undefined - mardi 27 mai 2025

Actu | Économie

L'AVIS DE L'EXPERT

Cyberattaques : les gestes essentiels à adopter en cas d'attaque

Propos recueillis par Sylvain Lartaud

Laurent Colas est expert-comptable et commissaire aux comptes à Oyonnax. Photo Studio Valmy Pascal Gabaud

En 2024, 348 000 crimes et délits numériques ont été enregistrés en France, avec une proportion alarmante ciblant directement les TPE et PME. Il est donc nécessaire et indispensable d'adopter, selon Laurent Colas, les gestes, les réflexes et les consignes pour identifier, réagir et se protéger face à ces menaces croissantes.

• Reconnaître une cyberattaque en cours

« Certains symptômes doivent immédiatement alerter :

▶ Impossibilité d'accéder à vos fichiers ou à vos logiciels habituels ;

▶ Fichiers chiffrés ou renommés avec des extensions inhabituelles ;

▶ Messages demandant une rançon pour récupérer vos données ;

▶ Ralentissement inhabituel des systèmes informatiques ;

▶ Comportements étranges de vos équipements (redémarrages intempestifs, programmes s'ouvrent « tout seuls ») ;

▶ Activités suspectes sur vos comptes bancaires ou professionnels.

Selon une étude relayée sur le site internet de « fancenum.gouv.fr », près de 90 % des sinistres cyber concernent des attaques par rançongiciel avec différentes méthodes d'intrusion dont les principales sont : l'hameçonnage (ou phishing) via des e-mails frauduleux (30 % des cas), les attaques par force brute en testant avec un logiciel, une à une, toutes les combinaisons possibles pour accéder aux données d'une entreprise (23 %), l'usurpation de compte (20 %) ou encore l'exploitation d'une faille de sécurité (20 %). »

• Les conséquences pour l'entreprise

« Les impacts d'une cyberattaque peuvent être dévastateurs et multi-dimensionnels :

▶ Un risque financier considérable. Les pertes financières sont souvent les premières conséquences visibles : coûts de rétablissement des systèmes, pertes de revenus pendant l'arrêt d'activité, frais juridiques potentiels et parfois des amendes réglementaires. Dans le cas d'un rançongiciel, les demandes peuvent atteindre plusieurs millions d'euros, bien que le montant des rançons reste généralement faible comparé au préjudice total subi.

▶ Paralysie partielle ou totale de l'activité. Une cyberattaque paralyse généralement votre système d'information, rendant impossible l'exécution des tâches quotidiennes comme la gestion des stocks ou la comptabilité. Cette interruption peut durer de quelques jours à plusieurs mois selon la gravité de l'attaque et votre niveau de préparation.

▶ Atteinte durable à la réputation. L'impact sur la réputation est souvent le plus durable. La confiance de vos clients, fournisseurs et partenaires peut être sérieusement érodée, particulièrement si des données sensibles ont été compromises. Cette perte de confiance peut entraîner la perte de contrats et un affaiblissement durable de votre image de marque. »

• Les premiers gestes essentiels en cas d'attaque

« Lorsqu'une cyberattaque est détectée, chaque minute compte. Voici les réflexes à adopter

immédiatement :

▶ Pour les collaborateurs

1. Ne pas éteindre l'appareil compromis : certains éléments de preuve contenus dans la mémoire de l'équipement seraient effacés ;

2. Débrancher immédiatement la machine d'internet ou du réseau informatique : débranchez le câble réseau et désactivez la connexion wi-fi ;

3. Alerter au plus vite le support informatique : pour que des mesures soient prises rapidement ;

4. Ne plus utiliser l'équipement potentiellement compromis : évitez de toucher à l'appareil pour préserver les traces utiles aux investigations ;

5. Prévenir les collègues de l'attaque en cours : afin d'éviter d'autres manipulations qui pourraient aggraver la situation.

▶ Pour les dirigeants

1. Constituer une équipe de gestion de crise : pour piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique) ;

2. Isoler les systèmes attaqués : pour éviter la propagation à d'autres équipements ;

3. Tenir un registre des événements et actions réalisées : pour en conserver la trace à disposition des enquêteurs ;

4. Préserver les preuves de l'attaque : messages reçus, machines touchées, journaux de connexion…

5. Ne jamais payer de rançon : cela encouragerait les cybercriminels à vous attaquer à nouveau et ne garantit en rien la récupération de vos données. »

• Une approche coordonnée indispensable

« Une cyberattaque est une situation de crise qui doit être gérée au plus haut niveau de l'organisation. En tant que dirigeant, vous devez :

▶ Piloter la communication interne et externe ;

▶ Mobiliser les ressources nécessaires (humaines et financières) ;

▶ Prendre les décisions stratégiques concernant la continuité de l'activité ;

▶ Assurer la liaison avec les autorités compétentes ;

▶ Engager les procédures d'assurance si vous disposez d'une police cyber (indispensable aujourd'hui).

La gestion d'une cyberattaque nécessite des compétences techniques spécifiques. N'hésitez pas à faire appel à votre prestataire informatique habituel, à des experts en cybersécurité spécialisés dans la gestion d'incidents et aux services de police ou de gendarmerie spécialisés. »

La cybersécurité n'est plus une option mais une nécessité. Laurent Colas

• Prévenir les récidives et renforcer sa protection

« Pour éviter de futures attaques, plusieurs actions sont indispensables :

▶ Renforcer les mots de passe et mettre en place l'authentification pour une double identification ;

▶ Effectuer régulièrement des sauvegardes externes de vos données ;

▶ Maintenir à jour vos systèmes d'exploitation et logiciels ;

▶ Former et sensibiliser régulièrement vos collaborateurs ;

▶ Mettre en place un plan de réponse aux incidents.

Plusieurs organismes à contacter :

▶ Cybermalveillance.gouv.fr, plateforme nationale d'assistance aux victimes de cyber-malveillance ;

▶ L'ANSSI (agence nationale de la sécurité des systèmes d'information) avec son service gratuit Mon Aide Cyber : un diagnostic personnalisé pour les entreprises de toute taille souhaitant s'engager dans une démarche de renforcement de leur sécurité numérique ;

▶ Les experts-comptables et commissaires aux comptes : peuvent vous orienter vers des solutions adaptées. »

• Conclusion

« Il faut prendre les devants en matière de cybersécurité. Collaborateurs et dirigeants sont la première ligne de défense de leur entreprise contre ces menaces invisibles mais bien réelles.

Face à la montée en puissance des cyberattaques, la préparation et la réactivité sont les meilleures armes. N’attendez pas d’être victime pour agir : formez vos équipes, mettez en place des procédures claires et établissez un plan de continuité d’activité en cas d’attaque.

La cybersécurité n’est plus une option mais une nécessité qui fait désormais partie intégrante d’une gestion d’entreprise responsable. »