Krisenmanagement als strategische Herausforderung im Zeitalter der Digitalisierung

Prof. Dr. Nils Herda, Prof. Dr. Stefan Ruf

Krisen begleiten unsere Gesellschaft – ob die weltweite Wirtschaftskrise ab 2007, deren ökonomische Auswirkungen wir bis heute spüren, das Hochwasser im Jahr 2002, das interessanterweise zu einer Begleiterscheinung des Bundestagswahlkampfs wurde, die Furcht vor einer Pandemie im Jahr 2009, die durch die Schweinegrippe als Auslöser befürchtet wurde, bis hin zu den Cyber-Angriffen russischer Hacker, die 2018 eine Eiszeit zwischen der EU und Russland ausgelöst haben.

Dies führt dazu, dass die Bundesrepublik Deutschland entsprechende Krisenpläne vorbereitet hat und diese generalstabsmäßig in groß angelegten Übungen plant. Doch was bedeuten Krisenszenarien für mittelständische Unternehmen? Müssen sie nicht auch regelmäßig – wie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe aber auch die lokale Feuerwehr – ihre Krisenfähigkeit testen? Gerade systematische Cyber-Angriffe auf Unternehmen des gehobenen Mittelstands und internationalen Geschäfts zeigen die Notwendigkeit.

1. Krisen

Eine Krise kann selten wirklich vorhergesehen werden. Sie stellt de facto den Höhepunkt einer Konfliktentwicklung dar, die zu einer massiven Funktionsstörung in einem sozialen oder betrieblichen System führt. Der Krisenbegriff wird in verschiedenen Wissenschaften und Disziplinen verwendet, aber unterschiedlich interpretiert. So ist für die Generalität einer Armee eine politische oder militärische Krise natürlich etwas anderes als für einen Naturwissenschaftler etwa die Klimakrise. Auslöser, zeitlicher Verlauf und Auswirkungen unterscheiden sich genauso wie die Methoden zur Eindämmung einer Krise.

Eine Krise führt zu einer massiven Funktionsstörung in einem sozialen oder betrieblichen System.

Grundsätzlich nimmt eine Krise einen typischen Verlauf, wie Abbildung 1 aufzeigt. Eine Krise hat einen Auslöser, der eine Funktionsstörung provoziert und diese dadurch sichtbar macht. Doch interessanterweise sind diesem Auslöser Ursachen vorgelagert, die aber eher nicht wahrgenommen oder zunächst nicht in einen Zusammenhang mit dem Auslöser gebracht werden. Erst eine Reihe – für sich genommen jeweils überschaubarer – Dominoeffekte mit immer dramatischeren Auswirkungen führt am Ende zu einem für alle sichtbaren Höhepunkt einer Krise.

Die psychologischen Auswirkungen einer Krise bei den Betroffenen sind vielschichtig: So ist diese – gefühlt – von einem Vertrauensverlust gekennzeichnet („Mein Geld ist nicht mehr sicher."), einem Verlust der Deutungshoheit („Denen kann man nichts mehr glauben"), einem Kompetenzverlust („Die haben es nicht im Griff"), einem Kontrollverlust („Ich löse das jetzt auf eigene Faust") bis hin zu Panik („Rette sich, wer kann – koste es, was es wolle") oder Resignation („Wir können nichts mehr tun").

2. Die Wirtschaftskrise ab 2007

Statistisch wusste man früher, dass sich etwa alle sieben Jahre ökonomische Krisen ereignen. Es war die Aufgabe von Politik und Notenbanken diese zu bekämpfen und wieder eine stabile wirtschaftliche Entwicklung einzuleiten. Die kleineren europä-

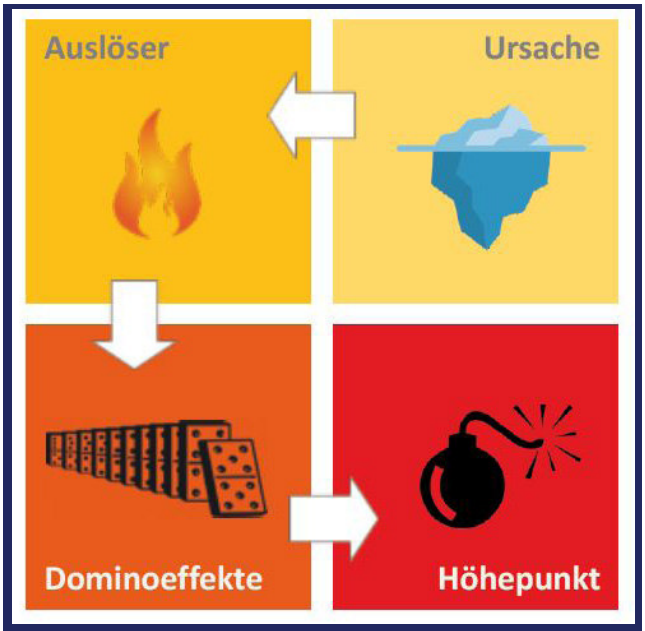

Abbildung 1: Typischer Verlauf einer Krise

ischen Länder haben sich etwa vor Einführung des Euro mit regelmäßigen Abwertungen ihrer Währungen geholfen und so nationale Krisen bewältigt.

Doch die Wirtschaftskrise ab 2007 wurde erst wirklich in der Finanzszene wahrgenommen, als es im August 2007 einen sprunghaften Anstieg der US-amerikanischen Interbank-Finanzkredite (zwischen den Kreditinstituten) gab, der in der Folge zu immer höheren Zinsen führte, die dann an die Kunden weitergegeben wurden, vgl. Abbildung 2 (Auslöser). Dies führte dazu, dass immer mehr Eigenheimbesitzer ihre Zinszahlungen nicht mehr bewältigen konnten und aufgeben mussten.

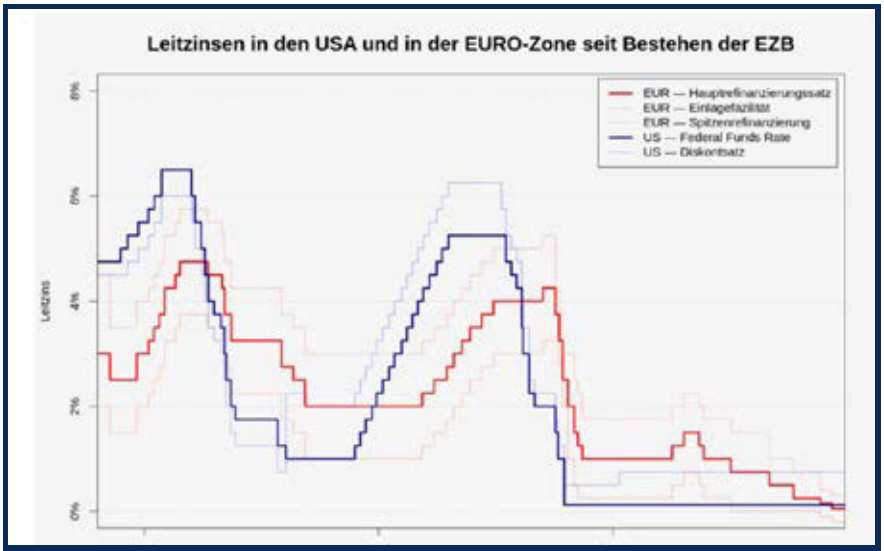

Abbildung 2: Verlauf der Leitzinsen der EZB (rot) und der US-amerikanischen Federal Reserve (blau) mit einem lokalen Maximum im Jahr 2007. (Quelle: Wikipedia)

Vorausgegangen war der politische Wille, u.a. in der Regierungszeit von Bill Clinton, mehr US-amerikanischen Familien zu Wohneigentum zu verhelfen. Doch in der Folge hat sich der Immobilienmarkt in den USA soweit aufgebläht, dass tendenziell sozial schwache Bürger und Familien sich mit viel zu hohen Krediten übernommen hatten (Ursache).

Da das amerikanische Kreditsystem – im Gegensatz zu Deutschland – keinen festen Zinssatz kennt, sondern auf Basis variabler Zinsen funktioniert und zudem die Beleihungsgrenze häufig weit über die 100% gedehnt wird, lagen also ungünstige Voraussetzungen für eine etwaige Zinsanpassung nach oben vor.

So waren in der Folge im Jahr 2006 bereits über 600 Mrd. Dollar in schlecht besicherten Immobilienkrediten verborgen (den sogenannten „Subprime"-Krediten). Diese wurden nun von den Hypothekenbanken weiterverkauft, von Investmentbanken als strukturiertes Anlageprodukt umgewandelt, wobei man „schlechte" Kredite mit Krediten guter Bonität gemischt hat.

Dem Auslöser einer Krise sind Ursachen vorgelagert, die nicht als solche wahrgenommen werden.

Diese Produkte wurden dann, zertifiziert von Rating-Agenturen wie Standard & Poors (S&P) sowie Moody's, international verkauft (weitere Ursache). Gerade deutsche Landesbanken haben viele dieser Produkte – als eine Art „Kreditersatzgeschäft" – gekauft, was dann u.a. ursächlich für die notwendig gewordenen Fusionen im Landesbanksektor wurde.

Der international spürbare Dominoeffekt führte dann dazu, dass die (lokalen) Risiken des US-amerikanischen Immobilienmarktes international exportiert wurden und weltweite Folgen provozierten (Dominoeffekte).

Der Höhepunkt war dann der Zusammenbruch der Investmentbank Lehmann Brothers, der politisch in Kauf genommen wurde und eine weltweit spürbare Zäsur darstellte. In Deutschland mussten Bundeskanzlerin Angela Merkel und Finanzminister Peer Steinbrück durch massive politische Intervention eingreifen und konnten die Märkte mit ihrer (vermeintlichen) Garantie der Spareinlagen beruhigen. ▶

3. Durch Cyber-Angriffe ausgelöste Krisen im Mittelstand

Nicht nur große, weltbekannte Unternehmen, sondern auch unsere mittelständischen Weltmarktführer werden systematisch durch Cyber-Angriffe unter Druck gesetzt. Insbesondere das für Wettbewerber hochinteressante immaterielle Vermögen dieser Unternehmen (wie etwa Produktionsgeheimnisse) stellen hier ein Angriffsziel dar, dem nur mit einer konsequenten Aufrüstung von IT-Security (technisch) und IT-Governance, Risk and Compliance Management (organisatorische Schutzmaßnahmen) begegnet werden kann. Auslöser dieser Angriffe ist häufig die Übermittlung von Schadsoftware, vgl. das Prinzip in Abbildung 3.

Abbildung 3: Typisches Angriffsszenario auf mittelständische Unternehmen. (Quelle:Presentationload)

Auch bei KMU kann ein Cyber-Angriff zum Auslöser einer unternehemensweiten Krise werden.

Es sind in der Cyber Security-Community Fälle wie dieser bekannt: Ein mittelständisches Unternehmen wird in einer kleinen, schlecht gesicherten Niederlassung angegriffen. Die Schadsoftware wird durch innerbetriebliche Kommunikation bis in die deutsche Zentrale übertragen. Verzeichnisse wurden verschlüsselt und waren nicht mehr lesbar. Das Unternehmen bekam ein Erpresserschreiben mit dem Hinweis, das „Lösegeld" in anonymen Bitcoins zu begleichen.

Auch wenn das Unternehmen das Lösegeld nicht zahlte und sich an das Landeskriminalamt wendete, so dauerte es bis zur Behebung der Attacke acht ganze Tage. Unter anderem wurde die Geschäftsführung zu spät informiert und die Produktion gestoppt. Mitarbeiter wurden nach Hause geschickt und Cyber-Experten eingeflogen. Die Folge war ein Millionenschaden für das mittelständische Unternehmen, der nur durch eine erhebliche Kapitalanlage des Eigentümers begrenzt werden konnte.

4. Erkenntnisse

Im digitalen Zeitalter steigt die Abhängigkeit von IT-Technologien erheblich (Digitalisierung und Vernetzung). Wenn nicht im entsprechenden Maße technische und organisatorische Maßnahmen durchgeführt werden, um das Unternehmen nach dem jeweils geltenden Stand der Technik abzusichern (Ursachen), so drohen nach einem Angriff (Auslöser) Dominoeffekte, die sich zu einer unternehmensweiten Krise ausweiten können.

Das zeigt einerseits, dass Digitalisierung und IT-Security eindeutig „Chefsache" sind und nicht nur den IT-Experten überlassen werden können. Andererseits ist es erforderlich, diese Investitionen in Technik und Prozesse auch regelmäßig zu üben, um die ganze Organisation nicht nur zu sensibilisieren, sondern auch den Abläufen im Krisenfall systematisch vorzubeugen.

Die Autoren

Prof. Dr. Nils Herda
Professor für
Wirtschaftsinformatik
herda@hs-albsig.de

Prof. Dr. Stefan Ruf
Professor für
Betriebswirtschaftslehre
rufs@hs-albsig.de