

Keine halben Sachen



Die Vorgaben von Basel II können Banken veranlassen, bei der Bonitätsbewertung eines Unternehmens auch die Sicherheit der EDV in Augenschein zu nehmen. Bestimmte Sicherheitsstandards sollten aber ohnehin erfüllt sein.

Nick Leeson hatte es leicht. Der Wertpapierhändler der Londoner Barings Bank kaufte und verkaufte an asiatischen Börsen und kontrollierte sich dabei selbst. Am Ende standen 1,2 Milliarden Euro Verlust, der Bankrott eines altherwürdigen Kreditinstituts – und einer der spektakulärsten Betrugsfälle in der Bankenbranche. Der Fall von 1995 war einer der Auslöser dafür, dass der Basler Ausschuss für das Bankenwesen seine Empfehlungen

für den Schutz von Einlagen neu formuliert hat – das Ergebnis: Basel II. Seit Anfang des Jahres gelten die Bestimmungen auch in Deutschland, hierzulande übrigens in den Solvabilitätsverordnungen festgehalten. Das Besondere: Nicht nur Risiken durch Betrugerein à la Leeson und Schäden durch andere Verfehlungen sollen verhindert und minimiert werden, in die Verordnungen fanden auch solche Risiken Eingang, die den EDV-Bereich

betreffen. Kreditnehmer sind von den Bestimmungen zwar nur mittelbar betroffen, denn in erster Linie sind die Kreditinstitute selbst angehalten, sowohl ihre Hard- und Software als auch die Organisation im IT-Bereich genauer im Blick zu haben, Risiken einzuschätzen und gegebenenfalls mit vertretbarem Aufwand zu minimieren. Doch um ihr eigenes Risiko zu mindern, können Banken nun auch die EDV ihrer Kunden überprüfen und

darauf schauen, ob ein Virus die Produktionsanlagen lahm legen, ein Feuer die Server vernichten oder ein Hacker die Kundendatenbank löschen könnte. Bedeuten aber Unsicherheiten in der EDV tatsächlich schlechtere Kreditkonditionen? „Im Detail ist das nicht ganz so einfach“, sagt Dr. Andreas Huber, Bereichsleiter Kreditrisiko- und Portfolio-Analysen bei der Creditreform Rating AG. „Doch im Prinzip ist das so.“

Einfluss auf Bonitätsbewertung

Eine zentrale Vorgabe von Basel II ist die folgende: „Operationelles Risiko ist die Gefahr von Verlusten, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten.“ Im Detail nennen die Bestimmungen Verluste, die durch den Ausfall von Hard- und Software oder der Telekommunikation entstehen können sowie durch Hackeraktivitäten oder den Diebstahl von Informationen. Den genauen Einfluss dieser Kriterien auf die Bonitätsbewertung bewerten Rating-Experten mit verschiedenen Formeln. Bei alledem ist aber klar: Zur IT-Sicherheit ist das Management von Unternehmen auch abseits von Basel II verpflichtet. Vorstände etwa können rechtlich persönlich belangt werden, wenn sie zukünftigen Risiken, die auch die EDV betreffen, nicht mit geeigneten Maßnahmen begegnen. Gleiches gilt für Kaufleute und auch GmbH-Geschäftsführer, denn auch ihnen sind IT-Sorgfaltspflichten auferlegt. Darüber hinaus sind bestimmte Berufsgruppen wie Ärzte oder Anwälte rechtlich verpflichtet, die Daten ihrer Kunden so aufzubewahren, dass sie nicht in die Öffentlichkeit gelangen. Natürlich gehen die entsprechenden Gesetzestexte wie das AG- oder das GmbH-Recht, die Datenschutzrichtlinien und auch Basel II nicht auf technische Details ein, wie Risiken zu minimieren sind. Was die Gesetze und Verordnungen und im Zweifel auch Richter verlangen, ist ein gutes Stück gesunder Menschenverstand, die Orientierung an üblichen Standards und Transparenz. Die Risiken erkennen, sie gemäß ihrer möglichen wirtschaftlichen Folgen für das Unternehmen einschätzen und angemessen mini-

mieren, so lautet – vereinfacht gesagt – die Formel. Detailliertere Hilfen bieten hierzu die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch die Definitionen verschiedener ISO-Normen. Eine Zertifizierung ist zwar nicht immer gewünscht, in manchen Branchen aber können sie ein Wettbewerbsvorteil sein. Und natürlich bieten auch externe Dienstleister bezahlte Unterstützung an. Für einen niedrigen vierstelligen Betrag kommen Experten für mehrere Tage ins Haus, analysieren und geben Empfehlungen.

Dass das Aufspüren von Risiken auch solche zutage fördern kann, gegen die kaum ein Kraut gewachsen ist, liegt dabei in der Natur der Sache. Aber selbst eine einfache Datensicherung scheint vielen Unternehmen nicht so wichtig zu sein. Studien zufolge verfügen bis zu 30 Prozent der kleinen und mittelständischen Unternehmen nicht über Systeme, um ihre Daten zu sichern. „Es kann nicht sein, dass Unternehmen ihre geschäftliche Basis riskieren, weil sie ihre Daten nicht sichern“, sagt Elke Flachberger, Beraterin der Wiesbadener K&P Computer Service- und Vertriebs GmbH, die Konzepte für Datensicherheit und Backup-Systeme anbietet.

Grundsätzlich empfehlen Experten, die IT-Sicherheit auf die geschäftlichen Ziele auszurichten. Beim Thema Datensicherung würde das bedeuten, dass zum Beispiel eine Druckerei die Druckdaten ihrer Kunden sichern wird, um bei einer Havarie die Aufträge weiter abarbeiten zu können und nicht gleich in die Pleite zu rutschen. Einem Handwerker dagegen sind vielleicht nur die Daten der Finanzbuchhaltung wichtig, um auch nach einem Absturz des Systems weiter Rechnungen und Mahnungen verschicken und das Geschäft am Laufen halten zu können.

„Business Continuity“ nennen das Experten, und wer so ein Konzept verfolgt, sollte es möglichst durchgängig tun. Motto: Keine halben Sachen. Fast schon zu den „modernen Sagen“ gehören Geschichten, in denen ein Band mit gesicherten Daten wahlweise bei einem Feuer im vermeintlich sicheren Safe des Geschäftsführers dahin schmorte oder nicht bemerkt wurde, dass es gar nicht die aktuell-

ten Daten enthielt, weil das Bandlaufwerk seit längerem defekt war. Solche vermeintlichen Legenden allerdings sind mitunter durchaus real und teuer. So hat das Oberlandesgericht Hamm die Klage eines Unternehmens auf Schadenersatz in Höhe von 14.000 Euro gegen einen IT-Dienstleister abgewiesen, der bei Wartungsarbeiten einen Serverausfall mit Datenverlust verursacht haben soll. Zum Einen ließ sich der Fehler nicht auf die Arbeiten des Dienstleisters zurückführen, zum Anderen hatte das Unternehmen seine Daten zwar gesichert, allerdings in unregelmäßigen Abständen.

Unsicherheit von innen

Um nicht selbst zur traurigen Legende zu werden, empfiehlt Beraterin Elke Flachberger automatisierte Back-ups nicht nur der geschäftlichen Daten, sondern auch der Einstellungen der Hard- und Software sowie der Profile der Mitarbeiter, damit sich bei einem Serverabsturz das System schneller wieder aufbauen lässt. Dazu sollten mit regelmäßigen Recovery-Tests die Back-ups überprüft werden und im Zweifel die Datenträger nicht in den Geschäftsräumen lagern.

Gerade im Bereich Sicherheit ist bei Maßnahmen und Kosten nach oben hin freilich reichlich Platz. So mag man zum Beispiel zu Recht bezweifeln, ob selbst ein kleines Unternehmen, dessen originärer Geschäftszweck zudem nicht auf Informationstechnik beruht, eine ausgefeilte IT-Security-Policy mit Notfallmaßnahmen und Verhaltensvorschriften für die Mitarbeiter benötigt. Sobald zum Beispiel aber Rechner von Mitarbeitern mit dem Internet verbunden sind, kommt man um bestimmte betriebliche Vereinbarungen kaum herum – und sei es nur der Hinweis, Dateianhänge in E-Mails mit unbekanntem Absender nicht zu öffnen.

Dirk Schäfer

Link-Service

Möchten Sie mehr Informationen zum Thema? Einfach eine E-Mail mit dem Betreff „Basel II“ an creditreform-service@vhb.de senden.