FONCTIONS SUPPORT

Informatique

Ingénieur(e)

cyber sécurité

L'ingénieur(e) cybersécurité contribue à la mise en œuvre de la politique de sécurité du système d'information notamment pour tout ce qui concerne les flux avec l'extérieur de l'entreprise (site, messagerie, paiement, identification…) Il/elle est chargé(e) d'évaluer la vulnérabilité du système d'information de l'entreprise, de proposer au RSSI des solutions pour développer la politique de sécurité et d'installer des procédures de protection des réseaux informatiques contre toute intrusion extérieure (virus, hackers...).

Profil de recrutement :

Selon le niveau d'expertise requis, le poste d'ingénieur(e) cybersécurité est ouvert à des personnes confirmées ou de jeunes diplômé(e)s possédant des profils techniques pointus dans le domaine réseaux télécoms (principalement en société de conseil).
Il faut également noter que ce poste a pu parfois être ouvert (chez certains éditeurs) à d'ancien(ne)s hackers/euses repenti(e)s quel que soit leur diplôme.

Formations Parcours recommandés :

- Écoles d'ingénieurs (informatique, télécoms, généralistes...)
- Masters spécialisés en sécurité informatique et/ou télécoms, sécurité des systèmes informatiques et des réseaux, sécurité, cryptologie et codage de l'information...

Pour aller plus loin : http://www.imfis.fr/

Passerelles métier :

- Responsable sécurité informatique
- Responsable de production informatique
- Responsable système réseaux

Pour aller plus loin :
http://www.macarrieredanslapharma.org/

Autres appellations :

- Consultant(e) sécurité des applications web
- Expert(e) sécurité des SI
- Ingénieur(e) / responsable sécurité web
- Auditeur/trice sécurité informatique

ACTIVITÉS

Analyse des risques, études et audit de la sécurité web

- Audition des systèmes de sécurité web, wifi, VoIP, éventuellement avec l'aide de prestataires (tests de pénétration et d'intrusion)
- Analyse des risques, des dysfonctionnements, des failles dans la protection, des marges d'amélioration des systèmes de sécurité
- Définition ou évolution des mesures et des normes de sécurité web et messagerie, en cohérence avec la nature de l'activité de l'entreprise et son exposition aux risques informatiques (politique de mots de passe, choix d'antivirus, certificats...)
- Réalisation des études techniques permettant au RSSI de faire les choix des dispositifs techniques les plus appropriés aux besoins de l'entreprise (firewall, cryptographie, authentification...)

Mise en œuvre et suivi du dispositif de sécurité Internet

- Mise en place des méthodes et des outils de sécurité web adaptés et accompagnement de leur implémentation auprès des utilisateurs/trices
- Élaboration et suivi des tableaux de bord des incidents de sécurité Internet (attaques virales notamment)
- Réparation des dommages causés au SI en cas d'intrusion dans le système ou de contamination par un virus, en analyser les causes et consolider les mesures de sécurité
- Test régulier du bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences (tests d'intrusion notamment)

FONCTIONS SUPPORT

Ingénieur(e)
cyber sécurité

Communication et formation sur les normes de sécurité en évolution des métiers

- Participation à la réalisation du référentiel de sécurité, sur la partie sécurité des réseaux (politique de mots de passe, d'authentification, d'utilisation de certificats, de niveau de sécurité antivirale sur les postes, de définition (censoriale) de sites de confiance…), l'actualiser régulièrement, en assurer la diffusion auprès des utilisateurs/trices et veiller à son application
- Réalisation des supports de formation et en assurer la diffusion principalement auprès des collègues du service informatique
- Sensibilisation des utilisateurs/trices aux risques encourus et suivi de l'application des procédures mises en place
- Mise en place des actions de communication auprès des salarié(e)s de l'entreprise en cas de risque majeur (information sur des types de mails infectés par exemple) ou de dommages au SI causés par une attaque

Veille technologique et réglementaire

- Veille technologique, notamment sur les protocoles, les nouveaux systèmes d'intrusion et les dernières techniques d'attaque sur le web ainsi que les évolutions des protections pour garantir la sécurité du système
- Identification des nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur le réseau mondial...
- Suivi des évolutions juridiques du marché en termes de sécurité Internet, afin de garantir que les mesures de sécurité web soient bien conformes au droit individuel et collectif

COMPÉTENCES CLÉS

←|→ Transverses

- Être curieux/euse et avoir le goût pour la technique
- Avoir le sens de la diplomatie, de l'écoute et de la persuasion
- Être intègre et avoir le sens de l'éthique
- Gérer le stress dans des situations de crise (intrusion, virus, problème de sécurité « matérielle » (incendies, fuites d'eau…) et prioriser les actions à mener
- Être pédagogue
- Travailler avec tous les niveaux d'interlocuteurs/trices de l'entreprise en adaptant son langage et son niveau d'explication

Métier

- Connaître la stratégie de l'entreprise, son organisation, ses métiers et ses enjeux
- Bien connaître le système d'information global, l'urbanisation et l'architecture du SI et des interfaces en applications
- Maîtriser les normes et les procédures de sécurité et les outils et technologies qui s'y rapportent : firewall, antivirus, cryptographie, serveurs d'authentification, tests d'intrusion, PKI, filtrages d'URL...
- Connaître les systèmes d'exploitation (MVS, UNIX, Linux, Windows…) et les langages de programmation associés
- Connaître les outils d'évaluation et de maîtrise des risques (méthode Marion), des réseaux et systèmes
- Connaître les méthodologies (ex : OSSTMM, OWASP…)
- Savoir analyser les risques et proposer des solutions
- Anticiper et avoir de la méthode afin de prévoir les actions à mener en cas de crise
- Connaître les principaux prestataires du marché de la sécurité informatique (éditeurs, sociétés de service...)
- Avoir de bonnes connaissances juridiques en matière de sécurité et de droit informatique
- Maîtriser l'anglais, car 90 % des documents relatifs à la sécurité sont rédigés en anglais

Evolution du métier

L'essor des technologies digitales impacte fortement le secteur de l'industrie pharmaceutique, notamment du fait du potentiel lié au big data, que ce soit en R&D (données massives en santé, données de vie réelle) ou en marketing (CRM, actions de communication ciblées…). Cela induit une vigilance particulière quant à l'intégrité et à la sécurisation des données. A l'instar des autres secteurs, les outils et process de travail se digitalisent également, nécessitant une protection accrue des systèmes. L'ingénieur(e) cybersécurité agit en prévention de ces risques, à la fois par la mise en place de solutions techniques et par la contribution à l'acculturation des collaborateurs/trices aux bonnes pratiques permettant de les limiter, en adoptant une approche pédagogique.

Les entreprises pharmaceutiques sont particulièrement exposées au risque de vol de données sur les avancées de leurs projets de R&D ou les formules de médicaments. Cette montée des risques oblige les ingénieur(e)s cybersécurité à alerter l'ensemble des métiers de l'entreprise sur les conséquences business et stratégiques des attaques. Ils/elles peuvent être de plus en plus amené(e)s à trancher entre les impératifs business et l'évaluation des risques encourus.