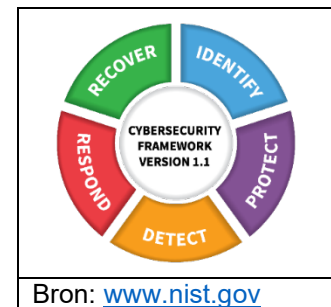


NIST-framework

Het National Institute of Standards and Technology (NIST) is een Amerikaans instituut dat zich inzet voor standaardisatie. Het NIST Cybersecurity Framework is een van deze standaarden. Het onderscheidt vijf functies / doelen:



- Identify - Identificeren**
 Identificeren gaat om inzicht te krijgen in alle zwakke plekken in uw organisatie en om het vaststellen van de risico's ten aanzien van de 'kroonjuwelen', de systemen, processen en data die cruciaal zijn voor de continuïteit van de organisatie.
- Protect - Beschermen**
 Voorkomen is beter dan genezen. Beschermen gaat het om het nemen van maatregelen: trainen van mensen, opstellen van procedures en inzet van technologie die erop zijn gericht om incidenten tot een minimum het beperken. Denk hierbij aan het versleutelen van data, wachtwoorden (incl. MFA), updates van software en toegangsbeveiliging.
- Detect - Meten**
 Meten gaat om de maatregelen met betrekking tot het monitoren van systemen en data door het registreren van verdacht, de afwijkingen die kunnen wijzen op een indringer. Denk hierbij aan anti-virus en anti-spy software en monitoringsystemen.
- Respond - Reageren**
 Als sprake is van een inbraak of indringer is snel en adequaat reageren cruciaal om schade te voorkomen. Denk hierbij aan een calamiteitenplan waarin is vastgelegd wie welke actie onderneemt.
- Recover - Herstellen**
 Herstellen gaat om de maatregelen om terug te keren naar de normale situatie na een security incident, inclusief het herstellen van eventuele schade. Denk hierbij aan de back-up en recoveryprocedure, inclusief het periodiek testen hiervan.

Voorbeeld

