AGORA SEA

EXPERTISE COMPTABLE

AUDIT - CONSEIL - PAIE

NEWSLETTER D'AVRIL 2023

Sommaire :

LES PRINCIPALES ÉTAPES À SUIVRE EN CAS DE CYBERATTAQUE

Sur l'année 2022, Cybermalveillance.gouv.fr a dû traiter plus de 280 000 demandes d'assistance sur la plateforme. Ces dernières font suite à de l'hameçonnage, du piratage de compte ou des rançongiciels. Si l'entreprise, en dépit des précautions prises en la matière, ne parvient pas à éviter une cyberattaque, elle doit néanmoins prendre immédiatement des mesures de gestion de la cyber-crise.

Aussi, nous vous proposons une liste des réflexes à adopter pour gérer efficacement une cyberattaque le jour J et maîtriser l'incident, en respectant scrupuleusement les étapes ci-dessous :

1. Adoptez une méthodologie de traitement du risque au jour de l'attaque

- Signalez l'attaque au service informatique ou au prestataire dans les plus brefs délais.
- Débranchez immédiatement votre ordinateur du réseau (débranchez le câble Ethernet), d'Internet et coupez votre wifi pour isoler les systèmes attaqués. L'objectif principal étant de déconnecter les terminaux infectés afin d'empêcher la propagation de l'attaque.
- N'éteignez pas (et arrêter d'utiliser) l'équipement corrompu pour ne pas effacer les preuves et tenez un registre des événements et actions réalisées. Cette étape permettra de conserver et de préserver la « scène de crime ».
- Ne payez jamais la rançon en cas de Ransomware car le paiement ne garantit en rien le déchiffrement des données et peut compromettre le moyen de paiement utilisé (notamment la carte bancaire).

2. Pilotez la crise

- Prévoyez des plans de secours (PRA : Plan de Reprise d'Activité, PCA : Plan de Continuité d'Activité) pour garantir la continuité d'exploitation et constituez une équipe en charge de la gestion de crise.
- Réunissez toutes les pièces permettant de documenter le dossier de plainte avec les éléments suivants : trace informatique des preuves d'attaque, remontée de logs (fichiers journaux), traces d'un troyen (trojan virus) sur la machine, fichiers encryptés, configuration des machines, disques durs des machines infectées, adresse(s) postale(s) des machines attaquées, ensemble des préjudices subis par l'attaque…
- Portez plainte auprès de la gendarmerie ou de la police nationale et fournissez toutes les preuves réunies ci-dessus, et ce, même s'il n'y a pas de préjudice direct, car les conséquences pourraient survenir ultérieurement. Il s'agit du seul moyen pour décourager les cybercriminels.
- Signalez les escroqueries (Pharos/Signal Conso).
- Déterminez l'origine de l'attaque pour corriger les sources de risques, en tirer les enseignements nécessaires pour éviter tout nouvel incident et/ou mieux gérer la prochaine cyberattaque.
- Identifiez les données qui ont été consultées, volées, modifiées ou détruites, et notifiez l'incident à la CNIL dans les 72h en cas de violation de données personnelles.
- Établissez un plan de communication rapide et efficace en cas de crise suite à une cyberattaque grave (transparence auprès des collaborateurs, des clients, des fournisseurs et de toutes les parties prenantes impactées…) pour les rassurer et éviter que l'image de l'entreprise ne pâtisse de trop de ce désagrément.
- Prenez en compte les risques psychosociaux qui peuvent affecter l'efficacité de vos équipes. En effet, les conséquences de cette dernière ne sont pas à prendre à la légère afin d'éviter l'effet de panique.

Si l'entreprise ne dispose pas de professionnels expérimentés en la matière, envisagez, en fonction de la gravité, de contacter des prestataires spécialisés de proximité, référencés par Cybermalveillance.

3. Contactez les structures d'assistance aux victimes de cyberattaques

- ACYMA Cybermalveillance : plateforme d'assistance aux victimes d'actes de cybermalveillance.
- CNIL : notification de violation de données personnelles.
- CERT : centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.
- Contactez votre assureur.
- Contactez la police/gendarmerie: 17.

ECF : SÉCURISEZ VOTRE SITUATION FISCALE EN VALORISANT L'IMAGE DE VOTRE ENTREPRISE !

Comme l'an dernier, les entreprises qui le souhaitent, peuvent nous solliciter pour réaliser un examen de conformité fiscale (ECF).

L'ECF permet de sécuriser la situation fiscale de l'entreprise sur les points courants et limiter les risques et les conséquences d'un contrôle fiscal, aucune pénalité ni intérêt de retard n'étant dû en cas de rappel d'impôt sur l'sur l'un des points validés lors de cet examen.

L'option pour l'ECF est exercée en cochant la case prévue à cet effet dans la liasse fiscale. Un compte rendu de mission (CRM) doit ensuite être déposé au plus tard le 31 octobre ou dans les 6 mois du dépôt de la liasse fiscale. Éventuellement une lettre d'absence de conclusion peut être adressée à l'administration.

Qu'est-ce que l'ECF ?

Il s'agit d'une prestation contractuelle au titre de laquelle votre expert-comptable s'engage, à votre demande, à examiner 10 points fiscaux précis et limités et à se prononcer sur leur conformité au regard des règles fiscales.

Quelles sont les entreprises éligibles au dispositif de l'ECF ?

Toutes les entreprises peuvent demander la réalisation d'un ECF quels que soient :

- Leur forme (entreprise individuelle ou société).
- Leur régime d'imposition (IR ou IS).
- Leur chiffre d'affaires.

Pourquoi réaliser un ECF ?

L'ECF permet de vérifier et sécuriser la conformité fiscale des déclarations des entreprises ainsi que le Fichier des écritures comptables (FEC) produits par l'entreprise. Celle-ci est ainsi libérée du souci que peut représenter le risque fiscal sur ces questions. L'administration tiendra compte de la présence d'un ECF dans le cadre de la planification des contrôles.

En cas de contrôle fiscal ultérieur, aucune pénalité et aucun intérêt de retard ne seront pratiqués en cas de rappel si :

- Le contrôle porte sur des points validés dans le cadre de l'ECF,
- et si l'entreprise est de bonne foi.

Par ailleurs, l'ECF **constitue un atout en terme de valorisation et de transmission**, ainsi que dans vos relations bancaires ou commerciales **dès lors qu'il renforce la fiabilité comptable et fiscale de votre entreprise.**

Quels sont les travaux à réaliser dans le cadre de l'ECF ?

L'expert-comptable réalise un audit et valide leur conformité avec la loi fiscale de 10 points expressément fixés et limités, portant notamment sur :

- La validité (1) et la conformité comptable (2) du Fichier des écritures comptables (FEC).
- La validité et la conformité du logiciel de caisse (3).
- L'archivage des documents (4).
- La bonne application des régimes d'imposition (5).
- La correcte comptabilisation des amortissements (6).
- La déductibilité des provisions (7) et des charges à payer (8).
- La déductibilité des charges exceptionnelles (9).
- Le respect des règles d'exigibilité en matière de TVA déductible et collectée (10).

L'examen se traduit par un compte rendu de mission (CRM) retraçant les travaux réalisés. Ce CRM est transmis à l'administration fiscale dans les 6 mois de la production de votre liasse fiscale.

Si vous souhaitez sécuriser votre situation fiscale en optant pour l'ECF, sollicitez votre chargé(e) de mission ou envoyez-nous un courriel à info@agora-sea.fr.