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)