SECURITY FIRST?

Top-Thema Sicherheit

IT-Security steht bei Schweizer CIOs und Firmenchefs ganz weit oben auf der Agenda. Die in letzter Zeit ruchbar gewordenen Abhöraktionen des US-Geheimdienstes NSA lösen zwar keinen blinden Aktionismus aus, bestärken aber die kompromisslose Haltung. → VON JENS STARK

Weder Panik noch Leichtsinn oder Gleichgültigkeit sind bei Schweizer Unternehmen in Bezug auf die IT-Sicherheit auszumachen. Ganz im Gegenteil: Dem Thema wird eine hohe Bedeutung beigemessen – und zwar über Jahre hinweg auf einem ähnlich hohen Niveau. Dies bestätigen auch die jüngsten Zahlen der aktuellen Swiss-IT-Umfrage. Nach der «Unterstützung der Fachbereiche bei der Optimierung der Geschäftsprozesse» gilt die «Erhöhung und Gewährleistung der IT-Sicherheit» bei den befragten IT-Verantwortlichen als zweitwichtigste Aufgabe der IT (vgl. S. 27, Grafik 1).

58 Prozent der Schweizer CIOs bzw. IT-Leiter halten das Thema für wichtig bis sehr wichtig. Weniger wichtig nehmen es 13 Prozent und komplett unwichtig ist es lediglich für 3 Prozent. Auf einer Skala zwischen 1 «unwichtig» und 5 «sehr wichtig» erhält IT-Security einen Durchschnittswert von 3,61 (vgl. Grafik 1, rechts). Historisch gesehen zeigt sich bei dieser Einschätzung eine erstaunliche Konstanz: Seit Jahren weist das Thema einen ähnlich hohen Stellenwert auf. Seit 2010 wird die Sicherheit mit einem gleichbleibend hohen Durchschnittswert zwischen 3,5 und 3,7 bewertet (vgl. Grafik 2, S. 18).

TOP-THEMA IM MANAGEMENT

Für die befragten Vertreter der Unternehmensführung besitzt IT-Sicherheit als Aufgabe der Unternehmens-IT einen noch höheren Stellenwert und liegt mit einem Durchschnittswert von 3,73 auf der absoluten Poleposition.

Interpretiert wird dieses Ergebnis unterschiedlich. Für Markus Rüdisüli, CEO der psychiatrischen Klinik Meissenberg in Zug, ist klar, dass ein Wandel in der Beurteilung der IT beim Management hinter diesem Ergebnis steht. «Früher wurde Security als reines IT-Problem angesehen. Heute haben viele CEOs erkannt, dass sie die Verantwortung für das Unternehmen haben und sie schlussendlich dafür geradestehen müssen, wenn etwas in Sachen IT-Security falsch läuft», sagt er. Als Beispiel nennt der Klinikchef – der früher selbst einmal CIO war – etwa einen Spionagefall. Der CEO müsse sich dann vom Verwaltungsrat den Vorwurf gefallen lassen, er hätte ein unzureichendes Risikomanagement betrieben. «Wie stelle ich sicher, dass keine Daten abfliessen, ist heute klar ein Thema für die Geschäftsleitung», meint er.

Dies trifft besonders für die Finanzindustrie zu, wie ein IT-Leiter, der nicht genannt werden will, aus besagter Branche gegenüber Computerworld bestätigt. Das Management werde bei einem Datenleck haftbar gemacht, was bis zu einem Bankenlizenzentzug einschliesslich einer Verantwortlichkeitsklage führen könne. Auch für Peter Ronchetti, Vorsitzender der Geschäftsleitung bei CSC Switzerland, ist klar, dass die Geschäftsleitung letztendlich persönlich für das unternehmerische Risiko haftet. «Das Bewusstsein, dass auch IT-Sicherheitsrisiken dazugehören, hat sich in den letzten Jahren bei den Entscheidungsträgern deutlich verstärkt», ist er überzeugt.

«Früher galt Security als IT-Problem. Heute haben viele CEOs erkannt, dass sie letztlich dafür geradestehen»

Markus Rüdisüli, CEO Klinik Meissenberg

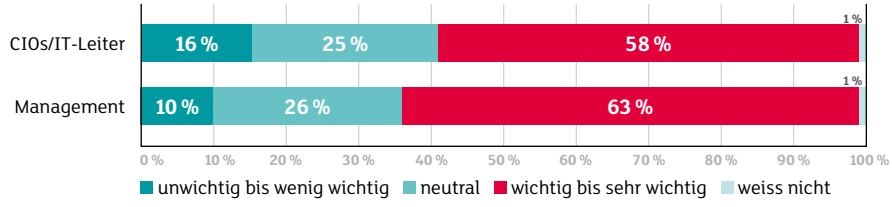
Angeseilt: Eiskletterer in einer Schlucht bei Pontresina

BILD: KEYSTONE/ARNO BALZARINI

SWISS IT 2014: GRAFIK 1

WIE WICHTIG IST SECURITY IN DER UNTERNEHMENS-IT?

Das Management hält das Thema IT-Sicherheit als Aufgabe der Unternehmens-IT für noch einen Tick wichtiger, als die IT-Leiter dies selbst tun. Quelle: Computerworld Swiss IT 2014 (n = 568/810)



ALS KOSTENTREIBER VERRUFEN

Anders nimmt Christoph Baumgartner, IT-Security-Experte und CEO von OneConsult, die Situation wahr. «Ich kann diese Aussage nicht bestätigen, da insbesondere in Industrieunternehmen auf Geschäftsleitungsebene die IT immer noch als notwendiges Übel, sprich: reiner Kostenfaktor, angesehen wird», erklärt er. «Im Alltag tun sich die CIOs und IT-Leiter nach wie vor schwer, Vorhaben im IT-Security-Umfeld bewilligt zu bekommen – egal, ob es sich dabei um technische oder organisatorische Massnahmen handelt», weiss er aus der Branche zu berichten.

Ebenfalls mit einem Fragezeichen versieht Bruno Kaiser, Chief Security Officer (CSO) von AdNovum, die Beobachtung, dass das Management die IT-Security als wichtiger ansieht als die IT selbst. Er glaubt, dass die CEOs nur so lange Feuer und Flamme für mehr IT-Security sind, bis ihnen die Rechnung präsentiert wird. «Das Management liest über das eine oder andere Bedrohungsszenario, wird verunsichert und wünscht sich dann eine hohe IT-Security», führt Kaiser aus. «Wenn dann aber die interne IT ausrechnet, was das kostet, überlegt man sich die Sache wieder und handelt schlussendlich nicht mehr in letzter Konsequenz.»

ENORME BRANCHENUNTERSCHIEDE

Wie dem auch sei, die unterschiedliche Einschätzung der IT-Security als zentrale Aufgabe der IT – sowohl durch CIOs als auch durch das Management – ist in gewissen Branchen eklatant. Am auffälligsten ist dies in der «hauseigenen» Branche «Information und Kommunikation». Hier finden laut Swiss-IT-Studie nur 46 Prozent der CIOs, dass IT-Sicherheit eine wichtige oder sehr wichtige Aufgabe im Unternehmen ist, gegenüber 74 Prozent aus dem Management des gleichen Geschäftsbereichs. Das Management fürchtet den Prestigeverlust bei eventuellen Datenlecks also deutlich mehr.

Es gibt aber auch den umgekehrten Fall: Sowohl in der Finanz- und Versicherungsindustrie als auch in der Energie- und Wasserversorgung erachten die CIOs die IT-Sicherheit als wichtiger (74 % wichtig, 61 % sehr wichtig) als das Management (63 % bzw. 56 %). Bei den Banken und Versicherungen fand sich allerdings auch kein einziges Mitglied aus der Geschäftsleitung, das IT-Security als unwichtig tituliert hätte – das ist nach den Steuerdatenskandalen der letzten Jahre auch kaum mehr möglich.

Vor allem im Bereich der Energie- und Wasserversorgung scheint sich in den Führungsetagen jedoch noch kein ausreichendes →

IT-Sicherheitsbewusstsein etabliert zu haben. 24 Prozent des Managements schätzen in dieser Branche die IT-Sicherheit als eher unwichtige oder ganz unwichtige Aufgabe der IT ein. Dies ist umso erstaunlicher, als gerade Vorfälle wie die Einschleusung von Malware in Steuerungen (Stichwort: Stuxnet) und die Tatsache, dass die Versorgung mit Energie und Trinkwasser vom Bund zu den besonders schützenswerten Infrastrukturen des Landes gezählt werden, auch in den jeweiligen Chefetagen zu einer grösseren Sensibilisierung gegenüber IT-Sicherheitsthemen geführt haben sollen.

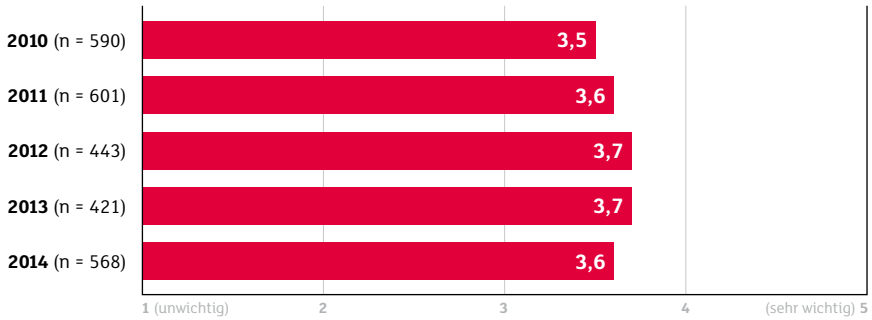
Defizite in der Wertschätzung der IT-Sicherheit im Rahmen der IT sind auch in der Branche Verkehr und Transport auszumachen. Hier sahen lediglich 35 Prozent der CIOs IT-Security als wichtig an, während genau gleich viele «unwichtig» angaben. Ebenfalls eher wenig von IT-Security halten CIOs im Handel. Hier sind lediglich 40 Prozent von der Wichtigkeit der Absicherung ihrer IT-Infrastruktur und Daten überzeugt, für 25 Prozent ist diese Aufgabe unwichtig.

Recht ausgeglichen ist das Urteil über die Wichtigkeit der IT-Sicherheit dagegen, wenn man die diesbezüglichen Antworten der Swiss-IT-Umfrage nach Firmengrösse aufschlüsselt. Hier zeigt sich nur, dass mittelgrosse Unternehmen IT-Security am meisten Bedeutung beimessen, während die kleinsten (bis 50 Mitarbeiter) und die grössten (über 5000 Mitarbeiter) – zumindest nach Meinung der CIOs – einen weniger starken Fokus auf das Thema legen. Bei Letzteren spielt sicherlich eine Rolle, dass die Security-Standards schon aus Compliance-Gründen bereits hoch sind.

SWISS IT 2014: GRAFIK 2

WIE WICHTIG IST FÜR CIOS DAS THEMA SECURITY?

Die Sicherheit der Unternehmens-IT wird seit Jahren auf etwa gleich hohem Niveau als wichtige Aufgabe der IT gesehen. Quelle: Computerworld Swiss IT 2010–2014



«Vor den NSA-Enthüllungen hiess es oft: Wir sind kein Ziel, was gibt es bei uns zu holen?»

Peter Ronchetti, General Manager CSC Schweiz

(KEINE) LEHREN AUS DER NSA-AFFÄRE

Die Enthüllungen rund um den US-Geheimdienst NSA (National Security Agency) haben bewiesen, dass sogar eine grundsätzlich befreundete Nation sowohl direkt als auch indirekt über Hintertüren bei Herstellern private und geschäftliche Daten sammelt sowie vermutlich auswertet und den eigenen Firmen zur Verfügung stellt. Angesichts dessen ist es interessant zu sehen, dass die Wichtigkeit der IT-Sicherheit als Aufgabe der IT im Urteil der CIOs nicht erhöht, sondern – wenn auch nicht signifikant – leicht abgenommen hat, konkret von einem Durchschnittswert von 3,66 im Jahr 2013 auf 3,61 im Jahr 2014. Erklärbar ist dies dennoch. «Hätte die NSA-Affäre einen IT-Security-Rutsch ausgelöst, so hätten sich viele Unternehmen vorwerfen lassen müssen, dass sie vorher zu wenig für IT-Security getan hätten», interpretiert Meissenberg-CEO Rüdisüli das Ergebnis. Es zeige darüber hinaus auch auf, dass den meisten bewusst sei, dass eine 100-prozentige Sicherheit nicht möglich ist, zumal dann nicht, wenn die Gegenseite über sehr weitreichende technische und finanzielle Mittel verfüge.

CSC-Schweiz-Chef Ronchetti beobachtet dagegen, dass «die Sensibilität für das Thema Informationssicherheit in letzter Zeit sicherlich zugenommen hat». Früher, also vor den NSA-Enthüllungen, sei von vielen Unternehmen das Risiko einer Cyberattacke nur gering bis mittel eingeschätzt worden: «Oft hiess es da: Wir sind kein Ziel, was gibt es bei uns zu holen? Heute hört man schon mal: Wir werden in jedem Fall abgehört! Das Risiko wird also hoch bis sehr hoch bewertet», so Ronchetti.

VERTRAUENSBRUCH UND MISSTRAUEN

Laut AdNovum-CSO Kaiser haben die Berichte über die Tätigkeit der NSA dazu beigetragen, dass nun die Allgemeinheit davon erfahren habe. «In der Branche waren die Abhörmethoden zumindest gerüchtemässig schon länger bekannt», sagt Kaiser und verweist auf einen Ar-

tikel im US-Magazin «Wired», in dem schon vor Jahren anhand der Beschreibung von NSA-Rechenzentren in den USA aufgezeigt wurde, was alles möglich sei. Sicherheitsexperte Christoph Baumgartner, CEO und Inhaber von OneConsult, bläst ins gleiche Horn. Seit der Verabschiedung des «Patriot Act» sei klar gewesen, dass US-amerikanische IT-Hersteller der Regierung technische Schnittstellen für den Zugriff auf Daten bereitgestellt hätten. «Dies ist nur eine logische Folge des Drucks, den die amerikanische Regierung und andere geheimdienstähnliche und -nahe Organisationen seit Jahren auf die Unternehmen ausüben», interpretiert Baumgartner.

Obwohl also die Machenschaften der NSA zumindest in der IT-Security-Szene bekannt waren, stellt Kaiser als Folge der NSA-Enthüllungen einen Vertrauensbruch fest, und zwar gegenüber Herstellern, Standardisierungsgremien und Staaten. «Das ist eine der Haupterkenntnisse aus der NSA-Affäre. In allen unseren Bedrohungsszenarien sind wir davon ausgegangen, dass es Akteure gibt, die sich gutmütig oder wohlwollend verhalten, nämlich befreundete Staaten, deren Organisationen und Standardisierungsgremien», erklärt Kaiser. Mit der NSA-Affäre habe man gemerkt, dass diese Einschätzung falsch gewesen sei. «Es gibt vielmehr Akteure, die – ohne es vielleicht selbst zu merken – unterwandert sind und in der Folge beispielsweise Standards abschwächen», gibt er zu bedenken. Als Konsequenz fordert Kaiser, «dass Standards wirklich in einer Community diskutiert und möglichst offen verhandelt werden». In diesem Zusammenhang hat er das Gefühl, dass Open Source wieder ein Revival erleben könnte, da hier grössere Transparenz herrsche.

IST «SWISSNESS» IMMER BESSER?

Eine der sichtbaren Auswirkungen der NSA-Enthüllungen ist die Werbung vieler Schweizer Betreiber von Rechenzentren mit ihrer «Swissness». Doch die Teilnehmer an der Swiss-IT-Studie lassen sich alleine durch das Schweizerkreuz auf der Webseite des Providers nicht blenden. So spielt bei fast doppelt so vielen Befragten die Sicherheit der Daten eine grössere und ausschlaggebende Rolle bei der Wahl des Cloud-Providers als der Standort der zugehörigen Rechenzentren in der Schweiz (vgl. auch Grafik auf S. 53).

«Nur weil eine Firma schweizerisch ist, ist sie nicht automatisch besser oder sicherer»

Bruno Kaiser, CSO AdNovum

Dieses Ergebnis ist unserer Expertenrunde zufolge durchaus nachvollziehbar. Die Swissness eines Betreibers sei nicht ausschlaggebend, meint Rüdisüli. Schliesslich könne auch ein Schweizer Provider die Daten irgendwo auf der Welt lagern. Allerdings erwähnt er im gleichen Atemzug, dass die Swissness insofern eine Rolle spiele, weil hierzulande qualitative Standards hochgehalten würden und auch eine gewisse Rechtssicherheit gewährleistet werde. «Des Weiteren darf man sehr wahrscheinlich den psychologischen Aspekt nicht unterschätzen. Wenn der Provider in der Schweiz sitzt, kann ich ihm einen Besuch vor Ort abstatten; somit wird das Ganze einigermassen greifbar», sagt Rüdisüli.

«Die Swissness spielt sicher eine Rolle bei der Auswahl der Datencenter, denn lokale Gesetze und Richtlinien bezüglich Offenlegung von Daten können die Entscheidung für die Speicherung der Daten beeinflussen», meint auch Candid Wüest, Sicherheitsexperte und Mitglied des Symantec Security Response Teams. «Aber auch Schweizer Firmen sind nicht immun gegen Datenpannen, die zu Datenverlusten führen», gibt er zu bedenken. Somit sei klar, dass die Sicherheit der Daten einen hohen Stellenwert habe. «Werden beispielsweise alle Daten lokal voll verschlüsselt, kann es egal sein, wo diese gehostet werden», ist Wüest überzeugt. Er räumt aber auch ein, dass dies nicht immer praktikabel ist.

Ebenfalls vor zu viel Vertrauen in die Swissness von Herstellern und Providern warnt AdNovum-CEO Bruno Kaiser. Die Schweiz habe als Standort zwar viele Vorteile wie ein gutes Datenschutzgesetz, politische und wirtschaftliche Stabilität, gute und ordentlich gewartete Infrastruktur sowie eine Mentalität bei den Bereitstellern von Computing-Diensten, die Langfristigkeit, Sicherheitsbestreben und weniger kurzfristige Gewinnmaximierung im Auge haben. «Aber die reichen nicht», gibt Kaiser zu bedenken und verweist etwa auf den historischen Fall der Zuger Crypto AG, Herstellerin von Verschlüsselungslösungen, der Anfang der 1990er-Jahre eine Kooperation mit der NSA nachgesagt wurde. «Nur weil eine Firma schweizerisch ist, ist sie nicht automatisch besser oder sicherer», sagt er und kritisiert auch die Entscheidung des Bundes, künftig nur auf Schweizer Anbieter zu setzen. Gescheiter wäre es laut Kaiser, ein Zertifizierungsprogramm in die Wege zu leiten, das die Hersteller von Hardware und Software durchlaufen müssten, um als Lieferant infrage zu kommen. ←