EXPERT·E EN SÉCURITÉ INFORMATIQUE

MOBILITÉ

ORIENTÉ SOLUTION

RESPONSABILITÉ

TRAVAIL EN ÉQUIPE

RÉACTIVITÉ

Les entreprises possèdent de nombreuses données : des données personnelles (fournies quand on utilise un service en ligne comme un réseau social, par exemple), des informations sur leurs clients, leurs fournisseurs, leur personnel, leurs produits, leurs productions (photos, textes, etc.)... Ces données ont énormément de valeur. C'est toi qui veilles à leur **sécurité** et qui les protèges contre les virus, le piratage, l'espionnage industriel, les erreurs de manipulations, etc.

Avant de travailler sur la sécurisation d'un système d'information (ce sont les ressources matérielles et logicielles permettant de stocker l'ensemble des données et de les faire circuler), tu **en identifies les menaces potentielles** et les points faibles.

Ta devise : c'est en connaissant ses ennemis qu'on peut le mieux s'en protéger ! Une fois ton diagnostic terminé, tu proposes et testes des solutions de protection adaptées. Tu configures les pare-feu et les antivirus, tu modères la modification et le droit d'accès aux données, tu sensibilises le personnel, etc.

Tu surveilles et adaptes sans cesse la sécurité contre les nouvelles menaces. Tu te tiens informé·e sur les nouvelles failles existantes. Tu élabores la politique de sécurité en t'assurant de l'engagement de la direction de l'organisation.

Enfin, tu **conseilles** les utilisateur·rices et leur donnes des exemples pratiques pour éviter les incidents les plus habituels.

OUTILS CLÉS

- Des outil d'analyse de risques
- Des outils de sensibilisation (outils de présentation, quizz en ligne, etc.)
- Des logiciels d'analyse de vulnérabilité et de détection d'intrusion
- Un logiciel de traitement de texte et un tableur
- Des outils de gestion documentaire et outils collaboratifs

TÂCHES PRINCIPALES

- Sensibiliser à la sécurité de l'information et à la protection des données à caractère personnel
- Analyser les risques et concevoir un plan de traitement des risques
- Mettre en place un système de gestion de la sécurité, garantissant l'amélioration continue (comme ISO27001)
- Présenter à la direction l'état des lieux de la sécurité dans mon organisation
- Réaliser une veille sur la sécurité, les attaques en cours, etc.

EXPERT·E EN SÉCURITÉ INFORMATIQUE

ÉTUDES ET FORMATIONS

- **Secondaire**
- **Supérieur**
  - **Type Court :** *Bachelier professionnalisant Haute École (3 ans)*
  - **Type Long :** *Master (en Haute École ou université, bachelier + 2 ans)*
- **Promotion sociale**
- **Centres de compétence TIC**
- **Autres organismes de formation**

COMPÉTENCES REQUISES

- Maîtriser des logiciels spécifiques (gestion de bases de données, outils de chiffrement des données,...)
- Maîtriser les aspects liés à la sécurité (normes et sécurité)
- Développer une stratégie de sécurité de l'information, des équipements et des données pour les protéger contre les attaques et les pannes
- Avoir connaissance des systèmes, matériels et logiciels de l'entreprise
- Avoir une connaissance technique des architectures des systèmes, réseaux et équipements
- Avoir le souci du détail et faire preuve de rigueur
- Faire preuve d'intégrité et respecter la confidentialité
- Connaitre l'anglais et l'anglais technique informatique
- Être capable d'anticiper des tendances et des innovations liées à son secteur
- Mener une veille (évolutions technologiques, nouveaux risques, mise à jour des compétences numériques essentielles à son secteur etc.)

PERSPECTIVES DE CARRIÈRE

www.interface3namur.be/orientation/fiches-metiers/