Assurance et Banque

Prévention Cyber

OFFRE CITOYENNE

Les risques Cyber pour votre entreprise

La transformation numérique des entreprises représente de formidables opportunités de développement économique. Mais qui dit opportunités, dit également risques : Piratage informatique, vol ou perte de données numériques, rançonnage, campagne de désinformation sur les réseaux sociaux, espionnage ou ingérence économique, vengeance d'un collaborateur... aucun secteur économique n'est à l'abri.

A l'ère numérique et de l'interconnexion généralisée rendant de fait toute entreprise internationale quelle que soit sa localisation géographique, la création de valeur ne peut se concevoir que par la confiance dans les systèmes d'information et la sécurisation des données sensibles de l'entreprise.

La cybersécurité est avant tout une composante essentielle des enjeux économiques, stratégiques et d'image qui relève de la responsabilité du dirigeant.

Quelles conséquences pour votre entreprise ?

Un enjeu économique

Il peut se manifester par exemple par un vol de savoir-faire ou de données commerciales, une « prise en otage » de votre système d'information, ou encore par l'interception de données confidentielles captées sur tout équipement numérique.

Les conséquences peuvent être redoutables :

- Pertes d'exploitation
- Pertes pécuniaires suite à un cyber détournement de fonds
- Frais d'expertise et d'assistance informatique
- Frais de reconstitution des données
- Frais de notification en conformité avec la réglementation sur la protection des données personnelles
- Frais de protection juridique...

Un enjeu opérationnel

Les conséquences peuvent porter atteinte durablement à votre capacité de production et de trésorerie.

Un enjeu d'image

Une campagne de dénigrement de votre entreprise sur des médias sociaux par des concurrents ou des salariés mécontents peut ternir durablement votre image auprès de vos clients et prospects, partenaires et donneurs d'ordre.

Un enjeu juridique et de conformité

La dimension internationale de la cybercriminalité s'est traduite par l'harmonisation des législations européennes et internationales afin de renforcer les moyens de lutte contre ce phénomène.

On peut citer à titre d'exemple l'entrée en vigueur du RGPD le 25 mai 2018. Selon les activités professionnelles, la responsabilité de l'entreprise et/ou du dirigeant peut être recherchée en cas de manquement aux obligations réglementaires ou de conformité. Des sanctions financières peuvent également être prononcées.

LES RISQUES CYBER EN QUELQUES CHIFFRES

71 %
des dirigeants se disent préoccupés pour leur entreprise par les risques Cyber

Source : Baromètre AXA 2023.

49 % des entreprises
ont été victimes d'une cyberattaque

Source : CESIN 2024.

La cybercriminalité coûterait
700 millions d'euros
par coût des cyberattaques pour les entreprises françaises en 2022 : 2 Md€

Source : ASTERES 2023.

LES BONNES QUESTIONS À SE POSER

→ Mes données clients sont-elles susceptibles d'intéresser un tiers, la concurrence ?

→ Mon système d'information est-il correctement protégé ?

→ En cas de cyberattaque, mon entreprise serait-elle affectée si je ne pouvais plus accéder à mon système d'information ou à mes données ? Une baisse significative d'activité est-elle à craindre ? Un arrêt total, mettant en péril l'existence même de mon entreprise, peut-il être envisagé ?

→ Ai-je mis en place un plan de continuité d'activité en cas d'indisponibilité de mon système d'information ou de mes données ?

→ Qui contacter en cas de cyberattaque pour gérer cette crise ?

Si vous n'avez pas de réponse satisfaisante à ces questions, vous êtes vulnérables.

Si vous êtes vulnérables, vous devez vous protéger...

Comment protéger votre entreprise ?

Dirigeants d'entreprise, découvrez la démarche P.A.A.R. à initier avec vos collaborateurs pour préserver votre entreprise des risques Cyber :

SOMMAIRE

- **PRÉVENIR** l'exposition de votre entreprise vis-à-vis des risques Cyber
- **ANTICIPER** la survenue d'une cyberattaque
- **ATTÉNUER** les conséquences d'une cyberattaque
- **RESTAURER** votre capacité de reprise d'activités
- **VOUS ACCOMPAGNER**

LE SAVIEZ-VOUS ?

Les e-mails et leurs pièces jointes

sont des éléments importants dans les cyberattaques, ils représentent le **1er vecteur d'attaques** (Phishing 79 %)

Source : Baromètre de la cyber sécurité des entreprises. Janvier 2020 - OpinonWay CESIN.

700 à 800 ordinateurs

portables sont oubliés par semaine à l'aéroport Charles de Gaulle (CDG) de Paris. Au total plus de **3 000 ordinateurs** sont égarés chaque semaine dans les 8 principaux aéroports en Europe

Source : Aéroports De Paris, 2019.

80 % des cyberattaques

peuvent être évitées par la mise en place de mesures simples et très peu coûteuses

Source : Centre for Internet Security CIS Controls - Basic Foundational Organizational, 2018.

PRÉVENIR : SENSIBILISER ET FORMER VOS COLLABORATEURS

La mise en place des mesures de prévention vous aide à réduire la probabilité de réussite d'une cyberattaque dont vous pourriez être la cible. Contrairement à une idée reçue, ces mesures ne sont pas uniquement techniques. Elles sont également de nature organisationnelle, managériale et humaine.

Le collaborateur est la première barrière de défense à la seule condition qu'il soit formé.

Les attaquants exploitent souvent les erreurs commises par les individus et également les vulnérabilités des organisations.

Sensibiliser vos collaborateurs :

- aux risques de cybercriminalité et de piratage des données,
- à la discrétion lors de leurs déplacements (aéroports, hôtels), aux règles de protection de l'ensemble de leurs équipements. Apporter une attention particulière en cas de déplacement dans certains pays étrangers,
- à la conduite à adopter en réaction lors d'un incident.

→ Identifier les informations sensibles et former vos collaborateurs à ne pas les diffuser sur les réseaux sociaux.

→ Développer une culture de sécurité et favoriser la mise en œuvre quotidienne de bonnes pratiques de prévention.

→ Vérifier régulièrement l'image de votre entreprise sur internet (e-réputation).

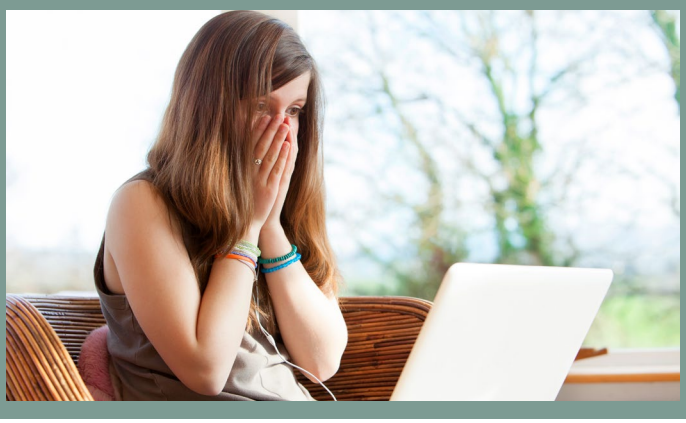
CAS PRATIQUE

RECEVOIR UN E-MAIL SUSPECT (LE PHISHING)

Vous recevez un e-mail suspect dans votre boîte mail dans lequel on vous demande de transférer des informations sensibles (type informations bancaires, mots de passe) ou de cliquer sur un lien, sur un ton urgent…

Pourquoi est-ce une situation à risque ?

Cette technique est appelée le phishing. Elle permet aux escrocs qui se font passer pour des personnes ou des services connus, de voler des informations très facilement en se faisant passer pour un tiers de confiance.



Boîte à outils

- Hack Academy
- MOOC ANSSI
- Guide ANSSI « bonnes pratiques lors des déplacements »

PRÉVENIR : DÉFINIR LES RÈGLES D'UTILISATION DU SYSTÈME D'INFORMATION ET DES RÉSEAUX

Une bonne cybersécurité sera difficile à atteindre si les politiques ou procédures de l'entreprise ne sont pas clairement définies.

- Adopter une charte informatique définissant les droits et devoirs des personnels (salariés, mais aussi stagiaires et intervenants externes…).
- Impliquer Direction Générale et DRH dans les processus de mutation et de départ de collaborateurs (exemple : suppression immédiate des droits d'accès suite à la mutation ou au départ d'un collaborateur).
- Faire signer des clauses de confidentialité à vos prestataires ou personnels temporaires (stagiaires).
- Cette charte doit clairement énoncer les sanctions encourues en cas de non-respect des règles.

C'EST ARRIVÉ

Un salarié, faisant l'objet d'une sanction disciplinaire, infecte via une clé USB un équipement de contrôle du site industriel qui l'emploie.

Cette attaque du système d'information provoque d'importantes nuisances au voisinage. Les riverains se plaignent aux autorités. L'entreprise doit engager des frais de détection et de décontamination de son système d'information et mobiliser des ressources internes pour gérer les conséquences de l'événement.

Mais les relations entre l'entreprise et les autorités en seront durablement affectées et des projets de développement retardés.

Boîte à outils

Exemple de charte CCI

PRÉVENIR : SÉCURISER VOTRE SYSTÈME D'INFORMATION

Effectuer un audit de la sécurité avec votre responsable informatique

Une évaluation de la vulnérabilité du système d'information basée sur les référentiels de bonnes pratiques vous permet d'identifier vos points faibles et les mesures de cybersécurité appropriées à mettre en place.

Gérer les droits d'accès et des mots de passe

La gestion des droits, tant physiques qu'informatiques, doit être adaptée à la situation de votre entreprise et aux fonctions des collaborateurs concernés. Une véritable politique de gestion des droits doit être mise en place au sein de votre entreprise.

Définir les modalités de gestion des mots de passe

- Changer les identifiants et mots de passe par défaut des nouveaux appareils.
- Adopter des mots de passe robustes.
- Changer périodiquement les mots de passe ou dès lors qu'il y a un soupçon de compromission.
- Rendre obligatoire l'authentification et les règles de gestion des mots de passe ci-dessus.

Autoriser les utilisateurs à accéder aux seules informations dont ils ont besoin pour effectuer leurs tâches.

Gérer les comptes utilisateurs

- Maintenir à jour une liste limitée et actualisée des comptes administrateurs.
- Bloquez l'accès à internet à partir des comptes détenant des droits administrateurs.

Désactiver immédiatement les comptes non utilisés (départ d'un collaborateur…).

CAS PRATIQUE

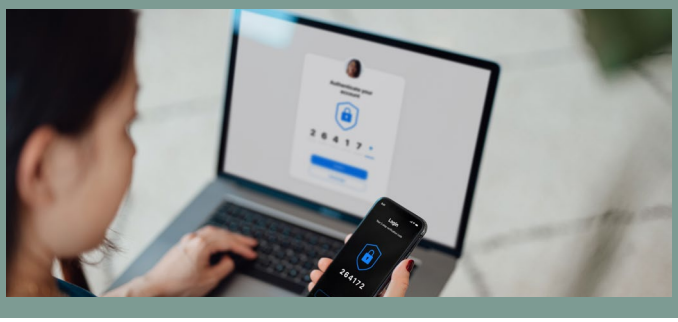
CHOISIR UN MOT DE PASSE ROBUSTE ET BIEN LE PROTÉGER

Le mot de passe que vous choisissez est très simple…

Vous craignez d'oublier votre mot de passe et vous le notez sur un post-it sur votre bureau…

Pourquoi est-ce une situation à risque ?

Le mot de passe protège vos accès aux ressources informatiques de l'entreprise ou a vos données confidentielles (banque, boite mail…). Des outils malveillants sont capables de le retrouver s'il est trop simple et permettent aux hackers d'usurper votre identité et de pénétrer dans un réseau ou de voler des données.



Boîte à outils

- Guide Cyber en 13 questions
- Kits.cybermalveillance.gouv.fr
- Guide d'hygiène informatique ANSSI

PRÉVENIR : SÉCURISER VOTRE SYSTÈME D'INFORMATION

Maintenir à jour les logiciels et applications depuis les sites de leurs éditeurs

Les mises à jour de sécurité permettent de corriger les vulnérabilités des systèmes d'exploitation, logiciels et applications. L'absence de mises à jour permet aux attaquants d'exploiter ces vulnérabilités pour mener des cyberattaques.

Installer des outils de protection

La protection de votre entreprise passe par la mise en place d'outils adaptés à la valeur de vos données ainsi qu'à votre dépendance à votre système d'information :

- Antivirus et Pare-feu
  Sont la base de la protection indispensable de tous systèmes d'information. Ils doivent être mis à jour de manière régulière, au mieux quotidiennement, et de manière automatique.
- Outils de filtrage
  Le pare-feu est efficacement complété par des outils de surveillance de type « Intrusion Détection Système » (IDS) et « Intrusion Protection Système » (IPS) qui filtrent les entrées et les sorties pour détecter et écarter un certain nombre d'intrusions malveillantes.
- Outils de détection comportementale
  D'autres intrusions malveillantes non stoppées par les outils de filtrage ne peuvent être détectées que par des outils de détection comportementale. Ces outils analysent le comportement des téléchargements ayant passé l'antivirus, afin de détecter ceux qui ont des actions suspectes.

Renforcer la sécurité physique des serveurs

La sécurité physique a pour objet de conserver l'intégrité matérielle des équipements informatiques. Un serveur informatique est au cœur du système d'information. Il peut stocker des données, gérer les e-mails, héberger des applications...
Un sinistre impactant un serveur (par exemple : dégât des eaux, incendie, intrusion physique, surtension électrique, température élevée) peut donc générer des pertes majeures pour votre entreprise.

- Choisir un emplacement idéal, en termes de contrôle d'accès, de prévention des risques liés à l'eau, au feu, à la température.
- Éliminer les menaces à proximité : sources de chaleur à proximité immédiate, tuyauteries et les gaines de climatisation surplombant les serveurs, blocs de multiprises électriques, …
- Assurer la maintenance des installations.
  Les risques peuvent provenir de pannes ou de dysfonctionnements parfois liés à la vétusté des installations.
- Sécuriser l'accès physique aux serveurs et composants de réseau.

C'EST ARRIVÉ

Un virus informatique paralyse une 1re fois la totalité du système d'information (services commerciaux, production et financiers) d'une PME.

Celle-ci tarde à installer les correctifs de sécurité nécessaires.

Une 2e attaque de même type survient moins de 2 semaines plus tard alors que l'entreprise finalisait la restauration de son système et reprenait à peine son niveau d'activité normal. Cette nouvelle attaque bloque une 2e fois le système d'information.

Cet exemple illustre l'importance d'une mise à jour régulière des logiciels et en particulier un déploiement rapide des correctifs de sécurité mis à disposition par leurs éditeurs.

PRÉVENIR : SE METTRE EN CONFORMITÉ AVEC LES EXIGENCES RÉGLEMENTAIRES

La mise en conformité avec les exigences réglementaires inhérentes à vos activités concoure à renforcer la robustesse de votre cybersécurité.

Depuis l'entrée en vigueur du RGPD (Règlement Général sur la Protection des Données) en mai 2018, toute entreprise qui traite des données à caractère personnel s'expose à des sanctions en cas de non-conformité avec la loi.

Par ailleurs en cas de violation de ces données, sa responsabilité pourra être engagée vis-à-vis des personnes concernées même si le traitement a été confié à une société spécialisée.

LE SAVIEZ-VOUS ?

Les services de l'État (Police / Gendarmerie) disposent de référents Sûreté économique et Protection des entreprises, ces référents territoriaux peuvent être sollicités pour vous accompagner dans la protection de votre patrimoine matériel et immatériel.

Boîte à outils

CNIL : check-list d'autoévaluation

Brochure
Brochure AXA / RGPD

ANTICIPER

Aujourd'hui, la menace a considérablement augmenté en lien avec la « professionnalisation » des hackers. La question n'est plus seulement « Quelle est la probabilité que je sois attaqué ? » mais « Quand vais-je être attaqué ? ».

Dans un contexte où cette probabilité d'occurrence est élevée, les entreprises doivent être en capacité de mobiliser rapidement des moyens humains et techniques visant à limiter les conséquences néfastes d'une cyberattaque. Elles doivent pour cela avoir, au préalable, mis en place une organisation et des procédures leur permettant de prendre les mesures qui s'imposent.

Sauvegarder vos données régulièrement

- Sauvegarder les données régulièrement (de façon quotidienne ou hebdomadaire).
- Héberger vos solutions de sauvegarde en interne (stockées hors ligne dans un coffre-fort).
- Ou auprès d'un hébergeur spécialisé situé en Europe, avec chiffrement des données.
- Tester régulièrement la restauration des sauvegardes.

Planifier une conduite à tenir en cas d'urgence

- Définir la conduite à tenir face à un cyber incident.
- Mettre en place un plan de réponse à incident.
- Évaluer périodiquement le maintien du caractère opérationnel du dispositif en place.

C'EST ARRIVÉ

Une entreprise victime d'un virus informatique constate que l'ensemble des données de son serveur de production sont chiffrées. De ce fait son activité est paralysée.

Elle parvient à restaurer les données depuis sa dernière sauvegarde datant d'il y a 2 jours, à l'exception des données comptables qui n'avaient pas été sauvegardées depuis plus d'un an.

De ce fait, une ressaisie manuelle complète des données comptables sur la totalité d'un exercice est rendue nécessaire, entraînant une durée de blocage supplémentaire d'un mois.

Boîte à outils

Kit cybermalveillance/ les sauvegardes

Kit PCA DGE/ CGPME

Offre PCA AXA

ATTÉNUER : BIEN RÉAGIR À CHAUD

Si les cyberattaques sont inévitables, elles ne sont pas nécessairement gravissimes si elles sont bien gérées.

Étape de réaction à chaud, l'objectif prioritaire est l'atténuation des conséquences de l'incident par l'activation de son dispositif de gestion de crise. Cette phase démarre à la détection de l'attaque et se termine avec la restauration du service.

Mettre en œuvre les 1res mesures d'urgence dès la détection de l'incident

Reconnaître les anomalies, signes d'un système d'information compromis comme :

- Impossibilité de se connecter à la machine.
- Fichier(s) disparu(s).
- Système de fichiers endommagés.
- Connexions ou activités inhabituelles.
- Ralentissement du système.
- Services ouverts non autorisés.
- Création ou destruction de nouveaux comptes.
- Création de fichiers.

Mettre en œuvre les bons réflexes afin de préserver les traces et faciliter l'analyse :

- Déconnectez immédiatement l'équipement du réseau.
- Ne pas éteindre la machine concernée, ne pas la redémarrer.
- Ne connectez plus aucun équipement sur le réseau.

Boîte à outils

Guide
Que faire en cas d'attaque ?

Les bons réflexes en cas d'intrusion sur un système information (CERT-FR)

Fiche technique AXA
Comment réagir en cas de sinistre ?

ATTÉNUER : BIEN RÉAGIR À CHAUD

Mettre en œuvre les 1res mesures d'urgence dès la détection de l'incident (suite)

Obtenir de l'aide rapidement :

Il est essentiel de se faire accompagner très rapidement par une équipe d'experts afin de pouvoir gérer la crise dans toutes ses composantes : technique, juridique, communication, psychologique.

- Assureur cyber.
- Plateforme ACYMA (voir encart « le saviez-vous ? »).
- Prestataire informatique.

Prendre toutes les mesures pour préserver les preuves

- Isoler physiquement la machine.
- Effectuer une copie de disque.
- Procéder à la recherche de traces.

Activer votre plan d'urgence (selon les conséquences de l'incident)

- Réunir l'équipe chargée de la réponse à incident.
- Évaluer l'ampleur et la gravité de l'attaque.
- Planifier les actions à mettre en œuvre.

LE SAVIEZ-VOUS ?

Si vous êtes victime d'un incident de cybersécurité, le Groupe d'Intérêt Public ACYMA a mis sur pied le site **cybermalveillance.gouv.fr** pour mettre en relation entreprises, prestataires spécialisés et organismes compétents proches de chez vous.

Boîte à outils

Comment anticiper et réagir en cas d'incident ?
En cas d'incident
Accompagnement Crise majeure
Assurance Cyber
Histoire d'assuré

ATTÉNUER : PORTER PLAINTE ET NOTIFIER

Porter plainte

Déposer plainte directement auprès des services spécialisés permet, selon le type d'attaque, de récupérer possiblement tout ou partie des sommes détournées et d'appréhender l'auteur des faits.

Déposer plainte auprès des services de police ou de gendarmerie territorialement compétents

- Identifier en amont les points de contacts des services spécialisés.
- Déposer plainte.

Tenir à disposition des enquêteurs tous les éléments de preuves techniques en votre possession

- Toute trace des dégâts engendrés par l'attaque (logs, traces d'un cheval de Troie,…) voire une copie physique du disque dur sur un support de sauvegarde magnétique.
- L'adresse postale exacte des machines attaquées : adresse de l'entreprise s'il s'agit d'un ordinateur ou celle de l'hébergeur du serveur du site Internet.
- La liste des préjudices subis : vol, suppression de données, blocage d'un site ayant entraîné une perte de chiffre d'affaires.

→ Notifier à la CNIL l'atteinte aux données personnelles selon les situations qui le nécessitent, dans les meilleurs délais et si possible dans les 72 heures.

LE SAVIEZ-VOUS ?

Si vous êtes victime d'un incident de cybersécurité, le Groupe d'Intérêt Public ACYMA a mis sur pied le site **cybermalveillance.gouv.fr** pour mettre en relation entreprises, prestataires spécialisés et organismes compétents proches de chez vous.

Boîte à outils

ANSSI : en cas d'incident

CNIL : Notifier une violation de données personnelles

RESTAURER

Étape de réaction à froid, l'objectif est la poursuite du retour à une situation normale.
Cette phase peut comporter le nettoyage, la correction des vulnérabilités, la restauration des systèmes et/ou des données compromises ou perdues...
Elle inclut également la collecte des éléments rendant possible la compréhension du mode opératoire de l'attaque, l'identification des lacunes de son dispositif de protection et les recommandations d'actions préventives, pour éviter que la même attaque ne se reproduise.

Remédier, restaurer et remplacer

- Restaurer les données et systèmes endommagés après s'être assuré de l'absence de compromission persistante du SI
- Corriger les vulnérabilités identifiées à l'origine de la cyberattaque
- Remplacer les mécanismes de contrôle compromis (mots de passe, par exemple)

Tirez les enseignements de cet incident

Le retour d'expérience est indispensable en vue d'améliorer la cybersécurité de son entreprise

Organiser un bilan post-incident

- Gouvernance de la cybersécurité
- Mesures de prévention / protection
- Gestion de l'incident

En tirer les enseignements

Améliorer son dispositif de cybersécurité

Boîte à outils

Cyber Security Coalition
Guide de gestion des incidents cyber

Fiche Capital
Expérience Cyber

POUR ALLER PLUS LOIN

ACYMA :
cybermalveillance.gouv.fr

ANSSI

Ma brigade numérique

VOUS ACCOMPAGNER

À l'aide de votre intermédiaire d'assurance, bénéficiez de démarches de prévention adaptées à vos besoins et de l'accompagnement d'experts pour vous aider à réduire les risques Cyber dans votre entreprise !

GUIDE PRÉVENTION CYBER

Disponible sur demande à votre intermédiaire d'assurance, vous bénéficiez de :

- conseil et outils (documents et vidéos) ;
- bonnes pratiques ;
- supports de sensibilisation / formation ;
- formation ;
- liens Web.

ACCOMPAGNEMENT EN CYBER SÉCURITÉ

SUR DEVIS

Compléter l'accompagnement avec l'option Expert Prévention

Nos experts vous accompagnent par une démarche coopérative et pédagogique d'analyse, de qualification, et d'amélioration de vos risques Cyber, adaptée à l'activité opérationnelle de votre entreprise :

- évaluation, analyse de risques et suivi de plans d'actions ;
- état de situation ISO 27002 ;
- action de sensibilisation et formation ;
- conseil en architecture informatique ;
- réalisation de tests d'intrusion infrastructure ou web ;
- pour certaines configurations, réalisation d'un contrôle de présence de menaces avancées persistantes (APT ou « Advanced Persistant Threat »).

Les services AXA

SUR DEVIS

PCA

Un accompagnement pour limiter les conséquences d'un sinistre majeur sur l'activité de l'entreprise.

Assistance en ligne

Un numéro de téléphone dédié Cyber Secure et disponible 24h/24 7j/7.
Pour déclarer vos sinistres et bénéficier de notre réseau d'experts.

Crise majeure

Une équipe de spécialistes, présente aux côtés de vos clients dans un moment crucial pour un service adapté et disponible 24h/24, 7j/7.

E-réputation

Des sociétés partenaires qui peuvent s'occuper du nettoyage / noyage de propos diffamatoires sur le Web.

AXA vous répond sur :

OFFRE CITOYENNE

CONFIANCE, PRÉVENTION, ENVIRONNEMENT, SOLIDARITÉ :
avec AXA, faites le choix d'une entreprise engagée. Nos offres citoyennes contribuent au respect de la planète, de tous et de chacun. Nos actions concrètes et la grille d'évaluation sont accessibles sur **axa.fr/demarche-citoyenne**

Réf : 2004992 03 2024 - Crédit photos : Getty Images, Shutterstock