ISO 22301: Vorbereitung auf den Ernstfall

Wie schnell kann es passieren, und ein System fällt aus? Oder ein Hacker verschafft sich Zugriff auf das Firmen-Netzwerk und verschlüsselt alle Dateien? Oder ein Naturereignis zerstört Teile der Infrastruktur? Oder ein wichtiger Mitarbeitender fällt aus? Die Gründe für einen Unterbruch der (IT-)Dienstleistungen sind vielzählig. Daher ist es wichtig, sich bereits vor dem Eintreten eines solchen Ereignisses Gedanken zu machen und entsprechende Vorbereitungsmassnahmen zu treffen.

Die ISO 22301:2019 (deutsche Ausgabe wurde im Jahr 2020 veröffentlicht) zeigt, wie ein Business Continuity Management System (BCMS) aufgebaut werden kann. Es trägt den Titel «Sicherheit und Resilienz – BCMS – Anforderungen».

Wer sich bereits mit Normen wie der 9001 oder der 27001 auseinandergesetzt hat, wird sich schnell zurechtfinden. Es hat den identischen Aufbau wie die erwähnten Management System Normen. Es beschreibt den Prozess in den Schritten: Leitlinie (die Norm nennt diese Politik) und Planung, Umsetzung und Betrieb, Leistungsbewertung, Managementbewertung und fortlaufende Verbesserung, deckt also den klassischen Plan-Do-Check-Act Kreislauf ab.

Was genau meint die Norm?

Wie aus anderen Normen bekannt, werden im Kapitel 3 die Begriffe, die nachfolgend verwendet werden, eindeutig beschrieben. Es lohnt sich, diese 31 Begriffe nicht zu überlesen, um zu wissen, was genau die Norm meint beziehungsweise fordert.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Im Kapitel 4 wird der Kontext der Organisation gefordert. Dazu gehören externe und interne Themen zu bestimmen. Diese Themen werden durch die Ziele der Organisation, ihrer Produkte und Dienstleistungen sowie den Umfang und die Art des Risikos, das diese eingehen darf oder nicht, beeinflusst. In einem zweiten Schritt gilt es die interessierten Parteien sowie deren Anforderungen zu kennen. Dies lenkt unter anderem die Definition der maximalen Ausfalldauer und/oder den maximalen Datenverlust. Auch die rechtlichen oder behördlichen Anforderungen gilt es zu dokumentieren und in das BCMS zu integrieren. Dies kann beispielsweise die DSGVO oder das neue Schweizer Datenschutzgesetz sein. Wie beim Aufbau des ISMS kann auch beim BCMS der Anwendungsbereich selbst festgelegt werden. Dies macht zum Beispiel beim Betrieb eines Rechenzentrums Sinn. Das Gebäude, die Räume und Betriebsmittel gehören dann in den Anwendungsbereich, aber nicht das gesamte Unternehmen. Diese Abgrenzung muss aber gut überlegt sein, um sich nicht unnötig das Leben mit den notwendigen Abgrenzungen und Schnittstellen schwer zu machen.

Das Kapitel 5 nimmt die oberste Leitung in die Pflicht. Sie muss sicherstellen, dass es eine BCM-Politik gibt, diese auf die Ziele zur Aufrechterhaltung der Betriebsfähigkeit festlegen, die notwendigen Ressourcen bereitstellen, die Anforderungen allen vermitteln, Personen anleiten, sicherstellen, dass die gesteckten Ziele auch erreicht werden sowie die fortlaufende Verbesserung fördern. In diesem Kapitel werden auch die Rollen, Verantwortlichkeiten und Befugnisse zugewiesen. Allen involvierten Personen muss klar sein, was ihre Aufgabe ist, aber auch welche Möglichkeiten zur Verfügung stehen.

Umgang mit Risiken und Chancen

Der erste Schritt in Kapitel 6 ist die Definition des Umgangs mit Risiken und Chancen. Dabei sollten die bereits erfassten Risiken des Unternehmens berücksichtigt und geprüft werden, ob es weitere Risiken gibt, die im Rahmen des BCMs auftreten und bewertet werden müssen. Weiter gehört die Festlegung von Zielen zur Aufrechterhaltung der Betriebsfähigkeit dazu. Diese müssen auf die erwähnte BCM-Politik abgestimmt werden. Zur Erreichung dieser muss bestimmt werden:

- was getan wird;
- welche Ressourcen erforderlich sind;
- wer verantwortlich ist;
- wann es abgeschlossen wird;
- wie die Ergebnisse bewertet werden

Das Kapitel 7 trägt den Titel «Unterstützung». Dazu gehören die notwendigen Ressourcen, die Sicherstellung der Kompetenz der involvierten Personen, das Bewusstsein (sprich Schulungen/Awareness) bei allen Mitarbeitenden, die Definition der Kommunikation und Regeln, wie Dokumentationen erstellt, aktualisiert und gelenkt werden.

Verzögerter Effekt auf die Verfügbarkeit

Wenn alle Vorarbeiten erledigt sind, geht es ans Eingemachte. Das Kapitel 8 definiert die Anforderungen an den Betrieb des BCMs. Der erste Schritt ist die Business-Impact-Analyse. In der Business Impact Analyse (BIA) wird untersucht:

- welche Geschäftsprozesse zeitkritisch sind und
- ab welcher maximalen Ausfallperiode (MTPD) nicht tolerierbare Auswirkungen zu erwarten sind und mindestens ein Notbetrieb aufgenommen werden muss.

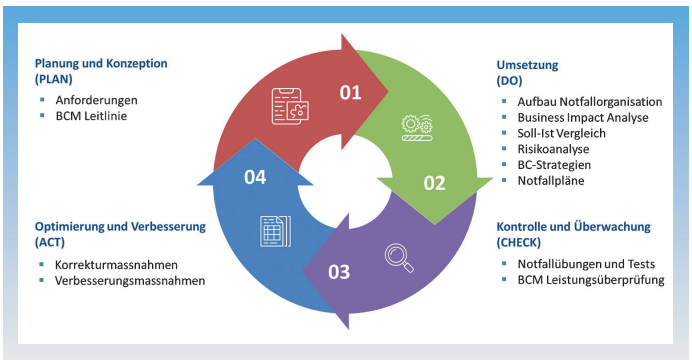
Ausserdem werden für diese zeitkritischen Prozesse:

- die Abhängigkeiten von anderen Prozessen ermittelt und
- die für deren Betrieb benötigten Ressourcen definiert.

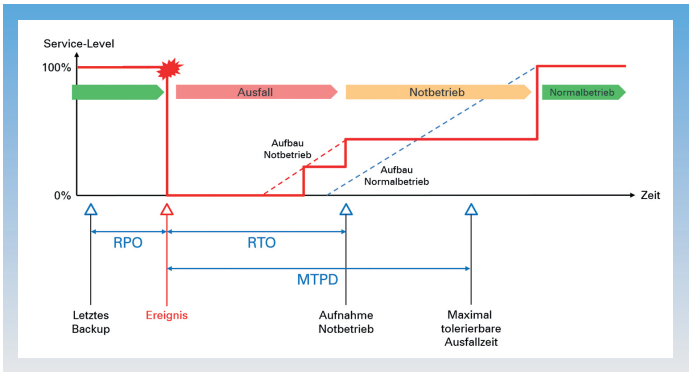
Schliesslich werden in einer vertieften Analyse dieser Ressourcen:

- deren Wiederanlaufparameter (RTO, RPO) festgelegt,
- diejenigen identifiziert, welche für den Notbetrieb zwingend funktionieren müssen,
- festgestellt, wo Single-Points-of-Failures bestehen, die mittels Vorsorgemassnahmen, wenn möglich, eliminiert werden sollten.

Es wird nur ein zeitlicher Ausfall der Verfügbarkeit eines Geschäfts-



Plan-Do-Check-Act Kreislauf.



Ausfall-Szenario.

prozesses und keine andere Beeinträchtigung betrachtet (zum Beispiel Integrität oder Vertraulichkeit).

Allerdings können solche Ereignisse einen indirekten und verzögerten Effekt auf die Verfügbarkeit eines Prozesses haben. Wichtig in diesem Schritt: Es werden nur die Konsequenzen eines Ausfalls und nicht dessen Ursachen betrachtet.

- RPO (Recovery Point Objective): beschreibt die Zeitperiode, für welche die Daten nicht wiederherstellbar sind. In der Praxis bedeutet dies die Zeit zwischen zwei Daten-Backups.
- RTO (Recovery Time Objective): beschreibt die Zeitspanne, bis der Prozess seinen Betrieb wieder aufnehmen kann. Der Betrieb darf allerdings eingeschränkt sein (Notbetrieb). Das RTO für einen Prozess muss kleiner sein als die entsprechende MTPD.
- MTPD (Maximum Tolerable Period of Disruption): ist die vom Prozess-Verantwortlichen festgelegte maximal tolerierbare Ausfalldauer des Prozesses, bis ein nicht-tolerierbarer Schaden auftritt.

Die Durchführung der BIA kann mittels Fragebögen, Workshops oder individuellen Interviews oder eine Kombination derselben erfolgen. Eine BIA ist dabei keine «exakte Wissenschaft» sondern beruht vielfach auf Annahmen und unscharfen oder qualitativ erhobenen Daten und Entscheiden. Es ist deshalb wichtig, dass immer wieder und vor allem in der Schlussbeurteilung eine «Top-Down»- oder «Helikopter»-Sicht auf die Ergebnisse und Folgerungen gemacht wird, um diese mit der allgemeinen Geschäftsstrategie in Einklang zu bringen.

Risiko-Analyse erstellen

Im zweiten Schritt werden die Erkenntnisse aus der BIA einer Risiko-Analyse unterzogen. Dies wird vor allem in Bezug auf die Bedrohungen gemacht. Wie gross ist die Wahrscheinlichkeit, dass ein Ereignis eintritt, welches den Betrieb stören kann? Je grösser die Wahrscheinlichkeit und/oder Auswirkung ist, umso schneller/umfassender müssen die (Gegen-)Massnahmen sein. Als Optionen kommen in Frage:

- Verringerung der Eintretens-Wahrscheinlichkeit eines Notfalls durch Vorsorgemassnahmen; Beispiel: durch physische Zutrittsbeschränkungen und Feuerschutz wird der Ausfall eines Serverraums weniger wahrscheinlich.
- Verringerung der Ausfallzeit bei einem Notfall durch Vorsorgemassnahmen; Beispiel: die Dauer eines Ausfalls eines Serverraums kann durch eine gespiegelte Server-Infrastruktur an einem anderen Ort reduziert (Cold-Standby) oder gar ganz verhindert werden (Hot-Standby).
- Vorsehen eines schnell zu etablierenden Notbetriebs mit potenziell niedriger Leistungsfähigkeit; Beispiel: für einen Prozess stehen zur Abdeckung von Spitzenbelastungen mehrere parallele Produktionsmaschinen zur Verfügung. Fällt nun eine aus, so kann der Prozess während einer gewissen Zeit mit verringerter Kapazität aufrechterhalten werden. Der allenfalls entstehende Rückstand wird nach Behebung des Notfalls durch Nacharbeit wieder aufgeholt.

Mit dieser Thematik beschäftigt sich das Kapitel 8.3 «Strategien und Lösungen zur Aufrechterhaltung der Betriebsfähigkeit» mit den folgenden Schritten:

- Identifizierung der Strategien und Lösungen
- Auswahl der Strategien und Lösungen
- Ressourcenbedarf
- Umsetzung von Lösungen

Mit den Resultaten geht es an die Pläne und Verfahren zur Aufrechterhaltung der Betriebsfähigkeit. Das Unternehmen muss Strukturen umsetzen und aufrechterhalten, die eine zeitnahe Warnung an und Kommunikation mit den relevanten interessierten Parteien ermöglicht. Sie muss Pläne und Verfahren für die Steuerung des Unternehmens und ihrer Prozesse während einer Störung bereitstellen. Die Pläne und Verfahren müssen verwendet werden, wenn dies zur Aktivierung von Lösungen zur Aufrechterhaltung der Betriebsfähigkeit erforderlich ist. Diese Pläne gilt es regelmässig zu testen und an die Veränderungen anzupassen.

Im Kapitel 9 geht es um die Bewertung der Leistung. Das Unternehmen muss definieren, was überwacht und gemessen wird, wie dies durchgeführt wird, wann und von wem die Kontrollen erfolgen, wie die Ergebnisse ausgewertet und an wen diese Informationen kommuniziert werden. Die Resultate sind als Nachweis zu dokumentieren.

Gibt es neue Erkenntnisse?

Damit das Management-System auch seinen Zweck erfüllt, muss ein oder mehrere Audit-Programme geplant, aufgebaut und umgesetzt werden. Dazu gilt es die Kriterien sowie den Umfang zu definieren, Auditoren so auswählen, dass die Objektivität und Unabhängigkeit gewährleistet ist und sicherstellen, dass die Ergebnisse empfängergerecht kommuniziert werden.

Mindestens jährlich (besser natürlich öfters) muss sich das Management im Rahmen der Management-Bewertung mit dem aktuellen Stand des BCMs auseinandersetzen. Erfüllt es noch seinen Zweck? Sind Anpassungen notwendig? Gibt es neue Erkenntnisse? Welche Massnahmen wurden aus Beinahe-Unfällen oder Störungen getroffen? Wie kann das BCMS fortlaufend verbessert werden?

Das letzte Kapitel 10 trägt den Titel «Verbesserung» und geht auf Nichtkonformitäten und Korrekturmassnahmen ein. Sollte eine Nichtkonformität (gemäss Definition eine Nichterfüllung einer Anforderung) auftreten, gilt es Massnahmen zur Überwachung und zur Korrektur zu ergreifen und mit den Folgen umzugehen. Dazu muss immer die Ursache, die dazu geführt hat, bestimmt werden. Nach der Umsetzung muss die Wirksamkeit jeglicher ergriffener Korrekturmassnahme überprüft werden. Auch hier gilt es einen dokumentierten Nachweis abzulegen.

Die ISO 22301 zeigt wirkungsvoll den kompletten Weg zu einem umfassenden Business Continuity Management Systems (BCMS). Werden die Schritte eingehalten, können Schutzmassnahmen, die sich an den Geschäftsprozessen orientieren, wirkungsvoll geplant werden, bevor es zu einem Ereignis kommt. Tritt doch eines ein, ist das Unternehmen vorbereitet und kann in kurzer Zeit die Notfallpläne umsetzen und wieder zum Normalbetrieb zurückkehren.