Checkliste zur Selbsteinschätzung 2024

Mit Business Continuity Management gut vorbereitet gegen Risiken und Bedrohungen!

WAN Consult

Wie ist diese Business Continuity Management Checkliste zur Selbsteinschätzung entstanden?

Erfahrung aus 500+ Kundenprojekten in den letzten 20 Jahren...

Kunden stellten mich immer wieder vor spannende Herausforderungen in der nationalen und internationalen Datenkommunikation. Die Anforderungen waren vielfältig:

- **Ausfallsichere Datenkommunikation** für Just-in-Time-Produktionen und leistungsstarke Netzwerke.
- **Unterbrechungsfreie Verbindungen** trotz Seekabelschäden, Monsunregen oder sogar einem Brand im Datacenter.
- **Redundante Datenkommunikation** in der Lebensmittelproduktion, um die ständige Verfügbarkeit sowie lückenlose Kühlketten zu gewährleisten.
- **Dual-Carrier-Strategien** und georedundante Leitungsführungen für einen verlässlichen Always-on-Betrieb.

Zusätzlich erhielt ich Anfragen zur **konzeptionellen Beratung** im Bereich Business Continuity Management und Disaster Recovery, um optimal auf Ereignisse wie Flugzeugabstürze, Pandemien oder Überschwemmungen vorbereitet zu sein.

Anstieg von Bedrohungen und Ereignissen…

- 2023 haben kriminelle Hacker wöchentlich Schweizer Unternehmen und Behörden angegriffen. 40 mehr oder weniger erfolgreiche Hackerangriffe hat die NZZ aufgezeichnet. Die meisten Fälle wurden wohl aber nie publik.
- Die Naturereignisse in der Schweiz und weltweit nehmen zu – Waldbrände, Überschwemmungen, Murgänge, Lawinen, Wasserknappheit und Vulkan-ausbrüche – mit den unterschiedlichsten Folgen.
- Es drohen die Gefahren von Energiemangellagen und Blackouts.
- Weiter hat sich die wirtschaftliche Prosperität in vielen Ländern verlangsamt und politische Krisen und kriegerische Auseinandersetzungen haben sich verstärkt.

Dies ist nicht nur mein und das Gefühl anderer – Statistiken belegen es!

Diese Jahre haben gezeigt, dass Business Continuity Management nicht bei der Informatik und der Datenkommunikation endet...

…manche Ereignisse haben einen viel grösseren und vielfältigeren Einfluss auf die Geschäftstätigkeit eines Unternehmens und das rasche Wiederanlaufen des Betriebes kann für dessen Zukunft entscheidend sein!

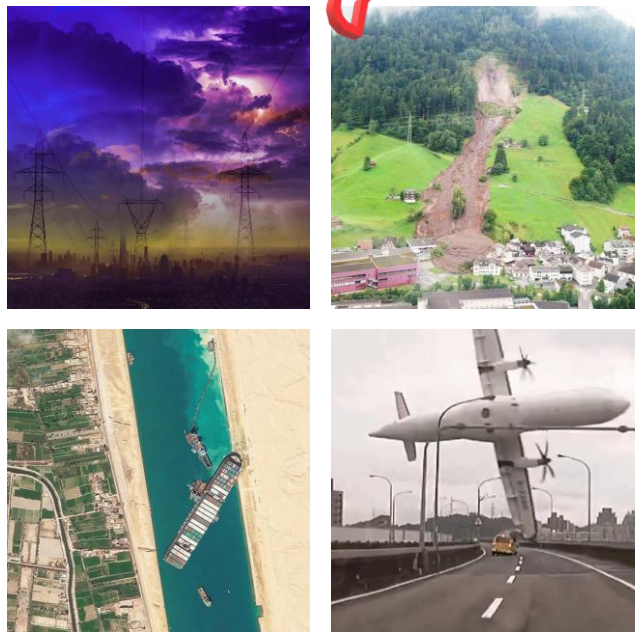
Wie können Sie nun Ihr Unternehmen auf Risiken und Bedrohungen vorbereiten?

1

Negative Auswirkungen – Das sollten Sie unbedingt vermeiden

Negativ: Mögliche Bedrohungen nicht zu kennen

- Cyberattacken, Datenverlust, Sabotage
- Energie-Mangellage, Blackout
- Naturgefahren (Hochwasser, Überschwemmung, Grundwasseranstieg, Murgang, Lawine, Vulkanausbruch)
- Brand und Brandanschlag
- Lieferunterbruch oder -engpass, Handelshemmnisse
- Patentverletzung oder -diebstahl
- Flugzeugabsturz
- Pandemie



Negativ: Keinen Kommunikationsplan zu haben

- Wer kommuniziert was?
- Wem sage ich es?
- Wann kommuniziere ich?
- Wer muss es zuerst wissen?

Wer keinen Kommunikationsplan mit klaren Verantwortlich-keiten hat, der kann möglicherweise von den Medien, den Kunden, den Lieferanten, den Mitarbeitenden oder der Öffentlichkeit überrascht werden.

Bedenke: Man kann nicht nicht kommunizieren!

Negativ: Keinen Wiederanlaufplan zu haben

Was für ein Ereignis es auch ist, je schneller sie wieder operativ sind, desto rascher können sie wieder Erträge generieren!

- Kann ich die Kunden von einem alternativen Standort aus bedienen und beliefern?
- Gibt es einen alternativen Produktionsstandort oder können befreundete Unternehmen aushelfen?
- Welche alternativen Lieferanten stehen zur Verfügung?
- Wo bringe ich als Hotelier meine Gäste unter?
- Welcher IT-Partner hat ein Forensik-Team und bringt die IT rasch wieder zum Laufen?

2

Positive Auswirkungen – Das stärkt Ihr Unternehmen, Ihre Organisation

Positiv: Ein Daten-Backup-System zu haben

- **System 3-2-1**
  Die 3-2-1-Regel ist eine Strategie zur **Datensicherung**, die besagt, dass Sie drei Kopien Ihrer Daten haben sollten, auf zwei verschiedenen Medien gespeichert, wobei eine Kopie extern gelagert wird. Dies minimiert das Risiko eines totalen Datenverlustes durch verschiedene Arten von Schäden oder Ausfällen.
- **Release-Management**
  Das Ziel des **Release-Managements** im Rahmen von **ITIL** ist es, sicherzustellen, dass die Software stabil und zuverlässig ist und dass neue Funktionen und Updates in einer Weise bereitgestellt werden, die den Anforderungen des Unternehmens entspricht.
- **Logging-Prozess**
  Als Logging bezeichnet man in der Informatik die **automatische Erstellung eines Protokolls (englisch log) von Softwareprozessen**. Logging dient der Aufzeichnung und Nachvollziehbarkeit von Fehlerzuständen des Softwareprozesses.

Positiv: Regelmässige Schulungen

- Arbeitssicherheitsschulungen
- Brandschutz
- Evakuierungsübungen zum Notfallsammelplatz
- IT-Sicherheit: Passwörter und Authentifizierung
- E-Mail-Sicherheit mit simuliertem Phishing-Training
- Clean-Desk-Kontrollen
- Besucher-Begleitung
- Compliance

Positiv: Lieferanten prüfen und bewerten

Generell heutige Lieferanten prüfen und bewerten sowie Zweitlieferanten abklären. Dabei sind die nachfolgenden Punkte zu bewerten:

Einstufung der Kritikalität: Bestimmen Sie, welche Lieferanten für Ihre Geschäftsprozesse besonders kritisch sind. Besonders IT-Lieferanten, die Ihre Infrastruktur, Daten oder wichtigen Anwendungen bereitstellen, müssen genau bewertet werden.

Notfallpläne: Fragen Sie nach den Business Continuity- und Disaster Recovery-Plänen der Lieferanten. Diese Pläne sollten mit Ihren eigenen BCM-Strategien kompatibel sein.

Überlebensfähigkeit in Krisen: Untersuchen Sie die finanzielle Gesundheit der Lieferanten, um sicherzustellen, dass sie auch in wirtschaftlich schwierigen Zeiten weiterhin Ihre Dienstleistungen erbringen können. Ein finanziell instabiler IT-Dienstleister kann ein erhebliches Risiko darstellen.

3

Wie resilient ist Ihr Unternehmen?
Checkliste zur Selbsteinschätzung

	Ja	Nein
Sind mehr als 3 der nachfolgend aufgeführten Bedrohungen für Ihr Unternehmen denkbar? Cyberattacken, Datenverlust, Sabotage, Energie-Mangellage, Blackout, Hochwasser, Überschwemmung, Grundwasseranstieg, Murgang, Lawine, Vulkanausbruch, Brand, Lieferunterbruch oder -engpass, Fachkräftemangel, Handelshemmnisse, neue gesetzliche Vorschriften, Patentverletzung oder -diebstahl, Flugzeugabsturz, Pandemie.	☐	☐
Könnte eine dieser Bedrohungen das Überleben des Unternehmens ernsthaft gefährden?	☐	☐
Könnte bei dieser Bedrohung der Fall eintreten, dass die finanziellen Folgen die Fortführung der Geschäftstätigkeit nicht mehr erlauben?	☐	☐
Gibt es dabei Bedrohungen, die alle Geschäftsstellen/Niederlassungen betreffen?	☐	☐
Gibt es Kern-Prozesse in Ihrem Unternehmen, die nicht klar dokumentiert sind und bei denen unklar ist, welche Auswirkungen ein Unterbruch oder längerer Ausfall hat?	☐	☐
Gibt es in Ihrem Unternehmen Prozesse, die an Partner/Lieferanten ausgelagert sind, die für Ihr Unternehmen kritisch sind, aber nicht klar dokumentiert sind, nicht kontrolliert werden und die Auswirkungen eines Ausfalls nicht antizipiert sind?	☐	☐
Könnte einer dieser Prozesse die IT Ihres Unternehmens betreffen und Sie kennen die Vorkehrungen des Partners im Falle einer Cyber-Attacke auf den Partner nicht?	☐	☐

	Ja	Nein
Gibt es Unsicherheiten und Unvollständigkeiten beim IT-Inventar Ihres Unternehmens, z. B. beim Release-Management (Planung/Durchführung der Softwareaktualisierungen)?	☐	☐
Muss in Ihrem Unternehmen noch eine Business Impact Analyse (BIA) durchgeführt werden? Mit einer BIA werden die Risiken und Bedrohungen für Unternehmen (alle Geschäftsstellen/ Niederlassungen) erfasst und beurteilt sowie die finanziellen Folgen bewertet.	☐	☐
Muss in Ihrem Unternehmen noch ein Business Continuity Management (BCM) erarbeitet werden? In einem BCM ist festgehalten, wie das rasche und sichere Wiederanlaufen der Geschäftstätigkeit nach einem eingetroffenen Ereignis erfolgt und wie die Auswirkungen eines Ereignisses minimiert werden sowie wie das Unternehmen sicherer, effektiver und effizienter weiterbetrieben werden kann.	☐	☐
Fehlt in Ihrem Unternehmen ein formeller Prozess, was im Falle eines Ereignisses bzw. einer Bedrohung zu tun ist?	☐	☐
Fehlen in Ihrem Unternehmen Ziele und Vorgaben (Recovery Time Objectives), wie schnell Prozesse nach einem Ereignis bzw. einer Bedrohung wieder anlaufen müssen?	☐	☐

	Ja	Nein
Müssen in Ihrem Unternehmen noch Prozesse für einen Notfall erarbeitet werden, welche im Falle eines Ereignisses zur Anwendung kommen?	☐	☐
Werden diese Prozesse anhand eines Schulungs- und Übungsplanes geübt?	☐	☐
Fehlen das Konzept für eine klare Krisenkommunikation und vorbereitete Statements für die wichtigsten Bedrohungen?	☐	☐
Planen Sie eine Business Continuity Management-Zertifizierung nach ISO 22301?	☐	☐
Gibt es gesetzliche oder regulatorische Anforderungen, die Ihr Unternehmen erfüllen muss und könnten Störungen oder Ausfälle zu Compliance-Problemen führen?	☐	☐

Ergibt Ihre Selbsteinschätzung mehr als 5 Antworten mit «Ja», dann lassen Sie uns darüber sprechen!

Schön, den ersten Schritt haben Sie getan!

In 60 Minuten die Selbsteinschätzung analysieren und darüber sprechen, was als nächstes kommt.
Und dies kostenlos!

Lassen Sie uns diesen zweiten Schritt gemeinsam tun!

Mit einer Business Impact Analyse (BIA) ergründen wir, wo der grösste Handlungsbedarf ist und welche finanziellen Konsequenzen drohen, wenn nichts getan wird!

Ja, so könnte es sinnvoll und substantiell weitergehen!

Grüezi! Vorstellung WAN Consult

Stephan Stamm
Geschäftsführer & Gründer

WAN Consult entstand aus einer langjährigen Karriere in der ICT-Branche und einem tiefen Verständnis für die Datenkommunikations-anforderungen von über 500 multinationalen Schweizer Unternehmen.

Anfänglich konzentrierten wir uns auf die Verbesserung der Daten-kommunikations-Resilienz. Doch schnell wurde klar, dass Resilienz in Unternehmen umfassender betrachtet werden muss.

Heute bieten wir Ihnen massgeschneiderte Dienstleistungen in den Bereichen Business Impact Analyse, Disaster Recovery und Business Continuity Management. Diese Themen stehen im Mittelpunkt unserer Arbeit mit Ihnen.

Persönlich standen diese Themen schon immer im Fokus der Tätigkeit unseres Gründers und Geschäftsführers.

Auf bald

www.WAN-Consult.ch

stephan.stamm@WAN-Consult.ch