Votre interlocuteur AXA

AXA Prévention

Créée en 1984, **AXA Prévention** est une association à but non lucratif. Sa mission est d'étudier et de mettre en œuvre toutes les mesures de nature à développer la culture de prévention des Français afin de prévenir et réduire les risques auxquels ils sont exposés en santé, sur la route, à la maison, devant les écrans, dans le milieu professionnel et face au réchauffement climatique.

ASSO VICA

ASsociation de SOutien aux VIctimes de Cyber Attaques

L'ASSociation de SOutien aux VIctimes de Cyber Attaques (ASSOVICA) est une association à but non lucratif créée en 2023 par un collectif composé d'expert(e)s techniques et non techniques afin d'aider et accompagner au mieux les victimes d'actes de cybermalveillance. L'une de ses missions est d'apporter aide et soutien aux victimes professionnelles des cyber attaques ciblant les organisations.

AXA Prévention : Association à but non lucratif - Loi 1901 - 313 Terrasses de l'Arche - 92727 Nanterre Cedex - service.axaprevention@axa.fr

Réf. : 2006422 0625 - CAR/OCA - Crédit photo : Adobe Stock.

AXA Prévention

Soyez vigilant sur le niveau de cybersécurité de vos prestataires

ASSO VICA

ASsociation de SOutien aux VIctimes de Cyber Attaques

Retrouvez tous nos conseils et services de prévention sur : **axaprevention.fr**

Soyez vigilant sur le niveau de cybersécurité de vos prestataires

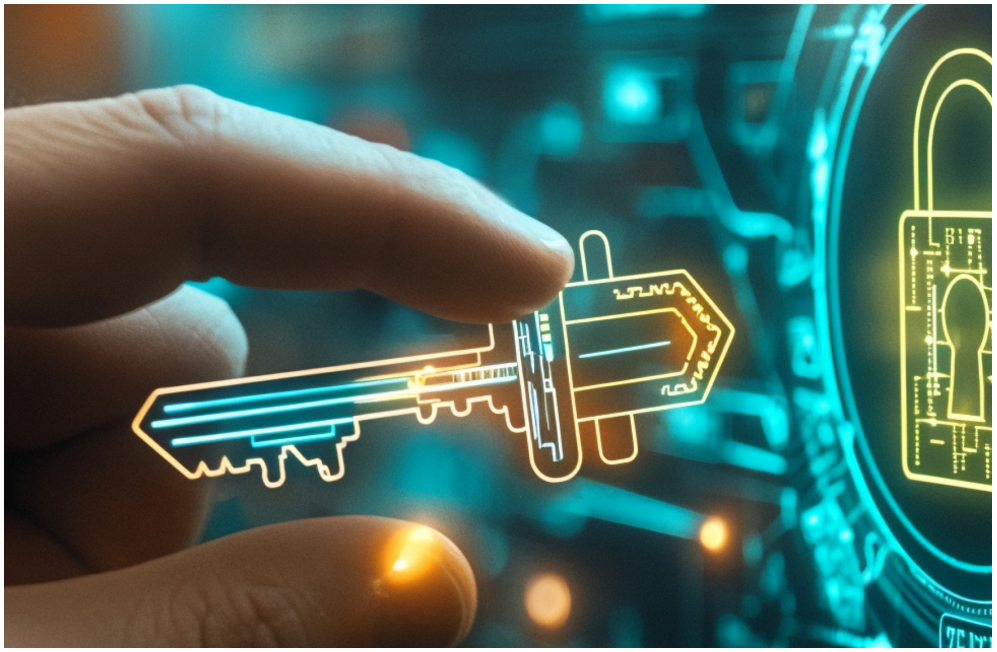
Dans un environnement où les entreprises sont de plus en plus interconnectées, la sécurité de la chaîne d'approvisionnement est devenue un enjeu critique.

Cette chaîne se compose de différentes entités externes (fournisseurs, prestataires de service, consultants…) soutenant les opérations d'une organisation.

Lorsque ces tiers accèdent à vos données ou à vos systèmes d'information cela élargit la surface d'attaque. Les cybercriminels exploitent les vulnérabilités techniques des fournisseurs tiers, les mises à jour des logiciels de gestion et même les composants matériels pour infiltrer votre système d'information.

Ces attaques entrainent souvent des perturbations opérationnelles, des pertes financières et des dommages à la réputation.

Les cybercriminels utilisent des techniques sophistiquées telles que le phishing ou les logiciels malveillants pour infiltrer les systèmes à travers des fournisseurs moins sécurisés. Une attaque réussie peut entraîner des fuites d'informations confidentielles, la compromission de données financières et une interruption des activités.



Afin de sécuriser votre chaîne d'approvisionnement, la première étape est d'évaluer les risques liés aux tiers :

1. Identifier vos prestataires critiques :
- Ayant accès à vos environnements critiques (infrastructures, données).
- Réalisant pour vous le traitement de données sensibles.
- Vous fournissant des services essentiels à vos opérations.

2. Analyser les risques associés :
- Cartographier les interconnexions entre votre système d'information et ceux de vos fournisseurs (accès, partages de données…).
- Recenser les processus externalisés.

3. Evaluer les mesures de sécurité mises en œuvre chez vos fournisseurs et leur conformité aux normes de votre secteur (certifications, procédures, audits réguliers…).

Pour atténuer les risques identifiés, adopter une démarche systématique afin de sécuriser chaque maillon de la chaîne d'approvisionnement :

- Intégrer les exigences de sécurité dans les documents d'appel d'offres et les contrats afin de garantir l'entente avec les fournisseurs sur les normes de sécurité.
- Mettre en œuvre des règles de résiliation claires afin de couper rapidement tout lien avec des fournisseurs qui ne respectent pas les normes de sécurité définies.
- Appliquer le principe de moindre privilège : limiter les accès des tiers au strict nécessaire par des contrôles d'accès et une surveillance stricte.
- Renforcer la sécurité physique par des mesures de contrôle d'accès.
- Surveiller les alertes et incidents et mettre en œuvre un plan de réponse.
- Former les collaborateurs aux meilleures pratiques de sécurité pour renforcer la culture de sécurité au sein de l'entreprise.
- Réaliser périodiquement des questionnaires pour réévaluer la conformité de vos fournisseurs et leurs pratiques de sécurité.