

Informationssicherheit ist Chefsache



Informationssicherheit muss in der Chefetage angesiedelt werden – dieser Sachverhalt lässt sich nicht nur aus der geltenden Gesetzgebung herleiten, sondern auch aus den ureigensten Interessen einer Unternehmung, die vorhandenen Vermögenswerte nicht unverhältnismässigen Risiken auszusetzen und damit die Fortführung der Firma zu gefährden.

Text: **Ferdinand Kobelt**, dipl. Ing. HTL, Partner,
Head of Technology & Security Risk Services;
ferdinand.kobelt@ch.ey.com

Tom Schmidt, Betr.-Oek. FH, NDS IT Security FH, CISA, CISSP,
Manager, Technology & Security Risk Services;
tom.schmidt@ch.ey.com

□ Aus der neusten Informationssicherheitsstudie «Global Information Security Survey 2004»¹ von Ernst & Young geht hervor, dass Firmen keine ausreichenden Massnahmen gegen die wachsende Bedrohung ihrer Daten treffen. Die Chefs sind sich heute zwar der intern entstandenen Risiken für die Sicherheit ihrer Daten mehrheitlich bewusst, treffen aber dennoch keine dafür notwendigen Vorkehrungen. Über 70% der antwortenden Unternehmungen geben an, dass internes Training und Sensibilisierung nicht zu den wichtigsten Initiativen gehören.

Verantwortung für Sicherheit lässt sich nicht delegieren

Aus gesetzlicher Sicht (OR Art. 716a, 716b und 717) haben der Verwaltungsrat und die von ihm eingesetzten geschäftsleitenden Organe unter anderem die Aufgabe, die Aufsicht über die Befolgung der Gesetze, Statuten, Reglemente und Weisungen wahrzunehmen und die Interessen des Unternehmens im Hinblick auf die langfristige Erfüllung des in den Statuten erwähnten Unternehmenszwecks zu wahren. Auch wenn die Geschäftsleitung einzelne Aufgaben im Bereich Sicherheit an Mitarbeitende oder externe Dienst-

1 Die Studie ist im Internet unter www.ey.com/ch/tsrs abrufbar.

Begriffsdefinitionen

Verfügbarkeit:

Sicherstellung des bedarfsorientierten Zugriffs auf Informationen und die damit verbundenen Vermögenswerte durch berechnigte Benutzer

Integrität:

Sicherstellung der Korrektheit und der Vollständigkeit von Informationen und Verarbeitungsmethoden

Vertraulichkeit:

Sicherstellung, dass nur berechnigte Personen auf Informationen zugreifen können

leistungserbringer delegieren kann, bleiben die Aufsicht und die Überwachung bezüglich Einhaltung der Vorgaben im Verantwortungsbereich des Managements oder, anders ausgedrückt, der Chefs – Informationssicherheit ist und bleibt Chefsache!


Die Schutzziele der Informationssicherheit

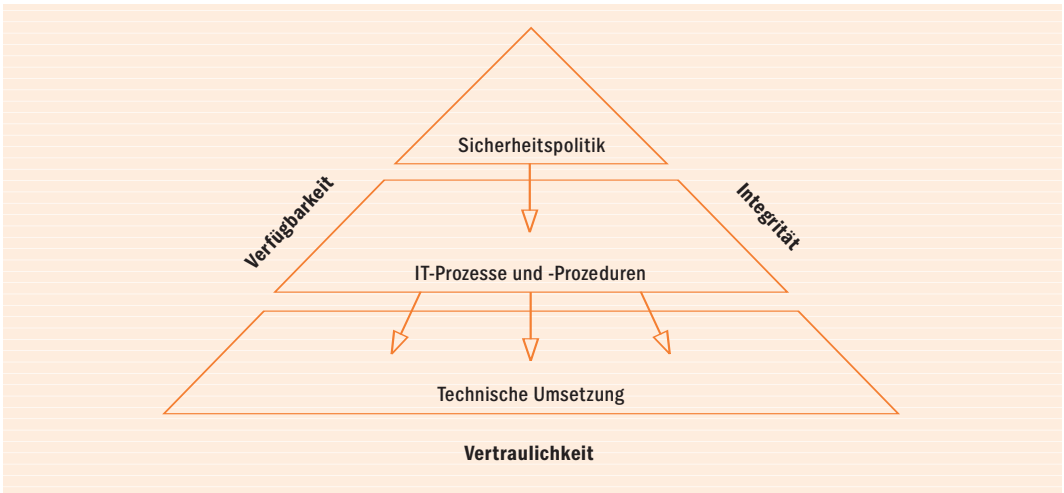
Mit der fortschreitenden Technologisierung und Automatisierung der Geschäftsprozesse und der Vernetzung der Systeme nimmt die Komplexität in der IT stark zu. Eine Unternehmung ist daher vielen neuen Risiken ausgesetzt – zum Teil bewusst, häufig jedoch unbewusst.

Bezüglich Informationssicherheit stellen vereinfacht dargestellt die folgenden drei Bereiche die zu berücksichtigenden Schutzziele dar: «Verfügbarkeit», «Integrität» und «Vertraulichkeit» (vergleiche Kasten). Von diesen drei Schutzzielen dürfte die «Verfügbarkeit» dem Management am geläufigsten sein, ist dieses Schutzziel aufgrund seiner wirtschaftlichen Bedeutung doch häufig Gegenstand von Vereinbarungen mit internen oder externen Informatik-Dienstleistungserbringern. Die beiden anderen Schutzziele sind jedoch ebenso wichtig, daher sollte ihnen dieselbe Auf-

merksamkeit beigemessen werden. In Bezug auf Buchhaltung und Rechnungslegung einer Unternehmung ist die Integrität der Daten und der zugrunde liegenden Prozesse von elementarer Bedeutung. Bezüglich Vertraulichkeit darf nicht vergessen werden, dass diese nicht nur wegen vertraulicher Unternehmensinformationen von Bedeutung ist, sondern dass vor allem auch Gesetze (z.B. das Datenschutzgesetz) entsprechend eingehalten werden müssen.

Das Sicherheits-Framework

Damit die erwähnten Schutzziele möglichst angemessen und ausgewogen berücksichtigt werden können, empfiehlt es sich, basierend auf einem Top-down-Vorgehen ein Sicherheits-Framework im Bereich der Informationssicherheit (siehe Grafik) zu definieren und dieses entsprechend umzusetzen. Neben den Sicherheitsvorgaben des Managements (Sicherheitspolitik) gilt es, den Informationssicherheitsgedanken auch in den Prozessen und Prozeduren zu verankern (u.a. durch Sicherheitskonzepte und -handbücher, Sensibilisierung der Mitarbeitenden usw.) und schliesslich auf technischer Ebene zu implementieren. Eine regelmässige Überprüfung 



stellt zudem sicher, dass das erreichte Sicherheitsniveau auch längerfristig aufrechterhalten werden kann. Nur auf diese Weise kann die Informationssicherheit durchgängig und möglichst umfassend angegangen werden. Andernfalls entsteht ein «Flickwerk», welches die Sicherheit in einzelnen Bereichen zwar erhöhen kann, die Gesamtsicherheit der Firma jedoch nicht nachhaltig positiv zu beeinflussen vermag.

Starker Fokus auf technische Massnahmen

In der Schweiz wird die Informationssicherheit jedoch nach wie vor sehr stark aus der technischen Perspektive betrachtet. Die Unternehmen investieren teilweise viel in Soft- und Hardware und haben dadurch das Gefühl, die Sicherheitsproblematik gelöst zu haben. Die eingangs erwähnte Studie von Ernst & Young zeigt jedoch auf, dass neben der Technologie auch der Umgang der Mitarbeitenden mit der Information wichtig ist. Anwender, Systembetreuer und Entwickler sollten deshalb mehr auf die Aspekte der Informatiksicherheit sensibilisiert werden. Dazu ist allerdings eine entsprechende Schulung notwendig.

Umdenken ist unerlässlich

Es braucht Veränderungen in der Denkart. Der Anstoss dazu sollte durch die Unternehmensleitung erfolgen, denn die Mitarbeitenden müssen spüren, dass Informationssicherheit vom Chef erwünscht ist. Auf oberster Ebene muss erkannt werden, dass durch Investitionen in die Sicherheit (Prozesse, Technologie, Überprüfung) letztlich viel Geld eingespart werden kann, da sich dadurch die Anzahl IT-Störungen und ausfälle reduzieren lässt und zusätzlich die Konkurrenzfähigkeit des Unternehmens verbessert werden kann.