CYBERSECURITY POLICY

LA SÉCURITÉ CHEZ NRB : UNE PRIORITÉ

NRB héberge et prend en charge les systèmes informatiques d'organisations essentielles au fonctionnement de notre pays, que ce soit dans le secteur public, le secteur privé ou le secteur des soins de santé. Nous avons donc la responsabilité cruciale d'assurer la continuité et la qualité de nos services. La sécurité des systèmes d'information et des données constitue naturellement un des éléments prioritaires dans la prestation de nos services et dans la protection de nos infrastructures.

COMMENT NRB PARTICIPE-T-ELLE À LA PROTECTION DE SES CLIENTS CONTRE LES CYBERMENACES ?

- Grâce à la confiance renforcée par la certification ISO27001, attribuée par une société d'audit indépendante, qui atteste de l'intégration de la sécurité dans l'organisation et de la mise en place de mesures destinées au maintien de la confidentialité, de l'intégrité et de la disponibilité des données.
- En utilisant un cadre couvrant tous les aspects de la sécurité, qui permet à NRB de répondre aux menaces actuelles et futures.

Source : NIST

CE CADRE EST BASÉ SUR 5 FONCTIONS QUI ORGANISENT LES ACTIVITÉS DE CYBERSÉCURITÉ :

Identifier : développer une compréhension commune pour gérer les risques sur les données, les actifs et les systèmes.

Protéger : développer et mettre en œuvre les contremesures appropriées pour assurer la protection et la disponibilité des services critiques.

Détecter : développer et mettre en œuvre les activités afin de détecter les occurrences d'événement de cybersécurité.

Réagir : développer et mettre en œuvre les activités appropriées pour donner suite à un événement de cybersécurité détecté.

Récupérer : développer et mettre en œuvre les activités appropriées pour maintenir la résilience et restaurer les services et données perturbés par un événement cybersécurité.

EN PRATIQUE CHEZ NRB, COMMENT CE CADRE EST-IL IMPLÉMENTÉ ?

FONCTION	OBJECTIFS ET ACTIVITÉS
Identifier	- NRB dispose d'une politique de sécurité et d'une organisation avec 3 lignes de défense (sécurité opérationnelle, gouvernance/pilotage et audit interne) - Les activités de NRB sont conformes au RGPD*, à la directive NIS* et à la norme ISO27001. - NRB dispose d'un processus de gestion des risques avec une méthodologie propre, inspirée de la norme ISO27005, ainsi que d'analyses récurrentes et de plans d'actions. - NRB effectue une évaluation continue des nouvelles cybermenaces. - Sur base des informations fournies par le client, NRB intègre les services et assets critiques du client dans ses processus. - Avec le client, NRB définit l'organisation et les canaux de communication pour ce qui concerne la sécurité.
Protéger	- Les datacenters de NRB ont été conçus et fonctionnent pour assurer la sécurité et la continuité (niveau équivalent à Tier 3+ Uptime Institute). - Le stockage de données est sécurisé avec notamment du cryptage. - Les données sont sauvegardées et l'intégrité des sauvegardes est vérifiée. - Des plans de *disaster recovery* sont en place et testés au moins annuellement. - Le *hardening* et le *patching* sont assurés à travers notre processus de gestion des vulnérabilités. - Tous les collaborateurs de NRB suivent une formation continue en matière de sécurité.
Détecter	- Le réseau de NRB est surveillé en permanence et tout comportement anormal par rapport à la base de référence définie génère une alerte. - Les activités des utilisateurs finaux sont surveillées afin de détecter les tentatives d'accès anormales. - Les événements de sécurité sont collectés sur les sources critiques et corrélées par notre outil de « Security Information and Event Management ». - Les évènements et alertes de sécurité sont analysés 24/7 par notre Security Operation Center. - Des dispositifs anti-malware sont actifs sur les postes de travail, les passerelles mail/web et les firewalls. - Des scans de vulnérabilités sont effectués de manière récurrente.

Réagir	- NRB a mis en place des processus de gestion des incidents et de gestion de crise pour traiter les cyberincidents de manière efficace et assurer la continuité des services. - NRB est en relation avec des partenaires (Cert.be, CCB, MSSP) pour échanger les informations relatives aux menaces et incidents. - NRB effectue les investigations et analyses forensiques en collaboration avec des prestataires externes spécialisés. - Les incidents sont analysés et catégorisés afin d'exécuter les plans d'actions prédéfinis. - Les incidents sont confinés et mitigés afin de limiter leurs impacts.
Récupérer	- Les plans de récupération sont exécutés pendant ou après résolution de l'incident. - Les relations avec les parties externes sont gérées dans le cadre du processus de crise. - Après résolution et récupération, les incidents et les actions effectuées sont analysées afin d'améliorer les processus de gestion et les plans d'actions.

*RGPD (Règlement général de protection des données) : L'objectif du RGPD est d'encadrer les pratiques en matière de collecte, de traitement et d'utilisation des données à caractère personnel.

*NIS (Network and Information system Security) : La directive NIS est un cadre réglementaire pour renforcer la cybersécurité des Fournisseurs de service numérique (FSN), c'est-à-dire essentiellement des entreprises de cloud et de moteurs de recherche.