A. Weisbecker, M. Burmester & A. Schmidt (Hrsg.): Mensch und Computer 2015 Workshopband, Stuttgart: Oldenbourg Wissenschaftsverlag, 2015, S. 37-44.

Betriebliches Kontinuitätsmanagement in kleinen und mittleren Unternehmen – Smart Services für die Industrie 4.0

Christian Reuter

Universität Siegen, Institut für Wirtschaftsinformatik

Zusammenfassung

Betriebliches Kontinuitätsmanagement (Business Continuity Management, kurz: BCM) ist im Sinne des betrieblichen Notfallmanagements integraler Bestandteil ziviler Sicherheit. BCM ist laut ISO 22301 (2014) ein ganzheitlicher Managementprozess, der potenzielle Bedrohungen für Organisationen und deren Auswirkungen auf Geschäftsabläufe ermittelt. Bei Betrachtung der aktuellen Studienlage liegt der Schluss nahe, dass die Anwendung von BCM in kleinen und mittleren Unternehmen (KMU) unterrepräsentiert ist und der Sicherheitslevel teilweise im nicht-wirtschaftlichen Bereich liegt. Dieser Beitrag stellt den Einsatz von BCM in KMU vor und diskutiert diesbezügliche Forschungsergebnisse. Hierauf aufbauend wird eine Matrix zu möglichen Auswirkungen vs. Umfang und Qualität des Notfallmanagements verschiedener Akteure dargestellt. Abschließend werden leichtgewichtige und einfach zu handhabende BCM-Sicherheitslösungen, in Form von Smart Services, als möglicher Lösungsansatz für die vermehrt von kontinuierlichem IT-Einsatz abhängigen Industrie 4.0 vorgestellt.

1 Einleitung

Die Stromausfälle in Indien 2012 (670 Millionen Betroffene), in Brasilien und Paraguay 2009 (87 Millionen Betroffene), in Europa 2006 (10 Millionen Betroffene) und in den USA und Kanada 2003 (55 Millionen Betroffene) zeigen, dass sich große unbeabsichtigte Unterbrechungen der Versorgung mit Elektrizität auch heute noch überall auf der Welt ereignen (Reuter & Ludwig, 2013). Der Deutsche Bundestag (2011) untersuchte die Gefährdung moderner Gesellschaften am Beispiel eines großräumigen und lang andauernden Ausfalls der Stromversorgung und kam zu dem Ergebnis, dass sich „aufgrund der nahezu vollständigen Durchdringung der Lebens- und Arbeitswelt mit elektrisch betriebenen Geräten […] die Folgen […] zu einer Schadenslage von besonderer Qualität summieren“ können.

Neben Stromausfällen gibt es eine Reihe weiterer möglicher Ursachen – wie der Orkan Kyrill in Europa 2007; die Tsunami- und Erdbebenkatastrophe in Japan 2011; der Hurrikan Sandy in den USA 2012; und auch vermeintlich kleinere Ereignisse. Deren Konsequenzen können so weitreichend sein, dass die Sicherheit der Bürgerinnen und Bürger nicht nur in ihrem privaten, sondern auch in ihrem beruflichen Umfeld gefährdet werden. Eine mögliche Konsequenz von Ausfällen ist die negative Beeinträchtigung der kontinuierlichen wirtschaftlichen Tätigkeiten von Unternehmen. Dies kann zu Problemen in Abläufen führen – wenn beispielsweise Workflow-Management Komponenten ausfallen (Reuter & Georg, 2008) und damit weitreichende Schäden nach sich ziehen.

Unternehmen sind seit der dritten industriellen Revolution – dem Einsatz von Elektronik und IT zur Automatisierung der Produktion – und spätestens seit der aufkommenden vierten industriellen Revolution – dem Zusammenwachsen der realen und virtuellen Welt zu einem Internet der Dinge, welche als Zukunftsprojekt Industrie 4.0 diskutiert wird – vermehrt vom kontinuierlichen Einsatz von IT abhängig (Bundesministerium für Bildung und Forschung, 2015). BCM soll zur Aufrechterhaltung der Belieferung von Produktions- und/oder Dienstleistungsprozessen einer Organisation, in zuvor festgelegten Niveaustufen, die nach einem Zwischenfall mit Betriebsunterbrechung ausfallen, beitragen (Bundesamt für Sicherheit in der Informationstechnik, 2008). In diesem Beitrag soll der Frage nachgegangen werden, ob und wie BCM auch in KMU eingesetzt wird, werden sollte und könnte.

2 Betriebliches Kontinuitätsmanagement

Business Continuity Management (BCM) ist laut ISO 22301 (2014) ein „ganzheitlicher Managementprozess, der potenzielle Bedrohungen für Organisationen und die Auswirkungen ermittelt, die diese Bedrohungen, falls sie umgesetzt werden, womöglich auf die Geschäftsabläufe haben." BCM stellt „ein Gerüst zum Aufbau der Belastbarkeit einer Organisation im Verbund mit der Fähigkeit einer effektiven Reaktion, die die Interessen ihrer zentralen Interessensgruppen, das Ansehen, die Marke und die wertschöpfenden Tätigkeiten sichert, bereit". Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008) wird das auch als Notfallmanagement bezeichnete BCM als „Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren", verstanden.

Als eine Form der Krisenbewältigung hat sich BCM – weniger geläufig das deutsche „betriebliche Kontinuitätsmanagement" oder Notfallmanagement – seit den 1970er Jahren als Reaktion auf die technischen und operationellen Risiken in Unternehmen entwickelt (Herbane, 2010b). Erst 2012 wurde mit dem ISO-Standard 22301:2012 (in deutscher Fassung: ISO 22301, 2014) der erste international gültige Standard für BCM veröffentlicht. Innerhalb des Standards werden Anforderungen spezifiziert, um ein dokumentiertes Kontinuitätsmanagementsystem zu planen, einzurichten, zu realisieren, betreiben, überwachen, überprüfen, unterhalten und kontinuierlich zu verbessern. Damit wurde der zuvor existente British Standard BS 25999 (2007) abgelöst. Weitere nationale Standards sind der US-amerikanische NFPA 1600 (2013) (Standard on Disaster/Emergency Management and Busi-

ness Continuity Programs) sowie der darauf basierende kanadische CSA Z1600 (Essentials Emergency Management and Business).

Der deutsche BSI-Standard 100-4 (2008) zum Notfallmanagement in Unternehmen zeigt einen systematischen Weg auf, „um die Kontinuität des Geschäftsbetriebs sicherzustellen". Aufgaben eines Notfallmanagements sind daher, „die Ausfallsicherheit zu erhöhen und die Institution auf Notfälle und Krisen adäquat vorzubereiten, damit die wichtigsten Geschäftsprozesse bei Ausfall schnell wieder aufgenommen werden können. Es gilt, Schäden durch Notfälle oder Krisen zu minimieren und die Existenz der Behörde oder des Unternehmens auch bei einem größeren Schadensereignis zu sichern."

3 BCM in kleinen und mittleren Unternehmen

Aufgrund der relativ geringen Wahrscheinlichkeit für Stromausfälle in Westeuropa ist die allgemeine Vorbereitung nicht optimal (Birkmann et al., 2010). Dieser Umstand wird seitens des BMI (2009) als *Verletzlichkeitsparadoxon* bezeichnet: „In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus". Gerade in „hoch industrialisierte, sehr komplexe Technologien" nutzenden Gesellschaften wird auf Störungen deutlich sensibler reagiert, da diese „sehr hohe Sicherheitsstandards und eine hohe Versorgungssicherheit gewohnt sind". Aufgrund „zunehmender Robustheit und geringerer Störanfälligkeit" kann sich demnach „ein durchaus trügerisches Gefühl von Sicherheit" entwickeln, so dass die „Auswirkungen eines ‚Dennoch-Störfalls' überproportional hoch" sind (Bundesministerium des Inneren, 2009, p. 10).

Jedoch gibt es auch den gegenläufigen Trend, dass sich öffentliche, jedoch vor allem private Infrastrukturbetreiber im Spannungsfeld lückenloser Daseinsfürsorge und ökonomischer Optimierung befinden (Kloepfer, 2005, p. 17). Es besteht daher die Gefahr, dass die Verfügbarkeit von Infrastrukturen auf das vertraglich und geschäftsmäßig notwendige reduziert wird. Die entstehende Lücke kann bestenfalls von großen Unternehmen, kaum aber von KMU oder gar Privatpersonen kompensiert werden.

BCM richtet sich an Unternehmen unabhängig von ihrer Größe. Gemäß der Definition der EU-Kommission (2003) zählt ein Unternehmen dann zu den KMU, wenn es nicht mehr als 249 Beschäftigte hat und einen Jahresumsatz von höchstens 50 Millionen Euro erwirtschaftet oder eine Bilanzsumme von maximal 43 Millionen Euro aufweist. Die Sicherheit von KMU ist von entscheidender Bedeutung für die europäische Wirtschaft, da diese 99% der Unternehmen repräsentieren (Thiel & Thiel, 2010).

Einer Studie des Netzwerks Elektronischer Geschäftsverkehr zufolge werden jedoch „lediglich in jedem fünften KMU IT-Notfallpläne erstellt" und in „jedem vierten KMU fehlt eine standardisierte Vorgehensweise, um IT-Notfälle möglichst zügig abzuwenden" (Duscha, 2009). Analog dazu konnten Studien feststellen, dass „45% der US-amerikanischen und europäischen KMU kein BCM-Konzept ausweisen können" (ENISA, 2009) und dass auf Basis einer Untersuchung in Großbritannien BCM in KMU signifikant weniger zu finden ist

(Musgrave & Woodman, 2001) bzw. 41% der Unternehmen nicht für Krisensituationen gleich welcher Art planen (Semantec, 2011).

Herbane (2010b) stellt anhand eines Vergleichs der Forschungsliteratur in den Bereichen der KMU-Forschung und des Krisenmanagements fest, dass angesichts der wirtschaftlichen Bedeutung und Verwundbarkeit von KMU mehr Aufmerksamkeit für die kombinierte Betrachtung beider Bereiche nötig ist. Insbesondere ist der Einsatz von BCM in und für KMU bisher noch wenig erforscht (Herbane, 2013). Auch in anderen Studien wird dargelegt, dass das Schutzlevel in KMU im Vergleich zu Konzernen signifikant geringer ist (Duscha, 2009; European Network and Information Security Agency (ENISA), 2009; Musgrave & Woodman, 2001). Als einen wesentlichen Hinderungsgrund für die Einführung von BCM in KMU nennt ENISA (2009) die Anstrengung, abstrakt und generisch beschriebene Schutzmaßnahmen in die betriebliche Praxis zu implementieren.

Zusammenfassend ermöglicht der Forschungsstand die Ableitung folgenden Modells (Abbildung 1): Einzelpersonen verfügen typischerweise über kein dezidiertes Sicherheitsmanagement im Sinne von BCM und wenig Sicherheitstechnik bei typischerweise geringen Auswirkungen im Falle eines Ausfalls. Konzerne beschäftigen sich intensiv mit diesem Thema bei gleichzeitig hohen wirtschaftlichen Auswirkungen (z.B. Produktionsausfälle, Prozessunterbrechungen). Gerade KMU weisen in diesem Bereich im Verhältnis zu den möglichen Auswirkungen eine Unterversorgung auf, wie oben erläutert (Duscha, 2009; ENISA, 2009; Thiel & Thiel, 2010). Folglich gilt es Ansätze zur Erhöhung des Umfangs und der Qualität des Notfallmanagements herzuleiten.

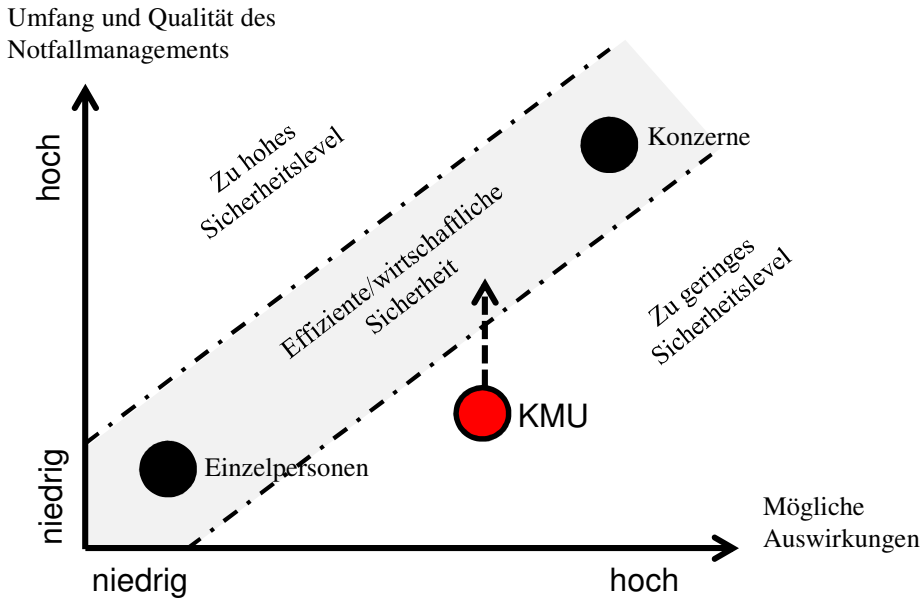

Abbildung 1: Wirtschaftliche Sicherheit: Einzelpersonen, KMU und Konzerne bzgl. Auswirkungen vs. Qualität des Notfallmanagements

4 BCM-Sicherheitslösungen für KMU

Als Problem für KMU wurde die Komplexität von BCM identifiziert: Vorgaben müssen in eine individuell passende und verständliche Sprache übersetzt werden; dieser Schritt ist für KMU nur schwer zu leisten (Thiel & Thiel, 2010). Gemäß der European Network and Information Security Agency (ENISA) (2009) existiert bei KMU jedoch ein großer Bedarf an vereinfachten Ansätzen des Sicherheits- und Risikomanagements. Ein leichtgewichtiges, einfaches und effizientes BCM als Service für KMU stellt derzeit noch eine Forschungs- und Entwicklungslücke dar.

Durch die Entwicklung neuer Geschäftsmodelle und hybrider Wertschöpfungsprozesse für leichtgewichtige und einfach zu handhabende BCM-Sicherheitslösungen für KMU soll sowohl die Phase vor Eintritt der Krise (Identifizierung wichtiger Daten, Prozesse und Arbeitsplätze, Risikoeinschätzung, Maßnahmenpläne, Übungen, Messung der Effektivität und Effizienz der Maßnahmen) als auch die Phase nach Eintritt der Krise unterstützt werden, um das Level des Sicherheitsmanagements zu erhöhen. Smart Services, d.h. Dienstleistungen, die integraler Bestandteil von Produkten sind (Allmendinger & Lombreglia, 2005), könnten hier das Investitions- und Komplexitätsniveau für KMU reduzieren.

Auch wenn dieser Bereich bislang vergleichsweise wenig erforscht ist, existieren bereits einige Ansätze um BCM in KMU zu erhöhen: In ihrem treffenderweise „why one size might not fit all“ betitelten Beitrag stellen Sullivan-Taylor & Branicki (2011) fest, dass unterschiedliche Unternehmensgrößen zu unterschiedlichen Anforderungen an den Einsatz von BCM-Systemen in KMU führen.

Thiel & Thiel (2010) stellen dementsprechend einen Leitfaden für KMU zur Implementierung eines unternehmensspezifischen BCM vor, der die besonderen Charakteristika, wie z. B. geringe Personalressourcen und kein Expertenwissen im Risikomanagement, berücksichtigen soll. Wedawatta & Ingirige (2012) schlagen die Kombination aus objektbasierten Schutzmaßnahmen und generischen BCM-Maßnahmen zur Stärkung der Resilienz von KMU vor. Li et al. (2015) fokussieren die Entwicklung eines agentenbasierten Modells zur Simulation und zur Ableitung von Bewältigungsstrategien für KMU bei Hochwassern.

Lee & Jang (2009) stellen die Informationssicherheit als einen besonderen Aspekt des BCM heraus und entwickeln ein Informationssicherheitsmanagement Systemmodell für KMU. Auch Horváth (2013) präsentiert ein integriertes System zur Verschmelzung von BCM- und Informationssicherheitsmanagement-Aktivitäten. Als eine leichtgewichtige, nicht von der Unternehmensgröße abhängige BCM-Sicherheitslösung kann das von Sapateiro et al. (2011) entwickelte mobile Tool zur Unterstützung kollaborativer BCM-Aktivitäten genannt werden, welches die Kollaboration, das Wissensmanagement, die Teamperformanz und das Situationsbewusstsein adressiert.

5 Zusammenfassung

Dieser Beitrag hat den Stand der Forschung im Bereich des betrieblichen Kontinuitätsmanagements (BCM) in kleinen und mittleren Unternehmen (KMU) untersucht und eine Matrix zur Positionierung von KMU in Bezug auf mögliche Auswirkungen vs. Qualität des Notfallmanagements abgeleitet.

Aus den untersuchten Forschungsergebnissen lässt sich ableiten, dass der Einsatz von BCM in KMU im Vergleich zu Konzernen signifikant geringer zu sein scheint (Duscha, 2009), jedoch genaue Erkenntnisse noch fehlen (Herbane, 2013). Existierende Forschungsergebnisse betrachten, wie dargestellt, jeweils allein Teilaspekte. Insbesondere ist erkennbar, dass KMU andere, dem Risiko und der Unternehmensgröße angepasste, Anforderungen an den Umfang von Lösungen haben (Sullivan-Taylor & Branicki, 2011).

Erkenntnisse zu leichtgewichtigen und einfach zu handhabenden BCM-Sicherheitslösungen für KMU als Smart Services, die auch Aspekte der Mensch-Maschine-Interaktion berücksichtigen, können auch im Zeitalter *emergenter IT-Nutzung* - d.h. dynamisch und nicht vorhersehbar (Reuter, 2014) - sowie der im Rahmen von Industrie 4.0 einhergehenden Notwendigkeit *unterbrechungsfreier IT-Nutzung*, dem gegenwärtigen Stand der Forschung nicht entnommen werden und stellen somit eine Forschungslücke dar.

Danksagung

Die Forschungsarbeiten wurden im Rahmen des BMBF-Projekts „KOKOS“ (Fö.-Kz. 13N13559) sowie im Rahmen des EU-FP7-Projekts „EmerGent“ (Fö.-Kz. 608352) gefördert.

Literaturverzeichnis

Allmendinger, G., & Lombreglia, R. (2005). Four strategies for the age of smart services. *Harvard Business Review*, *83*(10). doi:10.1225/R0510J

Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T., & Schmude, M. (2010). *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom / Stromausfall. Risk Management*. Berlin, Germany. http://www.sicherheit-forschung.de/schriftenreihe

Bundesamt für Sicherheit in der Informationstechnik. (2008). *Notfallmanagement – BSI-Standard 100-4*. Bundesanzeiger Verlag. https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Bundesministerium des Inneren. (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*. Berlin.

Bundesministerium für Bildung und Forschung. (2015). Zukunftsprojekt Industrie 4.0. Retrieved from http://www.bmbf.de/de/9072.php

Deutscher Bundestag. (2011). *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung*. (T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch, & U. Riehm, Eds.). http://dip21.bundestag.de/dip21/btd/17/056/1705672.pdf

Duscha, A. (2009). Netz- und Informationssicherheit in Unternehmen 2009. Studie des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“. http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/studie-it-sicherheit-2009-pdf

Europäische Union. (2003). *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. (2003/361/EG). Artikel 2 des Anhangs*. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=uriserv:OJ.L_.2003.124.01.0036.01.DEU

European Network and Information Security Agency (ENISA). (2009). Assessing a simplified Information Security approach. http://www.enisa.europa.eu/publications/archive/assessing-a-simplified-information-security-approach

Herbane, B. (2010a). Small business research - Time for a crisis-based view. *International Small Business Journal*, *28*(1), 43–64. doi:10.1177/0266242609350804

Herbane, B. (2010b). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002. doi:10.1080/00076791.2010.511185

Herbane, B. (2013). Exploring Crisis Management in UK Small and Medium Sized Enterprises. *Journal of Contingencies and Crisis Management*, *21*(2), 82–95. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/1468-5973.12006/full

Horváth, G. K. (2013). Information Security Management for SMEs: Implementating and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle. In *Proceedings of FIKUSZ* (pp. 133–141). Budapest, Hungary.

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

Kloepfer, M. (2005). *Schutz kritischer Infrastrukturen*. Nomos.

Lee, W., & Jang, S. (2009). A Study on Information Security Management System Model for Small and Medium Enterprises. *Recent Advances in E-Activities, Information Security and Privacy*, 84–87.

Li, C., Coates, G., Johnson, N., & Mcguinness, M. (2015). Designing an Agent-Based Model of SMEs to Assess Flood Response Strategies and Resilience. *International Journal of Social, Education, Economics and Management Engineering*, *9*(1), 7–12.

Musgrave, B., & Woodman, P. (2001). Weathering the storm - The 2013 Business Continuity Management Survey. *Airline Business*. doi:10.1111/j.1751-486X.2009.01490.x

National Fire Protection Association (NFPA). (2013). NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs. http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=1600

Reuter, C. (2014). *Emergent Collaboration Infrastructures: Technology Design for Inter-Organizational Crisis Management (Ph.D. Thesis)*. Siegen, Germany: Springer Gabler. http://www.springer.com/springer+gabler/bwl/wirtschaftsinformatik/book/978-3-658-08585-8

Reuter, C., & Georg, C. (2008). Entwicklung eines webbasierten Dokumentenmanagement-Systems für eine Fluggesellschaft. *Journal WIRTSCHAFTSINFORMATIK*, *50*(2), 142–145.

Reuter, C., & Ludwig, T. (2013). Anforderungen und technische Konzepte der Krisenkommunikation bei Stromausfall. In M. Hornbach (Ed.), *Informatik 2013 - Informatik angepasst an Mensch, Organisation und Umwelt* (pp. 1604–1618). Koblenz, Germany: GI-Edition-Lecture Notes in Informatics (LNI).

Sapateiro, C., Baloian, N., Antunes, P., & Zurita, G. (2011). Developing a Mobile Collaborative Tool for Business Continuity Management. *Journal of Universal Computer Science (j.ucs)*, *17*(2), 164–182.

Semantec. (2011). SMB Disaster Preparedness Survey. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=dpsurvey

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. doi:10.1080/00207543.2011.563837

Thiel, C., & Thiel, C. (2010). Business Continuity Management für KMU. *Datenschutz und Datensicherheit - DuD*, *34*(6), 404–407. doi:10.1007/s11623-010-0114-3

Wedawatta, G., & Ingirige, B. (2012). Resilience and adaptation of small and medium-sized enterprises to flood risk. *Disaster Prevention and Management: An International Journal*, *21*(4), 474–488.

Kontaktinformationen:

Dr. Christian Reuter, Dipl.-Wirt.Inf., Bereichsleiter Kriseninformationssysteme

Universität Siegen, Institut für Wirtschaftsinformatik (Fak. III), Kohlbettstraße 15, 57072 Siegen

christian.reuter@uni-siegen.de; www.profil.christianreuter.net