Gut vorbereitet für Krisenzeiten

Wie ein Telekommunikationsdienstleister seine Betriebs- und Geschäftsfähigkeit absichert

Unternehmen müssen trotz Cybergefahren, Klimaveränderungen oder Pandemien ihre Geschäfte absichern. Ein Telekommunikationsanbieter hat daher auf der Grundlage einer Risikobetrachtung ein Business-Continuity-Managementsystem aufgebaut. Zusammen mit einem Informationssicherheits-Managementsystems kann der Dienstleister nun mögliche Bedrohungen im Vorfeld abwenden oder Auswirkungen von Vorfällen geringhalten.

Antje Golbach

Aufgrund der steigenden Verzahnung von Geschäftsprozessen, der Abhängigkeit von IT Services sowie durch sich verändernde globale Rahmenbedingungen, Pandemien und unkalkulierbare Umwelteinflüsse müssen sich Unternehmen verstärkt auf die damit verbundenen Risiken einstellen. Unternehmen sind gefordert, diese Risiken zu bewerten und entsprechende Konzepte zu entwickeln, um im Falle eines Vorfalls die Betriebs- und Geschäftsfähigkeit schnell wieder aufzunehmen.

Vodafone Deutschland setzt für diese Aufgaben seit einigen Jahren ein Business-Continuity-Managementsystem (BCM-System) nach ISO 22301 ein. Bereits im Jahr 2011, als es noch den britischen Standard BS25999 gab, ließ Vodafone sein BCM-System durch TÜV Rheinland prüfen und zertifizieren.

Als Provider für Millionen Mobilfunk- und Festnetzkunden und als Anbieter von ICT-Lösungen für Geschäftskunden ist Vodafone darauf angewiesen – im Falle einer Störung oder eines Ausfalles – schnell handeln zu können. Bei Bränden, Hochwasser, Hitzeschäden oder Anschlägen auf Mobilfunkmasten ist es für Vodafone mitunter geschäftsentscheidend, zügig den Be- ›››

trieb wieder in Gang zu setzen. Daher ist ein BCM-System, das die entsprechenden Rahmen und Leitlinien für das betriebliche Kontinuitätsmanagement liefert ein elementarer Baustein.

Überdies stellt das Thema Business-Continuity-Management mittlerweile für Banken und Unternehmenskunden ein wichtiges Entscheidungskriterium für eine Zusammenarbeit dar und ist auch bei Vergabeprozessen von Kunden ein Pluspunkt.

Aus diesen unterschiedlichen Gründen und aufgrund der Anforderungen der Vodafone Group entschied sich Vodafone Deutschland schon frühzeitig für den Aufbau und Einsatz des BCM-Systems nach einem anerkannten Standard wie der ISO 22301.

Risikobetrachtung als Grundlage für den Aufbau eines BCM-Systems

Der erste Schritt beim Aufbau eines BCM-Systems nach ISO 22301 begann bei Vodafone mit der Analyse und Bewertung der neuralgischen Punkte im Unternehmen.

Welche Produkte, Prozesse, Systeme, Standorte und Dienstleister sind maßgeblich an der Erfüllung der Kundenservices beteiligt? Wie hoch ist das Risiko, dass hier ein Vorfall eintreten könnte, der die Geschäftstätigkeit und damit den Geschäftserfolg empfindlich treffen könnte?

Bei Vodafone sind es in erster Linie alle Produkte, Prozesse und Systeme, die unmittelbar mit den Kunden, mit der Abwicklung von Aufträgen und Services zu tun haben. Hierzu zählt als erstes die Sicherstellung des Netzbetriebs für die Services und Produkte an die Endkunden.

Aber auch Call-Center Prozesse, um die Erreichbarkeit von Vodafone für die Endkunden sicherzustellen, gehören dazu ebenso wie die Prozesse zur Kundenauftragsbearbeitung. Von diesen leiten sich die besonders schützenswerten IT-Systeme mit allen Kundendaten ab, die bei der Risikobewertung als Bestandteil des Kontinuitätsmanagements eine gewichtige Rolle spielen.

„Bei der Risikobewertung nutzen wir einen generischen Ansatz auf Prozessebene, der die Anforderungen der ISO 22301 erfüllt und es den Prozessverantwortlichen einfach macht, die Risiken zu identifizieren und die in ihrer Verantwortlichkeit liegenden Notfallstrategien zu entwickeln“, erklärt Astrid Wiesendorf, Referentin für Risk- & Business-Continuity-Management bei Vodafone Deutschland.

Die als kritisch eingestufte Systemtechnik wie Netzwerkelemente und IT-Systeme müssen zum Schutz vorgegebene Kontrollanforderungen erfüllen. Zu diesen Anforderungen zählen unter anderem der Wiederherstellungsplan und der regelmäßige Test zur Wiederherstellung.

Wichtige Faktoren bei der Risikobetrachtung

Auch wichtige Technikstandorte wie Rechenzentrumsstandorte und Vermittlungsstellen, die für den Erhalt eines intakten Fest-, Kabel- oder Mobilfunknetzes notwendig sind, fließen in die Risikobetrachtung und -bewertung ein. Die Technik setzt bereits bei der Planung auf eine resiliente Architektur, welche die Endkundenservices und IT Services gegen Ausfälle absichern soll und Redundanzen vorsieht.

Für dezentrale Verteilerstandorte, die in einer Baumstruktur eingebunden sind, besteht immer die Gefahr, dass die Netzverbindung für Kunden komplett ausfallen kann. Auch bei diesen Standorten werden je nach Kritikalität – das heißt Sicherheitseinstufung – präventive Maßnahmen umgesetzt, um das Ausfallrisiko zu minimieren. Zudem werden für die Worst-Case-Szenarien angemessene Notfallstrategien und -pläne implementiert.

Bei der Sicherheitseinstufung wird die Auswirkung eines Standortausfalls bewertet. Hierbei spielen Fragen eine Rolle wie: Wie schwer sind die Folgen bei Brandausbruch, bei Anschlägen, Gewitter, Vandalismus, bei Ausfall der Klimaanlage oder bei Hochwasser? Und wie hoch ist die Eintrittswahrscheinlichkeit dieser Gefahren?

In erster Linie konzentriert man sich beim Aufbau des BCM-Systems zunächst auf jene Gefahren, die hochkritisch und wahrscheinlich sind. „Bereits bei der Standortplanung werden Umgebungsgefahren wie Hochwasser oder Gefahren bewertet und – falls das Risiko zu hoch ist – der Standort dort erst gar nicht geplant“, erläutert Wiesendorf.

Die festgelegten BCM-Maßnahmen müssen vom Aufwand und den damit verbundenen Kosten im Verhältnis zur Auswirkung stehen. Je wichtiger und ausfallkritischer ein Prozess, ein System, ein Standort oder Verteilerknotenpunkt ist desto wichtiger und mitunter aufwendiger sind die BCM-Maßnahmen.

Interessierte Parteien und ihr Einfluss auf das BCM

Bei der Risikobetrachtung und der Implementierung des BCM-Systems nach ISO 22301 liegt der Fokus nicht allein auf dem Unternehmen selber, sondern es ist erforderlich, über die eigenen Unternehmensgrenzen hinauszugehen. So setzt Vodafone für spezielle Tätigkeiten und Services verschiedene Dienstleister ein. Diese zählen laut ISO 22301 zu den interessierten Parteien eines Unternehmens und sind gemäß Normanforderungen ebenfalls bei dem Kontinuitätsmanagement zu berücksichtigen. So hat Vodafone beispielsweise für das Gebäudemanagement, die Notstromversorgung, die Klimatisierung und das Monitoring verschiedene Dienstleister im Einsatz.

Die Lieferanten werden nach Kritikalität bewertet, entsprechende Notfallpläne beim Dienstleister eingefordert oder es wird eine Krisenmanagementvereinbarung festgelegt. Bei dem Onboarding-Prozess eines Dienstleisters führt Vodafone zum Teil auch Vor-Ort-Audits durch.

Dabei wird geprüft, ob das Unternehmen selber eine Risikobewertung durchführt und darauf abgestimmte Maßnahmen entwickelt hat oder, ob der Dienstleiser über Zertifikate wie eine BCM-Zertifizierung nach ISO 22301 oder ISO 27001 für Informationssicherheit verfügt.

„Diese Zertifikate erleichtern uns natürlich die Arbeit und verkürzen die Audits, da sie dokumentieren, ob ein Unternehmen bereits in Sicherheit und Notfallplanung investiert hat“, erläutert Oliver Harzheim als Corporate-Security-Officer der Vodafone GmbH.

Auch die Mitarbeiter zählen zu den interessierten Parteien. Mitarbeiter müssen zum einen geschult werden und für den Aufbau und den Betrieb des BCM-Systems entsprechende Kompetenzen mitbringen. Zum anderen gilt es auch, die Mitarbeiter im Falle einer Gefahr zu schützen. Hier stellt sich das BCM-Team von Vodafone die Frage: Wo sind typische Gefahrenquellen für unsere Mitarbeitenden und wie können wir Gefahrenpotenziale ausschalten oder zumindest erheblich verringern?

„Die Corona-Pandemie ist ein typisches und gleichzeitig außergewöhnliches Beispiel für eine gravierende Gefahr, die viele interessierte Parteien unmittelbar involviert und diese bedroht: unsere Mitarbeiter, Lieferanten und Kunden", erläutert Oliver Harzheim, der auch als Leiter der Corona Taskforce fungiert.

Das BCM-System nach ISO 22301 und die damit einhergehenden Maßnahmen und Dokumentationen liefern in solchen Situationen einen sehr hilfreichen Handlungsrahmen mit entsprechenden Leitlinien und Strukturen. So hatte Vodafone durch das BCM-System bereits ein Krisen- und Notfallteam etabliert und verfügte über spezielle Alarmierungs- und Kommunikationsprozesse, die schnell aktiviert werden konnten.

„Die Negativauswirkungen von Corona waren bisher geringer als befürchtet. Dieses liegt zum einen daran, dass wir gut vorbereitet waren. Zum anderen ist es sicher von Vorteil, dass Vodafone ein stark digital ausgerichtetes Unternehmen ist. Homeoffice wird von unseren Mitarbeitern seit Jahren in Anspruch genommen. So konnten unsere Mitarbeiter zügig auf das Homeoffice ausweichen, um die Ansteckungsgefahr zu reduzieren", erklärt Astrid Wiesendorf.

Das Audit- und Zertifizierungsverfahren

Die Wirksamkeit des BCM-Systems und die damit verbundenen Maßnahmen gilt es in festgelegten Intervallen zu überprüfen. Nach Vorgaben der ISO 22301 setzt Vodafone zum einen interne Audits um, zum anderen werden durch TÜV Rheinland-Auditoren, die das Unternehmen nach ISO 22301 zertifizierten, regelmäßige Audits durchgeführt.

Bei dem aus zwei Teilen bestehenden externen Auditverfahren schaut sich der TÜV Rheinland-Auditor zunächst die Dokumente über das BCM-System an und inwiefern diese die Normanforderungen erfüllen. Dabei stehen unter anderem Schulungs- und Notfallpläne, Ergebnisse der internen Audits und auch Ablauf und Ergebnisse von Notfall- und Wiederherstellungsübungen im Fokus der Betrachtung.

Einer der wichtigsten Pläne stellt – neben den Notfallplänen der Technik – der übergeordnete Krisenmanagement-Plan dar, dessen Funktionsfähigkeit Vodafone regelmäßig in Form von Live-Übungen prüft.

„Für die Wirksamkeit des BCM-Systems und der damit verbundenen Maßnahmen ist es wichtig, auch den Ernstfall zu planen, zu proben und die Ergebnisse zu messen, festzuhalten und möglicherweise das BCM-System auf Basis der Ergebnisse anzupassen", erläutert Thomas Kloos Auditor bei TÜV Rheinland.

Ein Messkriterium für die Wirksamkeit stellt beispielsweise der Faktor „Zeit" dar. Wie lange braucht es, bis im Krisenfall die Datenlast von einer anderen Sammlerstation übernommen werden kann? Wie lange dauert der Schwenk auf einen anderen Technikstandort nach einem schwerwiegenden Ausfall? Werden hier die zuvor definierten Zeitspannen im Rahmen der Live-Übung eingehalten?

„Die mit diesen Steps verbundenen Dokumente, Pläne und Ergebnisse schauen wir uns unter anderem an, um sicherzugehen, dass die Normanforderungen erfüllt werden und das Unternehmen bestrebt ist, mögliche Defizite zu erkennen, zu beseitigen und so den Reifegrad seines BCM-Systems zu erhöhen", so Kloos.

Die Vor-Ort-Begehung wichtiger Technikstandorte

In der zweiten Stufe des Audits folgt die Vor-Ort-Begehung des TÜV Rheinland-Auditors. Wichtige Technikstandorte wie beispielsweise die Vodafone-Sammlerstationen werden dabei berücksichtigt. In diesen Sammlerstationen werden Informationen verarbeitet, die via Funkmasten über Kabelverbindungen übertragen..

Der Auditor prüft beispielsweise, welche physikalischen Absicherungsmaßnahmen es für diese Stationen gibt, wie im Ernstfall eine Alarmierung stattfindet und wie die Verantwortlichkeiten in der Alarmierungskette aussehen. Die zweite Stufe des Auditverfahrens dient dazu, die Wirksamkeit des BCM-Systems festzustellen und inwiefern die in den Dokumenten dargelegten Schritte sowie Prozesse gelebt werden und in der Anwendung funktionieren.

Nach dem erfolgreichen Abschluss des Prüf- und Zertifizierungsverfahrens erfolgt in jährlichen Intervallen ein Überwachungsaudit. Im Rahmen der Überwachungsaudits wird stichprobenhaft überprüft, ob die Wirksamkeit des Systems weiter aufrechterhalten wird, bevor vor Abschluss des dritten Zertifizierungsjahres ein Rezertifizierungsaudit stattfindet.

„Die internen und externen Audits durch TÜV Rheinland unterstützen uns dabei, das BCM-System nutzbringend für unseren Schutzbedarf einzusetzen und weiterzuentwickeln", erklärt Astrid Wiesendorf.

Die Weiterentwicklung des BCM-Systems nach ISO 22301 stellt für Vodafone in dem gesamten Sicherheitskontext jedoch nicht das einzige Ziel dar. Da das Unternehmen auch ein Informationssicherheits-Managementsystem nach ISO 27001 betreibt, liegt es für Vodafone nahe, künftig beide Managementsysteme zu einem integrierten Managementsystem zusammenzufassen.

Die Grundlagen für die Erweiterung des Gesamtsystems sind jedenfalls geschaffen. Mit dem BCM-System nach ISO 22301 und dem Informationssicherheits-Managementsystems nach ISO 27001 hat Vodafone zwei wichtige Systeme in Betrieb, um mögliche Bedrohungen im Vorfeld abzuwenden und, falls dieses nicht möglich ist, die Vorfälle und ihre Negativeffekte möglichst gering zu halten oder gar komplett zu vermeiden.

„Gefahren können heutzutage aus unterschiedlichsten Richtungen auf Unternehmen einwirken. Mit einem BCM-System können wir uns in verschiedenster Hinsicht besser auf Cybergefahren, Klimaveränderungen oder Pandemien einstellen und trotz dieser Einflussfaktoren unser Geschäft absichern", erklärt Astrid Wiesendorf abschließend.

Auch hinsichtlich gesetzlicher Maßgaben, künftiger Regelungen und Kundenanforderungen sieht sich Vodafone mit dem BCM-System nach ISO 22301 sehr gut aufgestellt und kann seinen Sicherheitsanspruch gegenüber den verschiedenen Interessengruppen transparent mit dem TÜV Rheinland-Zertifikat darlegen. ■

INFORMATION & SERVICE

AUTOR

Antje Golbach ist Pressesprecherin Managementsysteme bei TÜV Rheinland, Köln.

KONTAKT

TÜV Rheinland
T 0221 806-4465
antje.goldbach@de.tuv.com
www.tuv.com