CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch

WISSENS-UPDATE

Für Notfälle und Krisen gerüstet – dank präventiven BCM-Massnahmen

Cyber-Angriffe oder Stromausfälle gefährden die operativen Prozesse und die strategische Handlungsfähigkeit von Behörden. Ein nachhaltiges Business Continuity Management (BCM) mit präventiv ergriffenen Massnahmen sorgt dafür, dass die Folgen extremer Ereignisse minimiert werden – und die Rückkehr zur Normalität so schnell wie möglich gelingt.

In der Schweiz ist ein schwerwiegendes Ereignis wie ein Blackout rund alle 30 Jahre einmal zu erwarten – aufgrund von Naturgefahren, technischen Ursachen, Cyber-Angriffen oder gar Terrorismus. Ein solches Extrem-Ereignis würde sämtliche Behörden des Landes auf allen föderalen Ebenen betreffen. Sie müssten sich in dieser Situation fragen: Wie bleiben wir trotz Stromausfall handlungsfähig? Wie halten wir die interne und externe Kommunikation aufrecht? Wie überbrücken oder reaktivieren wir computergestützte Prozesse? Welche Bereiche haben bei einer Strommangellage Priorität? Und wie schützen wir sensible Informationen der Bürger?

Vom Risikomanagement zum BCM
Unabhängig davon, ob sich ein einschneidendes Ereignis über wenige Stunden oder mehrere Wochen hinzieht: Behörden müssen Massnahmen treffen, welche die negativen Folgen minimieren und eine rasche Rückkehr zur Normalität ermöglichen. Stellt man sich den Ereignis-Impact als Kurve vor, dann gilt es, diese Kurve abzuflachen und zu verkürzen, um die Betriebskontinuität zu sichern. Im Business Continuity Management (BCM), auch Kontinuitätsmanagement, sind die Massnahmen dazu gebündelt.

Anders als beim Risikomanagement, das sich mit den Eintretenswahrscheinlichkeiten von bestimmten Ereignissen auseinandersetzt, fokussiert BCM auf die Bewältigung eines Ernstfalls:

Obwohl spezifische Risikoüberlegungen dabei natürlich einfliessen müssen, ist es primär ein organisationsweites Vorsorgesystem, um das Restrisiko zu bewältigen und auf lange Sicht die Widerstandskraft einer Behörde oder Verwaltungseinheit zu erhöhen. Aus Sicht des Risikomanagements ist das BCM somit als Massnahme auf der Auswirkungsseite zu betrachten.

Klare Trennung zwischen Krise und Notfall

Der Bund hat das BCM bereits in seinem Handbuch für Risikomanagement verankert. Auch viele kleinere Behörden verfügen über Pläne für Extrem-Ereignisse. Allerdings wird darin selten sauber zwischen Notfall- und Krisenmanagement unterschieden. Bei Notfällen handelt es sich in der Regel um kurzfristige Situationen, die den regulären Ablauf betrieblicher Prozesse stören und operativ bewältigt werden müssen. Krisen hingegen sind weitaus konsequenzenreichere Ereignisse: Sie dauern länger, können sich in unvorhergesehene Richtungen entwickeln und bedrohen nicht nur Prozesse, sondern das Funktionieren der gesamten Organisation. Krisenmanagement bedeutet folglich, strategisch handlungsfähig zu bleiben.

Im Spannungsfeld zwischen Ökonomie und Sicherheit ist es elementar, zwischen Krise und Notfall klar zu unterscheiden. Wird Notfällen nämlich mit umfangreichen Krisenmanagement-Massnahmen begegnet, ist das in der Regel nicht wirtschaftlich. Zudem wiegt es Organisationen in der falschen Sicherheit, dass die Werkzeuge zur Notfall-Bewältigung auch im Falle einer echten Krise greifen.

6 Gründe für Business Continuity Management

Ein nachhaltiges BCM muss beides umfassen: Krisenmanagement, um die Führungsfähigkeit der Behörde im Ernstfall sicherzustellen, und Notfallmanagement, um ein ausserordentliches Ereignis operativ zu bewältigen. Konkret heisst das:

1. Ein BCM bündelt Verfahren und Anweisungen für den Fall eines Ausfalls. Es umfasst die notwendige Planung und Vorbereitung, um die Auswirkung eines Ausfalls zu mildern. Und es stellt sicher, dass im Ereignisfall die geschäftskritische Funktionsfähigkeit von einzelnen Prozessen und der gesamten Organisation erhalten bleibt.

2. Es definiert Prozesse, Funktionen, Infrastrukturen oder Anbieter, welche nötig sind, um die Geschäftsziele unter Einhaltung der gesetzlichen und behördlichen Vorschriften zu erreichen. Zur Infrastruktur zählen unter anderem Gebäude, Arbeitsplätze, Daten, technische Plattformen und Netzwerke.

3. Das BCM legt fest, welche Ressourcen für die Begrenzung des Ausfallrisikos eingesetzt werden müssen. Diese Abschätzung erfolgt nach wirtschaftlichen Grundsätzen und in Zusammenarbeit mit den relevanten Stakeholdern.

4. Es stellt den Erhalt beziehungsweise die Wiederherstellung geschäftskritischer Prozesse im Ereignisfall sicher.

5. Das BCM steigert die Widerstandsfähigkeit der Organisation in Notfall- und Krisensituationen.

6. Es bewältigt die im Rahmen des Sicherheitsmanagements eruierten Restrisiken.

Wichtig ist: entscheidende Aspekte müssen laufend überprüft und Massnahmen wo nötig angepasst werden. Denn das Umfeld, in dem Behörden tätig sind, wandelt sich laufend. Das betrifft nicht nur die Geschäftsprozesse selbst, sondern auch die Gefahren, denen sie ausgesetzt sind. Dazu gehören einerseits Naturkatastrophen, andererseits aber beispielsweise auch Angriffe durch Cyber-

Attacken. Gerade die Bedrohungslage durch Cyber-Attacken ändert sich laufend. Es gilt also im Rahmen des BCM, auch im Bereich der Cyber Security möglichen Angreifern immer einen Schritt voraus zu sein.

In 3 Schritten zur umfassenden Sicherheitslösung
Auf dem Weg zu einem funktionierenden BCM gilt es drei Ebenen zu beachten: das Management, die Prozesse und die Technik. Die CyOne Security kann Behörden dabei unterstützen, die richtigen Schritte hin zu einer umfassenden Sicherheitslösung zu unternehmen.

1. **Die Management-Ebene**
   In einem ersten Schritt müssen Organisationen ihre Geschäftsprozesse und die dafür nötigen Verfügbarkeiten sauber analysieren. Anschliessend gilt es, diese den Restrisiken gegenüberzustellen und mögliche Schwachstellen zu erkennen. Eine Expertensicht von aussen kann sinnvoll sein, um die geplanten Mittel zur Behebung von Schwachstellen zu beurteilen.

2. **Die Prozess-Ebene**
   In einem zweiten Schritt braucht es konkrete Lösungen für den Ernstfall: Organisationen müssen alternative Prozesse definieren, um den Normalbetrieb wiederherzustellen. Dabei muss berücksichtigt werden, wie sich diese Alternativen auf die Verfügbarkeit von Informationen und Infrastrukturen auswirken.

3. **Die technische Ebene**
   Mit präventiven Massnahmen auf der technischen Ebene können Behörden bereits sehr viel erreichen. Das Expertenwissen der CyOne Security kann sie dabei unterstützen, ihre Softwarearchitekturen zu überprüfen und sicherer zu gestalten. Ergänzend braucht es Massnahmen zur Resilienzsteigerung der bestehenden Infrastruktur: Netztrennungen, Backupstrategien, sichere Virtualisierungen oder Hardware-protected Software. Schliesslich kann es sinnvoll sein, auf hochsichere Endgeräte wie das 9400-Officebook beziehungsweise die Applikation Secure Voice für Mobiltelefonie zu setzen.

Die nächste Krise, der nächste Notfall oder das nächste Schadensereignis lässt sich mit diesen Massnahmen nicht verhindern. Aber sie sind das Rüstzeug, damit Behörden im Ernstfall handlungsfähig bleiben und die Extremsituation rasch und weitgehend unbeschadet überstehen.

Beginnen Sie heute mit präventiven Massnahmen für ein erfolgreiches BCM.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Cyber Security-Experten Ihre aktuellen und zukünftigen Cyber-Sicherheitsbedürfnisse und entsprechende Sicherheitslösungen.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.