Guide d'exercice
Exercice d'équipe de crise Cyberattaque

controllit
Business Continuity Management

Contenu

Introduction

Des titres tels que "Cybercriminalité", "2 millions de données clients fuient", "Une attaque de pirates informatiques paralyse une entreprise pendant des semaines" faire la une dans les médias. Malgré toutes les mesures d'atténuation des risques et les précauti-ons prises par les entreprises, ce scénario se produit également en Allemagne plusieurs fois par an, avec des dommages se chiffrant en millions.

Votre entreprise est-elle préparée à ce scénario ?

Dans ce guide sur la cyberattaque lors d'un exercice de cellule de crise, nous souhaitons présenter les thèmes essentiels à la bonne gestion d'une telle crise.
Ce faisant, nous accordons une attention particulière aux objectifs classiques de la gestion de crise :

- **Protection de vos employé.e.s**/blessures aux personnes et à l'environnement
- **Réduction de l'impact économique**/minimiser les dommages économiques, éviter les dommages d'image, maintenir les processus d'affaires critiques (en temps)
- **Protection du fonctionnement normal** des services non affectés du siège

L'accent est également mis sur la coopération effective et efficace des membres de votre équipe de crise via une **checklist des tâches essentielles de l'équipe de crise** :

- Identification et analyse des situations de crise
- Définition d'une stratégie de gestion de crise
- Élaboration d'options d'action
- Évaluation des perspectives de succès, des risques et des opportunités
- Établissement de priorités et prise de décision
- Informer sur les mesures prises
- Délégation et contrôle des actions
- Évaluation et réévaluation

Mesures préventives

La gestion de crise est un processus réactif, mais il va de soi que vous préparez également votre organisation de gestion de crise à ses tâches par des mesures préventives.

Nous résumons ici les mesures clés dans la perspective d'un scénario de "cyberattaque" :

Vérifiez si tous les membres responsables de votre organisation de crise sont capables d'agir et prêts à agir (par exemple grâce à une formation régulière, une structure de réunion, un échange régulier d'informations, des mesures de sensibilisation) :

- Les membres de la cellule de crise, y compris leurs suppléants
- Participants au niveau tactique (chefs de service, etc.)
- Les exécutants au niveau opérationnel (employés des services spécialisés)

Tirez parti de votre système de gestion de la continuité des activités (PCA) lorsqu'il est mis en œuvre :

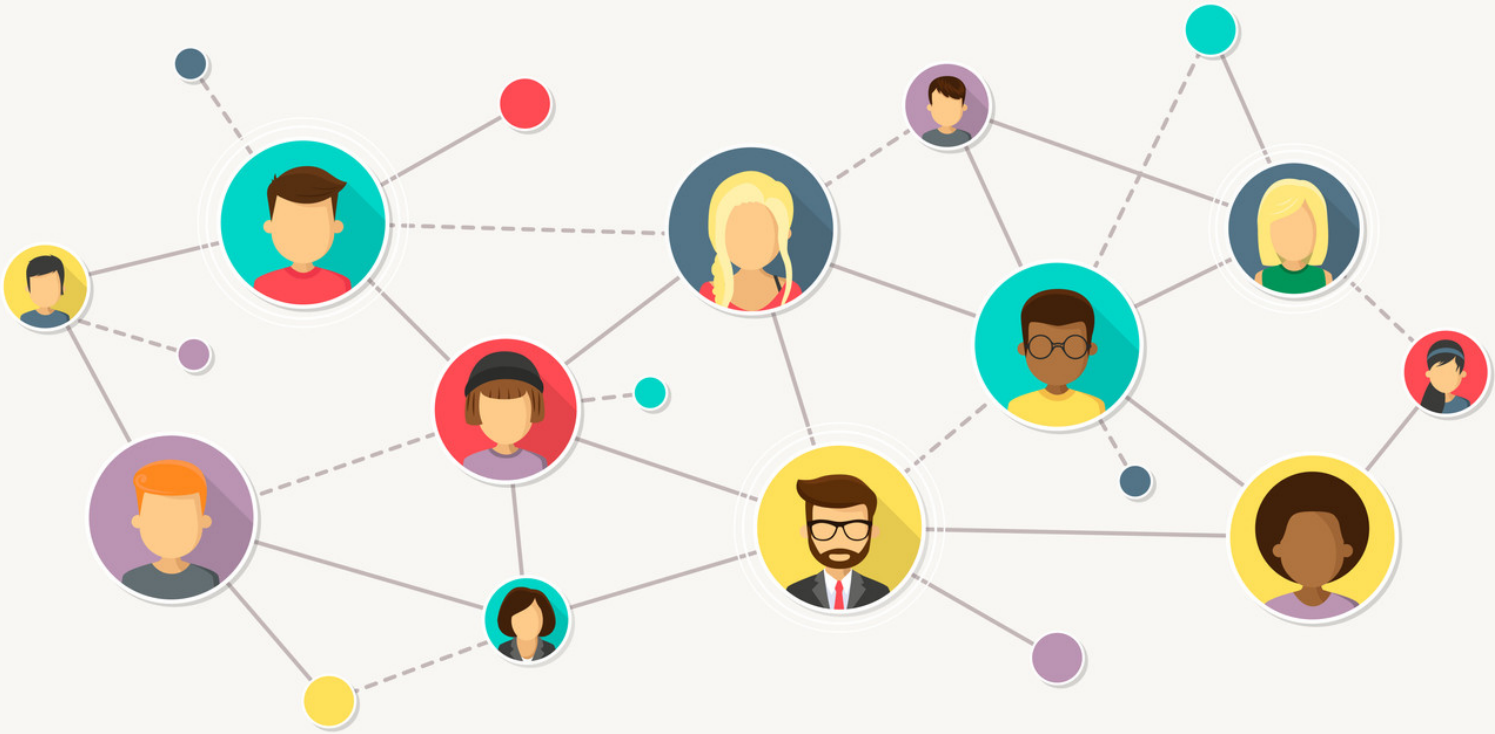
- Examiner l'opportunité et l'efficacité des plans de continuité des activités pour le scénario de panne informatique :
  - → En cas de panne informatique, les options de solution utilisées sont-elles capables de compenser temporairement la défaillance d'un processus métier (notamment en ce qui concerne les solutions de contournement mises en œuvre) ?
  - → Vos mesures de sauvegarde, telles que l'alternance chaud-froid, sont-elles efficaces et applicables ?
- Si vous n'avez pas mis en place un système de gestion de la continuité des affaires, vérifiez votre capacité opération-nelle sur la base des thèmes suivants

Tirez parti de votre système de gestion de la continuité des services informatiques (ITSCM) et de votre système de gestion de la sécurité de l'information (ISM) lorsqu'ils sont mis en œuvre :

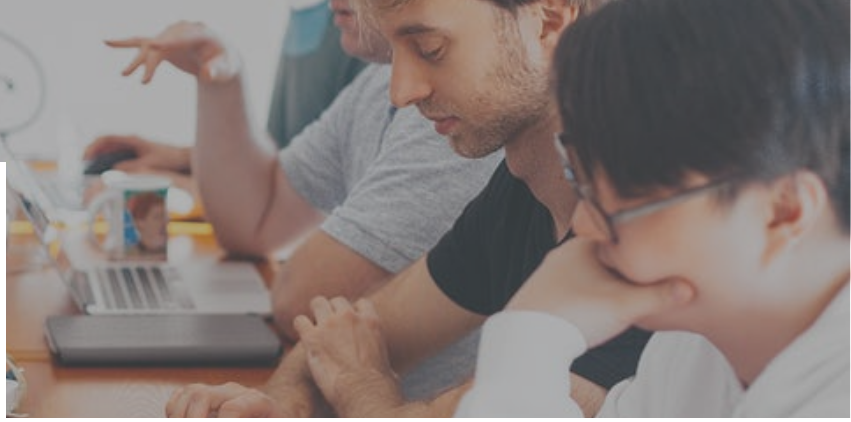
- En cas de panne informatique, les options de solution utilisées sont elles capables de compenser temporairement la défaillance d'un processus métier ?
- Vos KPI informatiques telles que l'objectif de temps de récupération (Recovery Time Objective, RTO) et l'objectif de point de récupération (Recovery Point Objective, RPO), peuvent-ils être atteints ?
- La disponibilité des services informatiques est-elle suffisamment garantie du point de vue de la gestion de la continuité des services informatiques (ITSCM) ?
- La récupération des ressources en cas d'attaque est-elle assurée de manière adéquate dans la gestion de la continuité des services informatiques (ISM) ?
- Les objectifs de protection de la gestion de la sécurité de l'information sont-ils adéquatement sauvegardés ?
- Si vous n'avez pas encore mis en œuvre des procédures l'ITSCM et/ou l'ISM, vérifiez votre état de préparation à l'aide des sujets énumérés ci-dessous

Mesures préventives

Utiliser la mise en place et la maintenance par le gestionnaire de crise d'interfaces ex-ternes (ici notamment des autorités telles que la police, les pompiers, vos authorités de tutelles etc.)



Créer une compréhension et une sensibilisation ainsi qu'une sécurité procédurale pour le sujet (mesures de sensibilisation)



Mesures réactives

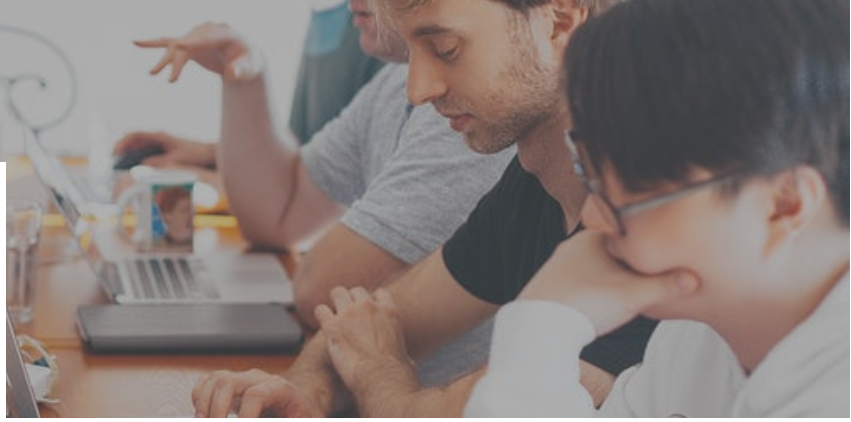
Les mesures réactives en cas d'incident sont au premier plan dans un exercice de gestion de crise (mais aussi si l'incident survient vraiment). Cela implique un lancement ordonné du travail de votre cellule de crise, soutenu par une vue d'ensemble des sujets. Les premières étapes ainsi que les points détaillés pour les différents membres de la cellule de crise sont présentés ci-dessous.

Aperçu général des thèmes

En cas de cyberattaque, des mesures initiales sont prises avec la participation de votre équipe IT et, si nécessaire, avec l'intervention d'autorités externes : L'accent est immédiatement mis sur la limitation des dommages et les mesures de sécurité.

En outre, les mesures et considérations suivantes sont essentielles :

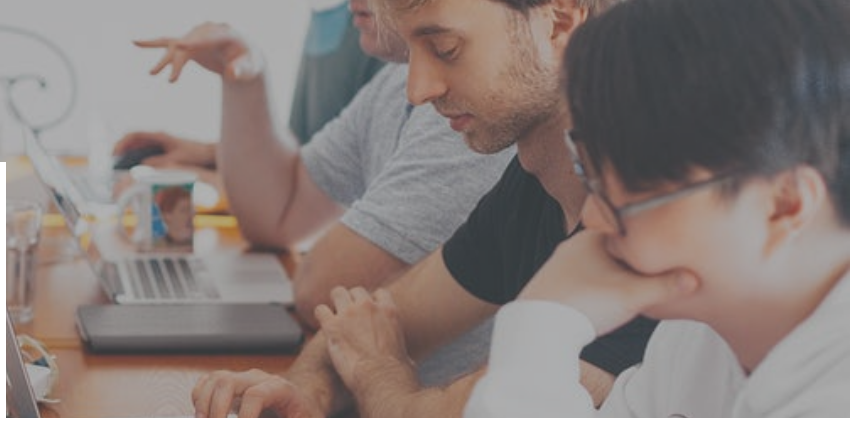
- Respecter les points suivants lors de l'alerte et de la constitution de l'équipe de crise:
  - → Salle d'équipe de crise utilisable (éventuellement utilisation d'une autre salle d'équipe de crise) ?
    - Votre salle d'équipe de crise peut-elle être utilisée de manière autonome par rapport à un ou plusieurs composants informatiques ?
    - Les outils virtuels avec connexion au système d'entreprise ne sont probablement pas disponibles !
  - → Identification des systèmes et logiciels informatiques disponibles (du téléphone au site web en passant par les ordinateurs portables d'urgence)
  - → Communication interne et externe rapide
    - Première information : Confirmation de l'événement sur la base de libellés prédéfinis (idéalement dans les dix minutes)
    - Une attention particulière doit être accordée au positionnement de l'entreprise et à la stratégie de communication externe (responsabilité, auteur/victime, etc.)
  - → Identification et délimitation de l'étendue actuelle et potentielle des dommages (interface ITSCM/IT)
  - → Activation des plans de continuité des activités (PCA) et du plan de reprise informatique (si disponible)
  - → Obtenir l'approbation du budget (si nécessaire)



Mesures réactives

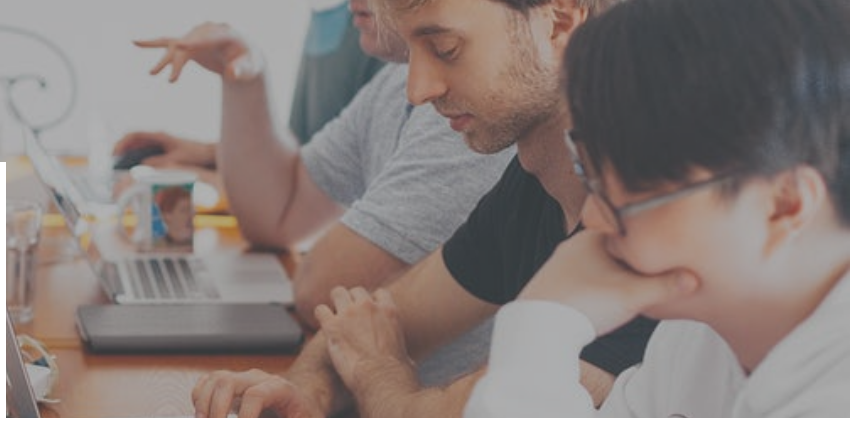
- Notez une cascade d'impacts dynamiques (ce qui est assez probable) : Généralement, un effet domino se produit au sein des systèmes informatiques
- Il convient de noter le dynamisme initial extrêmement élevé et la pression probable (due à une forte dépendance globale à l'égard des technologies de l'information) de la phase de chaos, notamment en termes d'information (abondance et rareté)
- Effectuer les tâches essentielles pour initialiser et assurer les opérations d'urgence
- Utilisez votre forme d'organisation : Y a-t-il une équipe d'assistance et de service (AST), une équipe de communication ou les membres de l'équipe de crise sont-ils responsables de la connexion structurée des services?
  - → Quels sont les canaux de reporting et d'information ?
  - → Comment intégrer les représentants de l'interface BCM, ITSCM et ISM dans l'équipe de crise ?
- Utilisez la connexion des services utilisateurs à l'assistance et de service (AST) ou au l'équipe de crise pour déterminer la situation :
  - → Quels sont les services concernés ?
  - → Quels sont les services capables ou non de travailler ?
  - → Quels sont les services informatiques concernés ?
  - → Quels services informatiques peuvent être utilisés ?
  - → Les données des employés et/ou des clients sont-elles affectées ?
  - → Quelles mesures de protection sont efficaces/peuvent être classées par ordre de priorité ?

- Assurer le flux d'informations et la connexion coordonnée aux interfaces externes (par exemple, les autorités telle que la police, les pompiers etc.) ainsi que la mise en œuvre en temps voulu des obligations de déclaration :
  - → Si nécessaire intégration d'experts externes (par exemple, experts en informatique) dans l'équipe de crise
  - → Le respect des délais de déclaration conformément aux exigences de l'entreprise et du secteur



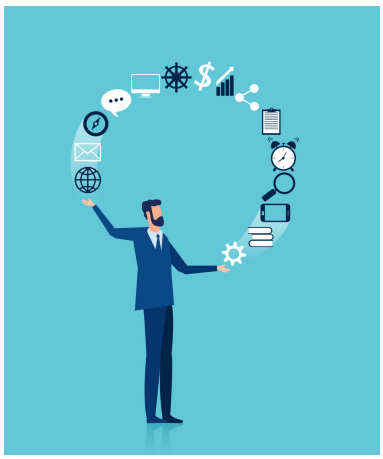
Mesures réactives

- Contrôlez votre vision globale de la situation : utilisez la visualisation pour une vue d'ensemble !
  - → L'étendue des dommages internes et externes : Quels services informatiques sont touchés ? Quels RTA (Recovery Time Actual) et RPA (Recovery Point Actual) sont actuellement réalistes ? Quelles données sont scénarios?
  - → Quels sont les services concernés ? En particulier : Quels processus d'affaires critiques en termes de temps et quels RTO (Recovery Time Objective) existent ?
  - → Quels sont les services qui peuvent ou ne peuvent pas fonctionner ? Existe-t-il des options de reprise d'activité ?
  - → Quels services informatiques sont nécessaires en cas d'urgence et sont utilisables/ récupérables ? Hiérarchisation des priorités sur le calendrier ?
  - → Responsabilité de l'événement : faute propre/faute extérieure/respect du devoir de diligence
  - → Aperçu des mesures et contrôle du statut
  - → Détermination des causes profondes pour une limitation optimisée des dommages (par exemple, par le biais de l'investigation informatique)
- Utilisez vos seuils !
  - → Les seuils sont-ils définis et quels sont les seuils dépassés ? Seuil potentiellement dépassé pour :
    - Défaillance informatique
    - Défaillance d'un fournisseur de services informatiques
    - Le cas échéant, valeurs seuils ITSCM (si disponible)
- Notez les implications pour le travail à domicile et à distance
  - → Les connexions VPN peuvent également avoir un impact sur les appareils privés des employés (bring-your-own-device)
- Évaluez les perspectives de votre équipe de crise
  - → En cas de panne informatique, l'équipe de crise sera probablement utilisé pendant une période plus longue (en fonction du type et du traitement de la cyberattaque)
- Commencez le processus de récupération en parallèle avec l'opération d'urgence (récupération informatique)
- Vérifiez votre couverture d'assurance et vos obligations de notification (par exemple, l'assurance contre les pertes d'exploitation)
- Accordez une attention particulière à l'assistance : lignes d'assistance téléphonique.
  - → Si la téléphonie fonctionne encore, il faut s'attendre à un volume supplémentaire élevé (demandes des clients et des médias)



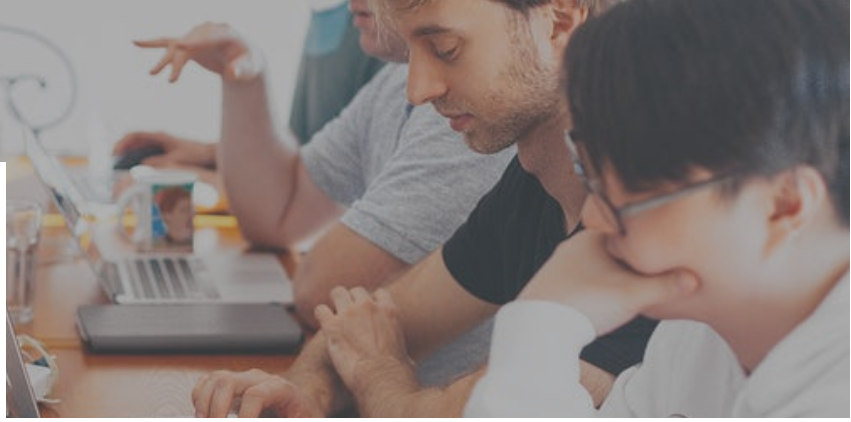
Mesures réactives

Tâches spécifiques des membres de la cellule de crise



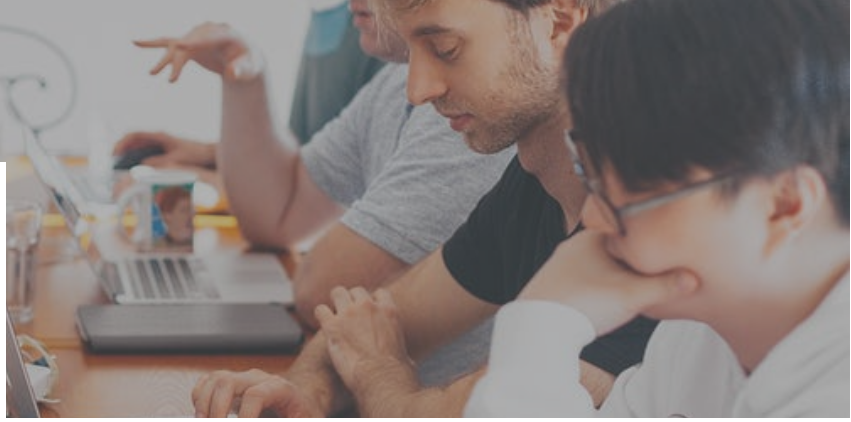
Certains membres de votre équipe de crise peuvent traiter leurs tâches selon la liste de contrôle dans le scénario de "cyberattaque" (par exemple, les titulaires de fonctions modération, gestion du journal de bord, visualisation, assistance, juridique et financière). Dans ce qui suit, les caractéristiques particulières des titulaires de fonctions sont présentées dans la perspective du scénario de "cyberattaque" :

- **Chef d'équipe de crise :**
  - → Assurer la capacité de travail de la cellule de crise (initiale et régulière)
    - Intégration des fonctions et des rôles pertinents
    - Disponibilité de ressources suffisantes (techniques, spatiales, etc.)
  - → Établir un cadre fonctionnel pour la coopération
    - Calendrier, briefings, documentation
  - → Respecter les obligations de déclaration dans le contexte de l'entreprise (si nécessaire, coopérer avec le service juridique)
  - → Gérer activement la coopération avec les autorités (si nécessaire, intégration des employés de l'Office national de la police ciminelle, criminalistique informatique).
    - Intégration de membres des autorités dans l'équipe de crise (si possible !)
  - → Si nécessaire et en cas de contraintes opérationnelles : consolider la priorisation aux opérations et aux parties prenantes.
    - Activités principales/processus principaux
    - Qu'est-ce qui est possible avec quels moyens (mot-clé disponibilité informatique) ?
  - → Vérifiez l'utilisation judicieuse des experts et des prestataires de services
  - → Fournir des informations proactives à la direction, à l'autorité décisionnelle et aux comités
    - Coordination des informations avant les apparitions dans la presse (en coopération avec le responsable de la communication)
  - → Observer la conformité avec le FORDEC
  - → Assurez-vous d'effectuer le contrôle de l'action et un contrôle de l'efficacité
  - → Garder un œil sur le budget et le contrôle financier
  - → Gérer activement l'information
  - → Pratiquez les soins actifs (ce scénario peut aussi être stressant)



Mesures réactives

- **Domaine de responsabilité Communication :**
  - ⟶ Vérifier quels sont les médias disponibles dans la situation actuelle (initiale et au cours de la crise)
    - Utiliser les médias disponibles (internes, externes, médias sociaux)
    - Utilisez vos prestataires de services pour la communication si nécessaire
  - ⟶ Veillez à la cohérence et à la fiabilité de votre communication externe et interne
    - Première information : Confirmation de l'événement sur la base de formulations prédéfinies (idéalement dans les dix premières minutes).
    - Une stratégie de communication appropriée (auteur/victime, responsabilité, ouverture, etc.)
    - Extension rapide de la communication à toutes les parties prenantes
    - Coordination au sein d'Équipe de crise, notamment avec l'IT, concernant les délais prévus (gérer activement les attentes internes/externes).
  - ⟶ Notez le grand intérêt pour la responsabilité de l'événement
  - ⟶ Utiliser et créer des FAQ (pour les besoins internes et externes)
    - Exploiter la gestion active de l'information avec les interfaces pertinentes
  - ⟶ Soutenez vos lignes d'assistance (et vos prestataires de services, le cas échéant) en leur fournissant des modèles de formulation afin de garantir la cohérence des communications externes



Mesures réactives

- **Domaine de responsabilité des ressources humaines (RH) :**
  - → Coordonner les éventuels manques et excédents de personnel (dotation flexible) :
    - Quels départements ont des besoins en personnel ?
    - Quels départements peuvent fournir du personnel ?
    - Quelles sont les compétences dont les employés disposent/ont besoin (gestion active des compétences) ?
  - → Coordonner le contrôle des données et les droits d'accès
  - → Veillez à ce que les dossiers du personnel soient accessibles à l'Équipe de crise si nécessaire et autrement verrouillés (par exemple, pour les délinquants internes)
  - → Coordonner la gestion de l'information sur le comité d'entreprise/le comité du personnel
  - → Conseiller sur les heures supplémentaires et le droit du travail si nécessaire (les solutions de contournement manuelles pour les pannes informatiques nécessitent généralement plus de temps et de personnel)
  - → Vérifier les obligations de paiement
  - → Utilisez les ressources de vos prestataires de services
  - → Coordonner les demandes de services de dotation en personnel, selon les besoins
  - → Gérer activement l'information
- **Domaine de responsabilité IT :**
  - → Informer vos prestataires de services (y compris les Data centers)
  - → Clarifier les responsabilités au sein de l'IT
    - Utilisation du manuel d'urgence informatique
  - → Rechercher et fournir une estimation de l'étendue de la panne informatique (voir ci-dessous pour l'étendue des dommages)
  - → Élaborer une prévision de la propagation des dommages
  - → Montrer les options pour les délais et la reprise informatique
    - Propositions de priorisation de la part du service informatique
    - Veuillez noter l'ordre de priorité établi par léquipe de crise
    - Observer les priorisations BCM/ITSCM
    - Intégrer les aspects temporels et économiques (faisabilité)
  - → Lancer l'initiative de mise en œuvre pour restaurer les services informatiques
  - → Identifier et coordonner les prestataires de services/experts informatiques raisonnables (y compris les experts en informatique légale)
    - pour le fonctionnement d'urgence
    - pour la récupération
  - → Gérer activement l'interface avec l'ISM et les responsables de la protection des données
  - → Pratiquez une gestion active de l'information

Mesures réactives

- **Domaine de responsabilité Service :**
  - → Vérifiez l'étendue des dégâts dans votre région
  - → Consolider et communiquer les besoins dans votre région (concernant l'informatique et le personnel supplémentaire si nécessaire)
  - → Examinez et utilisez vos priorités concernant les tâches principales
  - → Utilisez et testez la fonctionnalité et l'efficacité de vos mesures de transition.
  - → Utilisez votre expertise pour appliquer les options de solution de manière flexible et créative
  - → Gérer activement l'information
    - Direction l'équipe de crise
    - Coopération avec d'autres services

- **Domaine de responsabilité ISM et protection des données :**
  - → Vérifiez si les cibles de protection de l'ISM sont affectées.
  - → Vérifier l'efficacité des mesures ISM et les adapter en fonction des besoins et dans le respect de la loi
  - → Respectez les exigences en matière de reporting dans votre domaine de responsabilité et gérez activement les informations avec les autorités compétentes.
  - → Gérer activement les interfaces avec ITSCM, BCM et les responsables de la protection des données
  - → Gérer activement l'information
    - y compris la consultation de l'équipe de crise sur tous les sujets relatifs à la gestion de l'information et à la protection des données

Retour au fonctionnement normal et suivi

Le retour au fonctionnement normal après le déploiement actif de la cellule de crise nécessitera les mesures habituelles prévues

- **Assurez le retour à un fonctionnement normal selon votre processus de récupération**
  - → Assurer la fonctionnalité de base des services informatiques
    - Organisation des services informatiques sécurisés et peut-être pas encore totalement disponibles (par exemple, en ce qui concerne les performances, les fonctions, les restrictions d'utilisation)
  - → Coordination de la transmission des lots de travaux aux départements spécialisés
  - → Organisation du traitement de l'arriéré
  - → Achèvement ordonné des travaux de la cellule de crise (y compris la passation des pouvoirs, les lignes d'information, la sauvegarde des documents et des dossiers)

- **Assurer un suivi structuré ou une réévaluation des événements (processus de leçons apprises/analyse post-mortem)**

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

Statut: Octobre 2021

Controllit AG est votre partenaire pour la gestion de la continuité des activités (BCM). Depuis notre création, nous développons des concepts et des produits intégratifs pour la gestion de la continuité des activités, la gestion de la continuité des services informatiques et la gestion des crises. Nous vous aidons avec des concepts stratégiques, organisationnels et techniques pour sécuriser vos processus d'affaires contre les processus opérationnels contre les menaces et pour se préparer aux urgences.

Le contenu de ce document est destiné à fournir des informations sur l'organisation de crises virtuelles. Des modifications ultérieures sont possibles.

Crédits photos : S. 4: iStock.com/alphaspirit; S. 5: iStock.com/alphaspirit; iStock.com/Maike Hildebrandt; iStock.com/tudmeak; S. 7: iStock.com/SurfUpVector; S. 9: iStock.com/Feodora Chiosea; S. 10: iStock.com/ipuwadol