Recht allgemein

Neue Vorgaben für IT-Sicherheit in Banken

Die Europäische Bankenaufsicht ist von London in den Europlaza-Turm in La Défense, Paris übersiedelt. (c) Bloomberg (Christophe Morin)

15.09.2019 um 17:31

von **Oliver Völkel**

Die europäische Bankenaufsicht hat neue Richtlinien erlassen, die vor allem, aber nicht nur die Auslagerung von EDV betreffen.

Wien. IT-Systeme spielen in allen Lebensbereichen eine immer wichtigere Rolle. Auch in Banken geht ohne IT heute kaum noch etwas. Diese Abhängigkeit von IT stellt freilich ein beträchtliches Risiko dar, wie wohl jeder zu berichten weiß, der bereits einmal wegen eines Windows-Updates zu einer Kaffeepause gezwungen worden ist. Fällt die IT aus, fällt alles aus.

Das Risiko, das bereits allgemein von der IT-Abhängigkeit ausgeht, wird heute oft durch einen weiteren Faktor verschärft. Das Schlagwort dazu heißt Outsourcing oder Auslagerung. Wer Aufgaben an Dritte auslagert, kann daraus in aller Regel einen Wettbewerbsvorteil lukrieren. Anstatt selbst die notwendige Infrastruktur zu betreiben, Prozesse zu schaffen und Mitarbeiter zu beschäftigen, wird die Aufgabe an einen spezialisierten Dienstleister ausgelagert. Das ist auch bei IT-Prozessen mittlerweile gängige Praxis. Schlagworte wie Cloud-Computing oder „Software as a Service“ zeigen, dass die Auslagerung von IT an Dritte bereits üblich ist.

Wer seine IT-Prozesse an Dienstleister auslagert, der setzt sich dadurch allerdings auf einen Schlag völlig neuen Risken aus. Auf einmal ist nicht mehr der Ausfall der Hard- oder Software das einzige Risiko, sondern der Dienstleister selbst kann zum Risiko werden: Etwa dann, wenn der Dritte seine Dienstleistung nicht oder schlecht erbringt, oder wenn er zum Einfallstor für Spionage oder Sabotage wird.

Dass der Finanzsektor solchen Risken mit besonderer Vorsicht begegnen muss, hat der Ausschuss der Europäischen Aufsichtsbehörden für das Bankwesen (CEBS) bereits vor über einem Jahrzehnt erkannt und 2006 entsprechende Leitlinien zum Umgang mit diesen Risken erlassen. Im Februar diesen Jahres hat die Europäische Bankenaufsichtsbehörde (EBA) als Nachfolgebehörde der CEBS nun neue Leitlinien für die Auslagerung im Bankensektor erlassen (EBA/GL/2019/02). Die Leitlinien treten am 30. September 2019 in Kraft und ersetzen die alten CEBS-Leitlinien.

Obwohl es sich bei den neuen EBA-Leitlinien im Grunde genommen um unverbindliche Empfehlungen handelt, sind sie für die Bankenpraxis dennoch von größter Bedeutung. Einerseits geben sie vor, in welchem Rahmen die österreichische Finanzmarktaufsicht (FMA) ihren Prüfungsauftrag wahrnehmen wird. Andererseits erlangen sie über einen Umweg doch quasi-verbindliche Wirkung. § 39 BWG legt nämlich die allgemeinen Sorgfaltspflichten von Geschäftsleitern in Banken fest, und wer als ordentlicher Geschäftsleiter gelten will (Achtung: Haftung!), der wird sich wohl auch mit den EBA-Leitlinien auseinandersetzen müssen. Die FMA hat im Übrigen angekündigt, die Prüfung der IT-Sicherheit heuer zu einem ihrer Schwerpunktthemen zu machen.

Einkauf nicht mehr erwähnt

Für die Bankenpraxis ergeben sich aus den neuen Leitlinien durchaus Herausforderungen. Neu ist etwa bereits der Anwendungsbereich. Die Leitlinien gelten nur für Auslagerungen. Das sind Vereinbarungen zwischen einem Institut und einem Dritten, auf deren Basis der Dritte einen Prozess, eine Dienstleistung oder eine Tätigkeit ausübt, die ansonsten von dem Institut selbst ausgeübt werden müsste. Die alten CEBS-Leitlinien stellten diesem Begriff noch den Begriff des Einkaufs gegenüber. Der Einkaufsbegriff fehlt allerdings in den neuen Leitlinien, eine nicht unwesentliche Auslegungshilfe ist damit weggefallen.

Einer der Kernpunkte der EBA-Leitlinien ist die genaue Auseinandersetzung mit dem ins Auge gefassten Dienstleister, noch bevor ein Vertrag geschlossen wird. Institute müssen künftig im Rahmen einer Due-Diligence-Prüfung feststellen, ob der Dienstleister überhaupt die notwendigen Kenntnisse und Ressourcen, aber auch organisatorischen Strukturen vorweisen kann und die erforderlichen regulatorischen Berechtigungen und Registrierungen erfüllt.

Endet die Due-Diligence-Prüfung positiv, so schreiben die neuen EBA-Guidelines detaillierte Anforderungen an den Vertragsinhalt vor, wenn wichtige Tätigkeiten ausgelagert werden. Die Leitlinien enthalten hierzu nicht weniger als 17 Vorgaben, die etwa das anwendbare Recht betreffen oder die finanziellen Verpflichtungen, den

genauen Leistungsumfang, Subauslagerungen an Dritte, den Umgang mit Daten, Kündigungsmodalitäten, Ausstiegsstrategien, Versicherungspflichten, Notfallplanungen, Überwachungsrechte oder Berichtspflichten.

Serviceverträge aller Art

Zwei Vorbemerkungen in den EBA-Leitlinien dürften für die Praxis besondere Bedeutung erlangen. So führt die EBA einleitend aus, dass jede Form der Servicierung durch Dritte Risken berge, nicht nur Auslagerungen im oben definierten Sinn. Daher sollen bestimmte Anforderungen in den Leitlinien für alle Vereinbarungen gelten, selbst wenn sie keine Auslagerung betreffen. Das heißt: Die Leitlinien können für alle Arten von Serviceverträgen maßgeblich werden. Wie das in der Praxis gelebt wird, bleibt abzuwarten.

Die neuen EBA-Leitlinien legen eine Reihe weitere Anforderungen fest. Als Teil des Risikomanagements sollen Institute beispielsweise ein Register über alle Auslagerungen führen. Weiters ist für den Fall vorzukehren, dass ein Dienstleister die ausgelagerte Leistung nicht mehr ausreichend erbringt. Das Ziel des Instituts muss es in diesen Fällen sein, einen raschen und reibungslosen Wechsel zu gewährleisten, der nicht zu einer Unterbrechung des Geschäftsbetriebs führt.

Die Leitlinien enthalten auch umfassende Überprüfungs- und Überwachungspflichten, die auf ein ganzheitliches, institutsweites Risikomanagement abzielen. Institute können sich freilich nicht auf die Leitlinien verlassen, sondern sind weiterhin selbst dazu verpflichtet, sämtliche mit einer Auslagerung verbundenen Risken zu identifizieren und geeignete Maßnahmen zu implementieren.

Die EBA-Leitlinien geben vor, dass alle Auslagerungen den neuen Standards entsprechen sollen, die ab 30. September 2019 vorgenommen werden. Darüber hinaus sollen Institute alle bestehenden Auslagerungen überprüfen und erforderlichenfalls Verträge nach- oder neu verhandeln. Für bereits bestehende Auslagerungsverhältnisse sehen die Leitlinien eine Umsetzungsfrist bis 31. Dezember 2021 vor. Wer sich als Geschäftsleiter bis dato noch nicht mit den neuen Leitlinien

beschäftigt hat, für den wird es also höchste Zeit.

Dr. Oliver Völkel, LL.M. ist Partner in der Stadler Völkel Rechtsanwälte GmbH.