

Trust and Technology Blog

By PwC Deutschland | 18.10.2023

Zunehmende Relevanz des Business Continuity Management für den Finanz- und Versicherungssektor

In Zeiten von Unsicherheit und Veränderung, durch bspw. den Klimawandel und zunehmende Cyberangriffe, ist das Risiko von Störungen und Ausfällen in der Geschäftstätigkeit höher denn je.

Für Unternehmen, die auf kontinuierliche Betriebsabläufe angewiesen sind, ist es damit von zunehmender Relevanz effektive Maßnahmen zu ergreifen, um Störungen und Ausfälle zu verhindern. Ein effektives Business Continuity Management (BCM) zu implementieren ermöglicht es, diesen Risiken vorzubeugen und im Falle eines Notfalls schnelle und wirksame Gegenmaßnahmen zu treffen.

Business Continuity Management bezieht sich auf den Planungs- und Steuerungsprozess, der sicherstellt, dass ein Unternehmen seine kritischen Geschäftsprozesse aufrechterhalten kann. Ebenso umfasst es den Prozess der Notfallbewältigung, welcher im Falle einer Störung eine schnellstmögliche Wiederaufnahme regelt.

Im Finanzsektor kommt dieser Thematik eine besondere Bedeutung zu, da hier der Verlust von sensiblen Daten (z.B. Gesundheitsdaten bei einem Krankenversicherer oder Kreditdaten bei ein Baufinanzierung), die Störung finanzieller Transaktionen oder eine Unterbrechung anderer kritischer Geschäftsprozesse schwerwiegende Auswirkungen auf Kunden, Investoren und die Reputation des Unternehmens haben kann. Regulatorische Vorgaben (z.B. DORA, VAIT, BAIT) des Finanzsektors gehen daher explizit auf das Business Continuity Management ein. Geregelt ist unter anderem das Vorgehensmodell des BCM, sodass das Risiko der Unternehmen gesteuert werden kann:



COVID-19 hat auf dramatische Weise verdeutlicht, wie wichtig ein funktionierendes Notfallmanagement ist. In vielen Ländern mussten Bankfilialen und Niederlassungen schließen und die Mitarbeiter:innen konnten ihre Tätigkeiten nicht mehr in Büros ausüben. Unternehmen, die bereits vor der Krise ein umfassendes Notfallmanagement implementiert hatten, das auf eine Reihe an verschiedenen möglichen Szenarien vorbereitet war, waren in der Lage, schnell zu reagieren und ihre kritischen Geschäftsprozesse aufrechtzuerhalten. Mitarbeiter hatten die Möglichkeit, von zu Hause aus zu arbeiten und die IT-Infrastruktur sowie Prozesse liefen stabil, sodass ihre Kunden keine Serviceeinschränkungen hinnehmen mussten. Unternehmen sollten daher auch in Zukunft sicherstellen, dass sie über entsprechende Maßnahmen verfügen, um im Falle von Störungen schnell handeln zu können.

Ein weniger globales Beispiel ist der Cyberangriff auf eine US-amerikanische Kreditagentur, bei dem persönliche Daten wie Sozialversicherungs- und Kreditkartennummern sowie ganze Adressen von 143 Millionen Menschen gestohlen wurden. Der Vorfall führte zu einem massiven Vertrauensverlust in das Unternehmen, da diesem Kontroll- und Prozessschwächen nachgewiesen werden konnten. In der Folge verklagten Kunden das Unternehmen, was zu Gesamtkosten im mittleren dreistelligen Millionenbereich führte.



Derartige Schwächen werden in Deutschland idealerweise zukünftig bereits vor Eintritt eines tatsächlichen Notfalls durch die BaFin veröffentlicht, um eine Stärkung der Resilienz zu erwirken. Diese Öffentlichkeitswirksamkeit führt schlimmstenfalls zu Vertrauensverlust der Kunden und damit einhergehenden Reputations- sowie finanziellen Schäden. Des Weiteren kann die BaFin bei schwerwiegenden Verstößen Kapitalaufschläge verhängen.

Insgesamt zeigt sich also, dass der Aufbau eines effektiven Business Continuity Management für jedes Unternehmen, besonders solcher im Finanzsektor unabdingbar ist und nicht als Kostenfaktor betrachtet werden sollte. Stattdessen ist es viel mehr eine Investition in die Resilienz und Vertrauenswürdigkeit des eigenen Unternehmens. Unternehmen, welche bisher noch kein Notfallmanagement etabliert haben, sollten die Chance ergreifen und sich frühzeitig gegen Störungen wappnen.

Noch Fragen?

Verlieren Sie keine Zeit und sprechen Sie uns an. Wir unterstützen Sie mit unserer Marktkenntnis und Expertise und erörtern gemeinsam die Möglichkeiten für Ihr Unternehmen.

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

[Zu weiteren PwC Blogs](#)

Keywords

Datenschutz, Datensicherheit, Digitalisierung, IT-Sicherheit, Informationstechnologie (IT), Planung & Unternehmenssteuerung, Prozesse, Risk Management Banking, Risk Management Insurance

Contact



Rüdiger Giebichenstein

Köln

ruediger.giebichenstein@pwc.com