

Aansluitvoorwaarden SOC-dienstverlening Monitoring en Alarmering

Voor de definitie van de "aansluiteisen" wordt het NIST-CSF 2.0 als uitgangspunt gebruikt dat internationaal erkend is als een leidend referentiekader voor cybersecurity¹. Het Cybersecurity Framework (CSF) is een reeks *best practices* en aanbevelingen op het gebied van cyberbeveiliging van het National Institute of Standards and Technology (NIST). Het is een leidraad, gebaseerd op bestaande normen, richtlijnen en praktijken voor organisaties om cyberveiligheidsrisico's beter te beheersen en te verminderen.

Hoe verhoudt het CSF zich tot de BIO en de CSIR? Het CSF richt zich op het inrichten van een Security-functie en de onderdelen nodig voor een SOC-functie. De CSIR richt zich als implementatierichtlijn op risicobeheersing in de keten 'Keren en Beheren', het risico gedreven denken, werken en sturen. Gericht op het beveiligen van objecten (PA). De BIO is een implementatierichtlijn voor de ISO27001/2 met specifieke toevoegingen voor de overheid. Voor het SOC-ontwerp past het CSF beter omdat het breder is dan de BIO en de CSIR, die met het CSF volledig worden afgedekt.

Het NIST-CSF is opgebouwd uit zes basisfuncties. Slechts een deel hiervan zal/kan worden uitbesteed aan een SOC-dienstverlener (Opdrachtnemer). Dit betekent dat voor een volledige afdekking van de functies, een deel ervan bij de Deelnemers ligt.

Naast de uit het CSF voortvloeiende aansluiteisen, is een 'Data Protection Impact Assessment', DPIA uitgevoerd. De DPIA geeft de bepalingen en afwegingen weer die zijn gemaakt om de privacyrisico's van de gegevensverwerkingen die naar aanleiding van de af te nemen SOC-dienstverlening zullen plaatsvinden, te beperken. Op basis van de resultaten van de DPIA zijn naast de NIST-CSF vereisten de aansluitvoorwaarden opgenomen die voortvloeien uit de DPIA. Voor de herkenbaarheid zijn deze separaat benoemd en wordt een mogelijke dubbeling vanuit transparantie geaccepteerd.

Het is niet realistisch om te verwachten dat Deelnemers die in 2024 willen aansluiten op de gemeenschappelijke SOC-dienstverlening de toegewezen functies volledig geïmplementeerd hebben. Daarom beperken deze "aansluiteisen" zich tot de minimumonderdelen die door Deelnemers geïmplementeerd dienen te zijn voorafgaand aan het realiseren van de daadwerkelijke aansluiting. Ze omvatten een reeks specifieke maatregelen die Deelnemers moeten volgen om de capaciteiten van hun gezamenlijke SOC-dienstverlening te benutten, te optimaliseren en te waarborgen. Deze eisen zijn ontworpen om een solide basis te vormen voor het monitoren en alarmeren met betrekking tot cybersecuritydreigingen/ -incidenten. De eisen laten voldoende ruimte om iedere Deelnemer in staat te stellen ze organisatie specifiek in te richten.

Dit document is in de Nederlandse taal geschreven, om die reden zijn de Engelstalige NIST-CSF eisen vertaald naar het Nederlands.

Hieronder zijn de voor aansluiting op het SOC belangrijke onderdelen die door een Deelnemer moeten worden afgedekt, per functie opgenomen:

¹ <https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters>

BESTUREN

Omschrijving: Rollen, verantwoordelijkheden en bevoegdheden (GV.RR)

Rollen, verantwoordelijkheden en bevoegdheden op het gebied van cyberbeveiliging om verantwoording, prestatiebeoordeling en voortdurende verbetering te bevorderen, worden vastgesteld en gecommuniceerd.

Te nemen maatregelen:

- GV.RR-01: Organisatorisch leiderschap is verantwoordelijk en aansprakelijk voor cyberbeveiligingsrisico's en bevordert een cultuur die risicobewust, ethisch en voortdurend verbeterend is.
- GV.RR-02: Rollen, verantwoordelijkheden en bevoegdheden met betrekking tot risicobeheer op het gebied van cyberbeveiliging worden vastgesteld, gecommuniceerd, begrepen en gehandhaafd.
- GV.RR-03: Er worden voldoende middelen toegewezen in overeenstemming met de risicostrategie voor cyberbeveiliging, de rollen en verantwoordelijkheden en het beleid.
- GV.RR-04: Cyberbeveiliging is opgenomen in personeelsbeleid/ - management.

IDENTIFICEREN

Omschrijving: Activabeheer (ID.AM)

Activa (bijv. gegevens, hardware, software, systemen, faciliteiten, diensten, mensen) die de organisatie in staat stellen om bedrijfsdoeleinden te bereiken, worden geïdentificeerd en beheerd in overeenstemming met hun relatieve belang voor de doelstellingen van de organisatie en de risicostrategie van de organisatie.

Te nemen maatregelen:

- ID.AM-01: Er worden inventarissen bijgehouden van hardware die door de organisatie wordt beheerd (= actuele CMDB).
- ID.AM-02: Inventarissen van software, diensten en systemen die door de organisatie worden beheerd, worden bijgehouden.
- ID.AM-03: Representaties van de geautoriseerde netwerkcommunicatie en interne en externe netwerkgegevensstromen van de organisatie worden bijgehouden.
- ID.AM-04: Inventarisaties van door leveranciers geleverde diensten worden bijgehouden
- ID.AM-05: Activa worden geprioriteerd op basis van classificatie, importantie, middelen en impact op de missie (= identificatie "kroonjuwelen").
- ID.AM-07: Er worden inventarissen van gegevens en overeenkomstige metagegevens voor aangewezen gegevenstypes bijgehouden
- ID.AM-08: Systemen, hardware, software en diensten worden gedurende hun hele levenscyclus beheerd.

Omschrijving: Risicobehoordeling (ID.RA)

De organisatie begrijpt het cyberbeveiligingsrisico voor de organisatie, bedrijfsmiddelen en personen.

Te nemen maatregelen:

- ID.RA-01: Kwetsbaarheden in bedrijfsmiddelen worden geïdentificeerd, gevalideerd en vastgelegd.
- ID.RA-04: Potentiële gevolgen en waarschijnlijkheid van bedreigingen die kwetsbaarheden uitbuiten, worden geïdentificeerd en vastgelegd.
- ID.RA-05: Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden gebruikt om risico's te bepalen en risicoprioriteiten vast te stellen.
- ID.RA-07: Wijzigingen en uitzonderingen worden beheerd, beoordeeld op risico-impact, vastgelegd en bijgehouden.
- ID.RA-08: Processen voor het ontvangen, analyseren en reageren op bekendmakingen van kwetsbaarheden zijn vastgesteld.

BESCHERMEN

Omschrijving: Identiteitsbeheer, authenticatie en toegangscontrole (PR.AA)

De toegang tot fysieke en logische middelen is beperkt tot geautoriseerde gebruikers, diensten en hardware en wordt beheerd in overeenstemming met het ingeschatte risico op ongeautoriseerde toegang.

Te nemen maatregelen:

- PR.AA-01: Identiteiten en referenties voor geautoriseerde gebruikers, diensten en hardware worden beheerd door de organisatie.
- PR.AA-02: Identiteiten worden bewezen en aan referenties gebonden op basis van de context van interacties.
- PR.AA-03: Gebruikers, diensten en hardware worden geauthentiseerd.
- PR.AA-04: Identiteitsbevestigingen worden beschermd, overgebracht en geverifieerd.
- PR.AA-05: Toegangsrechten, -rechten en -autorisaties worden vastgelegd in beleid, beheerd, afgedwongen en herzien, en bevatten de principes van 'least privilege' en 'scheiding van taken'.
- PR.AA-06: Fysieke toegang tot bedrijfsmiddelen wordt beheerd, bewaakt en afgedwongen in overeenstemming met het risico.

Omschrijving: Bewustzijn en training (PR.AT)

Het personeel van de organisatie krijgt cyberbewustzijn en -training zodat ze hun taken op het gebied van cyberbeveiliging kunnen uitvoeren.

Te nemen maatregelen:

- PR.AT-02: Personen in gespecialiseerde rollen krijgen bewustzijn en training zodat ze de kennis en vaardigheden hebben om relevante taken uit te voeren met beveiligingsrisico's in gedachten.

Omschrijving: Gegevensbeveiliging (PR.DS)

Gegevens worden beheerd in overeenstemming met de risicostrategie van de organisatie ter bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

Te nemen maatregelen:

- PR.DS-01: De vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in ruste worden beschermd.
- PR.DS-02: De vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in doorvoer worden beschermd.
- PR.DS-09: Gegevens worden gedurende hun gehele levenscyclus beheerd, met inbegrip van vernietiging.
- PR.DS-10: De vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in gebruik worden beschermd.
- PR.DS-11: Back-ups van gegevens worden gemaakt, beschermd, onderhouden en getest.

Omschrijving: Platformbeveiliging (PR.PS)

De hardware, software (bijv. firmware, besturingssystemen, toepassingen) en diensten van fysieke en virtuele platformen worden beheerd in overeenstemming met de risicostrategie van de organisatie om hun vertrouwelijkheid, integriteit en beschikbaarheid te beschermen.

Te nemen maatregelen:

- PR.PS-01: Er worden configuratiebeheerpraktijken toegepast (o.a. change management en patch management).
- PR.PS-02: Software wordt onderhouden, vervangen en verwijderd in verhouding tot het risico.
- PR.PS-03: Hardware wordt onderhouden, vervangen en verwijderd in verhouding tot het risico.
- PR.PS-04: Logdata/ -bestanden worden gegenereerd en beschikbaar gesteld voor continue monitoring.
- PR.PS-05: Installatie en uitvoering van ongeautoriseerde software wordt voorkomen.

HERSTELLEN

Omschrijving: Uitvoering incidentherstelplan (RC.RP)

Herstelactiviteiten worden uitgevoerd om de operationele beschikbaarheid te garanderen van systemen en diensten die zijn getroffen door cyberbeveiligingsincidenten.

Te nemen maatregelen:

- RC.RP-01: Het herstelgedeelte van het incident response plan wordt uitgevoerd zodra dit is geïnitieerd vanuit het incident response proces
- RC.RP-02: Herstelacties worden bepaald, afgebakend, geprioriteerd en uitgevoerd.
- RC.RP-03: De integriteit van back-ups en andere herstelmiddelen wordt geverifieerd voordat ze worden gebruikt voor herstel.
- RC.RP-04: Kritieke missiefuncties en risicobeheer op het gebied van cyberbeveiliging worden overwogen om operationele normen voor na een incident vast te stellen.
- RC.RP-05: De integriteit van herstelde middelen wordt geverifieerd, systemen en diensten worden hersteld en de normale operationele status wordt bevestigd.
- RC.RP-06: De criteria voor het bepalen van het einde van het incidentherstel worden toegepast en de incident gerelateerde documentatie wordt voltooid.

Omschrijving: Communicatie over incidentherstel (RC.CO)

Herstelactiviteiten worden gecoördineerd met interne en externe partijen.

Te nemen maatregelen:

- RC.CO-03: Herstelactiviteiten en de voortgang in het herstel van operationele capaciteiten worden gecommuniceerd met aangewezen interne en externe belanghebbenden.
- RC.CO-04: Publieke updates over het herstel van het incident worden op de juiste manier gedeeld door gebruik te maken van goedgekeurde methodes en berichtgeving.

Aansluitvereisten vanuit de DPIA:

- Geïmplementeerd Monitoring- en Logbeleid, waarbij de inhoud van de logregels gevalideerd is vanuit privacy perspectief en controle is ingericht op de vastgestelde bewaartermijnen;
- Benoemen en ter beschikking hebben van security-expertise om use cases te testen en te valideren op onjuiste alerts, zowel tijdens implementatie als in de operationele fase;
- Rollen benoemen met bijbehorende verantwoordelijkheden voor het juiste mandaat om op te nemen in de DAP;
- RBAC ingericht t.a.v. logbestanden om toegang te beperken tot de juiste personen;
- Logging/ Audit op muteren, mogelijk manipuleren en verwijderen van logbestanden. Conform de BIO dient het ongewijzigde bestaan van logbestanden gegarandeerd te zijn;
- RBAC ingericht voor toegang tot SIEM en SOC-systemen;
- Ingericht en operationeel werkend vulnerability management op SOC/SIEM systemen
- Bestaan van een privacy-statement m.b.t. verwerken van data inclusief benoemen dat een SOC/SIEM wordt ingezet, inclusief communicatierichtlijnen ten aanzien van dit statement.