ATOUT MAJEUR
CONSEIL | FORMATION

Prenez de la hauteur

Sensibilisation Cybersécurité

Durée de la formation :
3 jours (21h)

Horaires de formation
08h45 – 12h30 / 13h45 – 17h00

Pré-requis
Aucun.

Public visé

Objectifs et compétences visées
À l'issue de cette formation, les participants disposeront des compétences pour comprendre les enjeux actuels de la cybersécurité, ainsi que les pratiques fondamentales à tenir au quotidien.

Organisation
Formation animée en présentiel. Groupe de 3 à 8 personnes. Emargement signée par ½ journée par les stagiaires et le formateur. A l'issue du stage les apprenants renseignent un questionnaire d'évaluation à chaud qui est ensuite analysé par nos équipes.

Le formateur
La prestation est animée par un consultant formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par Atout Majeur.

Moyens techniques et pédagogiques
Alternance entre théorie et pratique. Mise à disposition d'une salle équipée. Support de cours.

Validation des acquis et attestation
Les exercices réalisés permettent de mesurer le degré de compréhension et d'acquisition des compétences visées. Une attestation de formation comportant les résultats de l'évaluation des acquis est délivrée en fin de formation.

Module 1 : Introduction
Tour d'horizon de l'actualité cybersécurité.
Définitions générales.
Présentation des enjeux.

Module 2 : Les Menaces
Ce module propose un tour d'horizon des différentes menaces qui s'imposent à chacun, en s'appuyant notamment sur les référentiels de l'ANSSI. En particulier, les types de menaces suivants sont détaillés :
– Advanced Persistent Threat (APT),
– Cybercriminels,
– Hacktivistes,
– Hacker isolé,
– Script kiddies
L'objectif de cette présentation est de provoquer chez les participants la prise de conscience qu'ils peuvent faire l'objet d'attaques ciblées, mais aussi être la victime d'une criminalité opportuniste, qui frappe à l'aveugle et qui concerne tous les professionnels.

Module 3 : La messagerie (courriels)
La cybercriminalité utilise de façon massive les courriels et les services de messagerie pour contacter les victimes, en faisant un axe privilégié de compromission. Ce module passe ces menaces spécifiques en revue et met en particulier l'accent sur cinq point clés :
– Les courriers indésirables (pourriels / spam),
– Les arnaques au président,
– L'hameçonnage (phishing),
– Les arnaques de type « fraude 419 »,
– Les pièces jointes et leurs danger.
L'objectif est de faire prendre conscience aux participants que la messagerie est un point d'entrée vers le système d'information, et donc un vecteur d'attaque prisé des attaquants. Cela doit appeler une vigilance accrue lors de la réception de courriels et nécessite d'adopter les bons réflexes qui seront abordés en séance.

Module 4 : Utilisation du poste de travail d'Internet
L'utilisation d'un poste de travail au quotidien impose de respecter des bonnes pratiques en matière de cybersécurité pour en assurer la sécurité. Plusieurs axes d'attention sont abordés au sein de ce module :
– La bonne gestion des mots de passe, dans leur choix, leur stockage, leur changement régulier et plus généralement leur cycle de vie ;
– Les supports amovibles et plus particulièrement les dangers que représentent les clés USB en introduisant des virus au sein du système d'information ;
– La sécurité lors de la navigation sur Internet, en particulier la façon dont HTTPS permet de s'assurer de la bonne confidentialité des flux et de l'authenticité des sites visités ;
– Le téléchargement de fichiers, qui peut permettre l'installation de virus sur le poste de travail, ou de logiciels publicitaires ajoutés à des installeurs sur des sites de distribution.
L'objectif de ce module est de proposer aux participants d'acquérir les bonnes pratiques à appliquer au quotidien dans l'utilisation de leur poste de travail. Pour ce faire, il est nécessaire de provoquer chez eux une prise de conscience de leur rôle de premier plan dans le processus de sécurité.

Module 5 : Comportement des utilisateurs

Au-delà de l'utilisation du poste de travail au quotidien, le comportement général des collaborateurs est un élément important de la prise en compte de la sécurité au sein de l'entreprise. Plusieurs aspects, pouvant poser des problèmes de sécurité, sont abordés lors de ce module :

– L'utilisation des réseaux sociaux et les informations stratégiques qui peuvent naïvement être diffusées par des collaborateurs,

– L'ingénierie sociale, et l'ensemble des moyens non techniques pouvant être mobilisés par des attaquants pour obtenir un accès au système d'information,

– Le mélange entre utilisation personnelle et professionnelle, et les risques auxquels cela expose les ressources de l'information.

Les bonnes pratiques de sécurité ne relèvent pas uniquement de problématiques techniques, ni même de l'utilisation des ressources de l'entreprise, d'autres éléments plus généraux peuvent avoir un impact important.

L'objectif de ce module est de provoquer cette prise de conscience chez les participants et de leur transmettre les bons réflexes.

Module 6 : L'itinérance

De nombreux collaborateurs sont amenés à se déplacer fréquemment et à travailler en itinérance. Ce mode de fonctionnement impose des précautions particulières car il peut exposer le collaborateur, voire l'ensemble du système d'information, à une compromission. Ce constat est aggravé par le fait que les personnels se déplaçant fréquemment occupent souvent des postes stratégiques au sein de l'entreprise (dirigeants, responsables, etc.).

Ce module aborde les points d'attention lors de ces déplacements et traite en particulier les quatre aspects suivants :

– L'utilisation des terminaux mobiles, et comment assurer la sécurité des données contenues sur ces appareil qui voyagent beaucoup ;

– L'usage des technologies sans fil (Wi-Fi, Bluetooth) et l'utilisation des points d'accès publics dans les transports ou l'hébergement ;

– La sécurité physique des équipements et les conséquences d'un vol ou d'un accès à un terminal lors d'un déplacement ;

– Le stockage dans le cloud et les implications en matière de sécurité.

L'objectif est de faire prendre conscience aux participants que l'itinérance est une situation particulière, qui les expose de manière accrue aux risques de cybersécurité et impose une vigilance plus importante.

Pour vous inscrire

04.78.14.19.19

contact@atoutmajeur-ra.com / www.atoutmajeurlyon.com

(Mise à jour : 06-2023)