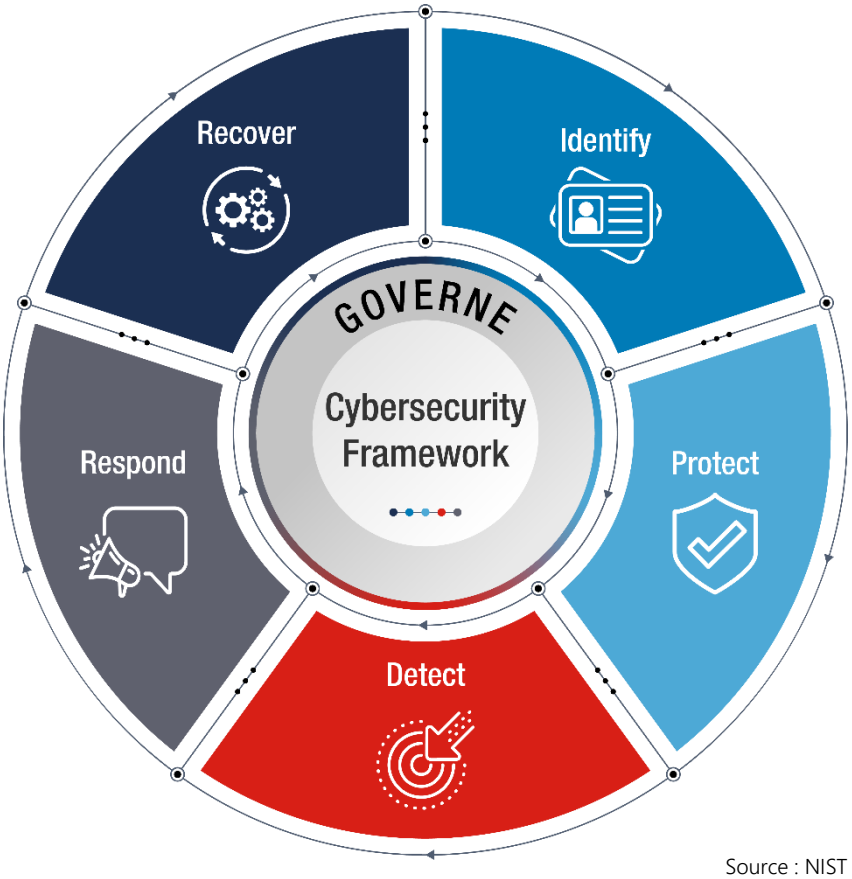
CYBERSECURITY POLICY

LA SÉCURITÉ CHEZ NRB : UNE PRIORITÉ !

NRB héberge et prend en charge les systèmes informatiques d'organisations essentielles au niveau européen, 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 fourniture 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 6 FONCTIONS QUI ORGANISENT LES ACTIVITÉS DE CYBERSÉCURITÉ :

Gouverner : Permettre de savoir ce que NRB peut faire pour atteindre et hiérarchiser les résultats des cinq autres fonctions dans le contexte de sa mission et des attentes de ses parties prenantes.

Identifier : Développer une compréhension des actifs de l'organisation, de ses fournisseurs et des risques de cybersécurité associés. Identifier les possibilités d'amélioration qui soutiennent la gestion du risque de cybersécurité.

Protéger : Développer et mettre en œuvre les contremesures appropriées afin de prévenir ou de réduire la probabilité et l'impact des événements négatifs en matière de cybersécurité sur les actifs et services critiques.

Détecter : Développer et mettre en œuvre les activités afin de découvrir et d'analyser les anomalies, les indicateurs de compromission et d'autres événements potentiellement défavorables qui peuvent indiquer que des attaques et des incidents de cybersécurité sont en cours.

Réagir : développer et mettre en œuvre les activités appropriées pour permettre de contenir les effets des incidents de cybersécurité.

Récupérer : développer et mettre en œuvre les activités appropriées pour favoriser le rétablissement rapide des opérations normales afin de réduire les effets des incidents de cybersécurité, et de permettre une communication appropriée pendant les efforts de rétablissement.

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

FONCTION	OBJECTIFS ET ACTIVITÉS
Gouverner	→ Une gouvernance de sécurité structurée en 3 lignes de défense est implémentée. → Une stratégie de cybersécurité alignée sur les objectifs organisationnels, en tenant compte des risques et des réglementations est définie. → Les activités de NRB sont conformes au RGPD*, à la directive NIS2* et à la norme ISO27001. → Les politiques et les procédures de cybersécurité sont revues régulièrement afin de répondre aux évolutions des menaces et des exigences réglementaires. → Les performances des mesures de sécurité sont surveillées et évaluées régulièrement via la remontée des KPI d'entreprise au Comité Exécutif. → Une culture de cybersécurité est promue et encouragée, afin que tous les collaborateurs reconnaissent leur rôle dans la protection des actifs numériques.

Identifier	→ 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 recense et maintient un inventaire de tous les actifs (dispositifs, systèmes, données) dans une base de données centralisée en incluant leur niveau d'importance dans le système d'information. → NRB inventorise les relations entre les différents systèmes dans une CMDB afin d'avoir une vue globale des dépendances et des impacts potentiels sur les systèmes. → Sur base des informations fournies par le client, NRB intègre les services et assets critiques du client dans ses processus. → NRB évalue les risques de cybersécurité associés aux partenaires, fournisseurs et autres tiers, et met en place des mesures pour les gérer. → Avec le client, NRB définit l'organisation et les canaux de communication pour ce qui concerne la sécurité. → NRB effectue des Pentests régulier (au moins 1 fois/an) afin d'évaluer le niveau de maturité des processus de protection et de détection.
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 chiffrement fort. → Les données sont sauvegardées et l'intégrité des sauvegardes est vérifiée. → Les données critiques sont sauvegardées au moyen de backups immuables. → Des plans de *business continuity* et 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. → Les systèmes sont protégés avec des pare-feux et anti-malwares (XDR) qui remontent les alertes vers notre SIEM/SOC. → Une gestion des identités rigoureuse et automatisée via notre outil IAM ainsi qu'un contrôle d'accès rigoureux, incluant l'authentification multi-facteurs, sont mis en place pour limiter l'accès des collaborateurs aux seuls systèmes et informations nécessaires. → Tous les collaborateurs de NRB suivent des formations continues et adaptées en matière de sécurité sur une plateforme d'e-learning.
Détecter	→ Le réseau et les systèmes de NRB sont surveillés 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 et corrélés 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 audits techniques sont effectués de manière récurrente afin d'identifier les faiblesses potentielles → Une veille constante est effectuée afin d'identifier les nouvelles menaces et de les intégrer dans nos outils et processus.

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. → Des protocoles de communication sont mis en place pour informer les parties prenantes internes et externes en temps opportun avant, pendant et après un incident. → 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. → Le CSIRT (Computer Security Incident Response Team) NRB effectue les investigations et analyses forensiques nécessaires, en collaboration avec des prestataires externes spécialisés si nécessaire. → Pour chaque incident majeur, une analyse post-mortem est effectuée pour identifier les leçons apprises et mettre à jour les processus et les stratégies de réponse en conséquence. → NRB est en relation avec des partenaires (Cert.be, CCB, MSSP) pour échanger les informations relatives aux menaces et incidents.
Récupérer	→ Les plans de récupération sont exécutés pour restaurer les services, les systèmes et les opérations critiques après un incident de cybersécurité. → Les priorités sont établies pour le rétablissement des fonctions essentielles et des capacités opérationnelles afin de minimiser les interruptions de service. → Les relations avec les parties internes et externes sont maintenues tout au long du processus de récupération pour assurer la transparence et la confiance. → 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.

*NIS2 (Network and Information system Security) : La directive NIS2 est un cadre réglementaire qui vise à renforcer la résilience des infrastructures critiques, à améliorer la réponse aux cyberincidents et à harmoniser les pratiques de cybersécurité au sein des États membres de l'UE.