

.02 Compliance als Chance für mehr Sicherheit

Michael Ghezze *

15|9|2008

Sicherheit wird vom Management oft als reine Kostenfrage gesehen. Zahlreiche rechtliche Neuerungen und wirtschaftliche Notwendigkeiten werden ein Umdenken erzwingen, meint Gerry Wallner, Mitglied der Geschäftsleitung der [Beck et al. Services GmbH](#). Er ist Experte für die Zusammenhänge zwischen Business und IT und stellt auf den Confare Seminaren der [www.cio-area.at](#) ein aktuelles White Paper zur Rolle der IT-Security in Unternehmen vor.

Inwieweit ist Sicherheit ein Thema, mit dem sich auch die Geschäftsführung befassen sollte?

Wallner: In Zeiten der Compliance, Governance, spielt der menschliche Faktor die größte Rolle, zusätzlich sind die gesetzlichen Anforderungen in der globalisierten Welt fast unüberschaubar geworden. Dies kann nunmehr keine Aufgabe der IT sein. Dies ist eindeutig eine Management Aufgabe. Abgesehen davon, durch die sogenannte „erweiterte Management Haftung“ ist das Management in persönlich haftbar falls der verordneten gesetzlichen Sicherheit und der damit im Vorfeld umzusetzenden Risikobewertung durch das Management eines Unternehmens nicht Genüge getan wird.

Dies betrifft inzwischen praktisch jedes Unternehmen, ob KMU oder weltweit tätiger Großkonzern. Stellen Sie sich das am Beispiel eines Automotive Zulieferbetriebes vor. Der Endkunde des Zulieferers ist der Fahrzeughersteller welcher deutlich mehr Gesetze (z.B Produkthaftung, SOX, EURO-SOX, KontraG) und diese auch noch weltweit zu erfüllen hat. Als KMU bin ich ein Teil der Lieferantenkette und bin damit auch ein Teil der Gesamtbetrachtung der Sicherheitskette des Herstellers.

Was sollte man beachten, wenn man das Thema (IT-) Sicherheit sauber angehen möchte? Wo passieren die grundlegenden Fehler?

Wallner: Eine Umsetzung ausschließlich durch Personal im Hause ist ein grundlegender Fehler, denn die Betriebsbrille macht blind. Man muss weg von einer technischen Betrachtung, die menschliche Komponente ist entscheidend. Denken Sie daran die Gefährdung der Sicherheit kommt heute zu über 80% vom eigenen Personal. Und dies noch nicht einmal bewusst. Ein schlechtes Arbeitsklima, oder ein frustrierter Mitarbeiter (Stichwort Innere Kündigung) der dem Arbeitgeber oder dem direkten Vorgesetzten zeigen möchte wie wertvoll er doch eigentlich ist, kann großen Schaden herbeiführen. Wenn man nun denkt der Mitarbeiter sei im Endergebnis dafür haftbar hat leider falsch gedacht, den im Endergebnis Management und die Unternehmensführung ist in der Endkonsequenz wiederum persönlich dafür verantwortlich & haftbar.

Welche organisatorischen und strategischen Herangehensweisen empfehlen Sie?

Wallner: Wichtig ist zu verstehen, dass das Thema Sicherheit eine gesamtheitliche, strategische Betrachtung und Herangehensweise verlangt. Wer weiß heute schon welchen Bedrohungen ich morgen ausgesetzt sein werde? Sie kennen das Sprichwort: „Der Dieb ist immer einen Schritt schneller als die Polizei“. Verhinderung und Betrachtung der eventuellen Risiken, deren Bewertung und Entscheidung durch das Management ist ein strategisches Thema. Organisatorisch muss das Unternehmen in der Lage sein neue Anforderungen oder Risiken schnell bewerten zu können. Dafür benötigen Sie Rollen, klare Verantwortlichkeiten, transparente Prozesse und vor allem KEINE isolierte Betrachtung der Sicherheit. Eine Bemerkung sei mir erlaubt. Man hört oft die Security im Unternehmen sei eher Verhinderer als Ermöglicher. Dies zeigt klar, dass

das Sicherheitsbewusstsein im Unternehmen noch nicht angekommen ist und hauptsächlich als Störfaktor denn als Überlebenssicherung gesehen wird.

Sind sich die Geschäftsführer der Bedeutung der Compliance-Anforderungen in der IT bewusst?

Wallner: Eindeutig nein. Die 8. Europäische Richtlinie, auch EURO-Sox genannt, ist vielen nicht bekannt. Dies wird fatale Auswirkungen ab dem nächsten Jahr haben. Das Urteils-Beispiel zu den „schwarzen Kassen“ vor einigen Wochen spricht hier eine klare Sprache. Auch wird oft gedacht, ich bin nicht an der Börse, nicht in den USA tätig und doch auch nur ein KMU. In der Lieferantenkette spielt dies keine Rolle, ihr Auftraggeber und Kunde mag aber davon betroffen sein und wird dies an sie als Anforderung durchreichen. Alleine um seine Compliance Anforderungen zu erfüllen. Die 8. Europäische Richtlinie betrifft auch kleinere Personen- oder Kapitalgesellschaften , z.B sind GmbH's erfasst. Hier ist dringender Handlungsbedarf und vor allem unbedingt Bewusstsein zu schaffen. Sonst könnte die Folge ein böses Erwachen sein.