Pratiques exemplaires en matière de cybersécurité à intégrer dans votre organisation

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
AOUT 2022 | ITSAP.10.102

Votre capacité à défendre vos réseaux, vos systèmes et vos données contre les auteurs de menace repose essentiellement sur vos pratiques exemplaires en matière de cybersécurité. Adopter des mesures de cybersécurité rigoureuses permettra à votre organisation de se protéger et de se défendre contre les cyberincidents, et d'assurer la reprise de ses activités par la suite.

Liste de vérification des pratiques exemplaires en matière de cybersécurité

Veiller à ce que votre organisation mette en place des pratiques exemplaires en matière de cybersécurité et en fait la promotion et la surveillance est une composante essentielle de sa posture en cybersécurité. Le tableau ci-dessous dresse la liste des mesures que votre organisation peut prendre pour renforcer les fondements de sa cybersécurité au moyen de mécanismes de protection améliorés mis en place sur ses réseaux, ses systèmes et ses données. Même si votre organisation ne peut pas mettre en œuvre l'ensemble des mesures indiquées ci-dessous, il est recommandé d'implémenter celles qui sont réalisables et durables pour améliorer sa posture de cybersécurité.

Protection des réseaux et des points terminaux

- ☐ Protégez le périmètre au moyen d'un antivirus ou d'un antimaliciel, d'un logiciel de gestion des menaces visant les applications mobiles, de pare-feux et de systèmes de détection et de prévention d'intrusion.
- ☐ Segmentez vos réseaux de manière à empêcher le trafic d'atteindre les zones sensibles ou d'accès restreint.
- ☐ Surveillez continuellement vos passerelles pour dispositifs Internet et mobiles, le trafic réseau, les points d'accès sans fil et les journaux d'audit pour relever les anomalies.
- ☐ Assurez la rotation des clés cryptographiques utilisées pour protéger vos systèmes, les utilisateurs distants authentifiés et vos sites Web.
- ☐ Surveillez votre serveur de système d'adressage par domaines (DNS pour Domain Name System) pour assurer la stabilité de votre site et maintenir la confiance des utilisateurs.
- ☐ Mettez en œuvre le service DNS de protection pour éviter que les utilisateurs visitent par inadvertance des domaines potentiellement malveillants sur Internet.
- ☐ Mettez en œuvre un système de gestion des informations et des événements de sécurité (GIES) pour permettre une surveillance continue en temps réel si de telles ressources sont disponibles.

Protection des systèmes

- ☐ Mettez en œuvre l'application automatique des mises à jour et des correctifs, en particulier pour les services et systèmes exposés à Internet, les micrologiciels, le matériel, les logiciels et les systèmes d'exploitation (SE).
- ☐ Utilisez des phrases ou mots de passe rigoureux et veillez à ce qu'ils demeurent confidentiels et en sécurité.
- ☐ Mettez en œuvre l'authentification multifacteur sur les comptes et les systèmes, tout particulièrement ceux ayant des privilèges d'administrateur.
- ☐ Utilisez des stations de travail dédiées pour les comptes d'administrateur et configurez-les de manière à ce qu'elles ne puissent pas accéder à Internet ou aux courriels.
- ☐ Appliquez le principe du droit d'accès minimal selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches autorisées.
- ☐ Passez en revue les privilèges d'utilisateur dans les systèmes et les droits d'accès aux données, en particulier ceux associés aux utilisateurs ayant des privilèges d'administrateur, et supprimez ou modifiez ceux qui sont inutiles.
- ☐ Gérez les appareils mobiles au moyen de solutions de gestion des appareils mobiles (MDM pour *Mobile Device Management*) ou de gestion unifiée des terminaux (UEM pour *Unified Endpoint Management*).
- ☐ Créez une liste d'applications autorisées pour contrôler qui ou quoi est autorisé à accéder à vos réseaux et à vos systèmes.
- ☐ Mettez en place un plan d'intervention en cas d'incident et testez-le dans le cadre d'exercices de simulation pour vous assurer qu'il est possible de restaurer les fonctions essentielles et d'assurer la reprise des activités en temps opportun.
- ☐ Sauvegardez régulièrement les données et les systèmes critiques hors ligne et assurez-vous que les sauvegardes sont isolées de toute connexion au réseau.
- ☐ Testez vos sauvegardes périodiquement pour vous assurer qu'il est possible de récupérer les données et les systèmes rapidement.
- ☐ Évaluez les applications de tierces parties pour déterminer si elles comportent des fonctions ou des composants qui devraient être désactivés en raison de leur inutilité ou qui nécessiteraient une intervention humaine avant d'être activés (comme les macros).
- ☐ Procédez à l'inventaire des biens matériels et logiciels de votre organisation et tenez-le à jour.
- ☐ Catégorisez vos biens de manière à identifier ceux qui sont les plus essentiels pour mener à bien les fonctions opérationnelles de votre organisation.

Sensibilisation des utilisateurs et autres mesures de protection

- ☐ Offrez à vos employés une formation sur mesure en matière de cybersécurité pour veiller à ce qu'ils sachent quoi faire s'ils détectent des courriels ou des liens suspects.
- ☐ Misez sur la sensibilisation de vos employés à la protection de la vie privée afin de réduire les risques d'atteintes à la vie privée.
- ☐ Repérez les sources d'information pertinentes pour votre organisation ou abonnez-vous à un service d'alerte afin de rester au courant des menaces qui pourraient toucher votre organisation.
- ☐ Mettez en place une liste de contacts internes et externes composée des principaux intervenants à aviser lorsque survient un événement.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada