# Interaktionsdesign eines Risiko-Bewertungskonzepts für KMU

Marc-André Kaufhold[1], Christian Reuter[2], Tobias Ermert[1]

Forschungsgruppe KontiKat, Institut für Wirtschaftsinformatik, Universität Siegen[1]
Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), TU Darmstadt[2]

**Zusammenfassung**

Betriebsstörungen, Naturkatastrophen und andere Notfälle bedrohen die Fortdauer von Unternehmen. Hierzu stellt Business Continuity Management (BCM) Maßnahmen zur Identifikation von Bedrohungen und Risiken sowie zum Aufbau der Belastbarkeit von Organisationen bereit. In der Forschung mangelt es jedoch an Ansätzen, welche BCM in kleinen und mittleren Unternehmen (KMU) unterstützen. In diesem Kurzbeitrag wird ein Konzept für KMU vorgestellt, welches die Identifikation und Bewertung von Risiken unterstützt, Bewältigungsmaßnahmen anbietet und unternehmensspezifische Risikoinformationen auf einem Dashboard visualisiert.

## 1 Einleitung

Unternehmen können von Betriebsstörungen, kriminellen Handlungen oder Naturkatastrophen betroffen sein (Sullivan-Taylor und Branicki, 2010), was Schutzmaßnahmen zur Prävention sowie der Erstellung von Plänen zur Bewältigung einer Krisensituation für Unternehmen erfordert. Eine Strategie für die Unterstützung dieser Maßnahmen ist BCM, welches in der Norm DIN EN ISO 22301 (2014) definiert wird als „*ganzheitlicher Managementprozess, der potenzielle Bedrohungen für Organisationen und die Auswirkungen ermittelt […] und der ein Gerüst zum Aufbau der Belastbarkeit einer Organisation […] bereitstellt*". Die BCM-Literatur fokussiert große Konzerne (Thiel und Thiel, 2010); KMU und die Implementierung eines an deren Bedürfnisse angepassten BCM-Systems werden selten thematisiert (Kaufhold et al., 2018; Reuter, 2015). Gleichzeitig verweisen Sullivan-Taylor und Branicki (2010) darauf, dass KMU ihr Risikomanagement von „muddle through" hin zu einem strategisch proaktiven Handeln entwickeln müssen. Um das Bewusstsein für die Notwendigkeit eines geeigneten Risikomanagements zu schärfen und gleichzeitig das unbürokratische und flexible Handeln der KMU zu bewahren, stellen wir das Konzept einer Anwendung vor, welche KMU bei der Identifikation und Bewertung von Risiken unterstützt, Bewältigungsmaßnahmen aufzeigt und Berichte des Risikomanagements erstellt.

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Tagungsband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-mci-0356

# 2 Risikobewertungskonzept für KMU

Das Konzept zur Unterstützung des **Risikobewertungsprozesses** wurde auf Basis einer Literaturstudie, einer Marktstudie 16 bestehender BCM-Systeme sowie sechs semi-strukturierten Interviews mit KMU, je zwei aus den Branchen IT-Dienstleistung, Produktion und Softwareentwicklung, als Mockup-Prototyp implementiert. Die Analyse der Interviews hat verdeutlicht, dass derartige Konzepte bei geringem Dokumentations-, Finanz-, und Personalaufwand die Anpassbarkeit an Organisationsspezifika, Einfachheit der Bedienung, Bewusstseinsförderung für Risiken und Vorschläge von Gegenmaßnahmen anbieten müssen.

**Risikoidentifizierung (I):** Durch fehlendes Wissen und Mangel an konsistenten Informationen stellt die Identifizierung relevanter Bedrohungen ein großes Problem für KMU dar (Bankole & Sambo, 2016), die mit geeigneten Funktionen unterstützt werden müssen (Abb. 1). Zur Identifikation sollten insbesondere Fragen adressiert werden wie „Welche Bedrohungen existieren?“ und „Was betrachten andere Unternehmen als Bedrohung?“.

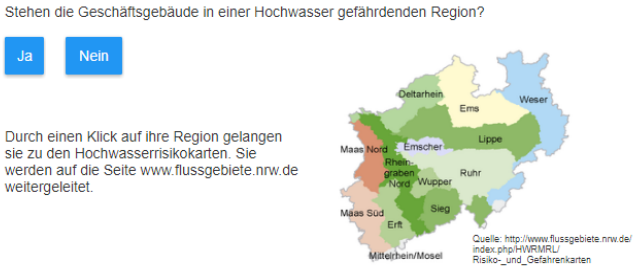


*Abbildung 1. Risikoidentifizierung hier am Beispiel des Hochwassers*

**Risikobewertung durchführen (II):** Die Risikobewertung wird mithilfe eines Fragenkatalogs zu vordefinierten Bedrohungen durchgeführt (Abb. 2). Dabei wird die Risikobewertung als Gesamtprozess betrachtet, die Risikoidentifizierung und Risikobewertung sind demnach nicht strikt voneinander getrennt. Am Beispiel der natürlichen Bedrohung „Überschwemmung“ werden die einzelnen Schritte der Risikobewertung demonstriert.

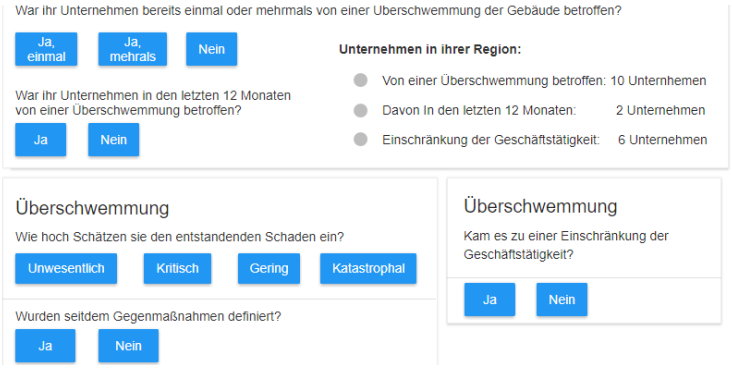


*Abbildung 2. Risikobewertung hier am Beispiel des Hochwassers*

**Ergebnis der Risikobewertung (III):** Das Bewusstsein für Risiken soll geschärft werden, indem die Anwendung dazu anregt, über vergangene Ereignisse zu reflektieren. Außerdem werden aggregierte, öffentliche Informationen über andere Unternehmen zur Sensibilisierung gegenüber der Bedrohung aufgelistet. Anschließend muss die Bedrohung entsprechend ihrer Eintrittswahrscheinlichkeit und dem Schadensausmaß beurteilt werden. Die Anwendung ermittelt dann, basierend auf den gewonnenen Erkenntnissen, das potentielle Risiko.

**Umgang mit dem Risiko festlegen (IV):** Den Risiken entsprechend kann der Nutzer den Umgang mit einem Risiko bestimmen. Dabei wird auf die Abstufung von Thiel und Thiel (2010) zurückgegriffen. Ein Risiko kann entweder (1) akzeptiert werden oder (2) akzeptiert und durch Vereinbarungen für Hilfeleistungen mit einer anderen Firma oder einem BCM-Partner abgesichert werden. Ein Risiko (3) möglichst reduziert und Vorkehrungen zur Hilfeleistung nach einem Vorfall getroffen werden oder (4) soweit reduziert werden, dass keine externe Hilfe mehr nötig ist. Darüber hinaus kann man ein Risiko (5) vermeiden oder auslagern.

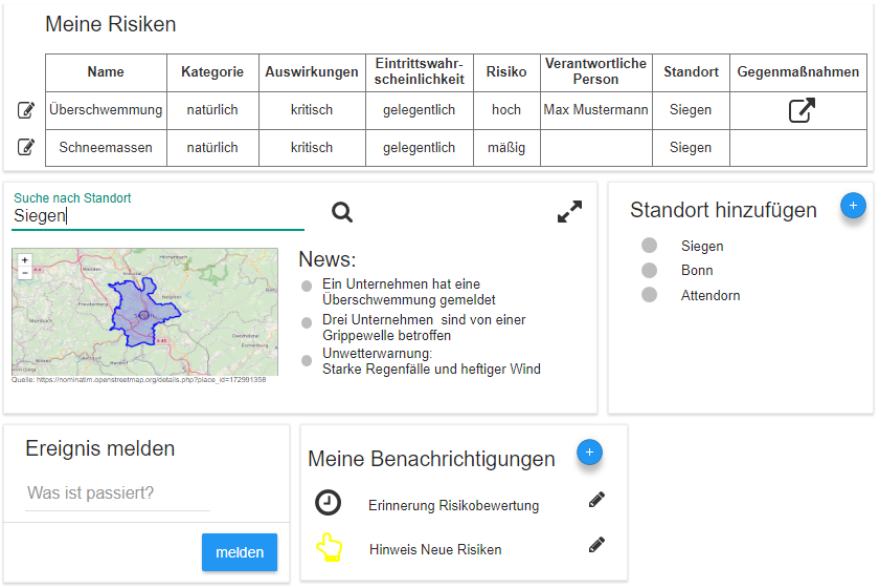


*Abbildung 3. Dashboard zur Darstellung und Verwaltung der identifizierten Risiken*

**Dashboard (V):** Zum Abschluss wird ein Dashboard-Report erstellt, der einen einfachen Überblick über definierte Risiken und Gegenmaßnahmen darstellt (Abb. 3). Es ist zudem möglich, mithilfe einer standortbasierten Suche auf regionale Daten zuzugreifen. Entsprechend der gesuchten Region kann das Ergebnis der Suche mit Informationen über Bedrohungen, welche durch andere Unternehmen gemeldet wurden, angereichert werden. Das Dashboard bietet zudem die Möglichkeit, eigene *Gegenmaßnahmen* zu definieren, zu denen neben der Bezeichnung und einer Beschreibung auch verantwortliche Personen und benötigte Ressourcen definiert werden. Zudem können *Erinnerungen* dazu genutzt werden, sich die Risiken immer wieder bewusst zu machen, um auf sich ändernde Strukturen und Prozesse reagieren zu können.

# 3 Diskussion und Fazit

In der vorliegenden Literatur konnte ermittelt werden, dass KMU im Hinblick auf BCM bei der Risikobewertung unterstützt werden müssen (Sullivan-Taylor und Branicki, 2010). Mit dem vorgestellten Konzept können KMU auf Bedrohungen aufmerksam gemacht werden, die sie noch nicht berücksichtigt haben. Durch eine einfache Bedienung und durch Verringerung des Dokumentationsaufwands kann die Risikobewertung vereinfacht werden. Ob dies ausreicht, um die Komplexität der Umsetzung von BCM so zu reduzieren (Thiel und Thiel, 2010), dass KMU eine angepasste Strategie umsetzen können, muss in weiteren Studien untersucht werden. Weiterhin müsste das vorliegenden Konzept mit KMU-Anwendern evaluiert werden, insbesondere im Hinblick auf fehlende Funktionalitäten und die Nützlichkeit des Konzepts.

**Danksagung**: Die Arbeitsgruppe KontiKat (Reuter et al., 2017) wird durch das Bundesministerium für Bildung und Forschung (BMBF) (no. 13N14351) gefördert.

# Literaturverzeichnis

Bankole, F., & Sambo, F. (2016). A Process Model for ICT Business Continuity Plan for Disaster Event in South Afrika Small and Medium Enterprises. In *Proceedings of UK Academy for Information Systems Conference*. Oxford University.

ISO 22301. (2014). *Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen (ISO 22301:2012); Deutsche Fassung EN ISO 22301:2014*.

Kaufhold, M.-A., Riebe, T., Reuter, C., Hester, J., Jeske, D., Knüver, L., & Richert, V. (2018). Business Continuity Management in Micro Enterprises: Perception, Strategies and Use of ICT. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*.

Reuter, C. (2015). Betriebliches Kontinuitätsmanagement in kleinen und mittleren Unternehmen – Smart Services für die Industrie 4.0. In A. Schmidt, A. Weisbecke, & M. Burmester (Eds.), *Mensch & Computer: Workshopband* (pp. 37–44). Oldenbourg-Verlag.

Reuter, C., Kaufhold, M.-A., Schorch, M., Gerwinski, J., Soost, C., Hassan, S. S., … Wulf, V. (2017). Digitalisierung und Zivile Sicherheit: Zivilgesellschaftliche und betriebliche Kontinuität in Katastrophenlagen (KontiKat). In G. Hoch, H. Schröteler von Brandt, V. Stein, & A. Schwarz (Eds.), *Sicherheit (DIAGONAL Jahrgang 38)* (pp. 207–224). Göttingen: Vandenhoeck & Ruprecht, Göttingen.

Sullivan-Taylor, B., & Branicki, L. (2011). Creating resilient SMEs: why one size might not fit all. *International Journal of Production Research*, *49*(18), 37–41.

Thiel, C., & Thiel, C. (2010). Business Continuity Management für KMU. *Datenschutz Und Datensicherheit - DuD*, *34*(6), 404–407.