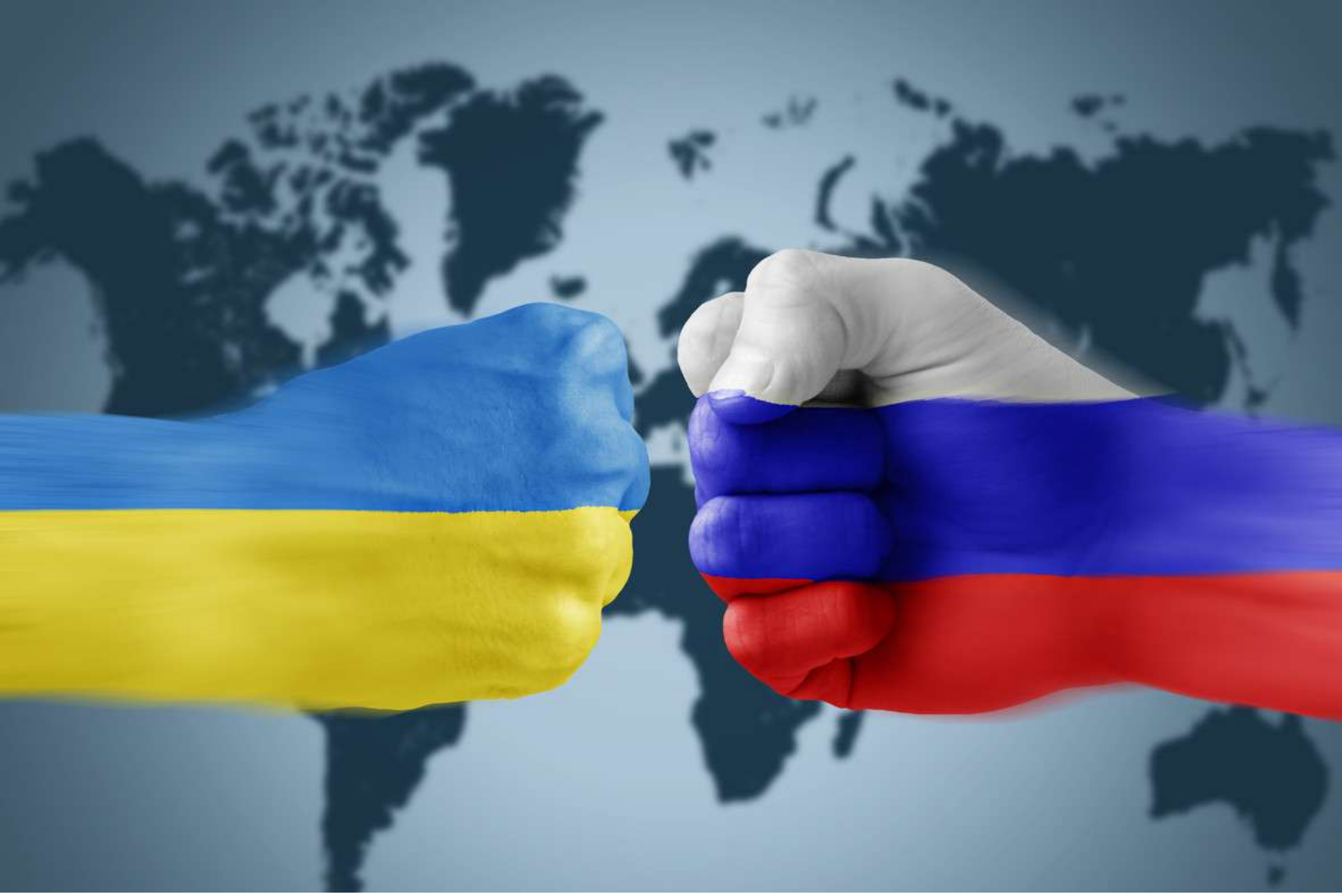


Livre blanc

Recommandations pour les entreprises internationales en activité dans le cadre de la guerre Russie-Ukraine 2022

controllit
Business Continuity Management

Contenu

Introduction

Les actes de guerre actuels en **Ukraine** et le conflit avec la **Russie** ne sont pas seulement préoccupants sur le plan médiatique, politique et personnel, ils ont également un impact massif sur les activités commerciales et l'économie européenne. Les affaires et les activités dans et avec le **Bélarus** ainsi que les **pays voisins** de l'Ukraine et la Russie sont également sous les feux de la rampe.

Les sanctions (encore volontaires pour la plupart) contre la Russie ont déjà des conséquences économiques importantes. De nombreuses entreprises réagissent en limitant leurs activités-commerciales, en se mettant en attente ou en cessant complètement leurs activités. Là où la production et la distribution ont été ou seront réduites, il s'agit de coordonner la fin des activités et de sécuriser les marchandises, les valeurs et les biens immobiliers.

Les secteurs de l'industrie automobile (fabrication et distribution), des transports (en particulier l'aviation), de la banque et de l'assurance, de l'énergie, du divertissement, de l'industrie et de la fabrication, de la logistique, de la technologie, des télécommunications, des fabricants d'articles de sport, de la production et de la distribution d'articles ménagers et des magasins de meubles réagissent en conséquence.

L'impact sur le champ de bataille en Ukraine même est dévastateur, et les pays voisins, non seulement dans les zones frontalières, ainsi que d'autres pays européens sont également impliqués.

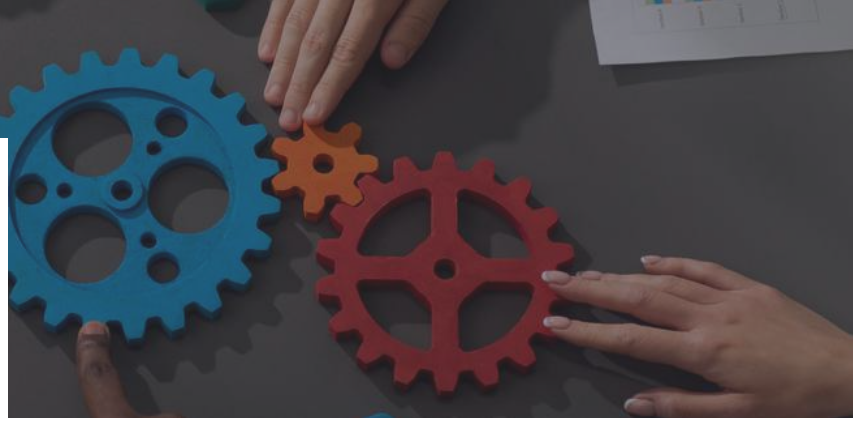
Introduction

Les conséquences sur l'évolution des coûts sont perceptibles (un programme de crédit de la banque publique de développement en Allemagne a été annoncé), les prévisions d'exportation de la DIHK (Chambre allemande de l'industrie et du commerce) ont été sensiblement revues à la baisse et des interruptions de production, même sur les sites indirectement touchés, sont à craindre en raison des difficultés rencontrées dans les chaînes d'approvisionnement. En outre, il existe une possibilité de pénurie et une augmentation probable des prix des matières premières.

Enfin, et ce n'est pas le moins important, la **préoccupation** et les **soins** directs aux employés sont une question déterminante : c'est là que la responsabilité et l'obligation de rendre compte de l'entreprise deviennent pertinentes, qu'il s'agisse d'évacuer les employés ou de fournir les meilleurs soins possibles aux employés qui veulent ou doivent rester sur le site.

Avec ces recommandations d'action, nous voulons donner une orientation à l'aide de la perspective classique de l'état-major et présenter des **options concernant les champs thématiques suivants** :

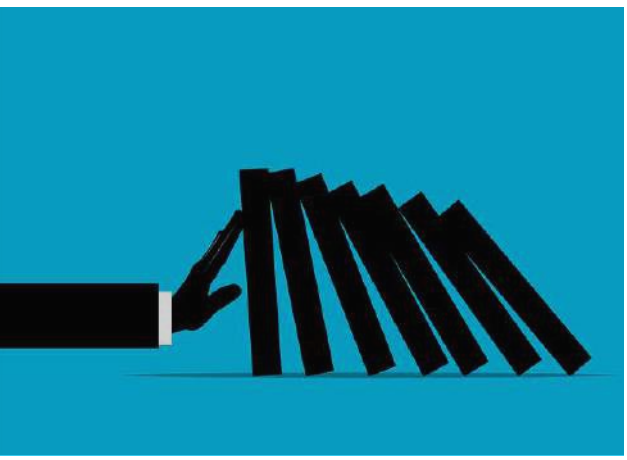
- Ressources humaines (y compris la sécurité)
- Évaluation (y compris la sécurité)
- Opérations
- Logistique
- Communication
- Informatique, sécurité de l'information et protection des données



Recommanda-tion d'action

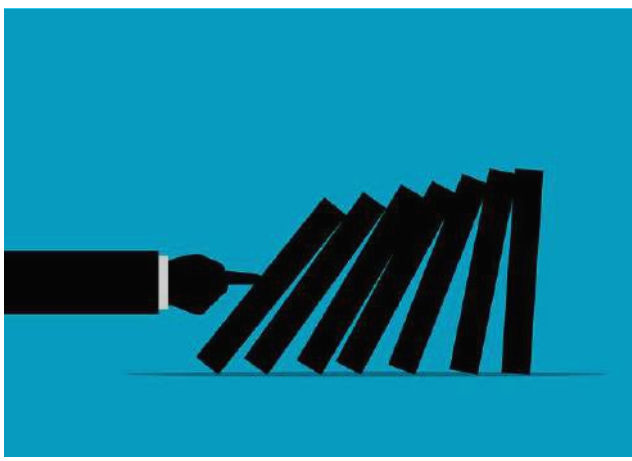
En principe, nous recommandons également une préparation solide et clairvoyante dans le conflit actuel (si disponible : utilisation des niveaux d'escalade et des seuils de votre entreprise) et l'élaboration de plans par étapes ou de scénarios.

La préparation concrète sert avant tout à l'évaluation ciblée (idéalement sur la base de vos seuils et priorités éventuellement actualisés). L'utilisation de plans par étapes ou de scénarios aide les entreprises à s'adapter de manière flexible à la situation concrète. D'autre part, la préparation réactive sert également à la coordination et au contrôle ciblés pour tous les scénarios d'arrêt, de mise au repos et de fermeture. Il existe ici une différence sensible entre une procédure ciblée et gérée de manière proactive et le simple fait de "laisser tomber". Même lors du retour à l'exploitation normale, un plan par étapes permet de structurer l'action et d'en assurer la souplesse.



Les procédures pour les entreprises actives en Russie, en Ukraine et en Biélorussie, pays directement concernés ou impliqués, sont différentes de celles des pays voisins, en fonction de la situation. Les questions et la gestion des interfaces sont toutefois très similaires. Dans les pays voisins, il s'agit aussi bien de la perspective d'être affecté dans les régions frontalières que d'une éventuelle extension du conflit.

Dans les chapitres suivants, nous vous donnons des recommandations d'action concrètes sur les champs thématiques et soulevons les questions nécessaires.



Ressources humaines

Le secteur du personnel peut être bien structuré et évalué grâce à l'interface partenaires ressources humaines et sécurité. D'une part, il est bien sûr important de garantir la sécurité physique et la santé du personnel, mais d'autre part, il est également important de gérer de manière proactive les compétences (capacités, aptitudes, qualifications), y compris les points de connaissance uniques (SPOK) de votre entreprise.

La question la plus importante dans une zone de guerre, de sanctions directes ou de frontière est celle de la sécurité physique. Mais la situation peut aussi évoluer de manière dynamique dans les pays voisins.

- Vérifiez la sécurité de votre personnel : vos consignes de voyage correspondent-elles à la situation actuelle (interdictions de voyager, etc.) ?
- Déterminez les collaborateurs que vous devez, devez ou voulez évacuer (pas seulement dans la zone de guerre immédiate).
- Demandez-vous si votre personnel est composé d'employés nationaux dans leur pays d'origine ou d'employés d'autres pays (éventuellement avec les nationalités des parties au conflit). Considérez également la nécessité et la possibilité d'évacuer les membres de la famille du personnel local.
- Suivez toujours les recommandations du ministère fédéral des Affaires étrangères (en Allemagne) et, bien sûr, des autorités du pays concerné.

Ressources humaines

- Déterminez les options et les moyens disponibles pour un départ/une évacuation. Il existe probablement des offres de soutien d'une part pour l'utilisation des moyens de transport, mais aussi de nature financière.
- Vérifiez s'il existe un soutien du gouvernement fédéral, de l'État fédéré, d'autres institutions ou d'entreprises de sécurité privées et si une assurance de votre entreprise intervient.
- Considérez le calendrier. Quelles activités immédiates sont nécessaires, quelles activités peuvent être préparées et mises en œuvre dans quel environnement et dans quel délai ?
- Planifiez les lieux de repli de vos collaborateurs. Dans une région en guerre, il peut être judicieux, sous la pression du temps, de commencer par un départ temporaire vers les pays voisins. Informez-vous et informez les personnes concernées sur les points de contact correspondants (par ex. les ambassades).
- Si vous pouvez contrôler les activités de départ, il faut absolument inclure le lieu d'affectation professionnel judicieux à moyen terme dans la réflexion sur la région de destination sûre.
- Pour ce faire, il est recommandé de procéder à une enquête approfondie afin de déterminer où les compétences libérées sont nécessaires. Y a-t-il déjà des réflexions sur des solutions de remplacement au sein de l'entreprise ou des besoins dans d'autres lieux sûrs ?
- Considérez également si du personnel local est nécessaire pour assurer la sécurité de vos biens et valeurs, pour des activités de surveillance ou des activités d'entreprise en cas de cessation ou de réduction ciblée de vos activités. Le point de vue de vos collaborateurs locaux et des autres collaborateurs sur place peut être une bonne aide à la décision.
- Dernier point, mais non le moindre : les employés des zones directement touchées auront probablement besoin d'un soutien psychosocial. Y a-t-il d'autres défis à relever en matière de santé mentale des employés ?

Évaluation

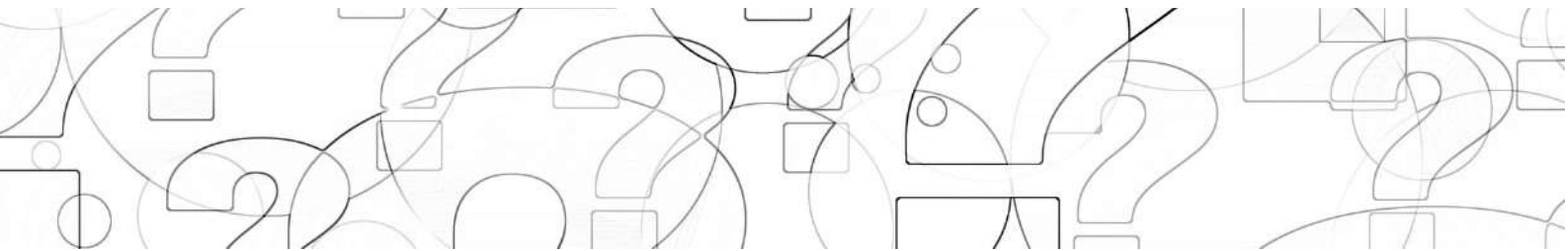
Déterminer une image de la situation dans une zone de guerre est toujours un défi avec quelques inconnues. Il est donc conseillé d'utiliser les informations officielles et médiatiques ainsi que les informations individuelles et de les compiler dans un tableau de la situation spécifique à l'entreprise. En outre, il existe en Allemagne des entreprises et des services spécialisés dans ce domaine. Vos professionnels de la communication (service de communication, etc.) et les responsables de la sécurité ainsi que vos employés directs, vos partenaires et/ou vos prestataires de services sur place sont des partenaires d'information pertinents. Vous recevrez également un précieux retour d'information sur la faisabilité de vos mesures via vos contacts locaux.

Pour élaborer votre plan par étapes sur la base du tableau de la situation, il est également important de savoir si vous parlez d'un arrêt complet, d'une réduction contrôlée ou limitée de vos activités commerciales. En outre, il existe bien sûr toutes les variantes de combinaison que vous devez envisager et évaluer. En outre, la situation en Ukraine, en Russie, au Bélarus ainsi que dans les pays voisins peut avoir un effet de rebond sur l'ensemble de votre entreprise. Idéalement, vous devriez également tenir compte des dépendances dans l'environnement international de votre organisation commerciale.

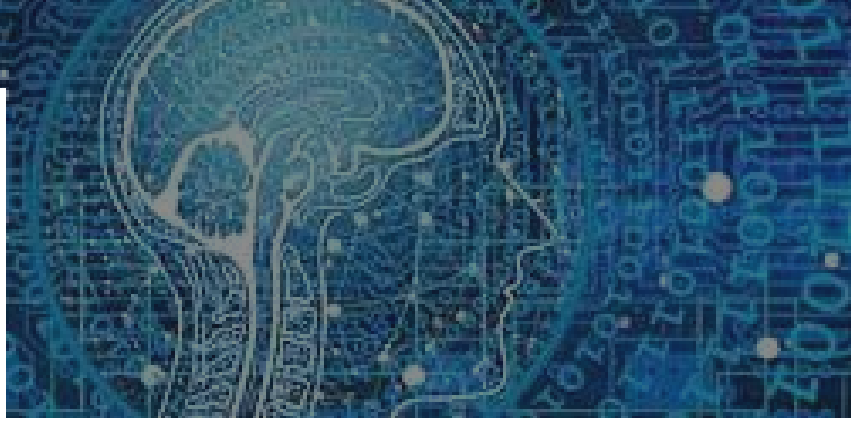
- Examinez quelles parties de l'entreprise sont actuellement concernées et dans quelle mesure elles le seront dans le futur. Définissez le cadre de votre réflexion en concertation avec votre direction (actuellement, il est recommandé d'envisager une perspective d'au moins six mois). Quels sont les dommages déjà subis et prévisibles (à moyen ou long terme) ?

Évaluation

- Incluez dans votre réflexion les dépendances de vos autres produits, chaînes de production et de livraison. Existe-t-il des "monopoles" ou des activités de base ?
- Vérifiez si vos clients, vos collaborateurs, leurs familles et leurs marchés sont concernés.
- Informez-vous sur l'évaluation et les perspectives de vos interlocuteurs directs sur place.
- Déterminez également comment l'échange d'informations avec les interlocuteurs locaux peut être maintenu à moyen et long terme.
- Déterminez l'état des ressources locales et les exigences locales (personnel, y compris le savoir-faire, les bâtiments, l'informatique, les prestataires de services ainsi que l'état du matériel, le stockage, la logistique, etc.)
- Pour évaluer et planifier les ressources, il est également recommandé de disposer d'informations sur la situation en matière d'approvisionnement, de transport et de sécurité en Ukraine, en Russie, en Biélorussie et dans les pays voisins.
- Lors de la collecte d'informations, veillez au sérieux des sources, posez régulièrement des questions critiques sur les informations sur la situation et communiquez les informations centrales sur la situation au sein de votre entreprise.
- Essayez d'anticiper la situation en décrivant et en évaluant les scénarios potentiels de conflit et de marché pour votre entreprise et en concevant des réponses appropriées.
- Vérifiez votre droit et utilisez les subventions fédérales et/ou les programmes de crédit.
- Observez et évaluez vos participations actuelles en actions à des intervalles appropriés (éventuellement plus courts) afin de garder un œil sur les cours fluctuants et de pouvoir agir et communiquer en conséquence.



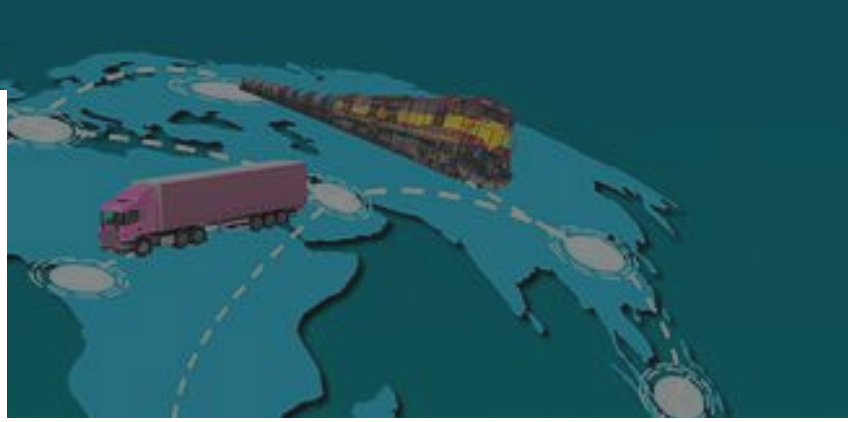
Opération



Lors de la prise de décision et de l'ajustement de vos mesures, il est conseillé de s'adapter à la situation de manière vraiment flexible en utilisant votre modèle de décision (par exemple FORDEC). En particulier, réexaminez les options de soutien possibles et utilisez vos seuils et vos priorités dans le modèle de niveau recommandé

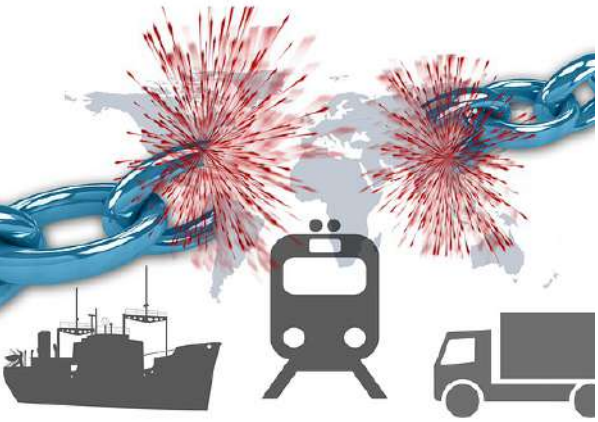
- Assurez-vous que vos priorités sont adaptées à la situation ou qu'elles pourront être modifiées à court terme.
- Vérifiez le temps et par quelles parties non affectées de votre entreprise des mesures de compensation peuvent être mises en œuvre.
- Vérifiez si et quelles alternatives et options d'expansion existent dans votre domaine d'activité.
- Déterminez si des interfaces internes et externes sont disponibles et lesquelles.

Logistique



Depuis le Covid-19, la sensibilité des mouvements de marchandises liés à l'entreposage et au transport a été mise en avant. Dans le contexte de conflits armés, ce domaine exige une coordination et une organisation particulières dans les pays concernés : Ukraine, Russie, Biélorussie ainsi que les pays voisins. Dans ce contexte, il est recommandé de réagir de manière flexible et sûre à l'image de la situation à l'aide de votre plan par étapes. Utilisez les interfaces du contrôle de gestion, de la gestion des risques, les responsables locaux et votre direction au niveau stratégique comme source d'information.

- Assurez-vous que vos produits et clients prioritaires sont à jour.
- Déterminez la disponibilité technique et matérielle actuelle, y compris l'équipement de vos entrepôts, de vos parcs de véhicules, des autres moyens de transport et des voies de fret (voir aussi Évaluation).
- Examinez vos alternatives : Y a-t-il des choix possibles concernant d'autres lieux de stockage (y compris la répartition), prestataires de services, transporteurs, moyens et voies de transport ?
- Déterminez les exigences de vos alternatives. Y a-t-il des particularités ou des obstacles ? Peut-être une combinaison d'alternatives est-elle judicieuse ?
- Examinez quelles pertes qualitatives et quantitatives sont acceptables.
- Évaluez les choix possibles en fonction de la sécurité (veuillez également tenir compte des perspectives à moyen et long terme), de la rentabilité (temps et coûts) et de la faisabilité (exigences en matière de personnel, durée de conservation de vos marchan-dises, exigences informatiques, utilisation de processus manuels le cas échéant, etc.)



- Gardez à l'esprit les exigences légales ou con-tractuelles et les répercussions sur la réputation ou l'image de votre entreprise ainsi que sur un éventuel lieu utilisable à plus long terme.
- Assurez-vous que vos alternatives sont également efficaces et efficientes dans tous les pays. Il est recommandé d'examiner la liberté de vos chaînes de transport et de vos flux de livrai-son, y compris en ce qui concerne le pays d'origine et le pays d'arrivée, ainsi que les exigences en matière de documentation.

Communication

Dans toutes les crises, le service de communication de votre entreprise est considérablement sollicité en ce qui concerne le volume à gérer et l'exigence de qualité. La perception interne et externe de votre gestion de crise est influencée par la communication de l'entreprise et détermine en grande partie le succès de votre gestion de crise.

Il en va de même dans la situation de guerre actuelle : l'attitude et la présentation de votre entreprise contribuent de manière significative à sa pérennité future. Il est conseillé d'activer en temps utile le soutien vécu du marketing et des autres réserves de l'entreprise en matière de communication.

- Aligner les options de la stratégie de communication en fonction de la situation. Filtrez spécifiquement les étapes stratégiquement utiles et faites une présélection ciblée.
- Vérifiez et adaptez vos modèles de wording (notamment en fonction de la présélection concrète).

Communication

Déterminez avec la direction les déclarations proactives et l'attitude que vous souhaitez communiquer en Ukraine, en Russie, en Biélorussie et dans les pays voisins, même si vous n'êtes pas directement impliqué. Par exemple, une prise de position en faveur de l'Ukraine correspond-elle à votre activité commerciale ? Donnez également des instructions à vos collaborateurs à ce sujet et recommandez ou interdisez un tel parti pris ou une solidarité proactive.

Activez votre monitoring des médias afin d'identifier à temps les évolutions pour votre entreprise.

Observez globalement la communication de l'entreprise vers l'extérieur (par exemple, ce qui se passe dans vos hotlines) **et vers l'intérieur** (quels sont les retours que vous recevez de la part de vos collaborateurs ?).

Préparez tous les supports de communication (internes/externes/médias sociaux) en fonction des destinataires. Tenez compte desnuances proactives et réactives.

Assurez votre pool de ressources : Avez vous suffisamment de personnel pour la communication de crise active (activez vos soutiens internes et externes) ? Avez-vous besoin de compétences linguistiques supplémentaires ?

Informatique, sécurité de l'information et protection des données

L'une des premières réactions, et la plus impressionnante, dans l'environnement informatique en Allemagne a été l'annonce par le groupe de hackers Anonymous qu'ils avaient déclaré la cyberguerre à la Russie. Cependant, il y a des professionnels à l'autre bout de la ligne, notamment en Ukraine et en Russie. Par conséquent, la protection dans le domaine de l'informatique, de la sécurité de l'information et de la protection des données est extrêmement importante (dans un domaine déjà sensible) afin d'éviter que votre entreprise ne subisse des dommages à moyen et long terme (même s'il ne s'agit que de dommages collatéraux involontaires).

- Si vous ne l'avez pas déjà fait, mettez en **place un programme de sensibilisation et d'information**. Il s'agit ici de se concentrer sur une communication régulière, notamment en ce qui concerne les incidents et les exemples actuels, sans exagérer la situation.
  - Collaborateurs en général
  - Collaborateurs disposant d'une informatique particulière ou de droits élevés (administrateurs)
  - Collaborateurs travaillant avec des données particulièrement sensibles et critiques (R&D, finance)

- **Sécurisez votre préparation opérationnelle contre une attaque DDoS dans cinq domaines clés :**
  - Réalisation de validations de services
  - Confirmation des contacts de service de mitigation autorisés
  - Vérification et mise à jour des runbooks
  - Réalisation d'exercices de préparation opérationnelle
  - Mise à jour des méthodes de communication en cas d'urgence

Informatique, sécurité de l'information et protection des données

- **Mettre en œuvre le géo-blocage.**
- **Vérifier si les correctifs pour les systèmes vulnérables sont appliqués au niveau de sécurité.** Il convient notamment de donner la priorité aux correctifs (de sécurité) qui ont été reportés jusqu'à présent.
- **Segmentez votre réseau pour vous protéger contre la menace des ransomwares.**

- Réduisez les risques en **actualisant** vos **règles d'autorisation et d'accès** actuelles **et en classant par ordre de priorité les projets et les points actuellement en suspens**.
- **Examinez d'un œil critique les externalisations informatiques actuelles ou passées, les achats ou les services provenant de Bélarus, d'Ukraine ou de Russie.** Si oui, envisagez la possibilité que ces systèmes ne soient plus disponibles ou soient compromis.

- **Préparez l'arrêt et la déconnexion de votre infrastructure informatique dans les pays susmentionnés.** Pensez également à sauvegarder et/ou à supprimer les informations critiques de l'entreprise.
- **Examinez et mettez à jour vos plans ITSC (en fonction des besoins).**

Perspectives

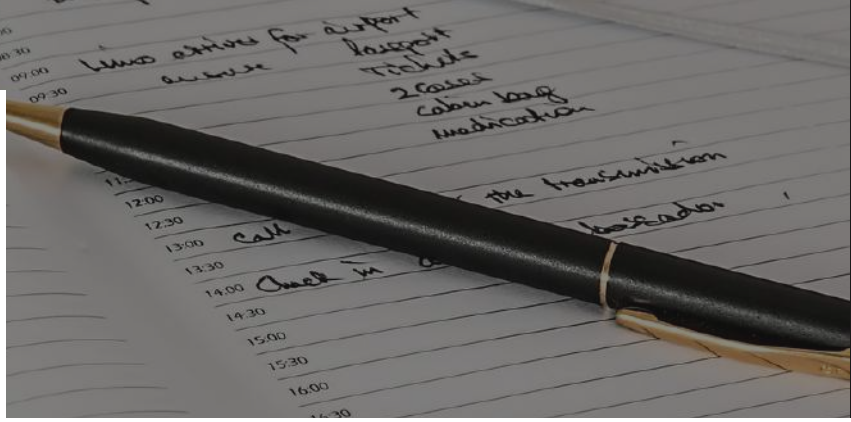
La durée de la guerre en Ukraine et ses conséquences sont actuellement difficilement évaluables, l'espoir d'un règlement des hostilités est grand, mais la certitude des effets à long terme l'est tout autant.

Le "retour à la normale" après la stabilisation de la crise au sein d'une entreprise et la fin de l'intervention active de la cellule de crise nécessite donc (comme toujours) des mesures concrètes et, dans ce cas particulier, une approche sensible.

Les plans par étapes et les scénarios, que vous pouvez adapter de manière flexible à l'évolution de la situation, conviennent également à cet effet

- Vérifiez si les directives et conditions nationales et internationales des autorités autorisent ou même soutiennent la reprise de votre activité.
- Est-il judicieux de reprendre une partie de votre entreprise ?
- Déterminez les disponibilités locales et la capacité d'intervention de votre entreprise : les ressources nécessaires (personnel y compris savoir-faire, bâtiments, informatique, prestataires de services ainsi que matériel, disponibilité des stocks, logistique, etc.) sont-elles disponibles ?
- Examinez la pertinence (réputation, autres intérêts) et la rentabilité (y compris le débouché) de la reprise/du démarrage partiel de votre activité.
- Élaborez un calendrier et un plan par étapes pour le redémarrage (de 0 à 100 ne fonctionne généralement pas sans heurts). Un examen individuel du site est en effet recommandé.
- Impliquer les parties prenantes concernées en temps utile (employés locaux, fournisseurs, prestataires de services, clients, etc.).

Perspectives



- Vérifiez et adaptez vos concepts commerciaux à l'évolution de la situation (de la sécurité à la santé et à la sécurité au travail, etc.).
- Avertissez explicitement vos collaborateurs, même à long terme, des cyber-attaques par ingénierie sociale (en général, des e-mails contenant des logiciels malveillants).
- Organiser un transfert complet vers les secteurs d'activité qui agissent désormais à nouveau de manière autonome.
- Communiquez des lignes d'information et des voies de signalement claires. Tenez compte d'une éventuelle nouvelle escalade. Vérifiez et actualisez donc vos seuils et vos priorités..
- Utilisez tous les moyens de vos professionnels de la communication pour une communication coordonnée, conforme à l'entreprise et appropriée (interne/ externe/médias sociaux) .

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

Mise à jour: 18 mars 2022

Controllit AG est votre partenaire pour le Business Continuity Management (BCM). Depuis notre création, nous développons des concepts et des produits intégratifs pour le Business Continuity Management, l'IT Service Continuity Management et la gestion de crise. Nous vous aidons à sécuriser vos processus commerciaux contre les menaces et à vous préparer aux situations d'urgence grâce à des concepts stratégiques, organisationnels et techniques.

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