Kolumne Netzwerk Südbaden Ausgabe März 2018

Business Continuity Management (BCM) - Vorbereitet für den Notfall

Die Notwendigkeit von Maßnahmen zur Fortführung des Geschäftsbetriebs im Störungs- oder Katastrophenfall gewinnt an Gewicht, auch wenn immer noch zu viele denken „Es ist ja immer gut gegangen!“. Denn der Ausbau von effizienten Serviceangeboten erleichtert die Umsetzung wirksamer und kostengünstiger Maßnahmen.

Glaubt man Wikipedia, so geht das Business Continuity-Management (BCM) historisch gesehen auf die Absicherung militärischer Strategien gegen Störung und Feindeinwirkung zurück. Schon früh beschäftigten sich die chinesische Literatur über die „Kunst des Krieges“ (Sunzi, 500 v. Chr.) mit der Entwicklung von Methoden, um die gesteckten Ziele auch im Falle des Ausfalls wesentlicher Ressourcen zu erreichen oder zumindest die Effekte abzufedern, um ein Scheitern auf ganzer Linie zu verhindern.

Auch wenn das zuweilen martialische Anmuten des modernen Geschäftsbetriebs manche Analogie zulassen würde, so genügt schon der gesunde Menschenverstand der Erkenntnis, dass das Vorhalten eines „Plan B“s auch abseits kriegerischer Handlungen einigen Sinn ergibt.

So simpel die Einsicht, so schwierig scheint die Umsetzung konkreter Maßnahmen zu sein. Statistiken aus Umfragen zeigen, dass nur ca. 40% der Unternehmen mit dem eigenen BCM zufrieden sind und 60% Handlungsbedarf sehen.

Als Grund für die Unzufriedenheit kann man anführen, dass sich der Druck auf die Unternehmen aktuell stark erhöht. Anforderungen von Kunden an ihre Lieferanten nach entsprechenden Nachweisen und gesetzliche Vorgaben, z.B. aus der im Mai vollständig in Kraft tretenden europäischen Datenschutz-Grundverordnung, erschweren es zunehmend, sich mit Unzulänglichkeiten zufrieden zu geben. Gerade auch kleine und mittlere Unternehmen müssen sich zunehmend nach Ihren BCM-Strategien fragen lassen. Gute Antworten hat nicht jeder parat.

Dabei ist die Entwicklung und Umsetzung eines wirksamen Konzepts zum Business Continuity Management nicht schwer und muss auch nicht mit hohen Kosten verbunden sein.

Die Standards des BSIs und andere Normen zum Notfallmanagement sehen eine mehrstufige Herangehensweise vor: Ein erster wichtiger Schritt stellt eine „Business Impact Analyse“ dar: Sofern noch nicht geschehen gilt es, alle geschäftskritischen Prozesse im Unternehmen zu finden, Abhängigkeiten zu dokumentieren und die Beziehung zu Ressourcen wie Standorte, Maschinen, IT, Personal, Lieferanten usw. zu erfassen. Welche Auswirkungen hätte welche Ausfallzeit jeweils? Wie lange kann das Unternehmen bestehen, ohne dass der jeweilig betrachtete Prozess verfügbar ist. Dabei ist das Augenmerk nicht nur auf die vordergründig wichtige Produktion selbst zu legen – im Falle eines Falles ist es elementar, schnell die geschäftliche Handlungsfähigkeit wiederherzustellen.

Die Folgen einfacher, vergleichsweise häufig eintretender Störungen sind durch entsprechende technische und organisatorische Maßnahmen gut zu managen, sinnvolle Schutzvorkehrungen sind in der Regel auch vorhanden: Vertretungspläne, dokumentiertes und verteiltes Knowhow schützt vor Personalausfall, Redundanz der Internetanbindung schützt vor Ärger mit dem Provider, regelmäßige Backups schützen vor versehentlichem Löschen und den Folgen mancher technischen Störungen an IT-Systemen.

Doch auch nicht alltägliche Szenarien sind zu berücksichtigen. Beispielhaft seien genannt: Die Folgen von Hochwasser, Feuer, Blitzschlag, andauernder Stromausfall, Industrieunfälle, …

Die Beeinträchtigungen durch solche Situation sind oft nicht mit einfachen und kostengünstigen Mitteln in Eigenregie abzufangen. Ein Ersatzrechenzentrum an einem entfernten Standort beispielsweise kann oder will sich nicht jedes KMU leisten – zu hoch scheint der Aufwand in Anbetracht der gefühlten geringen Eintrittswahrscheinlichkeit eines Totalausfalls. Es ist wichtig, dennoch auch für diese Fälle die Auswirkungen und mögliche Maßnahmen zu eruieren.

In nahezu allen Branchen ist die Abhängigkeit der Kernprozesse von der Verfügbarkeit zentraler IT-Systeme offensichtlich. Dementsprechend ist die Schaffung entsprechender Notfall-Strategien ein zentrales Element der BCM-Strategie.

Je nach tolerierbarer Ausfallzeit können unterschiedliche Maßnahmen erforderlich sein. Genügt bei einem kleineren Handwerksbetrieb gegebenenfalls die tägliche, händische Sicherung der Daten der Verwaltungssoftware auf ein transportables, extern gelagertes Medium, um in ausreichender Zeit die Handlungsfähigkeit wieder herzustellen, so bedarf es in anderen Unternehmen mit höherer IT-Abhängigkeit ausgereifteren, zuverlässigeren, automatisierten und überwachbaren Prozessen. So kann das händische, fehleranfällige Backup durch eine automatische zyklische Sicherung aller relevanten IT-Systeme zu einem externen Dienstleister (z.B. Continum CLOUD Backup) die nächste Stufe darstellen. Eine Wiederherstellung zentraler Systeme oder ganzer IT-Umgebungen ist dann verhältnismäßig schnell möglich.

Zeigt die „Business Impact Analyse“ jedoch, dass ein Ausfall wichtiger IT-Systeme für Tage oder Wochen für das Unternehmen katastrophale Auswirkungen hätte, so genügt es nicht mehr, den Backup-Prozess zu optimieren. Die relevanten Systeme sind so zu spiegeln, sodass im Katastrophenfall mehr oder minder verzögerungsfrei eine Wiederinbetriebnahme möglich ist. Klassisch wird diese Anforderung gelöst, indem ein zweites Rechenzentrum eingerichtet, dort entsprechende Hardware vorgehalten wird und die gespeicherten Daten gespiegelt werden. Seit langem gibt es hierfür ausgereifte, zuverlässige Lösungen. Offensichtlicher Nachteil dieser Lösungen sind jedoch die damit verbundenen sehr hohen einmaligen und wiederkehrenden Kosten. Ebenso hat nicht jedes Unternehmen überhaupt die Möglichkeit, ein zweites, geographisch mindestens 5 km entferntes Rechenzentrum (siehe Empfehlung BSI) aufzubauen. So gibt es viele Gründe, die Leistungen spezialisierter IT-Partner in Anspruch zu nehmen, welche für den Desaster-Fall erforderliche Ressourcen extern vorhalten und Dienste bereitstellen, die sich um die Spiegelung Ihrer IT-Systeme kümmern – vollautomatisch, überwacht und 24h am Tag.

Werden solche Dienste genutzt, so ist im Ergebnis sichergestellt, dass wichtige IT-Systeme ohne nennenswerte Unterbrechung an einem Reservestandort in Betrieb gehen können. Weder Standort noch Systeme sind durch das Unternehmen selbst aufzubauen, zu betreiben und zu warten.

Die Continum AG bietet z.B. einen solchen Dienst DRaaS (Disaster-Recovery-as-a-sevice) auf der Basis von Veeam an. Wird Veeam als Backuplösung im eigenen Unternehmen bereits eingesetzt, so ist die Nutzung von Continum DRaaS kostengünstig und ohne großen Aufwand zu bewerkstelligen. Einzelne IT-Systeme oder komplette IT-Infrastrukturen können so schnell und einfach abgesichert werden.

BCM bedeutet also, die Bedrohungen für das Unternehmen zu identifizieren regelmäßig und Schritt für Schritt Maßnahmen zu deren Minderung umzusetzen, so dass auch im Katastrophenfall die Handlungsfähigkeit erhalten bleibt.

Der Autor Thilo Rees arbeitet als IT-Architekt bereits viele Jahre mit solchen Fragestellungen und ist als Information Security Officer bei der Continum AG in Freiburg beschäftigt.