Basel II ab 2007 gesetzliche Pflicht: Schub für den IT-Projektmarkt?

(April 2006)

Inhalt dieses Artikels:

Mitte Februar dieses Jahres verabschiedete das Bundeskabinett den Gesetzesentwurf zur Umsetzung der Banken- und Kapitaladäquanzrichtlinie, besser bekannt unter dem Namen "Basel II". Damit sind Banken und Finanzinstitute in Deutschland ab 2007 gesetzlich verpflichtet, die Vorgaben des Basel II Abkommens umzusetzen. Für kreditsuchende Unternehmen bedeutet das vor allem, mehr in ihre IT-Sicherheit zu investieren, denn diese spielt für die Kreditvergabe eine noch größere Rolle als bisher.

Mit dem gesetzlichen Inkrafttreten von Basel II werden Banken und Finanzinstitute eine individuelle Bonitätseinschätzung des Kreditnehmers durchführen. Anhand dieser wird ermittelt, wie hoch das Ausfallrisiko des kreditsuchenden Unternehmens ist, also mit welcher Wahrscheinlichkeit der Kredit an die Bank zurückgezahlt werden kann. Je höher das Ausfallrisiko ist, desto mehr eigenes Kapital muss die Bank für den Kredit bereitstellen. Diese Pflicht wiederum gibt sie dann durch höhere Kreditkonditionen an das Unternehmen weiter.

Bessere Kreditkonditionen durch höhere IT-Sicherheit

Die Bonitätsprüfung führen die Banken anhand interner und externer Ratingverfahren durch. Neben allgemeinen Markt- und Kreditrisiken werden im Prüfverfahren auch operationale Risiken des Kreditnehmers berücksichtigt. Besonderes Augenmerk liegt hierbei auf dem operationalen Risiko "IT-Sicherheit". Warum? Zahlreiche Unternehmensprozesse hängen von einer funktionierenden IT-Infrastruktur ab. Fällt diese aus, steht nicht selten der ganze Betrieb still. Damit ist eine stabile, sichere IT ganz mitentscheidend für den Unternehmenserfolg. Aus diesem Grund prüfen die Banken, ob und inwieweit der Kreditnehmer Sicherheitsvorkehrungen getroffen hat, die ihn vor einem IT-Ausfall schützen. Dazu zählt aber weit mehr als nur die Installation von Antivirenprogrammen, Firewalls oder Datensicherungssystemen, denn neben der Technik spielen auch organisatorische und personelle Rahmenbedingungen eine wichtige Rolle. So stellt meist der Mensch ein weitaus unkalkulierbareres Risiko dar als die Technik. Dem muss durch entsprechende Sensibilisierung bzw. vertragliche Regelungen ebenso vorgebeugt werden.

Seitens des Bankenausschusses oder der Regierung gibt es bislang jedoch keinen Anforderungskatalog zur IT-Sicherheit. Der IT-Security Consultant Stefan Reelsen von der Firma reelance it consulting empfiehlt: "Einen guten Überblick bietet das Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI). Das Handbuch beschreibt die Sicherheitsmaßnahmen, die in keinem Unternehmen fehlen dürfen. Allerdings darf diese Zusammenstellung von Anforderungen nicht als schlüsselfertige Lösung gesehen werden, vielmehr stellt sie eine Basis dar. Das 'one-size-fits-all' Konzept, das die individuelle Einzelbetrachtung des Unternehmens, seiner Ziele und Risiken ersetzt, kann es nicht geben. Neben der technologischen Sicherheitsbetrachtung ist es erfolgskritisch, das Gesamtbild der Informationssicherheit nicht aus den Augen zu verlieren. Kaum jemand würde beispielsweise heute noch auf die Idee kommen, seine Haustür in Abwesenheit offen stehen zu lassen. Ebenso ist das Thema 'Physical Security' in keinem Unternehmen mehr fremd. Auf der anderen Seite neigen eine Reihe von Menschen dazu, einen Zweitschlüssel unter der Fußmatte oder im nächsten Blumentopf zu platzieren. Analog dazu sind Notizzettel mit Passwörtern am Monitor oder unter der Tastatur in Unternehmen mindestens ebenso gängige Praxis. Ein Sicherheitskonzept ist grundsätzlich nur so stark, wie das schwächste Glied in seiner Kette. Und das ist zumeist nicht die Technologie, sondern der Mensch. Nach einer britischen Umfrage würden 71 % der auf der Straße befragten Personen ihr firmeninternes Passwort für eine Tafel Schokolade verraten, 37 % nannten es bereits auf bloße Nachfrage", gibt Reelsen zu Bedenken.

Mehr Nachfrage durch mehr Investitionen?

Mit einem gut dokumentierten IT-Risiko-Management können Unternehmen die Chance auf günstige Kreditkonditionen durchaus erhöhen. Eine lückenhafte IT-Infrastruktur dagegen ergibt eine wesentlich schlechtere Kreditsituation, da in einem solchen Fall das Ausfallrisiko für die Bank eindeutig höher ist. Im Klartext heißt das für Unternehmer, dass sie sich nicht nur intensiver mit IT-Sicherheit befassen, sondern gegebenenfalls auch mehr in diese investieren müssen, wenn sie adäquate Kredite erzielen wollen.

Es ist also naheliegend, dass die Umsetzung der Basel II Vorgaben die Nachfrage nach externen IT-Spezialisten vorantreibt. Die Erwartungen sollten aber nach Ansicht von Stefan Reelsen nicht überschätzt werden: "Der gegenwärtig zu erwartende Anstieg der Nachfrage aufgrund von Basel II darf aus meiner Sicht nicht überbewertet werden. Die IT-Sicherheit ist aufgrund der immer weiter steigenden Abhängigkeit von der Informationstechnologie im operativen Geschäft eines jeden Unternehmens ein wichtiger Faktor. Im Bezug auf die Kreditrichtlinie handelt es sich jedoch nur um einen Baustein unter vielen. Auf der anderen Seite ist insgesamt ein Trend erkennbar, der der Sicherheitsthematik nicht zuletzt aufgrund steigender Komplexibilität der Bedrohungsszenarien einen höheren Stellenwert einräumt. Basel

II wird diesen Trend zweifelsohne befördern."

Neben Spezialisten mit produktspezifischem Know-how seien vor allem Berater gefragt, die in der Lage sind, die gesamte Prozesskette der Verarbeitung und Speicherung von Informationen zu betrachten und individuelle Schutzkonzepte entwickeln und umsetzen. Hierbei würden nichttechnische Themen eine bedeutende und oftmals unterschätzte Rolle einnehmen, so Reelsen weiter.

Schutz kleiner und mittlerer Unternehmen

Um kleine und mittlere Unternehmen (KMU) zu entlasten, hat die Regierung im Gesetzesentwurf eine sogenannte Mittelstandskomponente eingebaut. Diese sieht vor, dass Banken Kredite von unter einer Million Euro der Forderungsklasse "Retail" (wie für Privatpersonen) zuordnen können. Dann erhält der Kredit, unabhängig von der Höhe des Jahresumsatzes, ein um 25 % niedrigeres Risikogewicht als ein Unternehmenskredit. Mit diesem Mittelstandspaket reagiert die Regierung auf durchgeführte Untersuchungen, nach denen KMU im Schnitt eine höhere Ausfallwahrscheinlichkeit als Großunternehmen aufweisen. Deshalb wären Mittelstandskredite mit höheren Mindesteigenkapitalanforderungen belastet als Kredite an Großunternehmen, was schlechtere Kreditkonditionen für den Mittelstand zur Folge hätte.

Handlungsbedarf vielerorts noch notwendig

Doch Mittelstandspaket hin oder her, insgesamt gesehen werden Unternehmen durch die gesetzliche Umsetzung von Basel II stärker in die Pflicht genommen, ihre IT-Sicherheit zu analysieren und gegebenenfalls zu verbessern. Doch wie stehen Unternehmen dem Thema gegenüber bzw. ist es für sie überhaupt eines? Der IT-Security-Experte weiß: "Basel II ist für Unternehmen definitiv ein Thema, schließlich geht es um zukünftige Zinsbelastungen für Investitionen im Rahmen von Bankkrediten. Insbesondere bei mittelständischen Unternehmen besteht jedoch bislang noch ein Informationsdefizit und damit verbunden nicht selten dringender Handlungsbedarf."

Mit einem sprunghaften Anstieg der Investitionen für IT-Security ist nach Meinung von Reelsen aber nicht zu rechnen. Das Wachstum dieses Bereichs sei jedoch unverkennbar und sicherlich kein Hype, sondern ein Basisbaustein nachhaltiger Geschäftssicherung. "IT-Security ist ein Prozess, der in den verschiedenen Stadien der Unterstützung unterschiedlich spezialisierter Experten bedarf. Die meisten Unternehmen sind daher sehr gut beraten, dieses Know-how extern einzukaufen", so Reelsen.

Die gesetzliche Verpflichtung zur Umsetzung von Basel II ab 2007 wird die Nachfrage nach entsprechenden IT-Spezialisten sicherlich positiv beeinflussen und festigen, auch wenn der ganz große Schub ausbleiben wird. Langfristig gesehen wird aber das Thema "IT-Sicherheit" angesichts der wachsenden IT-Abhängigkeit sowie immer ausgefeilteren Bedrohungsszenarien für Unternehmen eine existentielle Rolle spielen und damit zu einem nachhaltigen Bedarf an IT-Security-Experten führen.

Der Gesetzesentwurf "Umsetzung von Basel II in nationales Recht" ist beim Bundesministerium der Finanzen abrufbar.

Stefan Reelsen ist CISSP zertifiziert und arbeitet als freiberuflicher IT-Security Consultant für Großkonzerne und mittelständische Unternehmen, vorwiegend in Europa. In dem breiten Spektrum seiner Tätigkeitsfelder bildet die Beratung zu Sicherheitsaspekten im Bereich der Netzwerk- und Kommunikationslösungen einen Schwerpunkt. Mehr Informationen zu seiner Person erhalten Sie unter http://www.reelance.com/.