Catalogue thématique : cours sécurité

Formateur d'une société certifié Qualiopi, tous les cours peuvent être financés par un opérateur de compétence !

Cette partie de catalogue est présentée suivant la logique d'un processus de sécurisation décrit ci-dessous.

Établissement d'un état des lieux et une analyse du risque. Réflexion sur **ce que l'on doit protéger, maintenir et/ou rétablir en priorité** (état de ce qui n'est pas indispensable, éventuellement que l'on accepte de perdre) en cas d'une attaque ou d'un problème réel. Définition et prise des mesures ad hoc que l'on est capable de maintenir dans la durée.

Un programme de formation est normalement constitué à partir des cours choisis dans la liste. Des cours non listés sur des problématiques spécifiques peuvent être y intégrés à la demande. Tous les cours, y compris des cours hors liste peuvent être donnés en dehors de tout programme.

Une première séance permet de faire le point des attentes et des connaissances des usagers, d'inventorier les équipements qu'ils utilisent et d'en déduire un programme de formation.

A Définir son périmètre et ses objectifs de sécurité

* Bilan de l'importance du numérique sur le site : liste : des terminaux, des objets connectés, des équipements domotiques ; emploi de équipements ; usagers et connaissance de leurs procédures/habitudes numériques.

* Vérification des points majeurs pouvant comporter des failles de sécurité, éventuellement prise de mesures correctives immédiates.

* Identifier les équipements et les informations sensibles et les risques majeurs. Définir un fonctionnement dégradé acceptable en déduire les mesures et l'investissement (temps) consenti.

B Mettre en place des mesures

Protéger les moyens numériques

- Assurer la sécurité physique des équipements.

Protéger les systèmes d'exploitation, les accès aux flux numériques

- Sécuriser le réseau : la "Box" et les équipements réseaux éventuels.
- Sécuriser son terminal[1] – Contrôler ses accès (réseau, son, vidéo) - savoir réinitialiser et paramétrer chaque terminal employé, mettre en œuvre les fonctionnalités sécurité et maintenance du système d'exploitation du niveau utilisateur.

Protéger les échanges et en limiter les risques

- Utiliser un navigateur (tous les paramétrages, choix des sites, décision de téléchargement, partage d'information), sortir de blocages simples.
- Sécuriser ses échanges : mails, appels téléphoniques et vidéo, achats en ligne ; protection des supports d'informations : cartes, clefs, disques...

Protéger les informations et l'entreprise

- Protéger les informations utiles (conjoncturelles et permanentes), organiser et sauvegarder ses informations, avoir une approche simple et rationnelle des logiciels qui les manipulent (utilité, formats…).
- Protéger son image numérique – Prendre des mesures de déception - Sécuriser son réseau social
- Déjouer les méthodes d'attaques par socio-engineering

Savoir réagir et relancer après un problème numérique

- Se préparer à faire face à des problèmes courants, avoir un plan de reprise sur incident testé et validé.

Connaître l'organisation de la Cybersécurité en France

- Le contexte légal – à qui demander de l'aide
- Les sources d'information

C Assurer la pérennité des mesures

Adopter une hygiène numérique et s'y tenir. Adoption d'un comportement et mise en œuvre de procédures les moins contraignants possible mais restant d'un niveau suffisant pour écarter les problèmes contre lesquels on veut se prémunir ou, au pire, en limiter leur conséquences.

Informer et sensibiliser tous les membres du personnel, les partenaires et l'entourage sur la nécessité et l'application des procédures.

D Cours pour les entreprises effectuant de la prospection et des transactions en ligne

Connaître les obligations légales pour la protection de données collectées et les mesures pratiques associées.

1 Ordinateur tablette et téléphone de tout type, objets connectés