CYBER-SÉCURITÉ POUR LES ORGANISATIONS PLUS PETITES

LISTE DE CONTRÔLE EN CAS D'INCIDENT

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 régulation locales 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 qu'ils doivent 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.**

- ☐ **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 sur les opérations professionnelles.**
- ☐ **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 plates-formes 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.**
- ☐ **Confirmez que les systèmes affectés fonctionnent normalement.**
- ☐ **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 plates-formes 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

CarnegieEndowment.org

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