



IT-Sicherheit – zuerst eine Frage geteilter Werte

von Rolf Heßling, Geschäftsführer Uptime Informations-Technologie

Seit etwa zwei oder drei Jahren rollt eine neue Welle des digitalen Lifestyle durch Deutschland, geprägt durch die Allgegenwart von sozialen Netzwerken sowie mobilen Geräten wie Smartphones und Tablets. Anwendungen und persönliche Daten müssen überall und auf einer Vielzahl von unterschiedlichen Geräten zur Verfügung stehen, mit der Konsequenz, dass die Cloud allgegenwärtig wird - jene ominöse Datenwolke, in der sich alles verteilt und bei Bedarf wieder zusammenfindet, ob es Kontaktdaten, Mails, Dokumente oder ganze Anwendungsprogramme sind.



Simple, aber wirksame Marketingbotschaften der Betreiber sozialer Netzwerke, Suchmaschinen oder Shopping-Sites verankern sich tief in unseren Hirnen und sollen Millionen Menschen dazu bringen, die neuen Möglichkeiten exzessiv zu nutzen und möglichst viele private Daten mit diesen Unternehmen zu „teilen“.

Eine neue Generation von Entscheidungsträgern wächst heran, die diese Denkweise und daraus folgende Anforderungen mit Selbstverständnis auch auf das berufliche Umfeld überträgt, was die IT-Landschaften von Unternehmen und Organisationen nachhaltig verändert. Es besteht wohl einiger Grund zu der Annahme, dass die erwähnten Marketingbotschaften hier oft unbewusst Entscheidungen beeinflussen, die besser mit klarem Kopf und ohne Emotionalität zu treffen sind. Denn in der Tat bietet die Cloud nicht zu unterschätzende Wettbewerbsvorteile für Unternehmen, ganz neue Möglichkeiten der Vernetzung und Zusammenarbeit mit Kunden und Lieferanten, schnelle Reaktionszeiten bei zeitkritischen Entscheidungen, Zugriff auf wichtige Dokumente -- auch am Strand mit dem Smartphone und in Bermudashorts.

Doch das Unbehagen über die Sicherheit der Daten und den Datenschutz bleibt, und das mit Recht. Denn die Cloud birgt über das Risiko des klassischen Datendiebstahls hinaus die Gefahr, dass sich auch mit der Verknüpfung von

scheinbar unwichtigen „Daten-Schnipseln“ aus einer Vielzahl von Kanälen wichtige Informationen gewinnen lassen. Viele Daten, die Sie verschicken oder Online-Diensten in der „Cloud“ anvertrauen, landen auf Servern von Firmen, die aus anderen Kulturkreisen stammen, andere Rechtsstrukturen und völlig andere Auffassungen bezüglich des Wertes von Daten haben. So wird in Deutschland Datenschutz als ein hohes Gut betrachtet, woanders hingegen eher als hinderlich angesehen. Diese Einstellung spiegelt sich in der Kultur und im Verhalten wieder. Gesetzliche Bestimmungen, die den Zugriff von Behörden und selbst privaten „Sicherheitsunternehmen“ auf sensible Daten erlauben, sind global gesehen keine Seltenheit, der Patriot Act in den USA soll nur als ein Beispiel dienen und wird von deutschen Datenschützern immer wieder kritisiert.

Hinzu kommt, dass mobile Endgeräte und die Einbindung von Cloud-Diensten die Komplexität der Firmen-IT erheblich steigern. Viele IT-Landschaften gleichen einem Dschungel, in dem Sicherheitslücken, gleich gut versteckten Fallgruben und Fußangeln, leicht unentdeckt bleiben. So bieten sie offene Einfallstore für Hacker - eine große Herausforderung für IT-Verantwortliche, die die Anforderungen des Business an Flexibilität und Effizienz erfüllen müssen, ohne Verfügbarkeit und Sicherheit zu gefährden.

Kann es also in diesen Zeiten überhaupt noch sinnvollen Datenschutz geben? Und ist der einzelne Unternehmer damit nicht überfordert? Sind es nicht zu viele Parameter und muss er nicht die gesamte Komplexität verstanden haben, um sinnvolle Entscheidungen treffen zu können?

Es ist eigentlich ganz einfach, sobald Sie zwei entscheidende Punkte berücksichtigen: Das Wichtigste ist das Bewusstsein vom Wert der eigenen Daten sowie die Erkenntnis, dass Sie selbst die Verantwortung für Ihre und die Ihnen anvertrauten Daten haben. Ein auf festen Werten gegründetes Unternehmen wird beinahe zwangsläufig aus diesen Werten die Bedeutung des Datenschutzes für sich selbst und seine Kunden ableiten. Dafür braucht es kein technisches Wissen über die Cloud. Wichtig ist nur, dass diese Stimme nie schläft - sowohl beim Unternehmer selber als auch in der gesamten Organisation. Gegebenenfalls ist an dieser Stelle Sensibilisierung nötig.

Der zweite wichtige Punkt ist ein Partner in der IT, der diese Werte teilt. Auch die Lions haben bereits ihre eigenen, leidlichen Erfahrungen mit Datendieben gemacht. Entsprechend sensibilisiert für das Thema Sicherheit hat der Lions Clubs Deutschland das Gespräch mit Uptime IT gesucht. Der Lions Clubs Deutschland fand in uns einen vertrauensvollen und kompetenten Partner für den IT-Betrieb von Mitgliederdatenbank und Website. Ganz unabhängig von technischen Fragen haben wir schnell festgestellt, dass wir in Fragen der Sicherheit die gleichen Werte teilen. Es mag uns geholfen haben, dass wir ein unabhängiges, inhabergeführtes deutsches IT Unternehmen sind. Wir machen genau das, was wir sagen - bei uns gibt es keinen

Unterschied zwischen IT-Marketing und IT-Betrieb. Wir handeln nach unserem Gewissen – und nach deutschem Recht. Persönlicher Austausch, Präzision bis ins Detail und exakte Absprachen über wechselseitige Rechte und Pflichten erleichtern allen Beteiligten nicht nur die Zusammenarbeit, sondern sorgen auch für ein hohes Maß an Vertrauen und Sicherheit.

Die Server für die Mitgliederdatenbank und die Websites der Lions Clubs werden daher nun auf der Plattform von Uptime IT in einem sicheren und professionellen Rechenzentrumsumfeld betrieben. Um es deutlich zu sagen: Ein IT-Manager, der heute die Chancen der Cloud nicht zu nutzen weiß, ist nicht mehr zeitgemäß; doch einer, der Sicherheit, Verfügbarkeit und Hoheit über die Daten nicht als seine vordringlichsten Aufgaben betrachtet, macht ganz einfach einen schlechten Job. Das war schon immer so und ändert sich auch im Cloud-Zeitalter nicht. Die IT-Verantwortlichen bei den Löwen werden diesen Weg konsequent weiter fortsetzen. Neue Dienste werden immer auch mit dem Blick auf die Sicherheit bereitgestellt. Es tut der Sicherheit mit Sicherheit gut, Datenschutz als einen kontinuierlichen, fest in der Kultur der Organisation verankerten Prozess zu begreifen, der zusammen mit einem Partner gelebt wird, der die eigenen Werte teilt. Das kostet zwar Arbeit und Mühe, doch alles andere kostet Sicherheit und möglicherweise Reputation.