Wolfgang Sidler – ruft die KMU zu vermehrter Auseinandersetzung mit dem Thema IT-Sicherheit auf

Immer noch blenden viele KMU das Thema der IT-Sicherheit aus ihren Geschäftsgrundsätzen aus. Erst wenn es zum Daten-GAU gekommen ist, werden entsprechende Massnahmen eingeleitet. Das muss nicht so sein, moniert der Sicherheitsexperte und Präsident des Vereins «InfoSurance» Wolfgang Sidler. asut-Redaktor Guido Wemans unterhielt sich mit ihm über die Problematik der IT-Sicherheit bei kleineren und mittleren Unternehmen und über notwendige Schritte zur Verbesserung.

asut: *Im ICT-Bereich gibt es eine ganze Reihe von Interessen-Verbänden, in denen auch KMU vertreten sind. Aber einen eigentlichen KMU-Verband gibt es meines Wissens nicht. Oder muss man sich auf der Stufe von lokalen oder kantonalen Gewerbeverbänden umsehen?*

Wolfgang Sidler: Es gibt den Schweizerischen Gewerbeverband, bei welchem eigentlich alle Berufsverbände Mitglied sind (www.sgv-usam.ch). Er vertritt die Interessen der kleinen und mittleren Unternehmen KMU in der Schweiz. Mitglieder des sgv sind die kantonalen Gewerbeverbände, Berufs- und Branchenverbände sowie die Organisationen der Gewerbeförderung.

Zusätzlich gibt es noch die Stiftung KMU Schweiz. Die Stiftung KMU Schweiz wurde als gesamtschweizerisch tätige Organisation im Jahre 1993 von verschiedenen schweizerischen Wirtschaftsverbänden errichtet (www.stiftung-kmu.ch).

Im Bereich der IT-Sicherheit sind wir als InfoSurance der massgebliche Verein. Wir engagieren uns für die Förderung der IT-Sicherheit bei Privatpersonen und KMU und führen jährlich den SwissSecurityDay und die LUTIS (Luzerner Tage der Informationssicherheit) durch.

Wie gehen Sie vor, wenn Sie dezidiert KMU erreichen wollen?

Einerseits über die verschiedenen Verbände und andererseits durch direkte Kontakte unserer Mitglieder. Ich schreibe entsprechende Fachartikel in den gängigen IT-Magazinen und anderen Zeitschriften und Zeitungen und nutze diverse Netzwerke.

Wenn es um Fragen der IT-Sicherheit geht, hat man das Gefühl, dass die entsprechenden Sicherheitsüberlegungen noch nicht bei allen KMU angekommen sind. Täuscht dieser Eindruck?

Leider täuscht dieser Eindruck nicht. Das Thema IT-Sicherheit hat bei den Geschäftsleitern und den Verwaltungsräten immer noch nicht den Stellenwert, den ich mir wünsche. Häufig höre ich die Bemerkung «Bei uns wird schon nichts passieren …» oder «Was kann denn schon bei uns gestohlen werden?» oder «Wir kennen die Risiken und tragen diese».

Speziell heute, in einer wirtschaftlich eher schwie-

rigen Zeit, sind die KMU angehalten, ihr Know-how vor Dieben zu schützen! Wie schnell ist heute ein Notebook oder ein USB-Stick mit sensitiven Informationen weg, gestohlen oder verloren.

Woran liegt das?
Ich denke, es liegt daran, dass die Unternehmen die Risiken nicht kennen und sich keine Zeit nehmen, das Thema «Sicherheit» ernst anzugehen. Sicherheit ist halt ein Thema, welches nicht interessant ist und meistens Kosten verursacht. Ich kann da nur sagen: Eine angemessene Sicherheit kostet, keine Sicherheit kostet mehr! Auch erlebe ich oft eine gewisse Ignoranz.

Auf was ist diese zurückzuführen? Ist die Materie zu technisch um allgemein verstanden zu werden?
Die Wahrnehmung im Bereich der IT-Sicherheit ist in der Tat immer noch sehr technisch. Bei Sicherheit denkt man zuerst an Viren, Würmer oder Firewalls. Über die anderen Sicherheits-Bedrohungen, wie Wirtschaftsspionage, Notebooks, USB-Sticks, Vernichtung von Dokumenten, Umgang mit E-Mail und Internet etc., wird nicht genügend oft berichtet. Hier ist das Thema Sensibilisierung ein wichtiges Thema. Alle Mitarbeiter eines Unternehmens sollen zielgerecht sensibilisiert werden. Mitarbeitende im Verkauf müssen anders sensibilisiert werden als die IT-Administratoren. Ein verständlicher Leitfaden, z. B. «Umgang mit Kunden- und Geschäfts-Informationen», für alle Mitarbeiter kann Wunder bewirken.

Was sind die häufigsten und schlimmsten Sünden bei den KMU punkto IT-Sicherheit?
Viele KMU ignorieren das Thema Sicherheit schlichtweg. Es heisst ja nicht, dass jedes Unternehmen einen sogenannten IT-Security Officer mit einer Vollzeitstelle beschäftigen soll. Das Management sollte sich mindestens die Zeit nehmen, mit einem externen Berater oder Coach die Risiken zu identifizieren und zu bewerten. Der Berater wird danach entsprechende Sicherheitsmassnahmen ausarbeiten und dem Management präsentieren. Somit hat das Management einen aktuellen Risiko-Katalog – Portfolio – analog eines Projekt-Portfolios. Dieser Risiko-Katalog ist die Basis, um entsprechende Massnahmen mit Prioritäten als Projekt in Auftrag zu geben. Zusätzlich gibt die Risiko-Analyse einen wichtigen Input für Risiko-Analyse des IKS (Internes Kontrollsystem).

«Viele KMU ignorieren das Thema Sicherheit schlichtweg.»

Des Öfteren erlebe ich die Situation, dass die KMU gar nicht wissen, welches ihr zu schützendes Gut ist. Sie kennen wohl ihre Geschäftsprozesse, aber deren Abhängigkeit zu den Applikationen und IT-Systemen ist ihnen meistens nicht bewusst. Da würde zum Beispiel eine Frage beim Security-Interview lauten: Wie lange können Sie Ihre Produkte noch produzieren, wenn das interne Netzwerk einen Tag nicht zur Verfügung steht?

Was empfehlen Sie?
Wünschenswert wäre es, wenn jedes KMU eine sogenannte Sicherheitsstrategie hätte. Dieses aus wenigen Seiten bestehende Dokument beschreibt sehr verständlich, dass die Geschäftsleitung das Thema Informationssicherheit ernst nimmt und alles daran setzt, diese auch effektiv und effizient umzusetzen.

In meiner Praxis habe ich oft gesehen, dass grosse IT-Projekt gestartet worden sind, ohne die Sicherheit

Der Verein InfoSurance entstand im Sommer 2005 aus der Stiftung InfoSurance, welche 1999 von grossen Schweizer Unternehmen und vom Bund gegründet wurde. Der Verein fokussiert seine Aktivitäten auf kleine und mittlere Unternehmen, respektive Verwaltungen, sowie auf die Bevölkerung. Erfahrungsgemäss verfügen diese Zielgruppen nicht über ausreichende Fachkompetenzen und Mittel, um das Thema in der nötigen Breite und Tiefe selbstständig zu behandeln. Um diesem Manko zu begegnen, entwickelt und publiziert der Verein InfoSurance einfach umsetzbare und kostengünstige Verfahren, mit welchen die Informationssicherheit verbessert werden kann. Beispiele für die Aktivitäten der InfoSurance sind das 10-Punkte-Programm, die KMU-Roadshow oder der Nationale Sicherheitstag SwissSecurityDay.
Im Gegensatz zur Stiftung soll der Verein InfoSurance über eine breite Basis von Mitgliedern verfügen: Einzelpersonen und KMU, welche sich für das Thema interessieren; Verwaltungen von Gemeinden und Kantonen; aber auch grosse Unternehmen, welche ihr Bestreben zur Verbesserung der Informationssicherheit kundtun wollen.

Wer ist Wolfgang Sidler?

Wolfgang Sidler, Wirtschaftsinformatiker mit FA und Inhaber eines Master of Advanced Studies in Information Security FH, war von 1997 bis 2005 bei der Bank Julius Bär in Zürich und New York als Security Officer tätig. Von 2005 bis 2008 hatte er verschiedene Führungsfunktionen bei Zurich Financial Services, der Swiss IT-Markt AG, der InfoGuard AG sowie bei der Crypto AG inne. Und 2008 war er für die Omanische Regierung als Senior Security Consultant und Projektleiter im Middle East tätig. Anfang 2009 kehrte Sidler in die Schweiz zurück und arbeitet seither als Geschäftsführer seiner eigenen Beratungsfirma Sidler Information Security GmbH sowie in einem Teilzeitpensum als Mitarbeiter des Datenschutzbeauftragten des Kanton Luzern.

bei Beginn mit einzubeziehen. Die Konsequenzen waren in einigen Fällen sehr weitreichend, vom Projektverzug bis zum Projektstopp. Ich kann nur empfehlen, bei einem Projektstart die Anforderungen an die Sicherheit zu definieren und diese entsprechend umzusetzen. Hier noch ein Tipp: Führen Sie nie eine technische Lösung ohne begleitende organisatorische Massnahme ein. Es nützt Ihnen nichts, wenn Sie eine Firewall installieren, ohne zu klären, wie diese korrekt betrieben und unterhalten (Betriebskonzept) werden soll.

Gibt es eine Art von Checkliste, anhand derer ein KMU den Stand seiner Sicherheit überprüfen kann?

Die InfoSurance hat bereits seit Jahren das sogenannte 10-Punkte-Programm für KMU. Seit Ende Oktober wird das neue und erweiterte 10-Punkte-Programm auf unserer neuen Webseite vorgestellt und kostenlos zum Download angeboten. Eigentlich zeigen wir anhand von 20 Themen auf, wie ein KMU die Sicherheit mit technischen und organisatorischen Massnahmen deutlich erhöhen kann. Ein sogenannter Security-Audit zeigt innert Kürze die Schwachstellen im Unternehmen auf und gibt einen sehr guten Überblick über den aktuellen Sicherheitszustand.

«Die Sicherheit eines jeden Unternehmens liegt in der Verantwortung der Geschäftsleitung.»

Wie kann der Informationsfluss von den Sicherheits-Experten zu den KMU verbessert werden? Wer ist sinnvollerweise der Adressat von sicherheitsrelevanten Informationen im Unternehmen?

Als InfoSurance haben wir uns dazu verpflichtet, die KMU mit dem entsprechenden Know-how und Tipps zu unterstützen. Die Sicherheit eines jeden Unternehmens liegt in der Verantwortung der Geschäftsleitung. Das heisst konkret, dass die Verantwortung nicht delegiert werden kann. Die Geschäftsleitung kann jedoch die Ausführung oder die Umsetzung mit entsprechender Kompetenz an den IT-Verantwortlichen oder an einen externen Berater übertragen. Die Geschäftsleitung hat jedoch die Aufgabe, die entsprechenden Mittel in Form von Finanzen und Ressourcen bereitzustellen und nicht zuletzt das Ergebnis der Umsetzung zu prüfen.

Können KMU im unteren Segment (bezüglich Zahl der Mitarbeitenden) eigene Leute für Sicherheitsfragen beschäftigen oder wird häufiger ein externer Berater zugezogen?

Kleinere und mittlere Unternehmen verfügen nicht über die finanziellen Mittel, einen eigenen IT-Security Officer zu beschäftigen. Hier eignet sich speziell das Modell eines IT-Security Officers auf Zeit. Je nach Grösse des Unternehmens ist der externe IT-Security Officer einen Tag in der Woche oder einen Tag im Monat im Betrieb und erledigt alle Pendenzen im Bereich der IT-Security, z. B. als Projektleiter, und erstellt die notwendigen Dokumente.

Wenn ein KMU eigene Leute ausbilden möchte, wohin kann es sich wenden?

Die Hochschulen bieten sehr gute Ausbildungsprogramme an. Speziell im Bereich der Informationssicherheit kann ich Ihnen die Ausbildung zum «MAS Information Security» oder «CAS Information Security» der Hochschule in Luzern empfehlen.

Wie gelangt man zu Adressen von seriösen und kompetenten Beratern? Gibt es da beispielsweise einen Berufsverband?

Ein eigentlicher Berufsverband ist mir nicht bekannt. Es gibt zwei führende Vereine, die SGRP und die ISSS. Und nicht zuletzt unterstützt InfoSurance die KMU. Die beste Referenz ist die Empfehlung eines Kunden. □