Anne-sophie Bonnat - MANA CYBER PACIFIQUE
manacyber@tipaeruiinvest.com
N°T/SEFI : F47007-002 000842

PROGRAMME DE FORMATION

Intitulé : Formation ludique de sensibilisation à la sécurité, cybersécurité et au RGPD

Objectif global :

Informer les salariés du paysage des menaces, de leur rôle et responsabilité dans la protection des données personnelles et sensibles par l'application des mesures de sécurité de l'entreprise.
Cette formation est dispensée sous un format innovant et ludique de jeu de rôles simulant la progression d'une organisation au travers d'activités et d'évènements.

Objectifs de conformité réglementaire satisfaits :

Réglementations	Références	Exigence
PCI-DSS	12.6 12.6.3	La sensibilisation à la sécurité est une activité continue. > Le personnel reçoit une formation de sensibilisation à la sécurité comme suit : .. - Plusieurs méthodes de communication sont utilisées.
RGPD	Art. 39-1. B	Les missions du délégué à la protection des données sont..: - contrôler le respect du présent règlement, d'autres dispositions.., y compris en ce qui concerne .., la sensibilisation et la formation du personnel participant aux opérations de traitement.
NIS v1	Arrêtés sectoriels Annexe 1	Règle relative à la politique de sécurité des systèmes d'information : - prévoit un plan de sensibilisation à la sécurité des SIIV au profit de l'ensemble du personnel ainsi qu'un plan de formation à la sécurité des SIIV
ISO 27001	Clause 7.2.2	Sensibilisation, éducation et formation à la sécurité de l'information : Tous les employés de l'organisation .. doivent recevoir une sensibilisation et une formation appropriées.
DORA (2025)	Art 13.6	Les entités financières élaborent des programmes de sensibilisation à la sécurité des TIC.

Objectifs détaillés :

- Comprendre les principes fondamentaux du RGPD appliqués à l'organisme
- Connaître les principaux risques ou évènements de sécurité et de cybersécurité auxquels mon organisation peut être exposée
- Apprendre les bonnes pratiques à adopter pour protéger son organisation et rappeler les mesures de sécurité de l'entreprise face à de tels évènements (PSSI)

Public : tous publics dans un contexte professionnel ou associatif.

Prérequis : aucun.

Durée et lieu : Sauf demande spécifique du CLIENT, la prestation se déroule dans les locaux du CLIENT.

Contenu détaillé :

Découvrir l'ensemble des activités digitales d'une organisation (appelées "traitements" en termes RGPD), comprendre leurs enjeux de sécurité grâce à une liste de mesures de sécurité

Découvrir les différents évènements ou incidents de sécurité auxquels une organisation peut être confrontée :

- Les principaux types d'attaques ou d'incidents de sécurité : ransomware, violation de données,..
- Comprendre les différentes mesures de sécurité pour s'en prémunir : chiffrement, contrat conforme, authentification 2FA,..

Identifier le vocabulaire RGPD et cyber ainsi que les termes associés

La séance de jeu est un prétexte d'échange avec les bénéficiaires pour qu'ils mettent en relation :

- Les activités de son organisation et les mesures de sécurité que l'on peut associer (Cloud → Authentification forte)
- Les risques et les mesures de sécurité pour s'en prémunir

Finalement, ils peuvent mettre en perspective le contenu de la séance avec la politique de sécurité et les projets de sécurisation menés par son organisation.

Moyens pédagogiques, technique et d'encadrement :

Moyen pédagogique :
La formation est dispensée sur la base d'un jeu de plateau à visée pédagogique.
Formateur
La formation est dispensée par un expert qualifié en sécurité informatique, cybersécurité disposant d'une expérience significative dans le domaine.
Réunion de lancement
La formation peut faire l'objet d'une réunion de lancement organisée avec LE CLIENT avant la formation. Elle peut également prendre la forme d'un pilote avec du personnel volontaire du CLIENT.
Bénéficiaires
Les bénéficiaires de la formation sont identifiés par LE CLIENT aux séances en accord avec MANA CYBER PACIFQUE. Le planning des séances de formation est établi conjointement avec LE CLIENT.
En général, chaque séance de formation est d'une durée de 2h et concerne 12 bénéficiaires au maximum.
Toute organisation différente sera étudiée.
Modalités matérielles
MANA CYBER PACIFIQUE fournit :

- Un Gameplay : un plateau de jeu, des cartes Activité et Évènement, des jetons de sécurisation et un dé
- Une description des principaux évènements de sécurité et recommandations en format numérique (QR Code)
- Un smartphone pour scanner les QR Code du jeu

LE CLIENT fournit :

- Une salle et table de réunion disposant d'un écran et d'un accès internet.
- Un smartphone recommandé par équipe, connecté à Internet pour scanner les QR Code du jeu. Le smartphone de l'animateur pourra être utilisé à la place.

En option, MANA CYBER PACIFIQUE peut fournir une salle de formation selon le besoin du CLIENT.

Évaluation du contrôle des connaissances :

La validation de la formation est réalisée pour chaque bénéficiaire avec à minima l'émargement de sa présence sur la durée de la formation.

Contrôle final des acquis
En option, MANA CYBER PACIFIQUE réalise un contrôle sous la forme d'un questionnaire transmis à l'ensemble des participants pour vérifier les acquis de cette formation.
Le contenu du questionnaire est validé par LE CLIENT et les résultats lui sont remis comme justification des acquis de son personnel.

Mode de validation de la formation

La participation du bénéficiaire à la formation est validée par la remise de la feuille de présence émargée au CLIENT, valant attestation de formation.