

## 1 Business Continuity und Risk Management

Das Risiko für die unternehmerische Sicherheit und die Geschäftsabläufe wächst aus der Perspektive der IT-Sicherheitsverantwortlichen ständig. Gründe hierfür sind erhöhte Gefahrenpotenziale durch Sabotage, Vandalismus und Terrorismus, die zunehmende Komplexität einzelner Prozesse und der Infrastrukturen sowie nicht zuletzt die immer höhere Zahl der IT-gestützten Prozesse in den Unternehmen. Dies und neue gesetzliche Anforderungen wie SOX, Basel II und KontraG liefern vielfältige Herausforderungen für die verantwortlichen Manager. Es besteht ein klarer Bedarf an umfassenden Business Continuity Konzepten.

Zunächst erfolgt ein professionelles Risk Assessment. Es hilft, mögliche Risiken zu erkennen, sie richtig zu bewerten und damit auch geeignete Maßnahmen zur Prävention, Risikovermeidung, Reduzierung der Schadenshäufigkeit oder -höhe sowie Risikoüberwälzung (Versicherungen oder Dienstleistungsvereinbarungen) zu definieren oder auch als nicht vermeidbar per Risk Acceptance zu akzeptieren. Dann sind, dem Risikopotenzial entsprechende, Wiederanlauf- und Notfallpläne zu schaffen.

Das Ergebnis eines solchen Prozesses ist oft eine ganz neue Transparenz im Unternehmen: Welche Prozesse haben den größten Einfluss auf den Unternehmenserfolg? Von welchen Anwendungen, Daten, Menschen und Infrastrukturen hängen diese wirklich ab? Worauf kann wie lange verzichtet werden? Die möglichen Risiken zu kennen, heißt sie beherrschbar zu machen. Da überrascht es nicht, wenn zahlreiche Studien zu dem Ergebnis kommen, dass krisensichere Unternehmen auch in Normalsituationen wirtschaftlich erfolgreicher sind!

Im Workshop werden Beispiele und Lösungsansätze diskutiert und mögliche Handlungsempfehlungen erarbeitet.

**Workshop-Leitung:** Monika Wohlrabe,  
ASIC Allianz Shared Infrastructure Services

**Co-Moderation:** Hans-Dieter Stangl, netsecure