Check-list

3

CYBERSÉCURITÉ
PRÉPARATION À LA GESTION DE CRISE
[À DIFFUSER LARGEMENT À TOUS LES COLLABORATEURS]

LES TRAVAUX PUBLICS FÉDÉRATION NATIONALE

La gestion de crise dans les entreprises se prépare **en amont**. L'objectif est de gagner en agilité en préparant des actions rapides et efficaces qui permettront de réagir lors d'une crise cyber et d'en limiter les impacts.

La **valise de crise** constitue un outil regroupant un ensemble de documents permettant à son utilisateur de réagir plus rapidement et de manière efficace à une crise cyber.

La valise de crise doit être stockée dans un lieu sûr notamment dans :

→ Un espace protégé et déconnecté du réseau de l'entreprise (par exemple sur deux clés USB ou bien en stockage en ligne chez un prestataire),
→ Ou un coffre-fort regroupant les différentes fiches imprimées.

Que préparer pour faire face à une crise cyber ?

Contenu de la valise de crise	ACTIONS RÉALISÉES (à compléter par l'utilisateur)	
	OUI	NON
Thème 1 : Les documents à introduire		
Les fiches «cybersécurité» de la FNTP (à imprimer de préférence).		
Les prescriptions de votre assureur en cas d'attaque cyber si votre entreprise a souscrit une garantie d'assurance du risque cyber.		
Un modèle d'accord de confidentialité pour les partenaires et un modèle d'accord de confidentialité pour les collaborateurs en vue de maîtriser l'information.		
Un modèle de contrat et de bon de commande pour contractualiser avec des prestataires ou pour acheter des outils d'urgence.		
Acheter quelques clés USB (selon la taille de votre entreprise) qui ne seront utilisées qu'en cas de crise.		
Regrouper les formulaires d'accès exceptionnels (nuit et week-end) au bâtiment.		
Thème 2 : La communication		
Mettre en place un annuaire regroupant : • Vos collaborateurs membres de la cellule de crise et la personne chargée de la communication, • Vos prestataires informatiques / vos fournisseurs cyber (anti-virus, détection, intervention...), • Votre fiche contacts de cyber-assurance (le cas échéant), • Vos numéros d'astreinte (gardiennage, alarme du site,...), • Les coordonnées du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques).		
Prévoir une boite mail indépendante (type : protonmail.com, laposte.net...).		
Prévoir un compte sur une messagerie instantanée pour chaque membre de la cellule de crise (type Signal).		
Disposer d'un téléphone / tablette connecté(e) au réseau 4G/5G ou d'une box indépendante pour éviter de passer par le réseau interne.		
Archiver les identifiants et mots de passe associés aux comptes des réseaux sociaux de l'entreprise (ex. Linkedin) par l'intermédiaire d'un logiciel de gestion de mots de passe (ex. Keypass, etc.).		
Thème 3 : Les sauvegardes		
Archiver les identifiants et mots de passe des sauvegardes et maintenir les procédures.		
Introduire la procédure actualisée de sauvegarde et de restauration.		
Pour aller plus loin		
Consulter pour contracter une assurance cyber		
Ouvrir la valise de crise au moins une fois par an pour vérifier l'exactitude des informations. Le cas échéant, réaliser une mise à jour.		
Tester le dispositif régulièrement au moins une fois par an : Exemple : • Appeler les différents contacts (prestataires, numéros d'astreinte), • Vérifier le fonctionnement du téléphone / tablette de sécurité, • Vérifier la disposition de clé USB, • Vérifier que tout est fonctionnel.		
Se former sur les MOOC à disposition (CNIL, ANSSI)		