PORTNET
الشباك الوطني الوحيد لتبسيط مساطر التجارة الخارجية
GUICHET UNIQUE NATIONAL DES PROCÉDURES DU COMMERCE EXTÉRIEUR

INGENIEUR SECURITE RESEAU
(REF : ISR/19)

Rattaché au Responsable des Infrastructures au sein de la Direction des Systèmes d'Information de PORTNET S.A, l'Ingénieur Sécurité Réseau 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 est chargé d'évaluer la vulnérabilité du système d'information de l'entreprise, de proposer des solutions pour développer la politique de sécurité et d'installer des procédures de protection des réseaux informatiques contre toute intrusion extérieure (virus, hackers...).

ACTIVITES

Auditer le système de sécurité web, wifi, VoIP, éventuellement avec l'aide de prestataires (tests de pénétration et d'intrusion).
Analyser les risques, les dysfonctionnements, les failles dans la protection, les marges d'amélioration des systèmes de sécurité.
Définir ou faire évoluer les mesures et les 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…).
Réaliser les études techniques permettant de faire les choix des dispositifs techniques les plus appropriés aux besoins de l'entreprise (firewall, cryptographie, authentification...).

Mettre en place les méthodes et outils de sécurité web adaptés et accompagner leur implémentation auprès des utilisateurs.
Élaborer et suivre les tableaux de bord des incidents de sécurité Internet (attaques virales notamment).
Réparer les 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.
Tester ou faire tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences (tests d'intrusion notamment).

Participer 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 et veiller à son application.
Réaliser des supports de formation et en assurer la diffusion principalement auprès des collègues du service informatique.
Mettre en place des actions de communication auprès des salariés 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.

Assurer une 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.
Identifier les nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur le réseau mondial...
Suivre les 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.

PROFIL RECHERCHE

De formation supérieure Bac+5, école d'ingénieurs ou universitaire.
Expérience significative d'au moins 2 ans sur un poste similaire.
Solides compétences en :

- FireWall (Fortigate, Fortinet, SOFOS) ;
- Load balancer ;
- Balalbit ;
- WSUS.

Rigueur, autonomie et organisation
Bon relationnel et esprit de travail en équipe.
Une bonne connaissance des processus logistiques et supply chain est un atout.
Langues : Arabe, Français, Anglais.