GUIDE AU NIVEAU DU RSSI : PROTÉGER LES CONNEXIONS À DES TIERS

IDENTIFIER LE RISQUE PAR LE BIAIS DE TIERS

- Créez et conservez une liste actualisée de toutes les relations avec les fournisseurs et les actifs et données exposés dans chacun d'eux.
- Passez en revue les données auxquelles chaque fournisseur ou tiers a accès. Assurez-vous que ce 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. Le respect des normes pertinentes est un bon point de départ. Élaborez un plan pour une évaluation régulière de la sécurité. 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 de votre organisation, 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 autres tiers, tels que les organisations financières avec lesquelles vous effectuez des transactions ou des partages de données. Toutes les exigences en matière de cyber-sécurité auxquelles votre organisation doit adhérer doivent également être respectées par vos fournisseurs et toute autre organisation avec lesquels vous partagez ou exposez des actifs.
- 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 fournisseur 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.
- Engagez-vous à partager en temps opportun les 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 pour améliorer les défenses de votre organisation, améliorer la connaissance de la situation et élargir l'apprentissage. Le fait de faire partie des organisations qui partagent des informations, par exemple le FS-ISAC, vous permettra de rester informé de l'actualité.

Comment choisir des fournisseurs en gardant à l'esprit la cyber-sécurité

Posez les questions suivantes aux fournisseurs potentiels pour évaluer leur préparation et leur sensibilisation en matière de cyber-sécurité, et par conséquent l'impact qu'ils auraient sur le profil de risque de votre organisation :

1. **Quelle expérience ont-ils ?** Renseignez-vous sur l'historique du fournisseur qui sert les clients. Have they served clients similar to your organization beåfore?
2. **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 ?
3. **Parmi vos données et/ou actifs, auxquels aura-t-il besoin d'accéder pour effectuer son service ?** Demande-t-il un accès apparemment inutile ?
4. **Comment prévoit-il de protéger les actifs et les données de votre organisation en sa possession ?**
5. **Comment gère-t-il ses propres cyber-risques tiers ?** Peut-il fournir des informations sur sa chaîne d'approvisionnement ?
6. **Quel est son plan pour la reprise après sinistre et la continuité des activités** en cas d'incident affectant les actifs et/ou données de votre organisation ?
7. **Comment gardera-t-il votre organisation à jour ?** Quel est son plan pour communiquer les tendances, les menaces et les changements au sein de son organisation ?

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
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