# Fiche métier : Expert en cybersécurité

*Ingénieur sécurité web, Expert sécurité web*

L'expert en cybersécurité est responsable de la sécurité du site Web. Sa mission principale est d'assurer la protection des données. Il doit mettre en échec les tentatives d'intrusion des pirates informatiques (hackers). Pour cela, il évalue le niveau de vulnérabilité du site et établit des solutions pour le sécuriser. Il peut être épaulé dans sa mission par des "hackers éthiques" : ces professionnels de l'intrusion l'aident à déceler les failles. L'expert en sécurité informatique exerce généralement son métier dans une ESN (Entreprise de Services du Numérique).

## Présentation

L'expert en cybersécurité contribue à la mise en oeuvre de la politique de sécurité d'une entreprise. Il doit faire remonter les risques en matière de sécurité informatique.
Il met en place des contrôles de prévention en amont, de détection en simultané, d'explication et de consolidation en aval, pour contrer des intrusions ou des dysfonctionnements des systèmes informatiques.
A ce titre, l'expert en cybersécurité participe à :

· La conception, le déploiement et la mise en oeuvre des architectures matérielles et logicielles
· La rédaction des politiques et des standards de sécurité
· La mise en oeuvre et le respect de la sécurité
· La conformité du réseau par rapport aux attentes des métiers

Ainsi, il oeuvre pour :

· L'intégrité des informations stockées depuis le moment de leur enregistrement
· La disponibilité permanente des logiciels et du système informatique
· Le respect de la confidentialité des échanges d'information
· L'authentification des accès aux documents stockés

## Missions

Responsable au quotidien de la sécurité des systèmes informatiques, l'expert en cybersécurité exerce son métier en véritable chef de projet. Il est soumis à une obligation de résultat. Il contribue par sa mission à la sensibilisation des collaborateurs comme à la formalisation et au respect des règles.
Il contribue, par son expertise, à l'ajustement des niveaux de sécurité aux besoins des différents métiers. Sa mission suppose la compréhension des besoins et des pratiques des différentes typologies d'utilisateurs.
Il donne son aval avant toute modification du réseau ou du système en s'alignant sur la politique de sécurité de l'entreprise. Il contribue à définir et à mettre à jour des processus de sécurité, il est responsable du renouvellement des antivirus systèmes et de la sensibilisation des utilisateurs.

## Domaines et périmètre d'intervention

L'expert en cybersécurité est rattaché au RSSI (Responsable de la Sécurité des Systèmes Informatiques) qui lui-même est généralement rattaché au Directeur Général ou au directeur informatique, selon la taille de l'entreprise.
L'expert en cybersécurité intervient sur l'ensemble du réseau en relation avec les différentes directions ou services.
Ses fonctions s'exercent dans le domaine de la sécurité des réseaux, des serveurs, l'ensemble des domaines des systèmes d'information.
"Hacker éthique", il cherche et repère les failles du système pour mieux les contrer.

## Activités et tâches

*Activités 1*

**Administrer les accès au réseau et aux données**

*Tâches*

Analyser :

· Le fonctionnement de l'ensemble de l'entreprise
· Les besoins d'accès aux informations et au réseau de chaque service

Qualifier la typologie des contributeurs en fonction des accès autorisés :

· Contribution
· Validation
· Administration

*Activités 2*

**Contrer les intrusions et les virus**

*Tâches*

Eviter piratages, vols, destruction de données :

· Achat de pare-feux, d'antivirus
· Mise en place de tunnels sécurisés
· Utilisation de la cryptographie

S'assurer de l'emploi des logiciels de protection par les salariés :

· Indicateurs de suivi
· Mécanismes d'alerte
· Analyse des logs

Mener des audits :

· Recensement des points faibles
· Rédaction des rapports
· Mise à jour des systèmes de protection
· Évolution de la structure du réseau

*Activités 3*

**Mettre en place les processus de sécurité**

*Tâches*

Assurer :

· Efficacité des sauvegardes
· Bon niveau de sécurité des serveurs
· Revue et validation des architectures en lien avec les services techniques

Créer des alertes :

· Notification de mise à jour
· Programmation d'échéance

Mettre en place les process adaptés :

· Sauvegarde des données sur plusieurs serveurs
· Externalisation des données

Lutter contre :

· La sortie d'information de l'entreprise
· Les importations de données potentiellement dangereuses

*Activités 4*

**Assurer la continuité de l'activité**

*Tâches*

Définir avec les différents services le plan de reprise d'activité en cas de :

· Sinistre (incendie, inondation)
· Mouvement social (grèves des transports, occupation des locaux)
· Acte malveillant (sabotage, terrorisme)

Assurer la continuité de l'activité d'un point de vue technique :

· Back up des serveurs
· Accès aux logiciels clés pour l'activité
· Locaux adaptés

Assurer la continuité de l'activité d'un point de vue humain :

· Recenser les métiers et les postes clés
· Mettre en place des back up
· Informer les personnes

*Activités 5*

**Sensibiliser les utilisateurs aux risques**

*Tâches*

*Activités 6*

**Effectuer une veille technologique**

*Tâches*

Identifier les évolutions nécessaires des réseaux et des systèmes de sécurité :

· Adaptations et ajustements
· Modifications
· Sécurité
· Fonctionnalités et services

Anticiper les risques :

· Adaptation et formation
· Renouvellement

« Benchmarker » les réseaux :

· Bonnes pratiques
· Références

## Compétences

*Savoirs*

Connaissance de :

· L'entreprise
· Ses services/produits
· Sa structure
· Son organisation
· Son environnement juridique

Vision globale et complète des systèmes d'information

· De l'entreprise
· Des organisations similaires

Connaissance technique approfondie des :

· Concepts et techniques d'architecture des systèmes et réseaux
· Procédures d'exploitation et des standards d'échange des données employées
· Procédures de Sécurité Informatique
· Systèmes d'exploitation et langages de programmation  associés
· Bases de données

*Savoir faire*

Pratique et expérience rédactionnelle :

· Actualités/brèves
· Articles de fond
· Dossiers

Maîtrise expérimentée « terrain » de l'outil informatique :

· Architecture des systèmes et réseaux
· Procédures d'exploitation et des standards d'échange des données employées
· Procédures de Sécurité Informatique
· Systèmes d'exploitation (Solaris, Linux) et des langages de programmation associés

Maîtriser les outils bureautiques : traitement de texte, tableur, outil de présentation.
Utilisation de logiciels spécifiques :

· Outils de chiffrement de disques durs ou de serveurs
· Pare feu (Firewalls)
· Outils d'identification

Maîtrise de l'anglais courant :

· Ecrit
· Oral

*Savoir être*

Sens de la communication vis-à-vis de différents publics :

· Diplomatie
· Adaptabilité
· Souplesse
· Force de persuasion
· Curiosité d'esprit
· Vif intérêt pour les nouvelles technologies et leurs enjeux

Sens pédagogique :

· Goût pour l'échange
· Aptitude à la communication vis à vis des utilisateurs variés
· Capacité de vulgarisation des enjeux et des risques

Gestion du Stress :

· Excellente gestion des situations d'urgence
· Hiérarchisation pertinente des priorités

Intégrité prouvée :

· "Hacker éthique"
· Respect de la confidentialité
· Rigueur

Sens de l'engagement :

· Implication et motivation
· Goût pour le travail en équipe
· Charisme et entraînement
· Force de proposition


Dernière mise à jour : 24 juin 2014.

## Contributeurs

· CELSA - Ecole des hautes études en sciences de l'information et de la communication, Université Paris IV-Sorbonne - MASTER 2 Ressources humaines et communication :
Marie
de LA ROCHE - mai 2009