FONCTIONS SUPPORT

Informatique

leem
les entreprises du médicament

Ingénieur(e)
cyber sécurité

L'ingénieur(e) cyber sécurité 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) sécurité est ouvert à des personnes confirmées ou de jeunes diplômé(e)s possédant des profils techniques pointus dans le domaine réseau télécoms (principalement en société de conseil). Il faut également noter que ce poste a pu parfois être ouvert (chez certains éditeurs) à d'ancien(e)s hackers 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…

Passerelles métier :

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

Autres appellations :

- Expert(e) sécurité des SI
- Consultant(e) sécurité des applications web
- 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 utilisateur(trice)s
- 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)

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 utilisateur(trice)s et veiller à son application
- Réalisation des supports de formation et en assurer la diffusion principalement auprès des collègues du service informatique
- 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

FONCTIONS SUPPORT

Ingénieur(e)
cyber sécurité

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(se) et avoir le goût pour la technique, car l'expert(e) sécurité doit être au courant en permanence des nouveaux risques et des nouvelles parades (virus et antidotes)
- Avoir le sens de la diplomatie, de l'écoute et de la persuasion pour convaincre les utilisateur(trice)s des risques encourus et du bien-fondé des procédures mises en place
- Être intégrité et éthique, car il/elle a accès à toutes les données sensibles de l'entreprise et il/elle doit maintenir un bon niveau de confidentialité
- Gérer le stress dans des situations de crise (intrusion, virus, problème de sécurité « matérielle » (incendies, fuites d'eau…) et à prioriser les actions à mener
- Anticiper et avoir de la méthode afin de pouvoir prévoir les actions à mener en cas de crise
- Analyser afin de planifier minutieusement les risques et leurs parades
- Proposer les évolutions pour la stratégie, ainsi que pour les pratiques
- Être pédagogue pour vulgariser les risques et les enjeux de la sécurité à tous les niveaux dans l'entreprise
- Travailler avec tous les niveaux d'interlocuteur(trice)s de l'entreprise en adaptant son langage et son niveau d'explication à la population avec laquelle l'ingénieur(e) sécurité web est amené(e) à travailler

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…)
- 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

Ingénieur(e)
cyber sécurité

L'essor du Web collaboratif, du cloud computing, des applications Web mobile, du paiement en ligne, la multiplication des standards (pour les applications mobiles) ainsi que certains exemples récents d'intrusions sur des sites d'entreprises a priori sécurisées, y compris d'émetteurs de certificats, expliquent l'importance que prennent les problématiques de sécurité informatique. Un nombre important de PME ont pendant longtemps négligé les investissements dans ce domaine, étant convaincues que l'usage d'un anti-virus et d'un firewall se révélait suffisant. La prise en compte du « risque informatique » est relativement récente et certaines entreprises ont pu se rendre compte qu'il était difficile de chiffrer les conséquences de pertes ou de corruption de données.

Certains secteurs, dont le secteur bancaire et des moyens de paiement sont en pointe dans ce domaine pour des raisons évidentes. Le risque zéro dans ce domaine n'existe pas et l'ingéniosité des hackers permet de penser que ce type de poste devrait encore se renforcer dans les années à venir. Par ailleurs, la montée des risques, oblige les ingénieur(e)s à alerter l'ensemble des métiers de l'entreprise sur les conséquences business et stratégiques des attaques. Il/elle peut être de plus en plus amené(e) à trancher entre les impératifs business et l'évaluation des risques encourus. Ainsi, sa posture évolue vers celle de pédagogue (communication/formation) pour sensibiliser les salarié(e)s mais aussi d'arbitre entre business et risques.

Observatoire paritaire Métiers des Entreprises du Médicament
APEC
En partenariat avec l'APEC