# Unerkannte Gefahr

## Outsourcing-Trend gefährdet unternehmenskritische IT-Systeme

***IT-Sicherheit hat auf dem Radarschirm des Top Managements oft keinen Platz. Unternehmen gehen unbemerkt erhebliche Risiken für das Geschäft ein. Bestes Beispiel: eine große Retail-Bank konnte wegen eines Systemausfalls für mehr als drei Stunden auf kein einziges Kundenkonto zugreifen, die Kunden wurden nervös. Obwohl sich zuletzt hier viel verbessert hat, baut sich bereits die nächste unerkannte Gefahr für die IT-Systeme auf – der zunehmende Trend zum Outsourcing.***

IT-Outsourcing wird meist begründet mit Argumenten wie Kostensenkung, Effizienzverbesserung, Economies of Scope oder Innovationsfähigkeit. Wenn man jedoch im Vertrauen mit Top Managern spricht, dann hört man oft den eigentlichen Grund für die Auslagerung dieser Funktion – die IT-Truppe verursacht immer nur Probleme, anstatt sie zu lösen, sie ist teuer und hält nie ihre Versprechen. Außerdem versteht man diese Leute nicht. Also: warum gibt man das ganze Thema nicht einfach ab an jemanden, der sich damit wirklich beschäftigen will.

Hierin liegt ein Grundübel der IT-Funktion: das Top Management möchte sich eigentlich nicht damit auseinander setzen, denn IT wird nicht als wichtiges Management-Thema begriffen. Hier verbirgt sich aber auch die Ursache für eine noch weitgehend unerkannte Gefahr, die viele Unternehmen in ihrer Substanz bedroht: man glaubt, auch das Systemrisiko mit auslagern zu können. Weit gefehlt!

**Risiko lässt sich nicht „outsourcen“**
Das Risiko trägt immer das Geschäft, man kann es nicht auslagern. Es lässt sich abfedern durch Versicherungsverträge oder durch operative Regelungs- und Kontrollmaßnahmen. Aber wenn ein System ausfällt, tritt der Schaden immer im Geschäft ein. Man stelle sich ein Mobilfunkunternehmen vor, das wegen eines Fehlers in den Kernanwendungen für zwei Tage die Telefonate der Kunden nicht exakt vermitteln und nicht erfassen kann - ein Umsatzausfall von mehr als einem Prozent und ein unglaublicher Schaden für Markenname und Image. Wie hoch ist der Schaden? Wer soll das bezahlen? Wie kann die Ursache präzise und justiziabel ermittelt werden? Wie viele Jahre gehen ins Land, bis der Systembetreiber schließlich einen Teil des Schadens übernimmt?

**Outsourcing steigert das IT-Systemrisiko erheblich**
Das Geschäftsmodell der großen IT-Dienstleister basiert auf einem einfachen und sehr wirksamen Mechanismus – „Reduce unauthorized work, avoid requirement churn!“ Der Outsourcing-Vertrag sorgt dafür, dass nach Übergabe des Systembetriebs an den IT-Dienstleister umgehend alle unautorisierten Tätigkeiten eingestellt oder nur gegen Extrabezahlung ausgeführt werden. In der Konsequenz werden alle undokumentierten Abstimmungs- und Erfüllungsprozesse, alle informellen Beziehungen zwischen Fachbereich und Systemtruppe und alle „kleine Dienstwege“ mehr oder weniger gründlich ausgelöscht.

Und hier liegt das Problem - Risikomanagement im Systembetrieb läuft im Tagesgeschäft operativ zum größten Teil über den kleinen Dienstweg. Diese Tatsache wird

häufig erst erkannt, wenn es zu spät ist. Denn die IT-Mitarbeiter wurden bei der Vorbereitung des Outsourcing Deals nicht gefragt, der Outsourcer selbst hat meist kein Interesse, vor Vertragsunterzeichnung auf die Risiken hinzuweisen, und das Management hat keine Vorstellung davon, wie das Systemgeschäft im Detail abläuft.

Es gibt also einen guten Grund, dass das BaFin die neuesten Outsourcing Deals der Großbanken mir sehr viel Argwohn unter die Lupe nimmt. Der Grund ist, dass selbst das Top Management dieser weitestgehend von IT-Systemen abhängigen Unternehmen nur zögernd die Bedeutung der Aufgabenstellung des IT Risk Managements gerade im Outsourcing Fall erkennen will.

**IT-Risikomanagement ist Kernaufgabe des Top Managements**

Das Risikomanagement darf nicht blauäugig dem IT-Dienstleister überlassen werden, denn er hat im Grunde kein wirkliches Interesse daran. Der Abnehmer selbst trägt letztendlich die Verantwortung dafür. Diese Herausforderung bekommt man in den Griff, indem man eine qualifizierte Truppe installiert, die im Vorlauf zum Outsourcing, aber auch beim Übergang und später während des externen Systembetriebs das IT-Risiko systematisch identifiziert, bewertet und geeignete Gegenmaßnahmen initiiert. Diese Mannschaft muss ein gutes Geschäftsverständnis und gleichzeitig eine intime Kenntnis des Systembetriebs mitbringen. Die Aufgabe darf nicht einer klassischen Stabsabteilung übertragen werden. Denn die Truppe benötigt im Notfall direkte Verfügungsgewalt und uneingeschränkten Zugang zum Top Management.

Die Deutsche Bank nimmt hier übrigens wie so oft eine Vorreiterrolle ein. Sie hat im Laufes dieses Jahres auf oberster Ebene ein globales Risk Management für IT Systeme installiert – ein Vorbild sicherlich nicht nur für die Bankenwelt!

Autor:
Peter Jumpertz
Senior Partner
Theron Business Consulting GmbH
Schlüterstraße 38
10629 Berlin
pej@theron.com
Tel. 030 – 864 9920
Fax 030 – 864 99299