INSTITUT LUXEMBOURGEOIS DE RÉGULATION

6 mesures de sécurité fondamentales

SERVICE NISS

Utilisez les 6 mesures de sécurité fondamentales non seulement comme point de départ vers la conformité à la directive NIS 2, mais surtout pour vous protéger des risques et des menaces cyber toujours plus sophistiquées !

Gérez tous vos actifs et les risques y relatifs

(Gestion des actifs, gestion des risques, sécurité dans la chaîne d'approvisionnement)

- Créer et gérer un inventaire détaillé avec tous les actifs (logiciels, matériels, …) y compris les actifs sous-traités
- Identifier, analyser, évaluer et traiter les risques les plus importants
- Considérer les fournisseurs et les prestataires de services dans le processus de gestion des risques
- Intégrer la sécurité dans tout le cycle de vie des actifs (sécurité par défaut)
- Surveiller et évaluer l'efficacité des mesures de gestion des risques

1

Protégez vos systèmes, réseaux et les communications

(Sécurité des systèmes et des réseaux, communications sécurisées)

- Mettre en œuvre des équipements et logiciels de sécurité (firewall, anti-virus, VPN, ...)
- Configurer les paramètres et fonctionnalités de sécurité (ports, services, protocoles, ...)
- Utiliser des solutions de cryptographie et de chiffrement
- Sécuriser vos connections WiFi et les équipements nomades (clés USB, smartphones, ordinateurs portables, …)
- Surveiller les activités et la performance et enregistrer les évènements

2

Sécurisez vos accès logiques et physiques

(Contrôle d'accès, authentification)

- Utiliser des mots de passes forts et uniques et des solutions d'authentification à plusieurs facteurs (MFA)
- Limiter les droits d'accès aux collaborateurs et aux systèmes
- Attribuer et autoriser les droits d'accès aux collaborateurs seulement sur base de leurs rôles et responsabilités
- Protéger et surveiller les accès aux environnements physiques (bâtiments, serveurs, data center, équipements, ...)
- Revoir régulièrement et, si nécessaire, modifier ou supprimer les droits d'accès

3

Gardez vos logiciels et systèmes à jour

(Gestion des vulnérabilités, gestion des correctifs et mises à jour)

- Utiliser des outils d'identification et d'analyse des vulnérabilités, tout en assurant leur suivi
- Appliquer les correctifs le plus rapidement possible, après avoir sauvegardé les données
- Surveiller les correctifs et les mises à jour publiés par les fournisseurs ou prestataires de services
- Tester et évaluer les correctifs et les mises à jour avant de les installer dans les systèmes de production
- Évaluer les impacts et les conséquences des changements envers les utilisateurs et les activités critiques de l'entité

4

Gérez vos incidents et assurez la continuité de vos activités

(Gestion des incidents, gestion de la continuité des activités)

- Réaliser régulièrement des sauvegardes des données et les tester
- Mettre en œuvre un plan pour gérer les incidents
- Mettre en œuvre un plan de continuité et de reprise des activités et le tester
- Établir et maintenir une liste des contacts clés (support technique, expertise sécurité, parties prenantes externes, …)
- Établir et maintenir des relations avec les autorités nationales compétentes

5

Sensibilisez et formez vos collaborateurs

(Sensibilisation et formation à la cybersécurité)

- Sensibiliser régulièrement les collaborateurs sur les menaces et les risques, ainsi que les mesures à prendre en compte
- Informer les collaborateurs et les parties tierces (consultants, fournisseurs, ...) des règles de sécurité de votre entité
- Offrir aux collaborateurs techniques (spécialistes réseaux, …) des formations sur la sécurité en lien avec leur fonction
- Former les membres des organes de direction aux risques cyber et à leurs rôles et responsabilités
- Tester et évaluer les connaissances des collaborateurs en matière de sécurité de l'information

6

Les images ont été générées par un système IA sur https://www.craiyon.com/