Programme de Formation

Maîtriser la Cybersécurité et la Protection des Données en Entreprise

Organisation

Durée : 28 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

La formation s'adresse aux **professionnels en entreprise** souhaitant renforcer leurs connaissances et leurs réflexes en cybersécurité et en protection des données.

Elle concerne notamment les **utilisateurs finaux**, les professionnels des **ressources humaines**, ainsi que les **managers** et les membres de la **direction** impliqués dans la sécurisation des pratiques et la conformité de l'organisation.

Objectifs pédagogiques

-Identifier les principales menaces cyber et comprendre le rôle central du facteur humain dans la survenue des incidents de sécurité.

-Appliquer au quotidien les solutions de sécurité basiques et les bonnes pratiques d'hygiène numérique pour réduire les risques au sein de l'entreprise.

-Réagir efficacement face à un incident de cybersécurité en mobilisant les ressources adéquates et en suivant une chaîne d'alerte adaptée.

-Appliquer les obligations légales liées au RGPD et anticiper les risques futurs grâce à une posture de veille et de stratégie de sécurité, notamment via les modules optionnels.

Description

La formation « Maîtriser la Cybersécurité et la Protection des Données en Entreprise » a pour finalité de permettre aux professionnels en entreprise de sécuriser les données de leur organisation, d'adopter les bonnes pratiques face aux cybermenaces et de se mettre en conformité, du collaborateur à la direction.

Le programme est structuré autour d'un **tronc commun obligatoire** composé des thèmes 1, 2 et 3, complété par deux modules **optionnels** (thèmes 4 et 5). La durée totale est de **3 à 5 jours**, à raison de **1 thème par jour**, selon que l'on suive uniquement le tronc commun ou l'ensemble du parcours.

Le **Thème 1** porte sur la découverte des risques, failles et vulnérabilités. Il aborde le panorama des cybermenaces telles que le phishing, le ransomware et l'ingénierie sociale, la notion de "faille" et le rôle crucial du facteur humain.

-La partie pratique comprend la restitution de l'audit préalable, des ateliers de simulation d'ingénierie sociale, l'analyse concrète d'e-mails et de SMS frauduleux afin de repérer les signaux faibles, ainsi qu'un test de vulnérabilité simplifié sur des cas fictifs.

Le **Thème 2** traite des solutions de sécurité basiques et de l'hygiène numérique. Il couvre les principes d'authentification, les mots de passe et la double authentification, la sécurisation des communications,

notamment sur Wi-Fi public et via VPN, ainsi que la gestion des sauvegardes et des mises à jour.

-La pratique prévoit la configuration d'un gestionnaire de mots de passe, l'activation de la double authentification (2FA) sur divers comptes professionnels et un atelier de sécurisation d'un poste de travail type, incluant le verrouillage et la confidentialité.

Le **Thème 3** est consacré aux ressources, à la gestion d'incident et à la remédiation. Il explique quoi faire en cas d'attaque, la chaîne d'alerte et la présentation des ressources utiles telles que cybermalveillance.gouv.fr, la CNIL et des prestataires locaux.

-Les activités pratiques prennent la forme d'un jeu de rôle sur une simulation de crise, par exemple une attaque par ransomware bloquant les postes, ainsi que d'une rédaction collaborative d'une procédure d'alerte simplifiée à afficher dans les bureaux.

Le **Thème 4**, optionnel, est dédié aux droits, devoirs et à la conformité RGPD. Il présente les grands principes du RGPD, les droits des clients et des salariés, ainsi que les responsabilités civiles et pénales de l'entreprise.

-La mise en pratique comprend un exercice de cartographie des données traitées par l'entreprise, la création ou mise à jour d'un registre de traitement simplifié et un audit de conformité d'un processus métier, comme le recrutement ou un fichier client.

Le **Thème 5**, également optionnel, porte sur l'anticipation des risques futurs et la stratégie. Il traite de l'évolution des menaces, notamment celles liées à l'intelligence artificielle, de la sécurité « by design » et de l'importance de la veille.

-La pratique comprend la mise en place d'outils de veille automatisés, l'élaboration d'un plan d'action cybersécurité post-formation sous forme de feuille de route, ainsi qu'un atelier de sensibilisation interne visant à créer un pitch cyber pour ses collègues.

La formation repose sur une répartition de **30 % de théorie et 70 % de pratique**. Elle peut être réalisée **en consécutif ou en fractionné**, selon l'organisation de l'entreprise.

À l'issue de la formation, une **attestation de compétences** est attribuée aux participants ayant suivi la totalité du parcours. Une **attestation de fin de formation** et un **certificat de réalisation conforme au code du travail** sont également remis.

Les tarifs indiqués sont de **350 € par jour**, soit **1050 €** pour le tronc commun obligatoire, **1500 €** pour la formation complète de 5 jours, et **400 € par thème** pour les thèmes 3 et 4 lorsqu'ils sont suivis en option.

Prérequis

Une **aisance avec l'outil informatique de base** est nécessaire pour suivre la formation dans de bonnes conditions.
Aucune expertise technique préalable en cybersécurité n'est requise.

Modalités pédagogiques

En présentiel

Moyens et supports pédagogiques

Les apprenants disposent des éléments nécessaires à la réalisation des exercices pratiques, notamment des cas fictifs, des exemples d'e-mails et de SMS frauduleux, ainsi que des situations de crise simulées pour les mises en pratique.

Les ateliers mobilisent également des outils et ressources de référence mentionnés dans le programme, tels que cybermalveillance.gouv.fr, la CNIL, des prestataires locaux, ainsi que des supports de travail pour la cartographie des données, le registre de traitement simplifié et le plan d'action post-formation.

Modalités d'évaluation et de suivi

L'évaluation repose sur la validation des acquis en fin de parcours, à travers la participation à l'ensemble des séquences et la réalisation des exercices pratiques intégrés aux différents thèmes.

À l'issue de la formation, les participants ayant suivi la totalité du parcours se voient remettre une **attestation de compétences**, ainsi qu'une **attestation de fin de formation** et un **certificat de réalisation conforme au code du travail**.