Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide au niveau du conseil : encadrement de la cyber-sécurité

Principes fondamentaux de la gouvernance des cyber-risques

Confirmez que vous pouvez répondre positivement aux questions suivantes :

1. Votre organisation **a-t-elle satisfait aux exigences légales et réglementaires pertinentes**?

2. Votre organisation **a-t-elle quantifié ses cyber-expositions et testé sa résilience financière?**

3. Votre organisation a-t-elle un **plan d'amélioration** en place pour garantir que les expositions s'inscrivent dans votre appétit au risque convenu?

4. Le conseil **discute-t-il régulièrement des informations concises, claires et exploitables relatives à la cyber-résilience de l'organisation et fournies par la direction**?

5. Votre organisation a-t-elle **des plans de réponse aux incidents en place qui ont récemment été testés**, y compris au niveau du conseil?

6. Les **rôles des personnes clés responsables de la gestion des cyber-risques** sont-ils clairs et alignés sur les trois lignes de défense?

7. Avez-vous obtenu **une validation et une assurance indépendantes** de la posture de cyber-sécurité de votre organisation?

Supervision

Au niveau le plus élevé de la direction de votre organisation, le conseil d'administration assume la responsabilité ultime de la gestion des cyber-risques et doit donc superviser la stratégie, les politiques et les activités de l'organisation dans ce domaine. Plus précisément, le conseil doit :

⇒ Assumer la responsabilité ultime de la supervision des cyber-risques et de la résilience, que ce soit en tant que conseil complet ou par délégation de supervision à un comité du conseil spécifique.
⇒ Assigner à un responsable de l'entreprise, généralement le RSSI, la responsabilité de signaler la capacité de votre organisation à gérer la cyber-résilience et les progrès dans la mise en œuvre des objectifs de cyber-résilience. S'assurer que ce responsable dispose d'un accès régulier au conseil d'administration, d'une autorité suffisante, de la maîtrise du sujet, de l'expérience et des ressources pour remplir ces obligations.
⇒ Définir annuellement la tolérance au risque de votre organisation ; assurer la cohérence avec votre stratégie d'entreprise et l'appétit au risque.
⇒ S'assurer qu'un examen formel et indépendant de la cyber-résilience de votre organisation est effectué chaque année.
⇒ Superviser la création, la mise en œuvre, les tests et l'amélioration continue des plans de cyber-résilience, en s'assurant que l'ensemble de votre organisation est aligné et que votre RSSI ou autre cadre responsable les signale régulièrement au conseil d'administration.
⇒ Intégrer la cyber-résilience et l'évaluation des risques dans la stratégie commerciale globale de votre organisation, la gestion des risques, la budgétisation et l'allocation des ressources, dans le but d'intégrer pleinement les cyber-risques au risque opérationnel global.
⇒ Passer régulièrement en revue vos performances pour ce qui précède et tenir compte des conseils indépendants pour une amélioration continue.

Rester informé

La surveillance efficace du cyber-risque du conseil dépend de la maîtrise du sujet par les membres et des informations à jour.

⇒ Assurez-vous que toutes les personnes qui rejoignent le conseil disposent des compétences et connaissances appropriées et actualisées pour comprendre et gérer les risques posés par les cyber-menaces.
⇒ Sollicitez des conseils réguliers de la part de la direction sur l'exposition au risque actuelle et future de votre organisation, les exigences réglementaires pertinentes, et les références du secteur et de la société pour l'appétit au risque. De plus, participez à des séances d'information régulières sur les derniers développements en ce qui concerne le paysage des menaces et l'environnement réglementaire, la planification commune et les visites aux pairs et aux leaders de la meilleure pratique en matière de cyber-sécurité, ainsi que dans des échanges au niveau du conseil sur la gouvernance et les rapports.
⇒ Donnez à la direction la responsabilité de signaler une évaluation quantifiée et compréhensible des cyber-risques, menaces et événements comme un élément permanent à l'ordre du jour lors des réunions du conseil d'administration.
⇒ Poursuivez la sensibilisation aux problèmes systémiques constants tels que les vulnérabilités de la chaîne d'approvisionnement, les dépendances courantes et l'écart dans le partage des informations entre les tableaux sur la gouvernance des cyber-risques.

Donner le ton

Parallèlement à la haute direction, le conseil doit définir et illustrer les valeurs fondamentales de votre organisation, la culture du risque et les attentes en ce qui concerne la cyber-résilience.

⇒ Favorisez une culture dans laquelle le personnel, à tous les niveaux, reconnaît ses responsabilités importantes pour garantir la cyber-résilience de votre organisation. Dirigez par l'exemple.
⇒ Supervisez le rôle de la direction dans la promotion et le maintien de la culture du risque de votre organisation. Favorisez, surveillez et évaluez la culture du risque, en tenant compte de l'impact de la culture sur la sécurité et la solidité, et apportez des changements si nécessaire.
⇒ Indiquez clairement que vous attendez de tout le personnel qu'il agisse avec intégrité et qu'il fasse remonter rapidement le non-respect observé au sein ou à l'extérieur de votre organisation.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide du niveau du PDG : encadrement de la cyber-sécurité

Gouvernance

La cyber-sécurité de votre organisation commence et se termine au plus haut niveau de gestion. Le PDG, avec le conseil d'administration, doit maintenir la compréhension des risques et assumer l'obligation de rendre compte et la responsabilité ultimes des activités de cyber-sécurité et du personnel de l'organisation. Vous devez :

⇒ Embaucher un responsable de la sécurité des systèmes d'information (RSSI) s'il n'y en a pas ou, si les ressources sont trop limitées, nommer une personne au sein de votre organisation pour remplir la fonction de RSSI.
⇒ Travailler avec le RSSI ou tout autre personnel technique pour établir et maintenir une stratégie et un cadre de cyber-sécurité adaptés aux cyber-risques spécifiques de l'organisation en utilisant les normes et directives internationales, nationales et industrielles.
⇒ Expliquer clairement les rôles et responsabilités du personnel en mettant en œuvre et en gérant la cyber-sécurité de l'organisation.

- Travailler avec le RSSI pour identifier les rôles de cyber-sécurité et les droits d'accès appropriés pour tous les niveaux de personnel.
- Superviser la communication et la collaboration afin de garantir que la gestion de la cyber-sécurité est holistique, surtout si les responsabilités en matière de cyber-sécurité sont partagées par plusieurs membres du personnel ou divisions au sein de l'organisation (comme de distinguer les secteurs verticaux de l'information, du risque et des technologies).

⇒ S'assurer que le RSSI dispose d'une ligne de communication claire et directe pour vous signaler les menaces en temps opportun, ainsi qu'au conseil d'administration.
⇒ Inviter le RSSI ou tout autre personnel technique à informer régulièrement la haute direction.
⇒ S'assurer que les politiques de sécurité, les normes, les mécanismes d'application et les procédures de l'organisation sont uniformes dans toutes les équipes et les secteurs d'activité.

Évaluation et gestion des risques

La garantie d'une sensibilisation et d'une préparation solides à la cyber-sécurité dépend de l'analyse continue basée sur les risques. Pour améliorer la cyber-sécurité de votre entreprise :

⇒ Établissez une évaluation et une gestion des risques de cyber-sécurité comme priorité dans les processus de gestion et de gouvernance des risques élargis de votre organisation. Travaillez avec votre RSSI ou tout autre personnel technique sur un plan pour effectuer une évaluation des risques impliquant les points suivants :

- Décrire les actifs de votre organisation et leurs différents niveaux de dépendance technologique ;
- Évaluer la maturité de votre organisation et les risques inhérents associés aux dépendances technologiques de ses actifs ;
- Déterminer l'état de maturité souhaité de votre organisation ;
- Comprendre où les menaces de cyber-sécurité s'inscrivent dans la liste des priorités de risque de votre organisation ;
- Identifier les écarts entre votre état actuel de cyber-sécurité et l'état cible souhaité ;
- Mettre en œuvre des plans pour atteindre et maintenir la maturité ;
- Réévaluer continuellement la maturité, les risques et les objectifs de cyber-sécurité de votre organisation ; et
- Envisager l'utilisation de tests d'intrusion de tiers ou une simulation ;
- Envisager des mesures de protection telles que l'achat d'une cyber-assurance.

⇒ Dirigez les efforts des employés pendant le processus d'évaluation des risques afin de faciliter les réponses opportunes de l'ensemble de l'établissement.
⇒ Analysez et présentez les résultats de l'évaluation des risques pour la supervision exécutive, y compris les principales parties prenantes et le conseil.
⇒ Supervisez les changements pour conserver ou améliorer la préparation à la cyber-sécurité souhaitée de votre organisation, en veillant à ce que les mesures prises pour améliorer la cyber-sécurité soient proportionnelles aux risques et rentables pour votre organisation.
⇒ Supervisez les performances de la surveillance continue afin de rester flexible et agile dans le traitement des cyber-risques en évolution.

Culture organisationnelle

La cyber-sécurité de votre organisation n'est pas un processus ponctuel ou le travail de quelques employés ; il s'agit d'un facteur à prendre en compte dans toutes les décisions et opérations de l'entreprise et d'une pratique qui doit être maintenue par tous les employés. Afin d'encourager une cyber-sécurité continue et holistique au sein de votre organisation :

⇒ Initiez des discussions sur la cyber-sécurité avec l'équipe de direction et communiquez régulièrement avec le personnel responsable de la gestion des cyber-risques.
⇒ Formez tous les employés à la cyber-sécurité, en veillant à ce que tout le personnel soit à jour sur (et ait signé des documents indiquant qu'ils acceptent de respecter) les politiques de cyber-sécurité de votre organisation et à ce que votre service informatique ou tout autre personnel technique les informe sur les meilleures pratiques.
⇒ Instaurez une formation récurrente à la cyber-sécurité pour tous les employés en ce qui concerne leurs responsabilités de sécurité à court et à long terme.
⇒ Veillez à ce que la cyber-sécurité soit toujours prise en compte lorsque votre organisation évalue les fournisseurs potentiels et partage des données avec des tiers.
⇒ Passez annuellement en revue les politiques de cyber-sécurité de votre organisation.
⇒ Encouragez le partage volontaire des informations sur les menaces et incidents de cyber-sécurité au sein de votre organisation et avec des homologues fiables.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide au niveau du RSSI : protéger votre organisation

Développer un programme de sécurité des informations basé sur les risques

1. Identifier les types d'informations que votre entreprise stocke et utilise
⇒ Énumérez tous les types d'informations que votre entreprise stocke ou utilise (par ex., noms des clients et e-mails).

2. Définir la valeur de vos informations
⇒ Posez des questions clés pour chaque type d'informations :

- Que se passerait-il si ces informations étaient rendues publiques ?
- Qu'adviendrait-il de mon entreprise si ces informations étaient incorrectes, par exemple, l'intégrité des données avait été manipulée ?
- Qu'adviendrait-il de mon entreprise si je/mes clients n'avaient pas pu accéder à ces informations ?

3. Développer un inventaire
⇒ Identifiez la technologie en contact avec les informations que vous avez identifiées. Cela peut inclure du matériel (par ex., ordinateurs) et des applications logicielles (par ex., e-mail du navigateur). Incluez la marque, le modèle, les numéros de série et les autres identifiants. Trouvez où se trouve chaque produit. Pour le logiciel, identifiez la ou les machines sur lesquelles le logiciel a été chargé.
⇒ Le cas échéant, incluez des technologies externes à votre entreprise (par ex., « le cloud ») et toutes les technologies de protection que vous avez en place, telles que les pare-feu.

4. Comprendre vos menaces et vulnérabilités
⇒ Examinez régulièrement les menaces et vulnérabilités que le secteur financier peut rencontrer et estimez la probabilité que vous soyez affecté. (Vous trouverez des informations via votre CERT national, FS-ISAC, votre section InfraGard local, etc.)
⇒ Effectuez une analyse des vulnérabilités au moins une fois par an.

5. Créer une politique de cyber-sécurité
⇒ Travaillez avec la haute direction de votre organisation pour établir et maintenir une stratégie de cyber-sécurité adaptée aux risques susmentionnés et informée par les normes et directives internationales, nationales et industrielles. Des directives telles que le cadre NIST, l'outil d'évaluation de la cyber-sécurité FFIEC et la norme ISO 27001 fournissent des modèles pour la construction et l'amélioration de ces politiques.
⇒ Formez tous les employés sur les détails de la politique et demandez-leur de signer des documents attestant de leur rôle dans le maintien permanent de la cyber-sécurité de votre organisation en respectant la politique.

Prévenir les dommages liés aux logiciels malveillants

⇒ Activez votre pare-feu et configurez les listes de contrôle d'accès (ACL) pour créer une zone tampon entre votre réseau et Internet. Limitez l'accès en utilisant un paramètre de liste blanche, et non en établissant une liste noire de certains services ou adresses IP.
⇒ Utilisez un logiciel antivirus et un logiciel anti-espion sur tous les ordinateurs et ordinateurs portables.
⇒ Corrigez tous les logiciels et micrologiciels en appliquant rapidement les dernières mises à jour logicielles fournies par les fabricants et les fournisseurs. « Mettez à jour automatiquement », le cas échéant.
⇒ Limitez l'installation de nouveaux programmes au personnel informatique avec des droits d'administrateur.
⇒ Conservez et surveillez les journaux d'activité générés par le matériel ou le logiciel de protection/détection. Protégez les journaux avec une protection par mot de passe et un chiffrement des mots de passe.
⇒ Maintenez toutes les horloges hôtes synchronisées. Si les appareils de votre organisation ont des paramètres d'horloge incohérents, la corrélation des événements sera beaucoup plus difficile en cas d'incidents.
⇒ Contrôlez l'accès aux supports amovibles tels que les cartes SD et les clés USB. Encouragez le personnel à transférer des fichiers par e-mail ou par stockage cloud. Informez le personnel sur les risques liés à l'utilisation de clés USB provenant de sources externes ou à la transmission de leurs propres clés USB à d'autres personnes.
⇒ Configurez la sécurité de la messagerie et les filtres de courrier indésirable sur vos services de messagerie.
⇒ Protégez toutes les pages de vos sites Web publics avec les outils de chiffrement et les autres outils disponibles.
⇒ Envisagez d'embaucher un service de test d'intrusion pour évaluer la sécurité des actifs et des systèmes de votre organisation.

Former les employés

⇒ Effectuez des formations obligatoires sur la cyber-sécurité lors de l'intégration des nouveaux employés et à intervalles réguliers pour tous les employés actuels, au moins une fois par an. Exigez des employés :

- qu'ils utilisent des mots de passe forts sur tous les appareils et comptes professionnels et encouragez-les à faire de même pour leurs appareils personnels et à utiliser un gestionnaire de mots de passe ;
- qu'ils maintiennent tous les systèmes d'exploitation, logiciels et applications à jour sur tous les appareils ;
- qu'ils utilisent une authentification à deux facteurs sur tous les comptes ;
- qu'ils conservent les détails des comptes et les cartes d'accès en sécurité et verrouillent les appareils lorsqu'ils ne les utilisent pas ;
- qu'ils s'abstiennent de partager les détails des comptes ou d'autres données sensibles via un e-mail non chiffré ou d'autres communications ouvertes ;
- qu'ils évitent d'ouvrir automatiquement des pièces jointes ou de cliquer sur des liens dans des e-mails non sollicités ou suspects ;
- qu'ils vérifient la validité d'un e-mail suspect ou d'une fenêtre contextuelle avant de fournir des informations personnelles, et qu'ils accordent une attention particulière à l'adresse e-mail ; et
- qu'ils signalent tout incident de sécurité interne ou externe potentiel, menace ou mauvaise manipulation des données ou des appareils au personnel technique de votre organisation et/ou aux cadres supérieurs.

⇒ Testez régulièrement la sensibilisation des employés à travers des problèmes simulés, par exemple en envoyant des e-mails de style hameçonnage à partir de faux comptes. Utilisez des défaillances comme opportunités d'apprentissage plutôt que de punir.

Protéger vos données

⇒ Effectuez des sauvegardes régulières de vos données importantes (par ex., documents, e-mails, calendriers) et vérifiez qu'elles peuvent être restaurées. Envisagez de sauvegarder sur le cloud.
⇒ Assurez-vous que l'appareil contenant votre sauvegarde n'est pas connecté de façon permanente à l'appareil qui détient la copie originale, ni physiquement ni via un réseau local.
⇒ Installez des protecteurs de surtension, utilisez des générateurs et assurez-vous que tous vos ordinateurs et périphériques réseau critiques sont branchés sur des alimentations sans interruption.
⇒ Utilisez une solution de gestion des appareils mobiles (MDM - Mobile Device Management).

Sécuriser vos appareils

⇒ Activez la protection des codes PIN et mots de passe pour les appareils mobiles. Configurez les appareils pour que, lorsqu'ils sont perdus ou volés, ils puissent être suivis, vidés à distance ou verrouillés à distance.
⇒ Gardez vos appareils (et toutes les applications installées) à jour, en utilisant l'option « Mettre à jour automatiquement » si disponible.
⇒ Lorsque vous envoyez des données sensibles, ne vous connectez pas aux points d'accès Wi-Fi publics ; utilisez des connexions cellulaires (y compris des dongles de connexion sans fil) ou utilisez des VPN.
⇒ Remplacez les appareils qui ne sont plus pris en charge par les fabricants par des solutions alternatives à jour.
⇒ Définissez des procédures de signalement pour les équipements perdus ou volés.

Utiliser des mots de passe

⇒ Assurez-vous que tous les ordinateurs utilisent des produits de chiffrement qui nécessitent un mot de passe pour démarrer. Activez la protection par mot de passe ou code PIN pour les appareils mobiles.
⇒ Utilisez des mots de passe forts, en évitant les mots de passe prévisibles (comme m0tdepasse) et les identifiants personnels (comme les noms de famille et d'animaux). Demandez à tous les employés de faire de même.
⇒ Utilisez l'authentification à deux facteurs (2FA) dans la mesure du possible.
⇒ Modifiez les mots de passe par défaut émis par le fabricant sur tous les appareils, y compris les périphériques réseau et IoT, avant de les distribuer au personnel.
⇒ Assurez-vous que le personnel peut réinitialiser facilement ses propres mots de passe. Vous pouvez également demander aux employés de modifier leur mot de passe à intervalles réguliers (par ex., trimestriel, semestriel ou annuel).
⇒ Envisagez d'utiliser un gestionnaire de mots de passe. Si vous en utilisez un, assurez-vous que le mot de passe « maître » (qui fournit l'accès à tous vos autres mots de passe) est un mot de passe fort.

Contrôler les autorisations

⇒ Assurez-vous que tous les employés disposent de comptes identifiables uniques qui sont authentifiés chaque fois qu'ils accèdent à vos systèmes.
⇒ Donnez uniquement des privilèges administratifs à un personnel informatique et un personnel clé fiables et révoquez les privilèges d'administrateur sur les postes de travail pour les utilisateurs standard.
⇒ Donnez uniquement aux employés l'accès aux systèmes de données spécifiques dont ils ont besoin pour leur travail et assurez-vous qu'ils ne peuvent installer aucun logiciel sans autorisation.
⇒ Contrôlez l'accès physique à vos ordinateurs et créez des comptes utilisateur pour chaque employé.

Sécuriser vos réseaux et appareils Wi-Fi

⇒ Assurez-vous que votre Wi-Fi professionnel est sécurisé et chiffré avec WPA2. Les routeurs sont souvent fournis avec le chiffrement désactivé, alors assurez-vous de l'activer. Protégez l'accès au routeur par un mot de passe et assurez-vous que le mot de passe est mis à jour à partir de la valeur par défaut prédéfinie. Désactivez les fonctions de « gestion à distance ».
⇒ Configurez votre point d'accès sans fil ou votre routeur afin qu'il ne diffuse pas le nom du réseau, appelé Identificateur SSID (Service Set Identifier).
⇒ Limitez l'accès à votre réseau Wi-Fi en autorisant uniquement les périphériques avec certaines adresses de contrôle d'accès aux médias. Si des clients ont besoin de Wi-Fi, configurez un réseau public distinct.
⇒ Activez la connexion DHCP (Dynamic Host Configuration Protocol) sur vos périphériques réseau afin de faciliter le suivi de tous les périphériques qui se sont connectés à votre réseau. ⇒ Déconnectez-vous en tant qu'administrateur après avoir configuré le routeur.
⇒ Gardez le logiciel de votre routeur à jour. Découvrez les mises à jour en enregistrant votre routeur auprès du fabricant et en vous inscrivant pour obtenir des mises à jour.

Éviter les attaques par hameçonnage

⇒ Assurez-vous que le personnel ne navigue pas sur le Web ou vérifiez les e-mails sur les serveurs ou à partir d'un compte avec des privilèges d'administrateur.
⇒ Configurez les filtres Web et de messagerie. Pensez à empêcher les employés de visiter des sites Web fréquemment associés aux menaces de cyber-sécurité.
⇒ Apprenez aux employés à détecter des signes évidents d'hameçonnage, comme l'orthographe et la grammaire médiocres, ou des versions de logos reconnaissables de mauvaise qualité. L'adresse e-mail de l'expéditeur semble-t-elle légitime ?
⇒ Effectuez une analyse anti-logiciels malveillants et modifiez les mots de passe dès que possible si vous soupçonnez une attaque. Ne punissez pas les employés s'ils sont victimes d'une attaque par hameçonnage (cela dissuade les personnes de signaler les problèmes par la suite)

Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide au niveau du RSSI : protéger vos clients

Conseils individuels pour les clients et les employés pour protéger les données financières

Conseillez à vos employés et à vos clients de suivre les directives de cyber-sécurité ci-dessous dans leur comportement personnel afin d'améliorer leur préparation et de protéger leurs données financières contre les cyber-menaces.

1. Mettez en œuvre des pratiques de base en matière d'hygiène de la cyber-sécurité sur vos appareils.

⇒ Utilisez des mots de passe forts sur tous les appareils personnels et professionnels, et envisagez d'utiliser un gestionnaire de mots de passe.

⇒ Gardez les systèmes d'exploitation et autres logiciels et applications à jour sur vos ordinateurs et appareils mobiles.

⇒ Installez des logiciels antivirus, anti-logiciels malveillants et anti-ransomware qui empêchent, détectent et éliminent les programmes malveillants.

⇒ Utilisez un programme pare-feu pour empêcher l'accès non autorisé à votre ordinateur.

⇒ Utilisez uniquement des produits de sécurité d'entreprises réputées. Lisez les commentaires des publications d'ordinateurs et de consommateurs et envisagez de consulter le fabricant de votre ordinateur ou système d'exploitation.

2. Soyez prudent avec les informations sensibles.

⇒ N'envoyez pas de mots de passe de compte bancaire ou d'autres données de comptes financiers sensibles via un e-mail non chiffré.

⇒ Soyez intelligent quant à l'endroit et à la manière dont vous vous connectez à Internet pour les services bancaires ou autres communications impliquant des informations personnelles sensibles. Les réseaux et ordinateurs Wi-Fi publics dans des lieux tels que les bibliothèques ou les centres d'affaires des hôtels peuvent être risqués.

3. Résistez à l'hameçonnage.

⇒ N'ouvrez pas automatiquement les pièces jointes des e-mails ou ne cliquez pas sur des liens dans des e-mails non sollicités ou suspects. Arrêtez-vous. Réfléchissez. Cliquez.

⇒ Méfiez-vous si quelqu'un vous contacte soudainement en ligne ou par téléphone et vous demande vos informations personnelles. Même lorsque vous communiquez avec des adresses connues, réduisez au minimum le partage des informations personnelles par e-mail.

⇒ N'oubliez pas qu'aucun établissement financier ne vous enverra un courrier électronique ou ne vous appellera et ne vous demandera des informations confidentielles qu'ils ont déjà vous concernant.

⇒ Partez du principe qu'une demande d'information d'une banque où vous n'avez jamais ouvert un compte est une arnaque.

⇒ Vérifiez la validité d'un e-mail suspect ou d'une fenêtre contextuelle avant de fournir des informations personnelles. Accordez une attention particulière à l'adresse e-mail.

Administrer des comptes

⇒ Exigez que les clients utilisent des identifiants et des mots de passe forts pour se connecter à vos services. Recommandez-leur de ne pas utiliser un mot de passe déjà utilisé pour d'autres comptes.

⇒ Utilisez la vérification instantanée, la vérification en temps réel, la vérification de dépôt d'essai, la vérification d'identité et/ou des questions à réponses ouvertes pour valider les clients réels et réduire l'opportunité de fraude.

⇒ Proposez, exigez idéalement, l'utilisation de l'authentification à deux facteurs pour les clients lorsqu'ils se connectent à vos services.

⇒ Vérifiez régulièrement les comptes des utilisateurs pour détecter des signes de fraude.

Protéger les données

⇒ Déterminez les données clients que votre organisation *doit* collecter pour exécuter ses services, et soyez prudent si vous collectez des données clients qui vont au-delà.

⇒ Définissez et distribuez des politiques de conservation des données. Supprimez les données clients lorsqu'elles ne sont plus nécessaires.

⇒ Chiffrez les données clients en transit et au repos.

⇒ Mettez en place des politiques de sécurité des données pour indiquer clairement quelles méthodes de transfert de données sont approuvées par rapport aux restrictions et pour spécifier ce qui est acceptable pour tous les employés lorsqu'ils traitent des données clients. Veillez à ce que ces politiques soient documentées, communiquées, appliquées à tous les employés, et régulièrement examinées et mises à jour.

Sécuriser des applications Web publiques

⇒ Appliquez le protocole HTTPS sur les applications Web publiques de votre organisation et redirigez tout le trafic HTTP vers HTTPS.

⇒ Utilisez une politique de sécurité du contenu sur votre ou vos sites Web pour éviter les attaques de scripts intersites, le détournement de clics et l'injection d'autres codes.

⇒ Activez l'épinglage de clé publique sur votre ou vos sites Web pour empêcher les attaques de type intermédiaire.

⇒ Assurez-vous que votre ou vos applications Web publiques n'utilisent jamais les cookies pour stocker des informations très sensibles ou critiques sur le client (comme les mots de passe) et qu'elles disposent de dates d'expiration conservatrices pour les cookies (mieux vaut tôt que tard). Pensez à chiffrer les informations stockées dans les cookies que vous utilisez.

⇒ Envisagez d'embaucher un service de test d'intrusion pour évaluer la sécurité de votre ou vos applications Web publiques au moins une fois par an.

Former les employés

⇒ Responsabilisez vos employés et apprenez-leur les stratégies pour minimiser l'erreur humaine qui pourrait exposer les données clients. Cela implique de leur recommander de :

- Minimiser leur accès et la transmission des données clients à seulement ce qui est nécessaire pour exécuter leur travail ;
- Maintenir des pratiques de sécurité solides sur tous les appareils et comptes qui traitent des données clients en utilisant des mots de passe forts, en activant l'authentification à deux facteurs, en gardant les logiciels à jour et en ne cliquant pas sur des liens suspects ; et
- Signaler tout incident de sécurité interne ou externe potentiel, menace ou mauvaise manipulation des données au personnel technique de votre organisation et/ou aux cadres supérieurs.

⇒ Assurez-vous que vos employés comprennent et ont signé des documents pour adhérer aux politiques de protection des données et de sécurité de votre organisation afin qu'ils ne les enfreignent pas, qu'ils les maîtrisent lorsqu'ils traitent avec les clients, et qu'ils ne communiquent pas avec les clients de manière non protégée.

Informer les clients

⇒ Comprenez l'environnement réglementaire de votre organisation en matière de gestion des violations de données clients afin de vous assurer que vous êtes prêt à vous y conformer en cas d'incident.
⇒ Lorsque votre organisation prend connaissance d'un incident d'accès non autorisé à des informations sensibles du client, enquêtez pour déterminer rapidement la probabilité que les informations aient été ou seront mal utilisées. Suivez les bonnes pratiques de notification et informez le ou les clients concernés dès que possible avec :

- Une description générale de l'incident et des informations qui ont été violées ;
- Un numéro de téléphone pour plus d'informations et obtenir une assistance ;
- Un rappel pour « rester vigilant » au cours des 12 à 24 prochains mois ;
- Une recommandation de signalement rapide des incidents d'usurpation d'identité suspectée ;
- Une description générale des mesures prises par l'établissement financier afin de protéger les informations d'un accès ou d'une utilisation non autorisé(e) ;
- Les coordonnées des agences d'évaluation de crédit ; et
- Toute autre information requise par les réglementations avec lesquelles votre organisation doit se conformer.

Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide au niveau du RSSI : protéger les connexions à des tiers

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. A-t-il servi des clients similaires à votre organisation auparavant ?

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 ?

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.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Renforcement des capacités de cyber-sécurité Boîte à outils pour les organisations financières

Guide de réponse en cas d'incidents

Préparation

⇒ Travaillez avec la haute direction de votre organisation et les autres membres du personnel concernés pour développer un plan de réponse aux incidents et de continuité d'activité basé sur les risques les plus pressants qui ont été identifiés dans l'évaluation des cyber-risques de votre organisation.

- Développez des scénarios de menaces pour les types d'incidents liés aux cyber-risques prioritaires de votre organisation. Concentrez-vous sur le renforcement des capacités à réagir à ces scénarios.
- Identifiez, enregistrez et mettez à disposition, dans votre organisation, une liste des points de contact pour une réponse aux incidents.
- Identifiez et enregistrez les coordonnées des agences de lutte contre la fraude et des fonctionnaires locaux et fédéraux.
- Établissez des dispositions précisant quels types d'incidents doivent être signalés, quand ils doivent être signalés, et à qui.
- Établissez des directives écrites qui décrivent la rapidité à laquelle le personnel doit réagir à un incident et quelles mesures doivent être prises, en fonction des facteurs pertinents tels que l'impact fonctionnel et d'information de l'incident, et la capacité de récupération probable de l'incident.
- Informez tous les employés de contacter votre équipe technique – le plus souvent, ce sera le personnel informatique et/ou le RSSI/DSI/autre responsable équivalent, lorsqu'un incident se produit.
- Déployez des solutions pour surveiller les actions des employés et permettre l'identification des menaces et incidents d'initiés.
- Incluez des plans de continuité d'activité pour coordonner la manière dont votre organisation travaillera avec les fournisseurs et les clients principaux pendant une urgence professionnelle, y compris la manière dont vous mèneriez des opérations professionnelles manuelles ou alternatives, si nécessaire.
- Incluez les procédures écrites pour l'arrêt et le redémarrage du système d'urgence.
- Développez et testez des méthodes de récupération et de restauration des données de sauvegarde ; testez régulièrement les données de sauvegarde pour vérifier leur validité.
- Disposez d'accords et de procédures établis pour mener des opérations professionnelles sur une autre installation/un autre site.
- Disposez d'un canal de diffusion clair pour tous les clients.

Pratiquer

⇒ Organisez de petits exercices avec tous les membres du personnel ou représentants de tous les niveaux du personnel, y compris les cadres de l'organisation, le personnel des relations publiques/de la communication, ainsi que les équipes juridiques et de conformité.
⇒ Identifiez et idéalement participez à des exercices sectoriels pertinents pour votre organisation.
⇒ Établissez un processus pour garantir que les enseignements tirés des exercices sont intégrés et traités dans la stratégie de cyber-sécurité de votre entreprise.

Apporter une réponse

⇒ Mettez en œuvre des actions du plan de réponse aux incidents afin de minimiser l'impact, y compris en ce qui concerne le préjudice de réputation.
⇒ Identifiez les systèmes affectés/compromis et évaluez les préjudices.
⇒ Réduisez les préjudices en éliminant (déconnectant) les actifs concernés.
⇒ Commencez à enregistrer toutes les informations dès que l'équipe soupçonne qu'un incident s'est produit. Tentez de conserver des preuves de l'incident lors de la déconnexion/séparation d'un actif identifié comme étant affecté ; par exemple, collectez les journaux de la configuration du système, du réseau et de la détection d'intrusion à partir des actifs affectés.
⇒ Informez les parties internes appropriées, les fournisseurs tiers et les autorités, et demandez de l'aide si nécessaire.
⇒ Initiez des activités de notification et d'assistance client conformément aux lois, réglementations et directives inter-agences.
⇒ Utilisez des plateformes de partage des menaces telles que FS-ISAC ou MISP pour informer le secteur de la menace.
⇒ Documentez toutes les étapes qui ont été prises pendant l'incident pour un examen ultérieur.

Récupération

⇒ Restaurez les actifs récupérés à des « points de récupération » périodiques si disponibles et utilisez les données de sauvegarde pour restaurer les systèmes au dernier état « correct » connu.
⇒ Créez des sauvegardes « propres » actualisées des actifs restaurés et assurez-vous que toutes les sauvegardes des actifs critiques sont stockées dans un emplacement sécurisé physiquement et de manière écologique.
⇒ Testez et vérifiez si les systèmes infectés sont entièrement restaurés. Confirmez que les systèmes affectés fonctionnent normalement.

Révision

⇒ Menez une discussion « enseignements tirés » après l'incident : rencontrez les cadres dirigeants, les conseillers de confiance et le(s) fournisseur(s) d'assistance informatique pour examiner les vulnérabilités possibles ou recommander de nouvelles étapes à mettre en œuvre.
⇒ Si possible, identifiez les vulnérabilités (que ce soit dans les logiciels, le matériel, les opérations professionnelles ou le comportement du personnel) qui ont conduit à l'incident, puis élaborez un plan pour les prévenir.
⇒ Élaborez un plan de surveillance pour détecter des incidents similaires ou supplémentaires liés aux problèmes identifiés.
⇒ Partagez les enseignements tirés et les informations sur l'incident sur les plateformes de partage des menaces telles que FS-ISAC.
⇒ Intégrez les enseignements tirés dans les protocoles de réponse aux incidents de votre organisation.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE