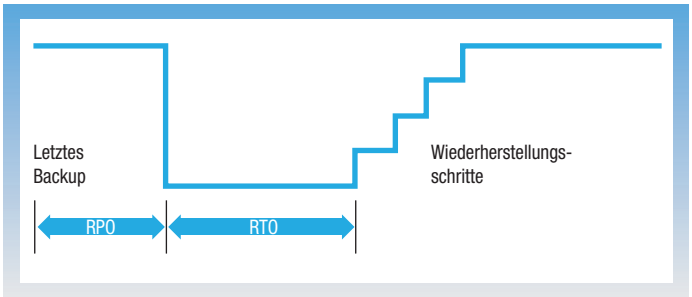
Genügend vorbereitet auf einen Notfall

Gerade in Krisenzeiten wird die Wichtigkeit einer guten Vorbereitung erkennbar. Tritt eine Krise oder ein grösseres negatives Ereignis ein, gilt es schnell zu reagieren. Zu diesem Zeitpunkt ist es aber zu spät, sich mit allen notwendigen Schritten im Detail auseinanderzusetzen. Nun muss reagiert und nicht mehr diskutiert werden.



RPO und RTO im zeitlichen Ablauf.

Die Business Impact Analyse (BIA) zeigt im Vorfeld, auf was der Fokus bei einem solchen Ereignis gelegt werden muss und welche Massnahmen zur Reduktion der Folgen ergriffen werden müssen. Das Krisenmanagement ist unabhängig von Unternehmensprozessen und das Ziel besteht darin, Menschen zu retten (zum Beispiel Gebäude-Evakuation) in der Schadensbegrenzung (Umwelt/Sachwerte) sowie eine Krisensituation generell zu bearbeiten. Auch die Betreuung von Mitarbeitern und gegebenenfalls Angehörigen sowie der richtige Umgang mit den Medien sind klassische Aufgaben des Krisenmanagements.

Kritische Prozesse identifizieren und bewerten

Gemäss ISO 22301 (Sicherheit und Ausfallsicherheit – Business Continuity Management-Systeme) und BSI 100-4 (Notfallmanagement) des Deutschen Bundesamts für Sicherheit in der Informationstechnik sieht das Vorgehen bei der Einführung und beim Betrieb eines BCM wie folgt aus:

1. Eigene Organisation (Struktur und Prozesse) verstehen (mittels Business Impact Analyse)
2. BCM-Strategie entwickeln
3. Reaktionsmassnahmen und Notfallpläne entwickeln und implementieren
4. BCM-Übungen durchführen
5. Reaktionsmassnahmen und Notfallpläne überprüfen und weiterentwickeln

Im nachfolgenden wird der erste Punkt, die BIA, im Detail angeschaut. Diese dient dazu, kritische Prozesse zu identifizieren und zu bewerten. Dabei werden Prozesse mit hohem Einfluss auf andere Prozesse und auch Abhängigkeiten von Prozessen untereinander erfasst.

In einem ersten Schritt werden die Prozesse in einem Unternehmen angeschaut. Dabei ist wichtig, diese zuerst ohne Bewertung oder grosse Diskussionen anzuschauen. Auch eher triviale Prozesse, wie den Briefkasten leeren, gehören da dazu. Gleichzeitig wird erfasst, ob Prozesse von anderen Prozessen abhängig sind.

Erst wenn alle erfasst sind, werden in den Prozessen auch die beiden Werte RPO und RTO bestimmt.

- RTO (Recovery Time Objective): Wie lange darf ein Geschäftsprozess/System ausfallen? Es ist also der Zeitbedarf, der vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung der Geschäftsprozesse reicht.
- RPO (Recovery Point Objective): Welcher Datenverlust kann in Kauf genommen werden? Dies gibt den maximalen Zeitraum an, der zwischen zwei Datensicherungen liegen darf.

Im zweiten Schritt werden die verarbeiteten Daten angeschaut. Dies können Kundendaten, technische Dokumente und Anleitungen, Strategien, interne Dokumente von Mitarbeitenden, Prozesslisten und vieles weitere sein. Diese Daten werden nach der Kritikalität bewertet. Dazu gehören die Vertraulichkeit, die Integrität und die Verfügbarkeit.

- Vertraulichkeit (Confidentiality): Schutz der Daten vor unberechtigter Offenlegung.
- Integrität (Integrity): Erkennung von Datenmanipulationen (Modifikation, Duplizierung).
- erfügbarkeit (Availability): Die Daten stehen dann zur Verfügung, wenn sie benötigt werden.

Im dritten Schritt werden die genutzten Anwendungen, Gebäude, involvierten Mitarbeitenden, Lieferanten und weitere Abhängigkeiten erfasst und mit den Prozessen verknüpft. Diese Elemente erben damit die vorher definierte Kritikalität.

Bei elektronischer Verarbeitung wird im vierten Schritt erfasst, auf welchen Systemen die Anwendungen laufen. Dabei wird nicht unterschieden, ob diese Systeme virtuell oder physisch sind. Jedoch muss bei virtuellen Systemen angegeben werden, auf welcher Hardware diese laufen. Je nachdem können nun auch die Netzwerke und die genutzten Räume (zum Beispiel Serverräume, Switch-Schränke, usw.) in einen Zusammenhang gebracht werden. Bei der Vererbung werden drei Arten unterschieden:

Maximumprinzip

Dabei wird die höchste Kritikalität übernommen (bezogen auf die Vertraulichkeit, die Integrität und die Verfügbarkeit).

Verteilungseffekt

Wenn genügend Redundanzen vorhanden sind, kann zum Beispiel die Verfügbarkeit reduziert werden. Dies ist beispielsweise dann der Fall, wenn Systeme in zwei redundanten Rechenzentren betrieben werden. Damit kann eines ausfallen, ohne dass der Prozess davon negativ beeinflusst wird.

Kumulationseffekt

Die Kritikalität wird erhöht. Typisch ist dies bei Hardware-Systemen, auf denen eine grosse Anzahl von virtuellen Maschinen betrieben werden. Die einzelnen virtuellen Systeme sind unkritisch, da aber bei einem Hardware-Ausfall viele gleichzeitig ausfallen, wird die Anforderung an die Verfügbarkeit des Servers erhöht.

Risiko-Analyse

Mit dieser Vererbung, und allenfalls Anpassung der Kritikalität, können Massnahmen geplant werden. Braucht es mehr Redundanzen? Müssen weitere Mitarbeitende oder externe Lieferanten involviert werden?

Prozessname	Beschreibung	RPO	RTO
Verkauf von Dienstleistungen	Prozess umfasst das Bereitstellen von Dienstleistungen und deren Vermarktung	1 Tag	2 Tage
Mitarbeiter-Rekrutierung	Prozess umfasst alle Schritte vom ersten Gespräch bis zur Einstellung	2 Tage	1 Woche

Beispiel für die Festlegung der Prozesskritikalität.

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

Daten	Beschreibung	Vertraulichkeit (C)	Integrität (I)	Verfügbarkeit (A)
Kundendaten	Informationen über Kunden (zum Beispiel Kaufverhalten)	Sehr hoch (sh)	Hoch (h)	Hoch (h)
Mitarbeiterdaten (HR)	Informationen der Mitarbeitenden (zum Beispiel Absenzen)	Sehr hoch (sH)	Normal (n)	Normal (n)

Beispiel für die Festlegung der Datenkritikalität.

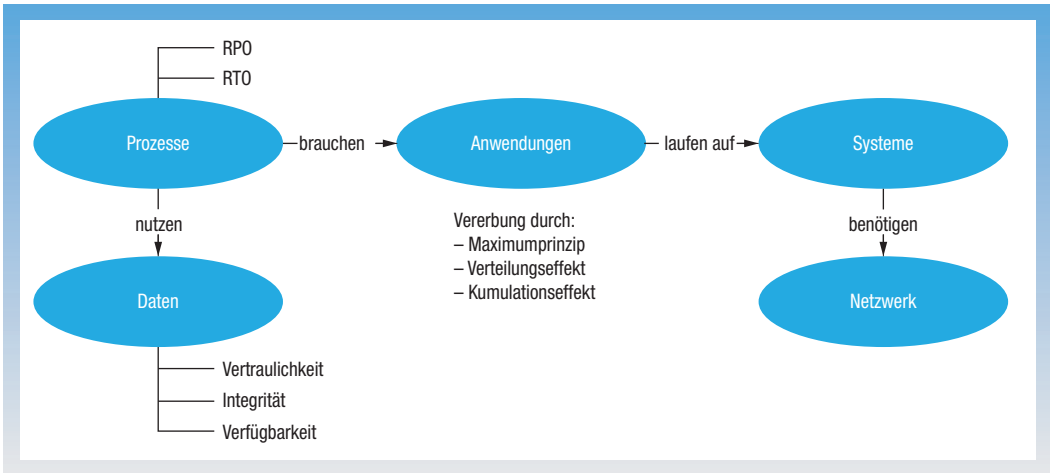
Dazu wird idealerweise eine Risiko-Analyse durchgeführt. Schauen wir uns den Fall eines Systemausfalls an. Die Eintrittswahrscheinlichkeit ist eher gering, aber die Auswirkung kann schnell kritisch werden. Als (Gegen-) Massnahme kann das System redundant aufgebaut, eine Offline-Sicherung mit kurzen Abständen oder eine Anpassung des Prozesses, zum Beispiel auf Papier, geprüft werden.

Kontrollen und KPIs

Aus der vorherigen Massnahme «Offline-Sicherung» sollte anschliessend eine Kontrolle abgeleitet werden. So sollte das Backup wöchentlich überprüft werden, um festzustellen, ob alle notwendigen Daten korrekt gesichert wurden. Eine weitere Kontrolle könnte ein Wiederherstellungstest alle drei Monate, das heisst quartalsweise, sein. Damit wird überprüft und geübt, dass in einem Notfall die Daten auch schnell und vollständig wiederhergestellt werden können. Zudem werden allfällige Stolpersteine identifiziert und können frühzeitig behoben werden. Aus Kontrollen können KPIs (Key Performance Indicator) definiert und gemessen werden. In Bezug auf das Backup könnten dies «Anzahl nicht überprüfter Backup-Jobs» oder «Anzahl nicht erfolgreicher Wiederherstellungstests» sein. Zu jedem KPI sollten auch die Messgrössen definiert werden. So bedeutet 0: «Alles in Ordnung», 1: «Tolerierbar», 2: «Nicht tolerierbar». Diese KPIs dienen als Information für Management-Bewertungen und allfällig notwendiger Korrekturen.

Fazit

Wird die Business Impact Analyse mit genügend Zeit und mit der entsprechenden Tiefe durchgeführt sowie regelmässig den sich ändernden Anforderungen angepasst, kann ein möglicher Notfall zwar nicht verhindert, aber die Folgen davon stark verringert werden. Durch das konsequente Weiterführen werden Massnahmen, Kontrollen und Messgrössen definiert und damit eine Rückmeldung zur Qualität der getroffenen Schritte ermöglicht. Die Business Impact Analyse kann damit ein Unternehmen ideal vorbereiten und vor einem grossen Schaden schützen.



BIA-Ablauf.