Whitepaper

Handlungsempfehlungen für international agierende Unternehmen im Russland-Ukraine-Krieg 2022

controllit
Business Continuity Management

Inhalt

EINLEITUNG

Die aktuellen Kriegshandlungen in der **Ukraine** und der Konflikt mit **Russland** beschäftigt uns nicht nur medial, politisch und persönlich, sie haben auch massiven Einfluss auf die Unternehmenstätigkeiten und die deutsche Wirtschaft. Auch Geschäfte und Aktivitäten in und mit Belarus sowie den Nachbarländern der Ukraine und Russland stehen im Blickpunkt.

Die (meist noch freiwilligen) Sanktionen gegen Russland haben bereits jetzt weitreichende wirtschaftliche Folgen. Zahlreiche Unternehmen reagieren mit Einschränkung ihrer Geschäftstätigkeit, befinden sich in Warteschleife oder beenden ihre Aktivtäten komplett. Wo Produktion und Vertrieb heruntergefahren wurden oder werden, geht es um ein koordiniertes Auslaufen und die Sicherung der Waren, Werte und Liegenschaften.

Von den Branchen der Automobilindustrie (Fertigung und Vertrieb), Verkehr (insbesondere Luftfahrt), Banken und Versicherungen, Energie, Unterhaltung, Industrie und Fertigung, Logistik, Technologie, Telekommunikation bis hin zu Sportartikelherstellern, Produktion und Vertrieb von Haushaltswaren und Möbelhäusern wird entsprechend reagiert.

Die Auswirkungen auf den Kriegsschauplatz Ukraine selbst sind verheerend, und auch die Nachbarländer, nicht nur in den Grenzgebieten, sowie Deutschland sind involviert.

EINLEITUNG

Die Folgen für die Kostenentwicklung sind spürbar (ein Kreditprogramm der staatlichen Förderbank wurde angekündigt), die Exportprognose des DIHK (Deutsche Industrie- und Handelskammertag) wurde deutlich gesenkt und Produktionsunterbrechungen auch an indirekt betroffenen Standorten zeichnen sich durch die Herausforderungen in den Lieferketten ab. Hinzu kommen eine mögliche Knappheit und ein wahrscheinlicher Preisanstieg bei Rohmaterialien.

Nicht zuletzt sind die direkte **Sorge und Fürsorge** für die Mitarbeiter ein bestimmendes Thema: Hier wird die unternehmerische Verantwortung von der Evakuierung der Mitarbeiter bis hin zu einer bestmöglichen Betreuung der Mitarbeiter, die vor Ort bleiben wollen oder müssen, relevant.

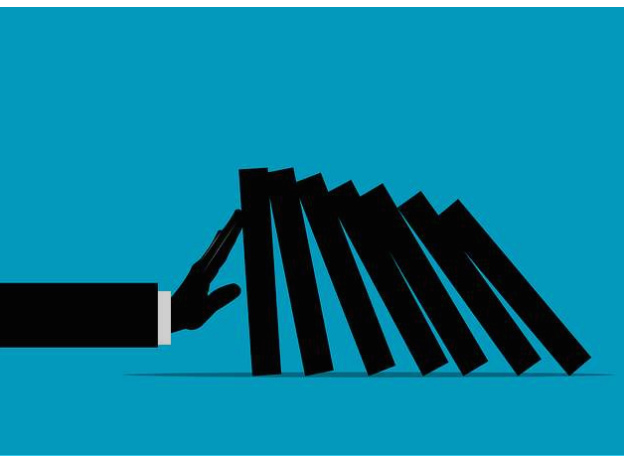
Mit diesen Handlungsempfehlungen wollen wir anhand der klassischen Stabsperspektive Orientierung geben und **Optionen zu den folgenden Themenfeldern** aufzeigen:

- Personal (inkl. Safety)
- Lage (inkl. Security)
- Einsatz
- Logistik
- Presse- und Medienarbeit
- IT, Informationssicherheit und Datenschutz

Handlungs-empfehlungen

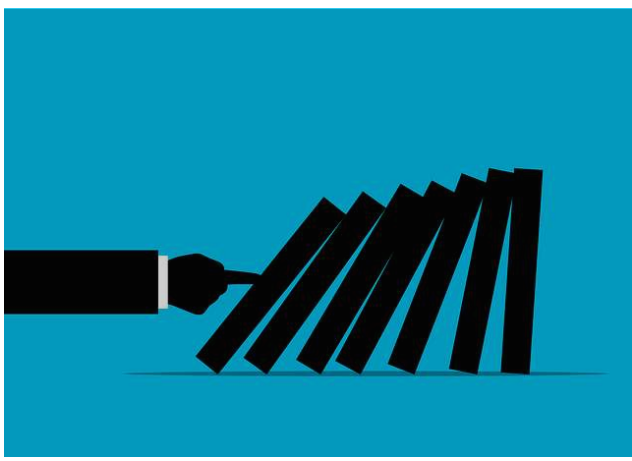
Grundsätzlich empfehlen wir auch im aktuellen Konflikt eine solide und weitsichtige Vorbereitung (wenn vorhanden: Nutzung der Eskalationsstufen und Schwellenwerte Ihres Unternehmens) und die Entwicklung von Stufenplänen oder Szenarios.

Die konkrete Vorbereitung dient vor allem der zielgerichteten Bewertung (idealerweise anhand Ihrer ggf. aktualisierten Schwellenwerte und Priorisierungen). Die Nutzung von Stufenplänen oder Szenarios unterstützt Unternehmen bei einer flexiblen Anpassung an die konkrete Lage. Zum anderen dient die reaktive Vorbereitung auch der gezielten Koordination und Kontrolle bei allen Auslauf-, Ruhe- und Stilllegungs-Szenarien. Hier gibt es einen spürbaren Unterschied zwischen gezieltem, proaktiv gesteuertem Vorgehen und einfachem „Fallenlassen“. Auch bei der Rückkehr in den Normalbetrieb gibt ein Stufenplan Struktur und flexible Handlungssicherheit.



Dabei sind die Vorgehensweisen für Unternehmen mit Aktivitäten in den direkt agierenden oder betroffenen Ländern Russland, Ukraine und Belarus situationsabhängig auf einer anderen Stufe als in den Nachbarländern. Die Fragestellungen und Ihr Schnittstellen-Management sind aber sehr ähnlich. In den Nachbarländern geht es sowohl um die Perspektive der Betroffenheit in den Grenzregionen als auch um eine mögliche Ausweitung des Konflikts.

In den folgenden Kapiteln geben wir Ihnen zu den Themenfeldern konkrete Handlungsempfehlungen und werfen notwendige Fragestellungen auf.



Personal

Der Sektor Personal ist mit den Schnittstellenpartnern Human Ressources (HR) und Security (SECU) gut zu strukturieren und zu bewerten. Hier gilt es zum einen natürlich, die physische Sicherheit und Gesundheit des Personals zu gewährleisten, zum anderen aber auch um eine proaktive Steuerung von Skills (Fähigkeiten, Fertigkeiten, Qualifikationen) inkl. der Single Points of Knowledge (SPOKs) Ihres Unternehmens.

Die wesentlichste Frage im Kriegs-, direkten Sanktions- oder Grenzgebiet ist die der physischen Sicherheit. Aber auch in den Nachbarländern kann sich die Lage dynamisch verändern.

- Prüfen Sie Ihre Personalsicherung: Entsprechen Ihre Reisevorgaben der aktuellen Situation (Reisesperren etc.)?
- Ermitteln Sie, welche Mitarbeiter Sie evakuieren müssen, sollen oder wollen (nicht nur im unmittelbaren Kriegsgebiet).
- Beachten Sie bei der Einschätzung auch, ob es sich um nationale Mitarbeiter in ihrem Heimatland oder Mitarbeiter aus anderen Ländern (ggf. mit Nationalitäten der Konfliktparteien) handelt. Beachten Sie hierbei auch den Bedarf und die Möglichkeit zur Evakuierung weiterer Familienangehöriger der lokalen Mitarbeiter.
- Beachten Sie immer die Empfehlungen des Auswärtigen Amtes sowie natürlich der Behörden im jeweiligen Land.

Personal

- Ermitteln Sie die Optionen und Mittel, die für eine Ausreise/Evakuierung zur Verfügung stehen. Vermutlich gibt es Unterstützungsangebote einerseits zur Nutzung von Verkehrsmitteln, andererseits aber auch finanzieller Natur.
- Prüfen Sie, ob es Unterstützung durch die Bundesregierung, des Bundeslandes, anderer Institutionen oder privater Sicherheitsunternehmen gibt und ob eine Versicherung Ihres Unternehmens greift.
- Betrachten Sie den Zeitplan. Welche unmittelbaren Aktivitäten sind notwendig, welche Aktivitäten können vorbereitet und in welchem Umfeld in welchem Zeitrahmen umgesetzt werden?
- Planen Sie die Ausweichstandorte Ihrer Mitarbeiter. In der Kriegsregion ist unter Zeitdruck ggf. erst einmal eine temporäre Weg-/Ausreise in die Nachbarländer sinnvoll. Informieren Sie sich und die Betroffenen über entsprechende Anlaufstellen (z. B. Botschaften).
- Wenn Sie die Ausreise-Aktivtäten steuern können, ist der mittelfristige berufliche sinnvolle Einsatzort unbedingt in die Überlegung zur sicheren Zielregion einzubeziehen.
- Dazu ist eine ggf. umfassende Ermittlung empfehlenswert, wo welche der nun freiwerdenden Skills benötigt werden. Gibt es vielleicht schon Überlegungen zu unternehmerischen Ersatzlösungen oder Bedarf an anderen, sicheren Standorten?
- Betrachten Sie auch, ob und welches lokale Personal zur Sicherung Ihrer Waren und Werte, für Überwachungstätigkeiten oder unternehmerischer Aktivitäten bei gezielter Einstellung oder Reduzierung Ihres Geschäftsbetriebs benötigt wird. Die Perspektive Ihrer einheimischen Mitarbeiter und der weiteren Mitarbeiter vor Ort kann hier eine gute Entscheidungshilfe sein.
- Last, but not least: Mitarbeiter aus direkt betroffenen Gebieten benötigen voraussichtlich psycho-soziale Unterstützung. Gibt es weitere Herausforderung zur mentalen Gesundheit der Mitarbeiter?

Lage

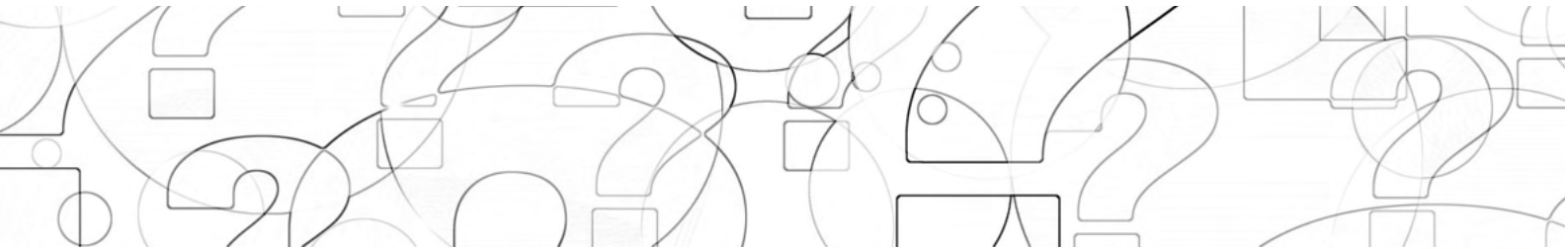
Ein Lagebild in einem Kriegsgebiet zu ermitteln ist immer eine Herausforderung mit einigen Unbekannten. Es empfiehlt sich daher, sowohl behördliche und mediale Informationen als auch individuelle Informationen zu nutzen und zu einem unternehmensspezifischen Lagebild zusammenzustellen. Zusätzlich gibt es Unternehmen und Services in Deutschland, die sich auf solche Dienste spezialisiert haben. Dabei sind sowohl Ihre Kommunikationsprofis (Kommunikationsabteilung o. a.) und Security-Verantwortlichen als auch Ihre direkten Mitarbeiter, Partner und/oder Dienstleister vor Ort relevante Informationspartner. Über Ihre lokalen Ansprechpartner erhalten Sie auch wertvolle Rückmeldung zur Umsetzbarkeit Ihrer Maßnahmen.

Zur Entwicklung Ihres Stufenplans auf Basis des Lagebilds ist auch wichtig, ob es sich um eine komplette Einstellung, eine kontrollierte oder eine limitierte Reduzierung Ihres Geschäftsbetriebs handelt. Hinzu kommen natürlich alle Kombinationsvarianten, die Sie betrachten und bewerten sollten. Außerdem kann die Lage in der Ukraine, in Russland, Belarus sowie den Nachbarländern einen Rücklauf-Effekt auf ihr Gesamt-Unternehmen haben. Betrachten sie also idealerweise auch die Abhängigkeiten im internationalen Umfeld Ihrer Unternehmensorganisation.

- Prüfen Sie, welche Unternehmensteile in welchem Umfang aktuell und perspektivisch betroffen sind. Legen Sie in Abstimmung mit Ihrer Geschäftsführung den Rahmen Ihrer Betrachtung fest (aktuell empfiehlt sich mindestens die Perspektive von sechs Monaten). Welcher Schaden ist bereits entstanden und (mittel- bis längerfristig) absehbar?

Lage

- Schließen Sie die Abhängigkeiten Ihrer weiteren Produkte, Produktions- und Lieferketten in die Betrachtung mit ein. Gibt es „Monopole“ oder Kerngeschäftstätigkeiten?
- Prüfen Sie die Betroffenheit Ihrer Kunden, Mitarbeiter und deren Familien und Märkte.
- Informieren Sie sich über die Einschätzung und Perspektiven Ihrer direkten Ansprechpartner vor Ort.
- Ermitteln Sie auch, wie der Informationsaustausch mit den lokalen Ansprechpartnern mittel- bis langfristig aufrechterhalten bleiben kann.
- Ermitteln Sie die lokale Ressourcenlage und die lokalen Anforderungen (Personal inkl. Know-how, Gebäude, IT, Dienstleister sowie Materialstand, Lagerhaltung, Logistik etc.).
- Zur Ressourceneinschätzung und -planung empfehlen sich auch Informationen zur Versorgungs-, Verkehrs- und Sicherheitslage in der Ukraine, in Russland, Belarus sowie den Nachbarländern.
- Achten Sie bei der Informationsgewinnung auf die Seriosität der Quellen, hinterfragen Sie Lageinformationen kritisch und regelmäßig und kommunizieren Sie zentrale Lageinformationen innerhalb Ihres Unternehmens.
- Versuchen Sie „vor die nächste Welle“ zu kommen, indem Sie potenzielle zukünftige Szenarien des Konflikts und des Marktes für ihr Unternehmen skizzieren, bewerten und geeignete Reaktionen entwerfen.
- Prüfen Sie Ihren Anspruch und nutzen Sie Fördermittel des Bundes und/oder Kreditprogramme.
- Beobachten und bewerten Sie Ihre aktuellen Aktienbeteiligungen in angemessenen (ggf. kürzeren) Intervallen, um die schwankenden Kurse im Auge zu behalten und entsprechend agieren und kommunizieren zu können.



Einsatz

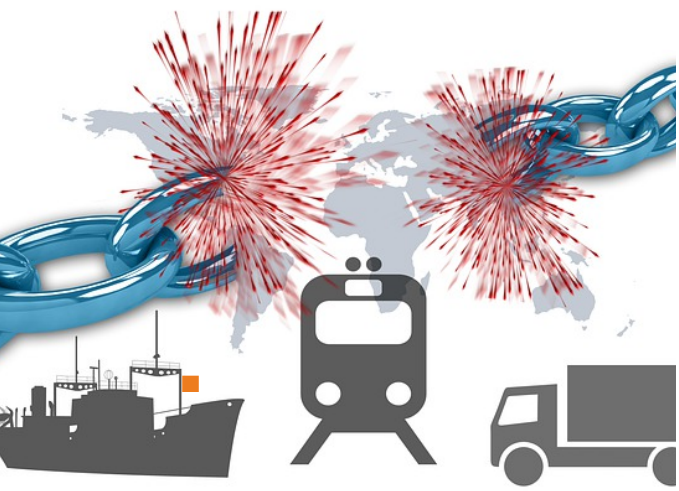
Bei der Entscheidungsfindung und Anpassung Ihrer Maßnahmen empfiehlt sich, die bitte wirklich flexible Anpassung an das Lagebild mittels Ihres Entscheidungsfindungsmodells (z. B. FORDEC). Betrachten Sie dabei insbesondere wieder mögliche Unterstützungsoptionen und nutzen Sie hier Ihre Schwellenwerte und Priorisierungen im Stufenmodell.

- Stellen Sie sicher, dass Ihre Priorisierungen an die Lage angepasst sind oder kurzfristig werden.
- Prüfen Sie, ob und durch welche nicht betroffenen Betriebsteile Kompensationsmaßnahmen umgesetzt werden können.
- Prüfen Sie, ob und welche Alternativen und Erweiterungsoptionen es in Ihrem Geschäftsfeld gibt.
- Ermitteln Sie, ob und welche internen und externen Schnittstellen zur Verfügung stehen.

Logistik

Seit Covid-19 ist die Sensibilität von Warenbewegungen in Verbindung mit Lagerhaltung und Transportwesen in den Fokus gerückt. Im Umfeld kriegerischer Auseinandersetzungen verlangt dieser Bereich besondere Koordination und Organisation in den betroffenen Ländern: Ukraine, Russland, Belarus sowie den Nachbarländern. Dabei empfiehlt sich wiederum, flexibel und handlungssicher mit Hilfe Ihres Stufenplans auf das Lagebild zu reagieren. Nutzen Sie die Schnittstellen im Controlling, Risikomanagement, die lokalen Verantwortlichen und Ihre Geschäftsführung auf strategischer Ebene als Informationsquelle.

- Stellen Sie die Aktualität Ihrer Prioritätsprodukte und -kunden sicher.
- Ermitteln Sie die aktuelle technische und materielle Verfügbarkeit inkl. Ausstattung Ihrer Lager, Fuhrparks, sonstiger Verkehrsmittel und Frachtwege (siehe auch Lage).
- Prüfen Sie Ihre Alternativen: Gibt es Auswahlmöglichkeiten zu anderen Lagerstätten (inkl. Aufteilung), Dienstleistern, Spediteuren, Transportmitteln und -wegen?
- Ermitteln Sie die Anforderungen Ihrer Alternativen. Gibt es Besonderheiten oder Hindernisse? Vielleicht ist eine Kombination von Alternativen sinnvoll?
- Prüfen Sie, welche qualitativen und quantitativen Einbußen akzeptabel sind.
- Bewerten Sie die Auswahlmöglichkeiten auf Sicherheit (bitte auch mit der mittel- bis langfristigen Perspektive), Wirtschaftlichkeit (Zeit und Kosten) und Umsetzbarkeit (Personalanforderung, Haltbarkeit Ihrer Waren, IT-Anforderungen, ggf. Nutzung manueller Abläufe etc.).



- Behalten Sie gesetzliche bzw. vertragliche Anforderungen und Auswirkungen auf die Reputation bzw. das Image Ihres Unternehmens sowie eine ggf. längerfristig nutzbare Lokation im Blick.
- Stellen Sie sicher, dass Ihre Alternativen auch länderübergreifend effektiv und effizient sind. Es empfiehlt sich, die Freiheit Ihrer Transportketten und Lieferströme auch mit Bezug zum Herkunfts- und Ankunftsland sowie die Dokumentationsanforderungen zu prüfen.

Presse- und Medienarbeit

Die Kommunikationsabteilung Ihres Unternehmens wird in allen Krisen erheblich in Bezug auf das zu bewältigende Volumen und den Qualitätsanspruch gefordert. Die innere und äußere Wahrnehmung Ihres Krisenmanagements wird durch die Unternehmenskommunikation geprägt und entscheidet maßgeblich über den Erfolg Ihres Krisenmanagements.

In der aktuellen Kriegssituation ist das genauso: Die Haltung und Darstellung Ihres Unternehmens trägt signifikant zur Zukunftsfähigkeit bei. Es empfiehlt sich, rechtzeitig die gelebte Unterstützung von Marketing und anderen Unternehmensreserven zur Kommunikation zu aktivieren.

- Sichern Sie die Optionen der Kommunikationsstrategie entsprechend der Lage ab. Filtern Sie gezielt die strategisch sinnvollen Stufen und treffen Sie eine gezielte Vorauswahl.

- Prüfen und passen Sie Ihre Wording-Vorlagen an (insbesondere in Anlehnung an die konkrete Vorauswahl).

Presse- und Medienarbeit

Stimmen Sie mit der Geschäftsführung ab, welche proaktiven Äußerungen und welche Haltung Sie ggf. auch ohne direkte Beteiligung in der Ukraine, in Russland, Belarus sowie den Nachbarländern kommunizieren wollen. Passt z. B. eine Parteinahme für die Ukraine zu Ihrer Geschäftstätigkeit? Weisen Sie diesbezüglich auch Ihre Mitarbeiter an und empfehlen oder verbitten Sie sich entsprechende Parteinahme oder eine proaktive Solidarisierung.

Aktivieren Sie Ihr Medienmonitoring, um frühzeitig Entwicklungen für Ihr Unternehmen zu erkennen.

Beobachten Sie insgesamt die Unternehmenskommunikation nach außen (z. B. auch, was in Ihren Hotlines passiert) **und innen** (welche Rückmeldungen erhalten Sie von den Mitarbeitern?).

Bereiten Sie alle Kommunikationsmedien (intern/extern/Social Media) adressatengerecht vor. Beachten Sie dabei die proaktiven und reaktiven Abstufungen.

Sichern Sie Ihren Ressourcenpool ab: Haben Sie ausreichend Personal für die aktive Krisenkommunikation (aktivieren Sie Ihre Unterstützer intern und extern)? Benötigen Sie zusätzliche Sprachkompetenzen?

IT, Informations-sicherheit und Datenschutz

Eine der hierzulande ersten und eindrucksvollen Rückmeldung im IT-Umfeld war die Ankündigung der Hacker-Gruppe Anonymous, dass sie Russland den Cyberkrieg erklärt haben. Allerdings sitzen auch und gerade in der Ukraine und Russland Profis am anderen Ende der Leitung. Daher ist die Absicherung gerade im Bereich IT, Informationssicherheit und Datenschutz von extremer Wichtigkeit (in einem ohnehin sensiblen Feld), um mittel- und langfristig Schaden von Ihrem Unternehmen fernzuhalten (auch wenn es nur unbeabsichtigte Kollateralschäden sein können).

- Wenn nicht schon bei Ihnen vorhanden, **bauen Sie ein Awareness- und Sensibilisierungsprogramm auf**. Hierbei ist eine regelmäßige Kommunikation, gerade im Hinblick auf aktuelle Vorfälle und Beispiele zu fokussieren, ohne die Situation zu überspitzen.
  - Mitarbeiter im Allgemeinen
  - Mitarbeiter mit besonderer IT oder erhöhten Rechten (Administratoren)
  - Mitarbeiter, welche mit besonders sensiblen und kritischen Daten arbeiten (F&E, Finance)
- **Sichern Sie Ihre operative Bereitschaft gegen einen DDoS-Angriff in fünf Schlüsselbereichen:**
  - Durchführung von Service-Validierungen
  - Bestätigung autorisierter Mitigation-Service-Kontakte
  - Überprüfung und Aktualisierung von Playbooks
  - Durchführung von Operational-Readiness-Übungen
  - Aktualisierung der Kommunikationsmethoden für Notfälle

IT, Informations-sicherheit und Datenschutz

- **Implementieren Sie Geo-Blocking.**
- **Prüfen Sie, ob die Patches für anfällige Systeme auf sicherem Niveau erfolgen.** Insbesondere sollten bisher aufgeschobenen (Sicherheits-)Patches priorisiert werden.
- **Segmentieren Sie Ihr Netzwerk, um sich vor der Bedrohung durch Ransomware zu schützen.**

- Minimieren Sie Risiken, indem Sie Ihre aktuellen **Berechtigungs- und Zutrittsregelungen aktualisieren und die aktuell offen Projekte und Punkte priorisieren.**
- **Prüfen Sie kritisch, ob Sie aktuelle oder vergangene IT-Auslagerungen, Bezüge oder Dienstleistungen aus Belarus, der Ukraine oder Russland beziehen bzw. bezogen haben.** Wenn ja, betrachten Sie die Möglichkeit ein, dass diese Systeme ggf. nicht mehr zur Verfügung stehen könnten oder kompromittiert werden.

- **Bereiten Sie das Herunterfahren und Trennen Ihrer IT-Infrastruktur in den oben benannten Ländern vor.** Denken Sie auch an das Sichern und/oder Löschen von kritischen Unternehmensinformationen.
- **Prüfen und aktualisieren Sie (anlassbezogen) Ihre ITSC-Pläne.**

Ausblick

Die Dauer des Ukrainekriegs und die Folgen sind aktuell kaum einschätzbar, die Hoffnung auf eine Beilegung der Kriegshandlungen groß, aber die Gewissheit über langfristige Auswirkungen ebenfalls.

Die „Rückkehr in den Normalbetrieb“ nach der Stabilisierung der Krise innerhalb eines Unternehmens und der Beendigung des aktiven Einsatzes des Krisenstabs bedarf daher (wie immer) konkreter Maßnahmen und in diesem besonderen Fall einem sensiblen Vorgehen.

Auch hierzu eignen sich Stufenpläne und Szenarios, die Sie flexibel auch auf wechselnde Lageentwicklungen anpassen können.

- Prüfen Sie, ob die behördlichen nationalen und internationalen Vorgaben und Rahmenbedingungen die Wiederaufnahme Ihres Geschäftsbetriebs erlauben oder sogar unterstützten.
- Ist ggf. eine Teilaufnahme des Geschäftsbetriebs sinnvoll?
- Ermitteln Sie die lokalen Verfügbarkeiten und die Einsatzfähigkeit Ihres Unternehmens: Sind die benötigten Ressourcen (Personal inkl. Know-how, Gebäude, IT, Dienstleister sowie Material, Lagerverfügbarkeit, Logistik etc.) verfügbar?
- Prüfen Sie die Relevanz (Reputation, sonstige Interessen) und die Wirtschaftlichkeit (inkl. des Absatzmarktes) der Wiederaufnahme/Teilaufnahme Ihres Geschäftsbetriebs.
- Entwickeln Sie einen Zeit- und Stufenplan für den Wiederanlauf (von 0 auf 100 klappt meist nicht reibungslos). Empfehlenswert ist tatsächlich die individuelle Standortbetrachtung.
- Binden Sie relevante Stakeholder rechtzeitig ein (lokale Mitarbeiter, Lieferanten, Dienstleister, Kunden etc.).

Ausblick

- Prüfen und passen Sie Ihre Geschäftskonzepte an die Lageentwicklung an (von Sicherheit über Arbeitsschutz etc.).
- Warnen Sie Ihre Mitarbeiter ausdrücklich auch langfristig vor Cyber-Attacken per Social-Engineering (i.d.R. E-Mails mit Schadsoftware).
- Organisieren Sie eine vollumfassende Übergabe an die nun wieder eigenständig agierenden Geschäftsbereiche.
- Vermitteln Sie klare Informationslinien und Meldewege. Beachten Sie eine mögliche erneute Eskalation. Prüfen und aktualisieren Sie also Ihre Schwellenwerte und Prioritäten.
- Nutzen Sie alle Mittel Ihrer Kommunikationsverantwortlichen für eine abgestimmte, unternehmenskonforme und angemessene Kommunikation (intern/extern/Social Media).

Controllit AG
Kühnehöfe 20
22761 Hamburg
Deutschland
www.controll-it.de

Stand: 18. März 2022

Die Controllit AG ist Ihr Partner für Business Continuity Management (BCM). Seit unserer Gründung entwickeln wir integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management und Krisenmanagement. Wir helfen Ihnen mit strategischen, organisatorischen und technischen Konzepten, Ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Fotonachweise: S. 1 :iStock.com/Aquir; S. 3: iStock.com/designer491;
S. 4: iStock.com/designer491, iStock.com/ake1150sb;
S. 5: iStock/comalphaspirit; S. 6: iStock.com/Andranik Hakobyan,
iStock.com/vege; S. 7: iStock.com/vege, S. 11: iStock.com/OstapenkoOlena;
S. 12: iStock.com/SurfUpVector