte im Datenverkehr definieren: Wer benötigt wann welche Informationen und wozu?
  - Zugriffsrechte regelmässig an personelle Veränderungen anpassen (Mutationsmanagement)
  - Schutz von Hard- und Software vor unberechtigten Zugriffen durch technische Massnahmen sicherstellen
  - Verträge und andere wichtige Dokumente auf ihre Informationssicherheits-Compliance überprüfen
- Eine IAM-Lösung für KMU bietet die

SOLVIS AG mit dem Produkt «Usercube», der nach Angaben des Unternehmens ersten Lösung für Inhaltsverwaltung für Active Directory. Benutzer können sich via Intranet, über ihr Windows-Login, automatisch mit Usercube verbinden. Damit erhalten sie Zugriff auf das Firmenverzeichnis und können auch einfache administrative Aufgaben wie Passwortänderungen, Gruppenzugehörigkeit oder Ressourcenzugriffe vornehmen – alles im Einklang mit den Sicherheitsstandards der Firma, da jeder Task mithilfe eines Workflows, der die Zustimmung der betroffenen Business User garantiert, gesteuert wird. Usercube steht unter [www.solvis.ch](http://www.solvis.ch) zum Download bereit. **www.solvis.ch**

## Rollen managen

Die Definition von Zugriffsrechten ist womöglich für einige KMU noch Neuland. «Es existieren Systeme grosser Hersteller wie etwa Siemens. Doch diese sind für KMU womöglich eine Nummer zu gross. Mittlerweile gibt es aber auch Produkte, wie Usercube, welche für kleinere Unternehmen massgeschneidert sind und ein auf die Unternehmensgrösse abgestimmtes sog. Rollenmanagement ermöglichen», so Krattiger. Eine Implementierung eines sog. Identity and Access Managements (IAM) lohnt sich sonst erst für Unternehmen ab einer Grösse von 300 bis 500 Mitarbeitenden. Gehören aber Forschung und Entwicklung oder sogar die Sicherheit an sich zur Kernkompetenz eines Unternehmens, «lohnt sich für abgesteckte Bereiche in jedem Fall eine IAM-Lösung oder ist sogar zwingend erforderlich», so Jerry Krattiger.

## Daten verschlüsseln

Etwas, was aber in allen Unternehmen heute schon gemacht werden kann, ist eine Daten-Chiffrierung auf allen Geräten. «Ein reiner Passwortschutz genügt nicht, denn Passwörter sind verhältnismässig leicht zu knacken.» Kommt dazu, dass die Nutzer es den Passwortknackern auch immer wieder allzu leicht machen, indem sie z.B. Eigennamen oder einfache Zahlenfolgen verwenden. Für Jerry Krattiger ein Horrorszenario: «Geht etwa ein Laptop verloren, z.B. gerade das Gerät des Geschäftsführers, kann dem Unternehmen daraus ein grosser Schaden entstehen, wenn die Daten zwar passwortgeschützt sind, aber nicht verschlüsselt.»

## Bewusstsein entwickeln

Neben aller Technik geht es in erster Linie um das Bewusstsein. «Jeder Anwender muss wissen, ob er mit vertraulichen Daten arbeitet und wie

## UNSERE GESPRÄCHSPARTNER

Die drei im Text zitierten Experten stehen Ihnen für individuelle Fragen zur Verfügung:



**Jerry Krattiger**, Executive MBA, Chairman & Director Business Consulting bei SOLVIS AG, Arnold Böcklin-Strasse 35, 4051 Basel, und Rue Baudit 6, 1201 Genf.  
[jerry.krattiger@solvis.ch](mailto:jerry.krattiger@solvis.ch)



**Stephan Richard**, dipl. Wirtschaftsprüfer und Certified IS-Auditor (CISA), Kapellenstrasse 6, 4573 Lohn-Ammansegg  
[stephan.richard@gawnet.ch](mailto:stephan.richard@gawnet.ch)



**Ursula Sury**, Rechtsanwältin und Professorin an der Hochschule Luzern; DIE ADVOKATUR SURY GMBH, Alpenquai 4, 6005 Luzern.  
[ursula.sury@dieadvokatur.ch](mailto:ursula.sury@dieadvokatur.ch)

er damit umzugehen hat», betont Stephan Richard und deutet dabei auf die Vielschichtigkeit der KMU-Welt hin. «Sehr vieles in KMU ist abhängig von einzelnen Personen. Musterlösungen im engeren Sinne gibt es nicht, das gilt wohl für die gesamte Betriebswirtschaft.» Auch von juristischer Seite gibt es kein Patentrezept. Ursula Sury weist darauf hin, dass die Beurteilung von Risiken den Kern eines Massnahmenkatalogs bilden muss. Sie empfiehlt etwa, alle Verträge zu kontrollieren: Sind sie klar formuliert? Ist klar, wer von wem was warum zu welchem Preis erhält? Und sind in der inhaltlichen Dimension auch die Risiken präzisiert bzw. vorteilswise auf den anderen Partner abgewälzt? Und ferner geht es um Führungsverantwortung. «Worin muss ich meine Mitarbeiter instruieren?, Welche Kontrollpflichten habe ich als Führungskraft? Dies beinhaltet nicht nur die Finanzkontrolle», so Ursula Sury weiter. Ein gewisses Mass an vergleichbaren Standards bieten Zertifizierungen, z.B. nach den Labels «GoodPrivacy» von SQS oder nach ISO – in den Worten von Ursula Sury ist «dies aber schon fast <High End>».

### Outsourcing: ein zweischneidiges Schwert

Soll man den Schutz von Informationen auslagern? Stephan Richard weist darauf hin, dass es beim Out-

sourcing viele Punkte zu beachten gilt. «Zunächst muss in den Unternehmen geklärt sein, was überhaupt auswärts gegeben werden soll und wie dies geregelt wird», macht er klar. Denn alles, was ausgelagert wird, muss sich auch überprüfen lassen. Es stellt sich deshalb die Frage, ob dies Aufgabe einer Prüfungsstelle sein soll, wenn die Kontrolle, ob mit den Daten korrekt umgegangen wird, nicht durch das Unternehmen selbst übernommen wird. «Das Risiko beim Outsourcing liegt darin, dass oft nur auf der einen Seite, nämlich beim Dienstleister, korrekt gearbeitet wird. Beim Unternehmen dagegen ist die Verantwortung bezüglich Outsourcing oft nicht klar geregelt und es herrscht vorbehaltlos <blindes> Vertrauen in den externen Partner», so die Feststellung von Stephan Richard. Deshalb sei es wichtig, die Kontrollaufgaben sauber im Outsourcing-Vertrag zu regeln, empfiehlt er.

### Cloud Computing bringt neue Herausforderungen

Gerade das Thema Sicherheit führt dazu, dass nicht wenige Unternehmen noch etwas vorsichtig mit dem neuen Trend Cloud Computing umgehen. Denn dass hier neue, sicherheitsrelevante Herausforderungen dahinterstecken, bestreiten auch unsere drei Experten nicht. «In der Cloud ist häufig nicht vollständig klar, wer wirklich

mein Vertragspartner ist und wo sich dieser befindet. Dies ist insofern nicht unwesentlich, weil ja dort die Daten aufbewahrt werden», gibt etwa Ursula Sury zu bedenken. Und Jerry Krattiger ergänzt, dass in der Cloud der Zugang zu Daten auch für Externe einfacher werde. Und ebenfalls würden die Grenzen zwischen Privat und Business zusehends verfließen. Eine wichtige Rolle komme der Identifizierung der Nutzer in der Cloud zu: «Ist der Herr Müller, der sich eingeloggt hat, nun wirklich dieser Herr Müller? Um dies sicherzustellen benötigt man eine PKI, eine Public Key Infrastructure, also eine eindeutig identifizierbare Verbindung

zwischen Person und Authentisierung. PKI kann man mit einem Pass fürs Internet vergleichen», so Krattiger. Stephan Richard wiederum glaubt, dass eine Herausforderung darin besteht, dass in der Cloud die Abgrenzung von MIR und DIR bei der Verantwortung für die Unternehmenswerten zusehends schwieriger wird. Doch vielleicht ist es ja gerade das «Wolkenhafte», welches das Bewusstsein für die ganzheitliche Betrachtung von Informationssicherheit weiter schärft. ■■■■

Teil 1 dieses Roundtable-Gesprächs erschien in ORGANISATOR 5-2010, nachzulesen auf [www.organisator.ch](http://www.organisator.ch).

### Anzeige



Ihr Spezialist für:

- Buchhaltung
- Steuerberatung
- Lohnwesen
- Controlling
- Unternehmensberatung
- CFO-Mandate

Erstklassige Dienstleistungen aus einer Hand zu fairen Preisen. Wir denken über die Zahlen hinaus. Wir denken auch an Sie!

ONE! Treuhand GmbH  
Leutschenbachstrasse 95  
8050 Zürich

Tel: +41 (0) 44 308 38 58  
Fax: +41 (0) 44 308 35 00  
E-Mail: [info@onetreuhand.ch](mailto:info@onetreuhand.ch)  
Internet: [www.onetreuhand.ch](http://www.onetreuhand.ch)