Solvinity
Secure Managed Cloud

NIST CSF 2.0 & ZERO TRUST

FUNDAMENTEN VOOR **CYBERWEERBAARHEID**

WHITEPAPER

Inhoud

Introductie

Cybersecurity is niet langer alleen een zaak van de IT-afdeling, zeker niet nu cyberdreigingen een direct bedrijfsrisico vormen. Cybersecurity is inmiddels een strategisch thema. De impact van een incident gaat verder dan het blokkeren of beschadigen van systemen. De kans is groot dat een cyberaanval serieuze impact heeft op jouw dienstverlening, reputatie en continuïteit. Het securitylandschap is bovendien complexer dan ooit. De digitale afhankelijkheid neemt toe, wet- en regelgeving wordt strenger en aanvallen steeds geavanceerder.

Veel organisaties hebben de basis redelijk op orde. Toch blijft de vraag: hoe kwetsbaar ben je eigenlijk en hoe blijf je de cyberweerbaarheid verbeteren? Frameworks, zoals het NIST Cybersecurity Framework (CSF) 2.0 bieden houvast. Belangrijker is echter hoe je deze richtlijnen naar jouw praktijk vertaalt. Daarnaast is het tegenwoordig een eis dat je aanpak duurzaam en aantoonbaar is, vanwege inspecties en compliance-eisen.

In deze whitepaper laten we zien hoe het NIST Framework en een Zero Trust-aanpak kunnen helpen om grip te krijgen op jouw beveiliging. Met de praktijk van Solvinity als vertrekpunt ontdek je hoe je als organisatie overzicht creëert, beveiliging gericht verbetert en aantoonbaar werkt aan cyberweerbaar-heid.

Krijg **grip op je beveiliging** met het NIST Cyber Security Framework 2.0 en een Zero-Trust aanpak

NIST CSF 2.0 als kapstok voor cybersecurity

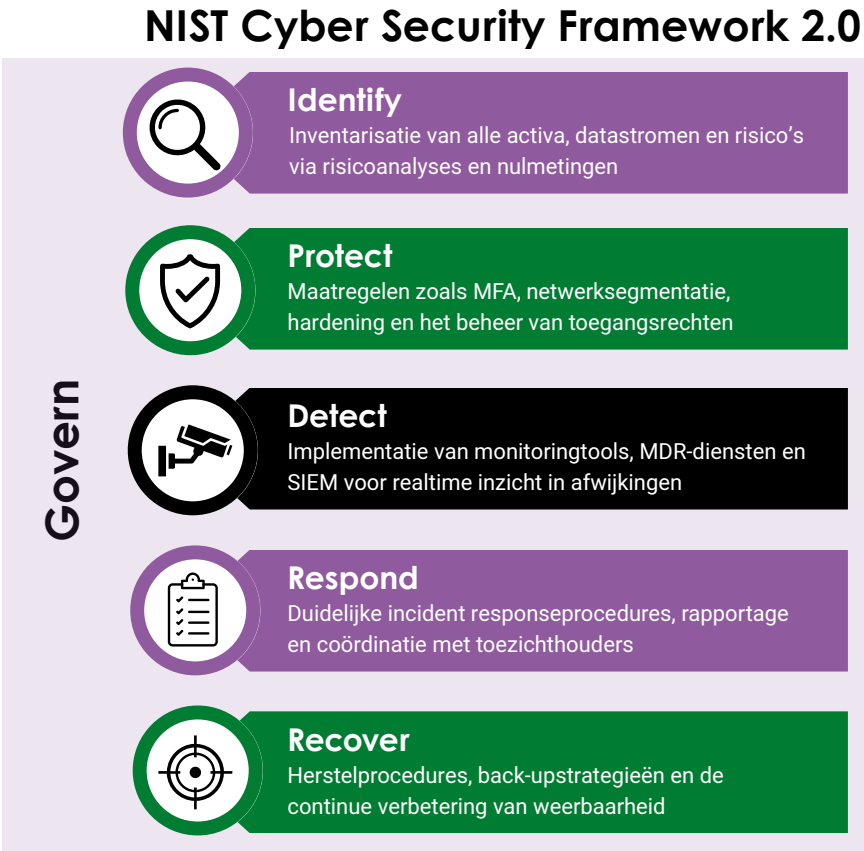
Bij veel organisaties is security organisch gegroeid met losse maatregelen en oplossingen, vaak ingegeven door incidenten of regelgeving. Bijvoorbeeld met firewalls van leverancier A, een monitoringtool van partij B en een SOC via partner C. Deze onderdelen zijn heel waardevol, maar zonder samenhang ontbreekt het overzicht.

Het NIST Cybersecurity Framework (CSF) 2.0 biedt structuur en verankert cybersecurity in beleid, techniek en gedrag. Je brengt maatregelen onder in zes samenhangende functies: Govern, Identify, Protect, Detect, Respond en Recover. Samen vormen deze een continu proces dat je in staat stelt om risico's beheersbaar te maken. Zo krijg je inzicht in wat je hebt op het gebied van infrastructuur, systemen, netwerken, applicaties en processen. Ook toont het de mogelijke risico's die de organisatie loopt door bijvoorbeeld ontbrekende of dubbele securitymaatregelen.

Bij Solvinity werken we intern en voor klanten op basis van dit raamwerk. Zo helpen we klanten bij het uitvoeren van risico-assessments, het verbeteren van monitoring en het stroomlijnen van toegangsbeheer. Door alles onder te brengen in het NIST-model ontstaat een logisch geheel, dat een structuur biedt voor compliance en audits.

Een van de sterke punten van het NIST Framework is dat het werkt als een gemeenschappelijk referentiekader voor zowel CISO's als bestuurders. Hoewel goede security voor iedereen noodzakelijk is, heeft elke organisatie eigen aandachtspunten. Met het NIST CSF kun je per onderdeel het volwassenheidsniveau bepalen: van ad-hoc en reactief naar aantoonbaar beheerst en strategisch ingebed.

Het NIST CSF is geen checklist of einddoel, maar een praktische tool voor structuur, volwassenheid en aantoonbaarheid in complexe omgevingen zoals de (semi)overheid, financiële sector en vitale infrastructuur.



Zero Trust: geen model, maar mindset

Zero Trust is een logische stap als je cybersecurity niet alleen reactief wilt inrichten, maar juist structureel wilt verbeteren. Het is geen product of project. Het is een manier van denken én werken. Het principe is duidelijk: vertrouw niet op locatie, rang of rol, maar verifieer altijd gedrag, context en identiteit om naar volledige zichtbaarheid toe te werken. Beveiliging richt zich hiermee op externe dreigingen en interne netwerken.

Realiseer je dat Zero Trust geen technologie is. Het is een architectuurprincipe dat helpt je IT-landschap veilig en bewust in te richten. Bij Solvinity is Zero Trust leidend in ontwerp en beheer. Onze infrastructuur is gebaseerd op het 'secure-by-design'-principe. Dat betekent: eerst goed nadenken voor je iets bouwt. We zorgen dat alles standaard is afgeschermd en pas toegankelijk is als het echt nodig is, gebaseerd op het principe van ‘least privilege’. De securitymaatregelen, netwerksegmentatie, authenticatie, hardening, en multi-factor authenticatie vormen de basis voor Zero Trust. Daarnaast zijn het juist de essentiële zaken, zoals continuous pentesting/red teaming en 24/7 security monitoring (Managed Detection & Response (MDR), die ervoor zorgen dat een Zero Trust-aanpak toe te passen is. Zero Trust staat overigens voor ‘niets vertrouwen en alles valideren’, dus continuous pentesting en security monitoring zijn een onlosmakelijk onderdeel van onze Zero Trust-aanpak.

In onze infrastructuur staat toegang standaard dicht en gebruiken we segmentatie, strikt toegangsbeheer, continue monitoring en geautomatiseerde detectie. Deze aanpak is stevig verankerd in de dagelijkse praktijk van Solvinity. Je ziet dit terug in de inrichting van onze secure managed clouds en in de samenwerking met partners als Securify. Dat voorkomt gebruik van ad-hoc oplossingen en maakt afwijkingen snel zichtbaar.

De koppeling met het NIST CSF

Zero Trust sluit naadloos aan op het NIST Cybersecurity Framework. Volledige zichtbaarheid, een kernprincipe van Zero Trust, komt direct terug in de Identify- en Detect-fases van het NIST CSF. Ook continue verificatie en strikte toegangscontrole vallen onder de Protect-functie. Incidentrespons en herstelprocedures sluiten aan bij Respond en Recover. Hiermee wordt Zero Trust geen abstracte strategie, maar een concrete werkmethode. De door NIST gepubliceerde richtlijn SP800-207 beschrijft praktische, stapsgewijze richtlijnen om Zero Trust in te voeren. Zo vertaal je de abstracte Zero Trust-principes naar een werkbare aanpak die aansluit op je infrastructuur en risicoprofiel.

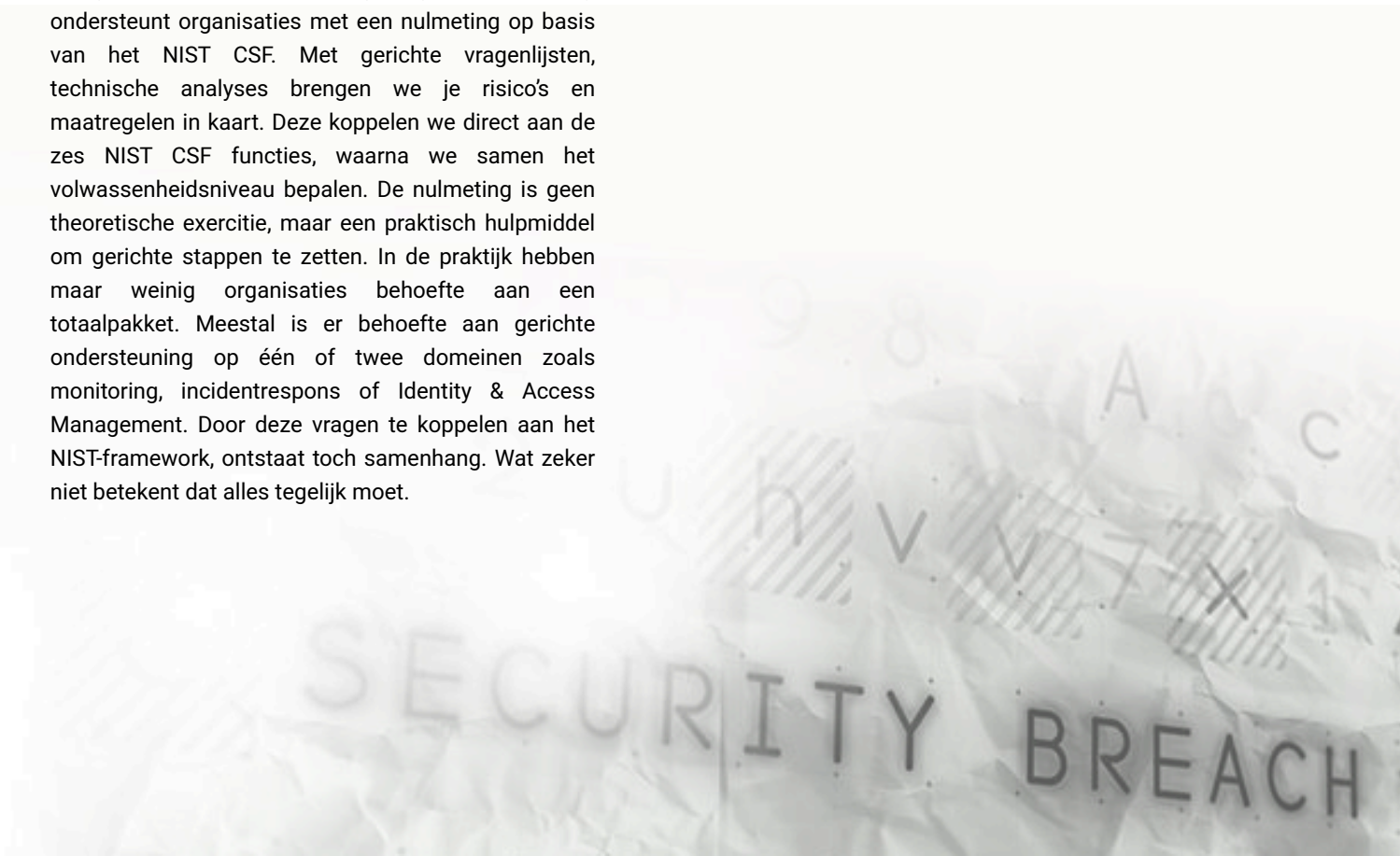
Echter, Zero Trust is geen oplossing die je eenvoudig als een soort 'product' uitrolt. Het is een manier van kijken naar je infrastructuur en processen. Voor veel organisaties betekent het een cultuurverandering: van impliciet vertrouwen en aannames, naar expliciete controle en meetbare maatregelen. Dit vraagt een continu proces van bewustwording, inrichting en evaluatie. Het helpt sneller in te grijpen, risico's te verkleinen en compliance eenvoudiger aantoonbaar te maken.

Waar sta je? Alles begint met inzicht

Bij veel organisaties stapelen de beveiligingsmaatregelen zich op. Verschillende leveranciers, ad-hoc oplossingen en interne processen sluiten niet altijd op elkaar aan. Het ontbreekt vaak aan samenhang en overzicht. Maatregelen zijn verspreid over afdelingen en leveranciers, processen zijn niet in lijn met elkaar en kwetsbaarheden blijven onduidelijk.

Een gestructureerde aanpak begint bij inzicht. Solvinity ondersteunt organisaties met een nulmeting op basis van het NIST CSF. Met gerichte vragenlijsten, technische analyses brengen we je risico's en maatregelen in kaart. Deze koppelen we direct aan de zes NIST CSF functies, waarna we samen het volwassenheidsniveau bepalen. De nulmeting is geen theoretische exercitie, maar een praktisch hulpmiddel om gerichte stappen te zetten. In de praktijk hebben maar weinig organisaties behoefte aan een totaalpakket. Meestal is er behoefte aan gerichte ondersteuning op één of twee domeinen zoals monitoring, incidentrespons of Identity & Access Management. Door deze vragen te koppelen aan het NIST-framework, ontstaat toch samenhang. Wat zeker niet betekent dat alles tegelijk moet.

Voor organisatie die meer diepgang willen, werken we samen met Securify. Met een pentest of red team-aanpak brengen we kwetsbaarheden realistisch in beeld, soms zelfs zonder dat medewerkers weten dat er getest wordt. Zo ontstaat een beeld van de werkelijke weerbaarheid.



Gedeeld eigenaarschap

Aantoonbare security is geen keuze. Niet alleen vanwege wet- en regelgeving zoals DORA of NIS2. Toezichthouders, auditors en ketenpartners verwachten niet alleen maatregelen, maar willen bewijs zien. Is er logging? Werkt het patch-management aantoonbaar? Zijn incidenten vastgelegd en opgevolgd? Je moet aantonen dat beveiligingsmaatregelen doordacht, effectief en actueel zijn.

Het NIST Cybersecurity Framework biedt een gestructureerd aanpak om dit aan te tonen. Elk onderdeel is te koppelen aan concrete maatregelen, tools en procedures. Dat maakt het eenvoudiger bewijs aan te leveren. Bovendien bevordert dit inzicht gedeeld begrip tussen IT, CISO's en bestuur. Tegelijkertijd blijft compliance een gedeel-de verantwoordelijkheid. Net als bij het 'shared responsibility model' in de cloud, ligt de basisveiligheid bij het platform of de dienstverlener, maar ben je als organisaties zelf verantwoordelijk voor inrichting, gebruik en controle. Solvinity ondersteunt daarbij, maar neemt die verantwoordelijkheid niet over.

Blijven verbeteren

Niemand begint bij nul met beveiliging. Tegelijkertijd zijn weinig organisatie echt 'veilig'. Cybersecurity is geen eindpunt, maar een voortdurend proces. Nieuwe dreigingen zoals AI versnellen aanvallen en vergroten het aanvalsoppervlak. Bijvoorbeeld met spearphishing of geautomatiseerde exploits. Tegelijk helpt AI ook bij verdediging, zoals in het analyseren van logbestanden of gedragsdetectie.

Solvinity zet AI al jaren in voor monitoring, maar ook wij blijven leren. We volgen de ontwikkelingen rondom quantum computing, datasoevereiniteit en nieuwe regelgeving op de voet en passen onze aanpak continu aan. Dat kan alleen met een solide fundament. Het NIST CSF 2.0 en Zero Trust bieden die basis. Zo blijft je organisatie veilig en wendbaar, zelfs als de tech-nologie verandert. Zo werk je niet reactief, maar strategisch aan digitale veiligheid.

"**Cybersecurity** is geen eindpunt, het is een **voortdurend proces**"

Van bewustwording naar aantoonbaar veilige aanpak

Cybersecurity draait om het beheersen van risico's die de continuïteit van je organisatie kunnen bedreigen. Het gaat echter verder dan risicobeheersing. Een goed beveiligde omgeving vraagt om inzicht, structuur en discipline. Met het NIST Cybersecurity Framework leg je een stevige, herkenbare basis. Zero Trust helpt je de juiste keuzes te maken bij de inrichting van systemen, toegang en monitoring. Samen vormen ze de ruggengraat van een veilige, toekomstbestendige IT-strategie.

Wie grip wil op risico's, compliance en continuïteit begint met inzicht. De nulmeting is daarbij de thermometer: hoe cyberweerbaar ben je, waar scoor je goed en wat moet beter? Dat vraagt om bewustwording en context, anders blijf je brandjes blussen. Daarom geloven wij in een aanpak die begint met overzicht en eindigt bij aantoonbare verbetering.24/7 monitoring, secure-by-design, segmen-tatie en MFA zijn hierbij geen losstaande onderdelen, maar vormen één geheel: een Zero Trust-aanpak die in de praktijk werkt.

Kortom: breng in kaart wat er is, bepaal waar versterking nodig is en werk stap voor stap aan een aantoonbaar veilige omgeving. Voordat risico's of aanvallen je inhalen.

Benieuwd hoe het NIST CSF en Zero Trust bijdragen aan de digitale veiligheid van jouw organisatie?

Ontdek het met een nulmeting op basis van het NIST-Framework. Zo krijg je direct inzicht in risico's, verbeterpunten én concrete vervolgstappen. Neem contact met ons op:

+31(0)20 364 3600

info@solvinity.com

÷ Solvinity
Secure Managed Cloud

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
www.solvinity.com

Met secure managed cloud services ondersteunt en adviseert Solvinity organisaties met hoge beveiligingseisen in hun digitale transformatie.

	Public Cloud Private Cloud Security Services Workspace
	Solvinity onderscheidt zich op het gebied van cybersecurity met een uitgebreid portfolio aan securitydiensten en oplossingen en biedt, met een meerderheidsbelang in Securify, aanvullende diensten op het gebied van pentesting, red teaming en agile security.
	Certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001, ISAE3402 Type I en II en PCI DSS. Als eerste Managed Service Provider in Nederland SOC 1 & 2 compliance rapporten voor de gehele beheeromgeving van niet alleen de private, maar ook de Azure cloud.
	Solvinity levert aan de (rijks-)overheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, Translink (OV-chipkaart), ING en Klaverblad.

300+

Amsterdam, Assen
Amersfoort, Den Bosch