Bild: Shutterstock / Joyseulay

Business Continuity Management

So sind Unternehmen für den Notfall gewappnet

Cyberangriff, Naturkatastrophe oder Brand – jedes Unternehmen kann betroffen sein.

Den November 2018 werden die IT-Verantwortlichen des Klinikums Fürstenfeldbruck im Westen von München nicht so schnell vergessen. Anfang dieses Monats wurde das Krankenhaus Opfer eines Hackerangriffs, der für etwa eine Woche alle rund 450 Rechner lahmlegte. Die Ursache: Ein Mitarbeiter hatte Schad-Software in einem E-Mail-Anhang geöffnet und damit das IT-System infiziert. Die Klinik konnte mehr als eine Woche lang nicht im Normalbetrieb arbeiten.

Angriffe wie dieser sind kein Einzelfall mehr. Dem Branchenverband Bitkom zufolge wurden 68 Prozent der deutschen Industrieunternehmen in den vergangenen zwei Jahren Opfer von Sabotage, Datendiebstahl oder Spionage. Der Gesamtschaden laut Bitkom: 43,4 Milliarden Euro.

Das Geschäft muss weiterlaufen

Kein Wunder, schließlich sind die Geschäftsprozesse in einer digitalen Welt mehr oder weniger vollständig von der Verfügbarkeit der IT-Infrastruktur abhängig. Da die Lieferketten internationalisiert sind, kann auch der Ausfall der IT-Systeme bei Zulieferern erheblichen Schaden verursachen. Doch nicht nur Cyberangriffe sind die Ursache für gestörte Geschäftsprozesse. Auch Naturkatastrophen oder Terroranschläge stellen das Notfall-Management auf den Prüfstand.

Aber: Viele Firmen sind nur unzureichend widerstandsfähig gegen solche Ereignisse. Das zeigt eine weltweite Umfrage des Sicherheitsspezialisten Tanium unter 4000 Entscheidungsträgern unter anderem in Deutschland. Danach gehört Business Resilience nur bei 54 Prozent der weltweit Befragten zur erweiterten Geschäftsstrategie ihres Unternehmens. Mit anderen Worten: Rund die Hälfte der Firmen ergreift keine aufeinander abgestimmten Maßnahmen, um sich gegen Geschäftsunterbrechungen, etwa durch Cyberangriffe, zu wappnen.

Es ist also an der Zeit zu handeln. Wie aber bekommen Unternehmen die Schäden durch digitale Attacken oder andere

Notfälle schnell in den Griff? Die Antwort lautet: Business Continuity Management (BCM). Ziel von BCM ist es, derartige Schäden zu begrenzen und bestmögliche Vorkehrungen für den Fall schwerer Störungen zu treffen.

Das ist BCM

„Business Continuity Management sichert zeitkritische Geschäftsprozesse eines Unternehmens, um bei einem Notfall die Schadensfolgen zu minimieren und mit Hilfe von Notfallkonzepten und -plänen einen zuvor definierten Notbetrieb zu erreichen. Zudem geht es um den möglichst zeitnahen Wiederanlauf in den Normalbetrieb", erklärt Matthias Hämmerle, Berater für BCM sowie Notfall- und Krisenmanagement.

Während sich Business Continuity Management auf die Geschäftsprozesse des Unternehmens konzentriert, hat das IT Service Continuity Management (ITSCM) oder auch Disaster Recovery die Wiederherstellung der IT-Anwendungen, Daten und IT-Systeme im Fokus. In der IT ergänzen sich laut Hämmerle beide Disziplinen. „Das BCM für die IT sichert die IT-Geschäftsprozesse und deren Ressourcen, ohne die eine Wiederherstellung der IT gar nicht möglich wäre, sowie elementare IT-Unterstützungsprozesse für die Fachbereiche."

Ein Beispiel: BCM betrifft übergeordnet die Geschäftsprozesse, wenn etwa in einer Bank der Zahlungsverkehr nicht mehr funktioniert, weil die IT ausfällt. Inhalt des BCM wäre hier, wie die Bank den Zahlungsverkehr ohne IT-Unterstützung bestmöglich weiterführt. Parallel versucht die IT im IT Service Continuity Management, die betroffenen IT-Systeme wiederherzustellen.

Risiken bewerten

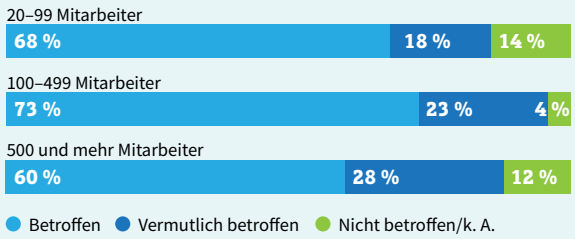
Der erste Schritt auf dem Weg zum BCM ist die Risikoanalyse. Es geht darum, Risiken oder kritische Prozesse zu identifizieren und sicherzustellen, dass sie nicht beeinträchtigt werden. Mittel der Wahl ist die Business-Impact-Analyse (BIA). Hier schätzen Firmen die Schadensfolgen bei einem Ausfall der Systeme (siehe Kasten unten). Die BIA erstreckt sich neben den Fachbereichen natürlich auch auf die IT, die mit den IT-Services das Rückgrat der Geschäftsprozesse stellt. Dazu gehören der Betrieb der Anwendungen und Systeme, die Anwendungsentwicklung, Help Desk oder die IT-Security. Die Fachbereiche bewerten in ihrer BIA, welche IT-Services wie kritisch für ihre Prozesse sind. Im Idealfall liegen Service Level Agreements (SLAs) vor, die die Anforderungen an die IT-Services und deren Verfügbarkeiten klar definieren. Daraus leitet die IT ab, welche Prozesse und Ressourcen sie benötigt, um die Anforderungen zu erfüllen.

„Die Kunst ist es, die IT tatsächlich dauerhaft aktuell zu halten und im Krisenfall schützen zu können. Im Krisenfall hilft es wenig, sich nur auf Manuskripte, die unterbrechungsfreie Stromversorgung (USV) und Schiffsdiesel sowie das Backup zu verlassen. Es bedarf auch einer krisensicheren Messaging-Lösung. Zudem sollten das Management von Cloud-Lösungen, virtuelle Systeme, Datenbanken, Applikationen samt Logiken und Priorisierungen abbildbar sein", erklärt Jürgen Kolb, Managing-Partner beim Security-Spezialisten iQSol.

Notfallplan

Die Risikobewertung bildet die Basis für den Notfallplan. Idealtypisch gibt es fünf Phasen für die Rückkehr aus der Krise in den regulären Betrieb: 1. Sofortmaßnahmen, 2. Wiederanlauf Notbetrieb, 3. Notbetrieb, 4. Wiederherstellung Normalbetrieb, 5. Nachbearbeitung. ▶

Gefährdete Mittelständler



Angriffe auf Unternehmen: In den vergangenen beiden Jahren traf es besonders den Mittelstand.

com! professional 3/19 Quelle: Bitkom Research, n = 503

BCM-Projekte – Tipps zur Umsetzung

Ein BCM-Projekt besteht im Wesentlichen aus den folgenden Etappen:

- **BCM-Leitlinie:** Die Leitlinie legt die Ziele von Business Continuity und den Geltungsbereich des BCM fest. Sie umfasst auch die Definition der Verantwortlichkeiten.
- **Business-Impact-Analyse:** In der BIA schätzen Firmen die Folgen bei einem Ausfall der Systeme. Das können finanzielle Einbußen sein, Image-Schäden oder der Verstoß gegen Gesetze und Verträge.

  Eng damit verbunden ist die Analyse und Bewertung von Risiken oder kritischen Prozessen im Unternehmen. Welche Themen bergen das größte Risiko für unsere Werte (Assets wie Informationen, Hardware, Software, Mitarbeiter, Reputation), Geschäftsprozesse und den Betrieb?
- **Notfallplan und Checklisten:** Der Notfallplan beschreibt in Form von Wenn-dann-Szenarien detailliert die Schritte, Prozeduren und Verfahren im Fall des Ausfalls der Systeme. Hilfreich sind Checklisten, damit die Mitarbeiter genau wissen, was im Notfall zu tun ist. Sehr wichtig sind auch die jeweiligen Kontaktdaten für die Alarmierung und die Kommunikationswege zur Steuerung und Überwachung einer kritischen Situation.
- **Tests und kontinuierliche Verbesserung:** Im Rahmen der PDCA-Methodik sollte man die BCM-Regeln mittels Übungen und Tests immer wieder prüfen und fortlaufend weiterentwickeln.

Interview

„BCM wird oft falsch verstanden“

Manfred Harwardt ist Business-Continuity-Manager und Krisenmanagement-Trainer beim IT-Dienstleister Fiducia & GAD IT. Im Interview mit com! professional erklärt er, was ein funktionsfähiges Business Continuity Management ausmacht und worauf Firmen beim Aufbau eines BCM achten sollten.

Manfred Harwardt

Business-Continuity-Manager und Krisenmanagement-Trainer für Banken bei Fiducia & GAD
www.fiduciagad.de

com! professional: *Herr Harwardt, wie definieren Sie den Begriff Business Continuity Management in der IT?*

Manfred Harwardt: Business Continuity Management in der IT wird oft falsch verstanden und führt auch zu Missverständnissen. BCM stellt die Verfügbarkeit von zeitkritischen Geschäftsprozessen sicher. Allerdings liegt der Fokus nicht auf den Prozessen, sondern vielmehr bei den Ressourcen der Prozesse. Ein Prozess kann nicht ausfallen – was ausfällt, sind Ressourcen. Das BCM definiert Anforderungen an die IT-Services, die die Geschäftsprozesse unterstützen. Das IT Service Continuity Management (ITSCM) unterstützt wiederum das BCM. Somit ist das ITSCM als integraler Bestandteil des übergeordneten BCM anzusehen. Im ITSCM werden IT-Risiken definiert und gemindert sowie sichergestellt, dass ein Mindestmaß an IT-Services im Notfall zur Verfügung steht.

com! professional: *Wie lassen sich kritische Geschäftsprozesse und Ressourcen identifizieren und effizient absichern?*

Harwardt: Grundsätzlich geht es im BCM um eine Absicherung der Unternehmensstrategie, aus der sich wesentliche und wertschöpfende Tätigkeiten ableiten.

Die einzelnen Fachbereiche hinterfragen für jeden Prozess die Zeitkritikalität in Bezug auf unterschiedliche Schadensszenarien und bestimmen die maximal tolerierbare Ausfallzeit. Sie ermitteln also die Zeitspanne, innerhalb derer ein Service, Prozess und IT-Service in einem Mindestmaß an Funktionalität wieder zur Verfügung stehen muss.

> **„Im Business Continuity Management geht es grundsätzlich um eine Absicherung der Unternehmensstrategie.“**

com! professional: *Was macht ein funktionsfähiges BCM aus?*

Harwardt: BCM ist ein proaktiver Prozess mit vielen planbaren Vorgängen und hat den Vorteil, dass Firmen bereits im Normalbetrieb Notfallteams zusammenstellen können. Getestete, funktionierende Notfallpläne finden in Notfällen und Krisen ihre Anwendung. BCM ist in Notfällen ein Teil des Krisenmanagements. Notfallpläne enthalten Elemente, die tatsächlich in derartigen Situationen umgesetzt werden: Was muss sofort, kurz-, mittel- und langfristig getan werden?

com! professional: *Wie sollten Firmen bei der Implementierung eines BCM-Systems vorgehen?*

Harwardt: Vor dem Start müssen Firmen Grundlagen und Ziele für das BCM definieren, festlegen und kommunizieren. Das betrifft den Geltungsbereich, die Organisation mit Rollen und Verantwortlichkeiten sowie Maßnahmen und Schnittstellen, die mit einbezogen werden sollen. Anschließend folgt die Business-Impact-Analyse. Welche wertschöpfenden Tätigkeiten hat mein Unternehmen? Wo gibt es verletzliche Punkte? Was darf wie lange ausfallen, welche Ressourcen werden benötigt? Ergebnisse dieser Analyse zeigen im Zeitverlauf an, welche Schäden Ausfälle zur Folge haben können. Was ich noch nicht kenne, sind Risiken, die dazu führen, dass die Prozesse ausfallen. In der anschließenden Risikoanalyse werden interne und externe Bedrohungen identifiziert, die eine Unterbrechung der Geschäftsprozesse zur Folge haben können.

com! professional: *Welche Schritte folgen nach den Analysen?*

Harwardt: Die Erkenntnisse der beiden Analysen bilden den Grundstock für alle weiteren Maßnahmen im BCM. Für die Prozesse müssen die Firmen nun für Worst-Case-Szenarien wie den Ausfall von Gebäuden, Personal, IT/Infrastruktur oder Dienstleistern Möglichkeiten finden, diese in Notfällen aufrechtzuerhalten. Dazu dienen die sogenannten Strategieoptionen. Bei dem Szenario „Ausfall der IT“ handelt es sich allerdings nicht um das ITSCM. Hier wird lediglich hinterfragt, was ich noch ohne IT machen kann.

Im nächsten Schritt werden die erforderlichen Pläne mit Beschreibungen der einzelnen Rollen, Verantwortlichkeiten und Handlungsweisen erstellt. Ziel ist es, diese Pläne durch regelmäßige Tests, Übungen und Audits zu verbessern. Wichtig sind zudem Awareness-Kampagnen, um das Bewusstsein zum BCM im gesamten Unternehmen zu verankern.

com! professional: *Und welche Funktionen und Merkmale sollte eine Lösung für BCM umfassen?*

Harwardt: Wichtige Funktionen und Merkmale sind die Verbindung zu anderen Disziplinen und eine Vermeidung von doppelter Datenhaltung. Da der Lifecycle des BCM und ITSCM eng miteinander verknüpft sind, sollten diese Disziplin sowie deren Aufgaben im Krisenmanagement mit verankert sein.

Der IT-Notfallplan beispielsweise legt Verantwortlichkeiten fest und beschreibt meist in Wenn-dann-Szenarien detailliert die Schritte und Verfahren bei Ausfall der kritischen Systeme.

„Am besten ist es, für Notfälle Checklisten zu erstellen, damit die Mitarbeiter genau wissen, was im Fall der Fälle zu tun ist. Diese Pläne funktionieren aber nur, wenn das beschriebene Szenario auch exakt so eintritt, wie es der Plan vorsieht", betont Matthias Hämmerle. Die Realität sieht oft anders aus. Es ist schlicht unmöglich, jeden Notfall detailliert zu planen. Dann benötigen Firmen eine Organisation, die die Maßnahmen koordiniert und die Pläne an die aktuelle Lage anpasst.

„Das ist der Krisenstab. Er steuert die Notfallmaßnahmen vor allem bei einer externen Wirkung, sprich wenn Kunden betroffen sind, die Presse vor der Tür steht oder die IT-Abteilung die Störung nicht mehr im Linienbetrieb beheben kann, etwa wenn Ransomware das Backup verschlüsselt hat. Der Krisenstab ist eher reaktiv, baut auf Notfallplänen auf, während das BCM mit seiner Notfallplanung eher präventiv agiert", so Hämmerle weiter.

Jürgen Kolb von iQSol sieht beim Thema BCM einen theoretischen und einen praktischen Teil. „Ein Notfallhandbuch sorgt für Klarheit, wer zuständig ist, welche Geräte und Abhängigkeiten es gibt und wo sich etwa Backups der Daten befinden, damit diese nach einem Crash schnell eingespielt werden können." In der Praxis geht es Kolb zufolge auch darum, schnell Maßnahmen zu ergreifen, „damit aus einem Notfall keine Katastrophe wird. Hier sind drei Schritte wichtig: Unregelmäßigkeiten im Netzwerk erkennen zu können, die unverzügliche, verlässliche Alarmierung der zuständigen Mitarbeiter in der IT und drittens das Ergreifen wirksamer Maßnahmen zum Schutz der Systeme."

Bild: Gartner

„Magic Quadrant for BCM Program Solutions 2017": Die Einschätzung von Gartner gilt für den internationalen Markt.

Ständige Tests

BCM sollte natürlich kein Papiertiger sein, sondern auch in der Praxis funktionieren. Firmen müssen daher ihr Notfallkonzept und ihr Krisenmanagement regelmäßig durch Tests und Übungen überprüfen. In den Disaster-Tests üben sie das Vorgehen, das im Notfallhandbuch festgelegt wird. Doch nicht alle Systeme verhalten sich entsprechend der Theorie. „Das Durchhaltevermögen von USVs ist mitunter kürzer als angenommen, Leitungen können defekt sein, es kommt zu wiederholten Starts der Systeme oder es fehlen schlichtweg Bediener", betont Jürgen Kolb.

Bild: Matthias Hämmerle

„Bereite dich auf alle möglichen Szenarien vor, dann kannst du im Notfall besser reagieren. Die Frage ist nicht, ob das passiert, sondern wann."

Matthias Hämmerle
Gründer und Inhaber von Hämmerle-Consulting
www.haemmerle-consulting.de

BCM ist ein permanenter Prozess und fordert die kontinuierliche Verbesserung nach der PDCA-Methodik:

- Plan: Definition des Soll-Zustands
- Do: Umsetzung des Soll-Zustands in den Ist-Zustand
- Check: Vergleich des umgesetzten Ist-Zustands mit dem zuvor definierten Soll-Zustand
- Act: Anpassung des Ist-Zustands aufgrund festgestellter Probleme ▶

Krisenstabsübungen

Eine der wichtigsten Maßnahmen in der Notfall- und Krisenprävention sind Krisenstabsübungen. Hier lernen die Teilnehmer des Krisenstabs den Umgang mit unerwarteten Ereignissen, um wieder Herr der Lage zu werden.

„Beim Erstellen von Drehbüchern für diese Übungen kann man seiner Fantasie freien Lauf lassen. Unwetter, Stromausfälle, Hackerangriffe, Terroranschläge, Epidemien, alles ist möglich. Es ist nicht schwer, relativ realistische Stress-Situationen hervorzurufen und Zeitdruck aufzubauen. Wir nutzen dazu Medientechnik, um eingehende Meldungen zu simulieren, Berichte aus dem Radio oder TV darzustellen und vieles mehr", sagt Manfred Harwardt, Business-Continuity-Manager und Krisenmanagement-Trainer für Banken bei Fiducia & GAD (siehe auch Interview). Der Krisenstab ist das wichtigste Gremium beim Management derartiger Extremsituationen. Der engere Krisenstab besteht meist aus dem Leiter des Krisenstabs, seinem Assistenten, einem Protokollanten, einem Mitarbeiter, der alle entstandenen Probleme und deren Status visualisiert, sowie einem Mitarbeiter für die Krisenkommunikation, der alle Berichte zur Katastrophe in Presse, Radio, TV und Social Media überwacht und der Öffentlichkeit Rede und Antwort steht. Der erweiterte Krisenstab kann aus Teilnehmern wie IT- oder Prozess-Spezialisten, Personalabteilung oder Juristen bestehen.

Ziel des Krisenstabs ist es, die Lage wieder unter Kontrolle zu bringen. Er entscheidet, welche Teams und Notfallpläne in welcher Reihenfolgen aktiviert werden, leitet zusätzliche Maßnahmen ein, die nicht in Plänen stehen und sich nicht vorbereiten lassen, und überwacht, welche Quellen in welcher Weise über die Katastrophe berichten (Monitoring).

Im letzten Schritt werden die Ursachen der festgestellten Abweichungen abgestellt, der PDCA-Zyklus beginnt wieder von vorn.

CEO muss unterstützen

In den Augen von Matthias Hämmerle besteht Business Continuity Management aus einem ganzen Strauß von Maßnahmen auf unterschiedlichen Ebenen. „Die Kernbotschaft zu BCM lautet: Be prepared – bereite dich mittels Notfallplänen und vor allem im Rahmen von Tests und Übungen auf alle möglichen Szenarien vor, dann kannst du im Notfall besser reagieren. Die Frage ist nämlich nicht, ob das passiert, sondern wann."

Entscheidend für den Aufbau eines nachhaltigen BCM ist das Mandat der Geschäftsleitung. Der CEO muss die BCM-Konzepte unterstützen, die Fachbereiche mit ins Boot holen, sowie die finanziellen und personellen Ressourcen bereitstellen. „Die größte Hürde ist gemeistert, wenn ein Bewusstsein darüber existiert, dass wirklich etwas passieren kann", weiß Jürgen Kolb. Sinnvoll ist es zudem, das BCM als Stabsstelle unterhalb der Geschäftsführung einzurichten. „Schon jetzt werden Business-Continuity-Manager aufgewertet und erhalten eigene Budgets. Dieser Trend wird sich fortsetzen, damit sie im Krisenfall auch operativ tätig sein können."

Orientierung an Standards

Beim Aufbau, Betrieb und der Optimierung eines BCM-Systems empfehlen die von com! professional befragten Experten die Orientierung an Standards und Best Practices wie ISO 22301, ISO 27031 oder BSI 100-4. ISO 22301 beispielsweise basiert auf dem PDCA-Zyklus (Plan, Do, Check, Act) und enthält neben Planung, Überprüfung und Training auch die Ver-

Anbieter von BCM-Tools (Auswahl)

Anbieter / Produkt	Internet	Zentrale Funktionen	Besonderheiten
Controllit / alive-IT	www.controll-it.de	Planung und Bewältigung von Notfällen sowie die Abbildung von BCM, ITSCM und Krisenmanagement mit allen üblichen Funktionen (Analysen, Notfallpläne, Tests); vermeidet doppelte Datenpflege durch automatisierte Schnittstellen	Flexibel und kundenindividuell zu gestalten; Webbrowser als Frontend (Java), keine Client-Installation notwendig. Controllit entwickelt nicht nur die Software, sondern berät auch zu den Themen BCM, ITSCM, und Krisenmanagement
Finanzinformatik / Beluga	www.finanzinformatik.ch	Notfallvorsorge- und IT-Sicherheits-Management nach aktuellen Vorgaben von BaFin und FINMA mit den üblichen BCM-Funktionen (BIA und Risikoanalyse, Erstellung von Notfallplänen, Übungen etc.)	Webbasiertes BCM-System; Tool verbindet Notfallvorsorge mit Management von Informationssicherheit und Datenschutz; Schwerpunkt Finanzwesen; ständige Aktualisierung aller relevanten Detailpläne und Informationen
Fuentis / Fuentis BCM	www.fuentis.com	Strukturierte IT-Notfallplanung; Integration mit verschiedenen Systemen möglich; BIA, IT-Notfall- und IT-Betriebshandbuch, Darstellung von Verantwortlichkeiten etc.	BCM-Modul ist Teil eines integrierten Managementsystems für Governance, Risk & Compliance; bildet Abhängigkeiten zwischen Prozessen, Services und der IT ab; Aufgaben-Management und Webmodul zur strukturierten Pflege
GRC Partner / DocSetMinder (Modul Notfallmanagement)	www.docsetminder.de	Business-Impact-Analyse, Risikoanalyse, Notfallplanung, Alarmierung/Notifier, Krisenmanagement, Testunterstützung, Wartungs-Workflow, Erstellung Notfallhandbuch	DocSetMinder-Modul „Notfallmanagement" basiert auf dem BSI-Standard 100-4 und ISO 22301; bildet die PDCA-Methodik zum Aufbau eines adäquaten Notfallmanagement-Systems ab; Integration in die bestehende IT-Landschaft, mandantenfähig
HiScout / HiScout BCM	www.hiscout.com	Business-Impact-Analyse, Risikoanalyse, Notfallpläne und Pläne zum Wiederanlauf und zur Wiederherstellung, Planung und Dokumentation von Notfallübungen und Tests, Analyse von Notfall- und Krisenszenarien, Unterstützung von Audits	HiScout BCM ist Teil einer umfassenden Plattform für das Management von IT-Governance, Risk & Compliance; bildet alle Phasen des Business-Continuity-Management-Cycles ab; unterstützt die Standards ISO 22301 und BSI 100-4
iQSol / iQSol LogApp, iQSol AMS, iQSol PowerApp	www.iqsol.biz	LogApp erkennt Auffälligkeiten im Netzwerk mittels Log-Management; AMS alarmiert im Notfall per E-Mail, Anruf oder SMS zuständige Mitarbeiter und berücksichtigt dabei auch aktuelle Dienstpläne; PowerApp fährt alle Systeme herunter und wieder hoch, Disaster-Tests sind ebenfalls möglich	Deckt den BCM-Prozess technisch ab mit dem Management der gesamten IT bis hin zu virtuellen Systemen. Entwicklung einer BCM-Strategie für die Kunden in Zusammenarbeit mit der Netzwerkberatung Antares-NetlogiX
WMC / QESC	https://wmc-direkt.de	Business-Impact-Analyse, Risikobewertung, Notfallplanung, Notfalltests für Geschäftsprozesse, Überprüfen und Bewertung der Dokumentation für kritische Asset-Gruppen (IT-Notfallplan, Betriebshandbuch, Wiederanlaufplan)	Modulare QSEC-Suite für Compliance Management, Datenschutz, BCM, IT-Risikomanagement, Business-Impact-Analyse; PDCA-Methode; Maßnahmenvorschläge/Musterdokumente; Integration in die bestehende IT-Infrastruktur – keine Doppelerfassung von Daten

besserung von Organisationsprozessen. ISO 27031 konzentriert sich auf die Schnittstellen zwischen BCM und IT-Notfallmanagement, der BSI-Standard 100-4 zeigt einen systematischen Weg für den Aufbau eines Notfallmanagements etwa in einer Behörde.

BCM-Tools

Als weitere Hilfe gibt es spezielle Software-Lösungen, die Unternehmen unterstützen. Sie bieten eine zentrale Datenhaltung für Geschäftsprozesse und IT-Anwendungen sowie Schnittstellen zu Systemen etwa zur Alarmierung oder zur IT-Strukturanalyse.

Eine erste Orientierung böte eigentlich der „Magic Quadrant for Business Continuity Management Program Solutions" von Gartner, der wichtige Hersteller umfasst. Der Haken: „Der Gartner-Quadrant betrifft den internationalen Markt. In Deutschland können diese großen Anbieter nur schwer Fuß fassen", erklärt Matthias Hämmerle.

Bild: iQSol

„Schon jetzt werden Business-Continuity-Manager aufgewertet und erhalten eigene Budgets. Dieser Trend wird sich fortsetzen, damit sie im Krisenfall auch operativ tätig sein können."

Jürgen Kolb
Managing-Partner bei iQSol
www.iqsol.biz

Auf dem deutschen Markt gibt es laut Hämmerle einige wenige spezialisierte Hersteller von BCM-Tools mit Funktionen wie Business-Impact-Analyse und Notfallplan, darunter etwa HiScout, Controllit oder die Beluga-Lösung der Finanzinformatik GmbH. Zudem integrieren auch Anbieter von Lösungen für den Aufbau von Information-Security-Management-Systemen zunehmend BCM-Funktionalitäten in ihre Tools. Ein Beispiel dafür ist Fuentis.

Fazit

Grundsätzlich gilt: Es gibt keine hundertprozentige Sicherheit. Unternehmen müssen das Restrisiko minimieren und mögliche Schäden transparent machen. Genau darum geht es bei BCM. Zu einem guten BCM gehören die Business-Impact-Analyse mit Risikobewertung, das Design der Notfallkonzepte für die kritischen Ressourcen, die eigentliche Implementierung sowie Tests und Übungen zum Überprüfen der Pläne. Ein BCM-Plan umfasst zudem die Kontaktdaten und Alarmierungsketten, Notfallprozeduren für den Notbetrieb, interne und externe Kommunikation im Notfall sowie Verfahren für den Wiederanlauf in den Normalbetrieb.

BCM funktioniert jedoch nur, wenn es in die Gesamtstrategie der Firma eingebunden ist. Die Geschäftsleitung muss BCM unterstützen. ■

Jürgen Mauerer/kpf
kpf@com-professional.de