CYBER-SÉCURITÉ POUR LES ORGANISATIONS PLUS PETITES

LISTE DE CONTRÔLE DU RSSI : PROTÉGER LES CONNEXIONS À DES TIERS

CHOISIR DES FOURNISSEURS EN GARDANT À L'ESPRIT LA CYBER-SÉCURITÉ

Chaque fois que vous évaluez un fournisseur potentiel, passez en revue les questions suivantes :

- ☐ **A-t-il déjà servi des clients similaires à votre organisation ?**
- ☐ **A-t-il documenté leur conformité aux normes de cyber-sécurité connues (comme le cadre NIST ou ISO 27001, ou peut-il fournir un rapport SOC2) ?**
- ☐ **Parmi vos données et/ou actifs, auxquels aura-t-il besoin d'accéder pour effectuer son service et demande-t-il un accès apparemment inutile ?**
- ☐ **Comment prévoit-il de protéger les actifs et les données de votre organisation en sa possession ?**
- ☐ **Comment gère-t-il ses propres cyber-risques tiers et peut-il fournir des informations sur la sécurité de sa chaîne d'approvisionnement ?**
- ☐ **Quel est son plan pour la reprise après sinistre et la continuité des activités en cas d'incident impactant votre organisation ?**
- ☐ **Comment maintiendra-t-il votre organisation à jour en termes de communication des tendances, menaces et changements au sein de son organisation ?**

IDENTIFIER LE RISQUE PAR LE BIAIS DE TIERS

Effectuez une évaluation des cyber-risques tiers, en incluant les étapes suivantes :

- ☐ **Créez et mettez constamment à jour une liste de toutes les relations avec les fournisseurs et les actifs et données exposés dans chacune d'elle.**
- ☐ **Examinez les données auxquelles a accès chaque fournisseur ou tiers, en vérifiant que chaque niveau d'accès respecte le principe du « privilège minimum ».**
- ☐ **Classez vos relations fournisseurs et tiers (faible, moyen, élevé) sur la base de l'impact qu'une violation de leurs systèmes aurait sur votre organisation.**
- ☐ **En commençant par les fournisseurs les plus à risque, évaluez les capacités de cyber-sécurité de chaque fournisseur et la conformité aux normes pertinentes.**
- ☐ **Élaborez un plan pour une évaluation régulière de la sécurité, en gardant à l'esprit que vous pouvez vouloir mener occasionnellement des évaluations sur site des fournisseurs présentant le plus haut risque et/ou un accès plus important aux données clients.**

GÉRER LA SÉCURITÉ DES TIERS

- ☐ Effectuez une vérification approfondie. Établissez des attentes en matière de cyber-sécurité dans les demandes de proposition, les contrats, la continuité d'activité, la réponse aux incidents et les contrats de niveau de service avec les fournisseurs. Convenez des responsabilités et obligations en cas de cyber-incident.
- ☐ Renseignez-vous sur les pratiques en matière de cyber-sécurité des organisations financières et des autres entités avec lesquelles vous effectuez des transactions ou des partages de données, en gardant à l'esprit que vos fournisseurs et tiers doivent également respecter les mêmes exigences de cyber-sécurité que celles que votre organisation doit respecter.
- ☐ Utilisez les mesures établies et convenues pour surveiller la conformité de vos fournisseurs avec les normes de cyber-sécurité.
- ☐ Vérifiez auprès de vos fournisseurs qui traitent des données sensibles s'ils proposent l'authentification à deux facteurs, le chiffrement ou d'autres mesures de sécurité pour tous les comptes dont vous disposez.
- ☐ Assurez-vous que tous les logiciels et matériels tiers que vous installez disposent d'un protocole de transfert de sécurité de sorte que les processus de démarrage soient sécurisés via des codes d'authentification et ne s'exécutent pas si les codes ne sont pas reconnus.
- ☐ Si vous rencontrez des produits de fournisseurs qui sont contrefaits ou ne correspondent pas aux spécifications, travaillez pour négocier une résolution ou une stratégie de sortie.
- ☐ Évaluez annuellement les contrats des fournisseurs et assurez-vous qu'ils continuent à répondre à vos exigences stratégiques et aux exigences de sécurité des données réglementaires. Lors de la résiliation du contrat, incluez des stipulations vous permettant de récupérer vos actifs ou données et de vérifier que les actifs ou les données sont entièrement effacés du côté du fournisseur, et désactivez tout accès à vos systèmes ou serveurs.

PARTAGER DES INFORMATIONS

- ☐ Assurez-vous de disposer de canaux de communication clairs et de points de contact pour communiquer sur les problèmes de sécurité avec les fournisseurs et les homologues de votre organisation.
- ☐ Assurez-vous d'avoir des procédures en place pour garantir un partage opportun des informations de cyber-sécurité fiables et exploitables avec les parties prenantes internes et externes (y compris les entités et les autorités publiques au sein et en dehors du secteur financier).
- ☐ Suivez les mises à jour pertinentes sur les expériences des autres organisations avec leurs tiers en termes de menaces, vulnérabilités, incidents et réponses en faisant partie des organisations qui partagent des informations, comme FS-ISAC, et en cherchant d'autres sources d'informations sur les menaces.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

INTERNATIONAL MONETARY FUND · THE WORLD BANK IBRD • IDA | WORLD BANK GROUP · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE · ICBA Independent Community Bankers of America®