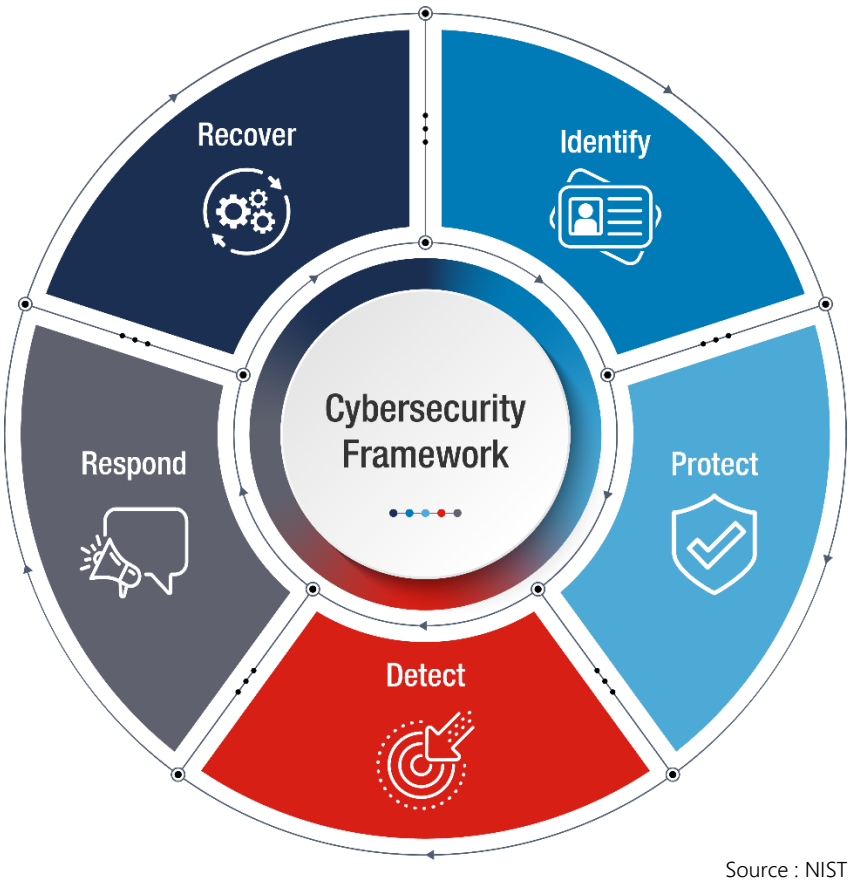
CYBERSECURITY POLICY

SECURITY BIJ NRB: EEN PRIORITEIT

NRB *hosts* en ondersteunt de IT-systemen van organisaties die essentieel zijn voor het functioneren van ons land, of het nu gaat om de publieke, private of de gezondheidszorgsector. Wij hebben dan ook een cruciale verantwoordelijkheid om de continuïteit en de kwaliteit van onze dienstverlening te waarborgen. De beveiliging van informatiesystemen en gegevens is dan ook een van de prioritaire elementen in de dienstverlening aan onze klanten en in de bescherming van onze infrastructuur.

HOE KAN NRB HELPEN HAAR KLANTEN TE BESCHERMEN TEGEN CYBERDREIGINGEN?

- Door hen vertrouwen te geven via onze ISO27001-certificering. Dit certificaat, toegekend door een onafhankelijk auditbedrijf, getuigt van de integratie van de veiligheid in onze organisatie en van de implementatie van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te behouden.
- Door gebruik te maken van een *framework* dat alle aspecten van de veiligheid omvat, zodat NRB kan reageren op huidige en toekomstige bedreigingen.



Source : NIST

DIT *FRAMEWORK* IS GEBASEERD OP VIJF FUNCTIES. DEZE MAKEN HET MOGELIJK OM DE CYBERSECURITYACTIVITEITEN TE ORGANISEREN:

Identificeer: Ontwikkel een gemeenschappelijk begrip om risico's met betrekking tot gegevens, activa en systemen te beheren.

Beschermen: Ontwikkelen en uitvoeren van passende tegenmaatregelen om de bescherming en beschikbaarheid van kritieke diensten te garanderen.

Detecteer: Ontwikkelen en uitvoeren van activiteiten om het optreden van cybersecuritygebeurtenissen op te sporen.

Reageer: Ontwikkelen en uitvoeren van passende activiteiten voor de follow-up van een gedetecteerde cybersecuritygebeurtenis.

Herstel: Ontwikkelen en uitvoeren van passende activiteiten om voldoende resilience te behouden en diensten en gegevens te herstellen die door een cybersecuritygebeurtenis zijn verstoord.

HOE WORDT DIT FRAMEWORK BIJ NRB GEÏMPLEMENTEERD?

FUNCTIE	DOELSTELLINGEN EN ACTIVITEITEN
Identificeer	- NRB heeft een securitybeleid en een organisatie met drie verdedigingslinies (Operationele Veiligheid, Governance/Piloting en Interne Audit) - NRB voldoet aan GDPR*/NIS*/ISO27001. - NRB heeft een risicomanagementproces met een eigen methodologie op basis van ISO27005, terugkerende analyses en actieplannen. - NRB voert een doorlopende evaluatie uit van opkomende cyberdreigingen. - Op basis van de door de opdrachtgever verstrekte informatie integreert NRB de kritische diensten en bedrijfsmiddelen van de opdrachtgever in haar processen. - NRB bepaalt samen met de klant de organisatie en de communicatiekanalen met betrekking tot de veiligheid.
Beschermen	- De NRB-datacenters zijn ontworpen en worden geëxploiteerd om de veiligheid en continuïteit te waarborgen (Tier 3+ Uptime Institute niveau). - De gegevensopslag is beveiligd met encryptie. - De gegevens worden opgeslagen en de integriteit van de back-ups wordt gecontroleerd. - Disaster recovery plannen zijn opgesteld en ten minste eenmaal per jaar getest. - Harding en patching worden verzekerd door ons *vulnerability management process* (beheer van kwetsbaarheden). - Alle NRB-medewerkers worden voortdurend getraind op het gebied van veiligheid.

Detecteer	- Het NRB-netwerk wordt permanent bewaakt en elk abnormaal gedrag ten opzichte van de gedefinieerde waarden genereert een waarschuwing. - De activiteiten van de eindgebruiker worden gecontroleerd om abnormale toegangspogingen op te sporen. - Beveiligingsgebeurtenissen worden verzameld uit kritieke bronnen en gecorreleerd met onze '*Security Information and Event Management*' tool. - Beveiligingsevents en -waarschuwingen worden 24/7 geanalyseerd door ons *Security Operation Center*. - Anti-malware is actief op werkstations, mail/webgateways en firewalls. - Kwetsbaarheidsscans worden op een terugkerende basis uitgevoerd..
Reageer op	- NRB beschikt over incident- en crisismanagementprocessen om effectief met cyberincidenten om te gaan en de continuïteit van de dienstverlening te waarborgen. - NRB staat in contact met partners (Cert.be, CCB, MSSP) om informatie over bedreigingen en incidenten te delen. - NRB voert forensisch onderzoek en analyses uit in samenwerking met externe gespecialiseerde dienstverleners. - Incidenten worden geanalyseerd en gecategoriseerd om vooraf gedefinieerde actieplannen uit te voeren. - Incidenten worden afgezonderd en onder controle gebracht om de gevolgen ervan te beperken.
Herstel	- Recoveryplannen worden uitgevoerd tijdens of na afloop van het incident. - De betrekkingen met externe partijen worden beheerd als onderdeel van het crisisproces. - Na oplossing en herstel worden de incidenten en de ondernomen acties geanalyseerd om de managementprocessen en actieplannen te verbeteren.

*GDPR (General Data Protection Regulations): Het doel van het GDPR is een kader te bieden voor activiteiten met betrekking tot het verzamelen, verwerken en gebruiken van persoonsgegevens.

*NIS (Network and Information System Security): De NIS-richtlijn is een regelgevend kader om de cyberveiligheid van aanbieders van digitale diensten (DSP's), d.w.z. voornamelijk cloud- en zoekmachinebedrijven, te versterken.