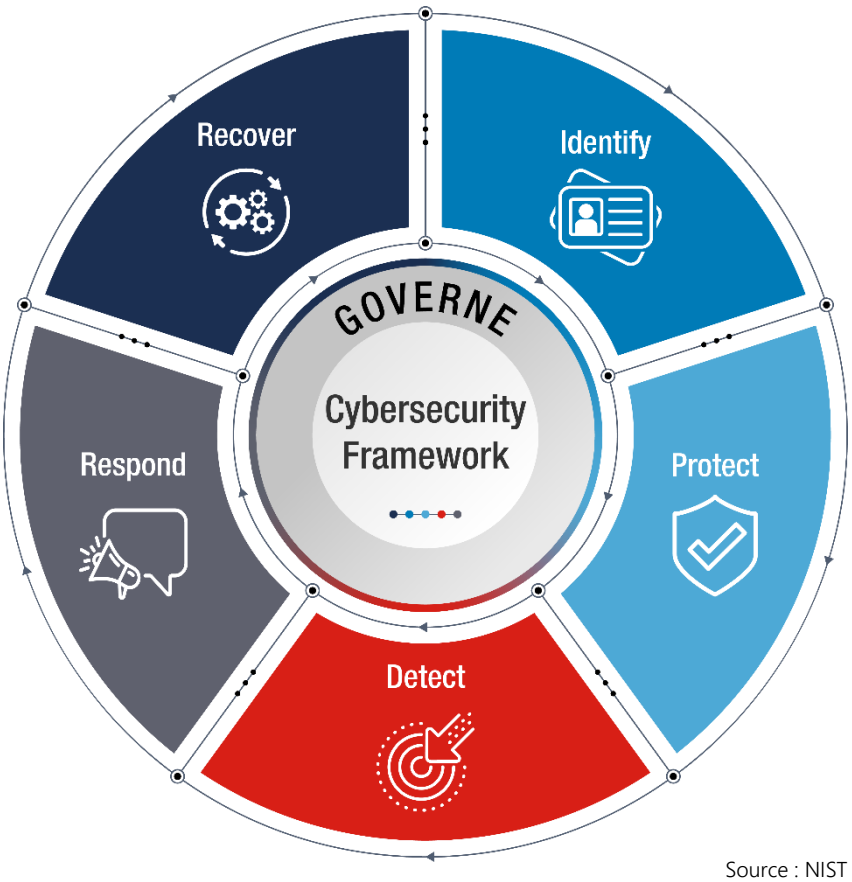
CYBERSECURITY POLICY

VEILIGHEID: EEN PRIORITEIT BIJ NRB!

NRB host en beheert de IT-systemen van organisaties die essentieel zijn op Europees niveau of het nu gaat om de publieke, private of de gezondheidszorgsector. We hebben daarom de cruciale verantwoordelijkheid om de continuïteit en de kwaliteit van onze diensten te waarborgen. De beveiliging van informatiesystemen en data is uiteraard een van de topprioriteiten bij het leveren van onze diensten en de bescherming van onze infrastructuren.

HOE HELPT NRB HAAR KLANTEN TE BESCHERMEN TEGEN CYBERDREIGINGEN?

- Dankzij het vertrouwen dat wordt versterkt door de ISO27001-certificering, toegekend door een onafhankelijk auditbedrijf, dat getuigt van de integratie van beveiliging in de organisatie en de implementatie van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van data te behouden.
- Door een kader te gebruiken dat alle aspecten van beveiliging omvat, kan NRB reageren op huidige en toekomstige bedreigingen.



Source : NIST

DIT RAAMWERK IS GEBASEERD OP 6 FUNCTIES DIE CYBERBEVEILIGINGSACTIVITEITEN ORGANISEREN:

Beheren: Vaststellen wat NRB kan doen om de resultaten van de andere vijf functies te bereiken en deze te prioriteren in de context van zijn missie en de verwachtingen van zijn stakeholders.

Identificeren: Inzicht ontwikkelen in de bedrijfsmiddelen van de organisatie, haar leveranciers en de bijbehorende risico's voor cyberbeveiliging. Mogelijkheden voor verbetering identificeren die het risicobeheer voor cyberbeveiliging ondersteunen.

Beschermen: Passende tegenmaatregelen ontwikkelen en implementeren om de kans op en de impact van negatieve cyberbeveiligingsgebeurtenissen op kritieke bedrijfsmiddelen en diensten te voorkomen of te verkleinen.

Detecteren: Activiteiten ontwikkelen en implementeren om anomalieën, compromitteringsindicatoren en andere potentieel ongunstige gebeurtenissen te ontdekken en te analyseren die erop kunnen wijzen dat er cyberbeveiligingsaanvallen en -incidenten aan de gang zijn.

Reageren: Passende activiteiten ontwikkelen en uitvoeren om de gevolgen van cyberbeveiligingsincidenten in te dammen.

Recupereren: Ontwikkelen en implementeren van passende activiteiten ter ondersteuning van het snelle herstel van normale activiteiten om de effecten van cyberbeveiligingsincidenten te beperken, en passende communicatie mogelijk maken tijdens herstelinspanningen.

HOE WORDT DIT KADER IN DE PRAKTIJK GEÏMPLEMENTEERD BIJ NRB?

FUNCTIE	DOELSTELLINGEN EN ACTIVITEITEN
Beheer	→ Beveiligingsbeheer gestructureerd rond 3 verdedigingslinies is geïmplementeerd → Een cyberbeveiligingsstrategie afgestemd op de organisatorische doelstellingen en rekening houdend met risico's en regelgeving. → De activiteiten van NRB voldoen aan de AVG*, de NIS2*-richtlijn en de ISO27001-norm. → Het beleid en de procedures voor cyberbeveiliging worden regelmatig herzien om gelijke tred te houden met veranderende bedreigingen en wettelijke vereisten. → De prestaties van beveiligingsmaatregelen worden regelmatig gecontroleerd en beoordeeld door KPI's voor het bedrijf te rapporteren aan het uitvoerend comité. → Een cultuur van cyberbeveiliging wordt bevorderd en aangemoedigd, zodat alle werknemers hun rol in het beschermen van digitale assets erkennen.

dentificeer	→ NRB heeft een risicobeheerproces met een eigen methodologie, geïnspireerd op de ISO27005-norm, evenals terugkerende analyses en actieplannen. → NRB identificeert en onderhoudt een inventaris van alle bedrijfsassets (apparaten, systemen, gegevens) in een gecentraliseerde database, inclusief hun belang voor het informatiesysteem. → NRB inventariseert de relaties tussen de verschillende systemen in een CMDB om een globaal overzicht te geven van afhankelijkheden en mogelijke gevolgen voor systemen. → Op basis van de informatie van de klant integreert NRB de kritische diensten en bedrijfsmiddelen van de klant in zijn processen. → NRB beoordeelt de cyberbeveiligingsrisico's van partners, leveranciers en andere derden en neemt maatregelen om deze risico's te beheersen. → NRB bepaalt samen met de klant de organisatie en communicatiekanalen met betrekking tot veiligheid. → NRB voert regelmatig Pentests uit (minimaal één keer per jaar) om de maturiteit van zijn beschermings- en detectieprocessen te beoordelen.
Beschermen	→ De datacenters van NRB zijn ontworpen en werken om veiligheid en continuïteit te garanderen (niveau gelijk aan Tier 3+ Uptime Institute). → De dataopslag is beveiligd, vooral door sterke versleuteling. → Er wordt een back-up gemaakt van de gegevens en de integriteit van de back-ups wordt gecontroleerd. → Van kritieke data wordt een back-up gemaakt met behulp van identieke back-ups. → Plannen voor *business continuity* en *disaster recovery* zijn aanwezig en worden ten minste jaarlijks getest. → *Hardening* en *patching* worden gewaarborgd via ons proces voor kwetsbaarheidsbeheer. → De systemen worden beschermd door firewalls en anti-malware (XDR) die waarschuwingen sturen naar ons SIEM/SOC. → Streng, geautomatiseerd identiteitsbeheer via onze IAM-tool en strikte toegangscontrole, waaronder meerstapsverificatie, wordt ingesteld om de toegang van medewerkers te beperken tot alleen de systemen en informatie die ze nodig hebben. → Alle medewerkers van NRB krijgen doorlopend beveiligingsopleidingen op maat via een e-learningplatform.
Detecteren	→ Het netwerk en de systemen van NRB worden voortdurend bewaakt en elk abnormaal gedrag ten opzichte van de gedefinieerde baseline genereert een waarschuwing. → Activiteiten van eindgebruikers worden gecontroleerd om abnormale toegangspogingen te detecteren. → Beveiligingsgebeurtenissen worden verzameld en gecorreleerd door onze "Security Information and Event Management"-tool. → Beveiligingsgebeurtenissen en waarschuwingen worden 24/7 geanalyseerd door ons Security Operation Center. → Er worden regelmatig technische audits uitgevoerd om mogelijke zwakke punten op te sporen. → Er worden voortdurend controles uitgevoerd om nieuwe bedreigingen te identificeren en deze op te nemen in onze tools en processen.

Reageren	→ NRB heeft processen voor het beheer van incidenten en crisisbeheer geïmplementeerd om cyberincidenten doeltreffend af te handelen en de continuïteit van de dienstverlening te waarborgen. → Er zijn communicatieprotocollen geïmplementeerd om interne en externe belanghebbenden tijdig te informeren voor, tijdens en na een incident. → Incidenten worden geanalyseerd en gecategoriseerd om vooraf gedefinieerde actieplannen uit te voeren. → Incidenten worden geïsoleerd en ingeperkt om hun impact te beperken. → Het CSIRT (Computer Security Incident Response Team) van NRB voert de nodige forensische onderzoeken en analyses uit, indien nodig in samenwerking met gespecialiseerde externe dienstverleners. → Voor elk groot incident wordt een post-mortemanalyse uitgevoerd om de geleerde lessen te identificeren en de reactieprocessen en -strategieën dienovereenkomstig aan te passen. → NRB werkt samen met partners (Cert.be, CCB, MSSP) om informatie over bedreigingen en incidenten uit te wisselen.
Recupereren	→ Herstelplannen worden uitgevoerd om kritieke services, systemen en activiteiten te herstellen na een cyberbeveiligingsincident. → Er worden prioriteiten gesteld voor het herstellen van essentiële functies en operationele capaciteit om dienstonderbrekingen tot een minimum te beperken. → Relaties met interne en externe partijen worden tijdens het herstelproces onderhouden om transparantie en vertrouwen te garanderen. → Na de oplossing en het herstel worden incidenten en genomen acties geanalyseerd om beheerprocessen en actieplannen te verbeteren.

*AVG (Algemene Verordening Gegevensbescherming): Het doel van de AVG is om een kader te bieden voor praktijken met betrekking tot het verzamelen, verwerken en gebruiken van persoonsgegevens.

*NIS2 (Network and Information system Security): De NIS2-richtlijn is een regelgevingskader dat tot doel heeft de veerkracht van kritieke infrastructuren te versterken, de respons op cyberincidenten te verbeteren en de cyberbeveiligingspraktijken binnen de EU-lidstaten te harmoniseren.