Quel est le rôle de la House of Cybersecurity et quelles sont les obligations des RH en matière de sécurité numérique au Luxembourg ?

Réponse courte

La House of Cybersecurity (HoC) est l'organisme national chargé de coordonner la cybersécurité au Luxembourg. Elle centralise les initiatives publiques et privées, diffuse des informations, propose des formations et sert de point de contact unique pour la prévention, la gestion et la réponse aux incidents de cybersécurité. Les RH peuvent solliciter la HoC pour des conseils, des outils d'auto-évaluation, des guides et des formations adaptées.

Les responsables RH ont l'obligation de veiller à la sécurité des systèmes d'information, à la protection des données personnelles et à la prévention des risques numériques, conformément au Code du travail, à la législation sectorielle et au RGPD. Ils doivent intégrer les recommandations de la HoC dans leurs procédures internes, assurer la traçabilité des accès, documenter les actions de prévention et de formation, et notifier les incidents de sécurité. La négligence en la matière peut engager la responsabilité civile et pénale de l'employeur.

Définition

La House of Cybersecurity (HoC) est l'organisme national de coordination en cybersécurité au Luxembourg. Elle a pour mission de centraliser les initiatives publiques et privées visant à renforcer la résilience numérique des organisations, en agissant comme point de contact unique pour la prévention, la gestion et la réponse aux incidents de cybersécurité. La HoC assure également la diffusion d'informations, la sensibilisation et la formation des acteurs économiques, y compris les employeurs et les services des ressources humaines.

Conditions d'exercice

Toutes les entreprises établies au Luxembourg, quel que soit leur secteur ou leur taille, sont concernées par les actions de la HoC. Les employeurs sont soumis à des obligations légales en matière de sécurité des systèmes d'information, de protection des données à caractère personnel et de prévention des risques numériques, conformément au Code du travail et à la législation sectorielle. Les responsables RH doivent veiller à la conformité des pratiques internes avec les recommandations et alertes publiées par la HoC, notamment en matière de gestion des accès, de confidentialité des données du personnel et de prévention des fraudes numériques.

Modalités pratiques

Les services RH peuvent solliciter la HoC pour obtenir des conseils, participer à des sessions de sensibilisation ou signaler des incidents de sécurité. La HoC met à disposition des outils d'auto-évaluation, des guides sectoriels et des formations adaptées aux besoins des entreprises. Les RH doivent intégrer les recommandations de la HoC dans leurs procédures internes, notamment lors de l'intégration de nouveaux collaborateurs, de la gestion des accès informatiques et de la mise en place de politiques de télétravail. Il est également nécessaire d'assurer la traçabilité des accès aux données sensibles et de documenter toutes les actions de prévention et de formation.

Pratiques et recommandations

Il est recommandé aux responsables RH de :

- Formaliser des politiques internes de sécurité numérique, en s'appuyant sur les ressources de la HoC.
- Sensibiliser régulièrement le personnel aux risques cyber (phishing, usurpation d'identité, fuites de données).
- Mettre en place des procédures strictes de gestion des mots de passe et des accès aux systèmes RH.
- Limiter les droits d'accès aux données personnelles au strict nécessaire et assurer leur traçabilité.
- Collaborer avec la HoC pour organiser des audits internes et des exercices de simulation d'incidents.
- Intégrer la cybersécurité dans le processus de recrutement, en vérifiant la fiabilité des outils numériques utilisés pour la gestion des candidatures et des dossiers du personnel.
- Garantir l'égalité de traitement et la non-discrimination dans l'application des mesures de cybersécurité.

Cadre juridique

Les obligations en matière de sécurité numérique et de cybersécurité pour les employeurs et les RH au Luxembourg reposent sur les textes suivants :

- **Code du travail luxembourgeois** :
    - Article L.261-1 et suivants : obligations générales de sécurité et de santé au travail, incluant la sécurité des systèmes d'information.
    - Article L.121-6 : égalité de traitement et non-discrimination dans l'accès aux outils numériques et la gestion des données.
    - Article L.261-2 : obligation de formation et d'information des salariés sur les risques professionnels, y compris numériques.

- **Loi du 28 mai 2019 relative à la sécurité des réseaux et des systèmes d'information du secteur privé**, telle que modifiée par la loi du 15 juillet 2023 :
    - Obligation de notification des incidents de sécurité.
    - Mise en œuvre de mesures techniques et organisationnelles appropriées.

- **Loi du 1er août 2018 sur la protection des personnes à l'égard du traitement des données à caractère personnel** :
    - Articles 32 à 34 : sécurité du traitement, notification des violations de données à caractère personnel.

- **Règlement (UE) 2016/679 (RGPD)** :
    - Article 32 : sécurité du traitement.
    - Article 33 : notification des violations de données à caractère personnel.

- **Obligation de traçabilité et d'encadrement humain** dans la gestion des systèmes automatisés et des outils numériques utilisés par les RH.

La négligence en matière de cybersécurité peut engager la responsabilité civile et pénale de l'employeur, notamment en cas de fuite de données personnelles des salariés. Il est impératif de documenter toutes les actions de prévention, de formation et de sensibilisation menées en collaboration avec la House of Cybersecurity, et de garantir la traçabilité des accès et des interventions sur les systèmes RH.