

Sicherheit muss Chefsache sein

Abstimmung von Organisation und Prozessen ebenso wichtig wie die Technologie

Von Stefan Arm*

Sicherheit geht alle Firmenbereiche etwas an, denn sie betrifft nicht nur die IT, sondern auch die Geschäftsprozesse und die Organisation. Umfassende Sicherheitsprogramme müssten nach vierzig Jahren kommerzieller Informatik eigentlich überall selbstverständlich sein, man findet sie aber nur selten. Dies dürfte sich schnell ändern, da für das oberste Management das Thema Sicherheit zunehmend relevanter wird.

IT-Governance peilt die Unterstützung und Durchsetzung einer Firmenstrategie durch IT-Systeme an. Sie versucht also Business-Ziele eines Unternehmens mit den IT-Zielen abzustimmen. Zu diesen gehören auch die Security-Aspekte als integraler Bestandteil einer umfassenden Unternehmenspolitik. Erst jüngst eingeführte regulatorische Massnahmen und die wachsende Konvergenz der in den Unternehmen eingesetzten Software-, Hardware- und vor allem der aktuellen Netzwerktechnologien sorgen für eine Sensibilisierung und ein Umdenken des lange vernachlässigten Sicherheitsbereichs.

Ein Thema primär für Praktiker

Die Umsetzung einer konsequenten, vorsorglichen IT-Security-Politik ist nach wie vor erst bei wenigen Branchen – etwa bei den Finanzdienstleistern – anzutreffen. Das hat mehrere Gründe: Erstens kostet Sicherheit Geld. Laut einer im letzten Jahr publizierten Studie der Meta Group beansprucht sie einen Anteil von rund 5 bis 10 Prozent des gesamten IT-Budgets. Erfahrungsgemäss dürfte dieser Anteil im Schweizer Finanzumfeld bedeutend höher sein. Von den Investitionen in die Sicherheit entfällt rund ein Drittel auf die Absicherungsbereiche Gebäude, Netzwerk und Server, ein weiteres Drittel auf die Abschirmung der Software auf den Ebenen der Betriebssysteme, Applikationen und Werkzeuge sowie das letzte Drittel auf Notfallvorkehrungen für die Business Continuity wie Back-up und «Disaster Recovery». Zweitens ist oft unklar, wer im Unternehmen die Vorgaben macht, wie sichere IT-Lösungen zu gestalten seien. Obwohl das Problem der Security viele komplexe Aspekte in sich vereinigt, lassen sich drittens die meisten universitären Forscher von diesem Thema kaum bewegen. Auch die Lehre hilft also nicht weiter. Ist Security ein Fall nur für Praktiker?

Es scheint so. Einer der wenigen, der sich in der Schweiz damit akademisch befasst, ist der ETH-Privatdozent Hannes Lubich. Als ehemaliger Sicherheitsverantwortlicher der Bank Julius Bär und heutiger Mitarbeiter einer grossen amerikanischen Softwarefirma entpuppt auch er sich rasch als Praktiker. Der Sicherheitsexperte bezeichnet als wesentliche Aufgaben einer IT-Governance und damit einer Gesamt-Security einerseits die Definition von Vorgaben für den Betrieb der Informatik, andererseits die Überwachung und Steuerung der Informatik bezüglich Einhaltung der Vorgaben sowie die Erkennung und Behebung von Abweichungen als zentrale Probleme. Es verstehe sich von selbst, schreibt Lubich in der deutschen IT-Fachzeitung «Computerwelt», dass sich die Sicherheit keineswegs auf Technologie allein beschränke.

Zunehmende Ansprüche von aussen

Dem ist zuzustimmen. So werden heute vermehrt regulatorische Ansprüche von aussen an die Unternehmen herangetragen. Diese haben einerseits Auswirkungen auf den Einfluss der IT

auf den Geschäftsverlauf und nehmen andererseits leitende Unternehmensorgane vermehrt in die Verantwortung. So sind beispielsweise häufiger verschärfte Controlling-Bestimmungen etwa durch die Sarbanes-Oxley Act zu beachten. Dieses nach zwei Abgeordneten benannte Gesetz wurde infolge des Enron-Skandals letzten Sommer in den USA in Kraft gesetzt und ist für die Finanzberichte aller börsennotierten US-Unternehmen verbindlich. Ab 2005 gilt das Gesetz auch für deren Töchter und mittelbar auch für die Zulieferer. Diese Unternehmen müssen demzufolge nicht nur interne Kontrollstrukturen und -prozeduren für ihre Finanzberichte berücksichtigen, sondern deren Wirksamkeit auch belegen. Dazu sind prinzipiell sämtliche Geschäftsprozesse zu analysieren und zu dokumentieren. Dabei bleibt es nicht. Als weitere Auflagen kommen etwa die für Finanzinstitute relevanten Eigenkapitalregeln (Basel II), EBK-Richtlinien und Datenschutzgesetze hinzu. Alle diese rechtlichen Vorgaben müssen mit den technischen, operationellen und betriebsorganisatorischen Bedingungen und Möglichkeiten in Einklang gebracht werden.

Daten sichern und Prozesse definieren

In den Systemlandschaften der meisten Grossunternehmen wird die Security vermehrt als «stack» oder Stapel in alle IT-Betriebs-Schichten hineinverwoben. Dabei kommt der Abbildung der technischen, organisatorischen und operationellen Aspekte auf entsprechende betriebliche Strukturen, Weisungen, Richtlinien und Prozesse entscheidende Bedeutung zu. Im technischen Bereich zielen die Sicherheitsvorkehrungen primär darauf ab, Daten und Informationssysteme vor unerlaubtem externem und internem Zugriff zu schützen. Berechtigte Datenzugriffe wollen authentifiziert, verschlüsselt, kontrolliert, protokolliert werden und sollen trotzdem schnell erfolgen. Die Authentifizierungs- und Public-Key-Infrastruktur spielen in der Umsetzung eine zentrale Rolle. Dazu kommen operationelle Faktoren wie einfache Konfigurierbarkeit und hohe Skalierbarkeit für einen kostenoptimierten Betrieb und Unterhalt der Systeme. Die zentrale Herausforderung in heterogenen Systemumfeldern grösserer Unternehmen stellt im Internet-Zeitalter für die IT eine auf Evolution, Migration und Interoperabilität ausgerichtete Sicherheitsinfrastruktur dar. Im Unternehmen, aber auch im Management muss dafür aber zuerst ein besonderes Verständnis geschaffen werden. Dazu braucht es zum Beispiel Bedrohungsszenarien und das Aufzeigen der möglichen Kosten und Folgen für das Unternehmen und die Geschäftsprozesse bei einem Schadensfall oder bei der Einführung einer technologischen Neuerung.

Doch Letzteres kann die IT-Abteilung nicht allein erstellen, geschweige denn richtig beziffern. Hier helfen Business-Impact-Analysen und qualitative Risikoanalysen, wie sie beispielsweise vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen werden. Als

etwa die Finanzdienstleisterin PostFinance angefangen hat, ihre IT-Sicherheit zu überarbeiten und ihre unternehmensweiten Daten und Informationssysteme und deren Benutzer in ein neues Sicherheitsgesamtprogramm überzuführen, hat sie als eines der ersten Unternehmen hierzulande einen sogenannten Security Program Manager engagiert. Dieser fungiert auf Initiative des obersten IT-Managements als Gesamtkoordinator, der zwischen den einzelnen Projekten, den Security-Verantwortlichen und den verschiedenen involvierten Organisationseinheiten wie Logistik, Compliance und IT zu vermitteln hatte. Er stellte strategisch, taktisch und operationell sicher, dass Organisation, Prozesse und Technologien im Security-Bereich aufeinander abgestimmt sind und sich gemeinsam in der durch die IT-Sicherheitsstrategie vorgegebenen Richtung bewegen. Ziel des gesamten Projekts war es, alle IT-Security-Aktivitäten der PostFinance unter einen Schutzschild zu konsolidieren. Die Aggregation der Einzelteile sollte schliesslich mehr als die Summe der Einzelteile ergeben.

Richtlinien als Hilfsmittel

In der Regel ist ein solches Sicherheitsprogramm in einen übergeordneten Masterplan eingebettet, der dem Top-Management laufend zur Kontrolle der vielfältigen Aktivitäten dient. So werden etwa mit einer Schutzbedarfsanalyse die geschäftskritischen Daten, sozusagen die Kronjuwelen des Unternehmens, ermittelt. Sie zeigt auf, welche Anwendungen, Hardware, Netze, Gebäude und Teile der Energieversorgung mit welchen Massnahmen abgesichert werden müssen. Die anschliessende qualitative Risikoanalyse bewertet die Ist-Situation auf der Grundlage des ermittelten Schutzbedarfs. Aufgrund von Praxiserfahrungen lassen sich damit konkrete Massnahmen identifizieren und Kosten abschätzen. Für die Analysen des Soll-Zustands und die Massnahmenvorschläge stehen Hilfsmittel wie die Management-Leitlinien BS7799-2:2002 zur Verfügung. Diese informieren, wie sich der entsprechende ISO-Standard anwenden und vor allem wie sich ein sogenanntes Information Security Management System (ISMS) aufbauen, betreiben, unterhalten und optimieren lässt.

Speziell beim Sicherheitsprogramm wird schliesslich besonders darauf geachtet, dass die Aspekte Organisation und Prozesse mindestens gleich stark gewichtet werden wie die Technologie. Denn erfahrungsgemäss bringt die beste Technik wenig, wenn die Organisation nicht auf deren Einführung und Verwendung vorbereitet ist. Ein konsequentes Sicherheitsprogramm macht die IT-Infrastruktur nicht nur sicherer, sondern erlaubt es auch, dass ein Unternehmen das Security-Risk-Management im Griff hat und bei jedem neuen Erweiterungsprojekt optimal zwischen Kosten und Sicherheitsanspruch abwägen kann.

* Der Autor ist CEO und Gründer der Zürcher Software-Firma AdNovum Informatik.