MANIFEST

SAMEN SNELLER DAN DE DREIGING

NEDERLAND BOUWT AAN EEN COLLECTIEVE DIGITALE VERDEDIGING DIE MEEGROEIT MET AI

DIGITAL HOLLAND
where innovation starts

PROMETHEUS
samen sneller dan de dreiging

WIE DIT MANIFEST DRAGEN

Dit manifest is het open document: het spreekt uit waar wij samen voor staan en het is het instrument waarmee anderen zich aansluiten. Ondertekenen kan doorlopend; de groep groeit met elke organisatie die meedoet. Het initiatief wordt ontwikkeld vanuit de Actieagenda Cybersecurity Technologies en wordt aangevoerd door Digital Holland. Het is uitdrukkelijk een open, publiek-private samenwerking, bedoeld om als nationale beweging verder te worden gebracht.

DIT MANIFEST WORDT GEDRAGEN DOOR DRIE GROEPEN, ELK MET EEN EIGEN BELOFTE

Initiatiefnemers

De koplopers van het Prometheus-initiatief bouwen de collectieve verdedigingslaag en stellen de resultaten beschikbaar voor heel Nederland, niet voor zichzelf alleen.

Essentiële en belangrijke entiteiten

De organisaties in de vitale sectoren die de Cyberbeveiligingswet aanwijst: energie, zorg, vervoer, betalingsverkeer, drinkwater, digitale infrastructuur, overheid en meer, nemen wat gebouwd wordt als eerste en op grote schaal in gebruik, en trekken zo hun hele keten van (mkb) toeleveranciers mee omhoog.

Ketenpartners

Softwareleveranciers, systeemintegratoren, IT- en OT-dienstverleners, en de brancheorganisaties die hen en hun klanten vertegenwoordigen, brengen wat hier gebouwd wordt door de keten heen: naar hun klanten, hun leden en hun achterban, tot bij de kleinste organisaties. Geen organisatie is veiliger dan de software en de diensten waarop zij draait; daarom is deze groep geen aanvulling, maar een voorwaarde.

INITIATIEFNEMERS

AISLE · DIVD · eset · HADRIAN · NS · NORTHWAVE CYBER SECURITY · Nationaal Cyber Security Centrum, Ministerie van Justitie en Veiligheid · Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Justitie en Veiligheid · SCHUBERG PHILIS · SIG Software Improvement Group · TNO innovation for life

< NAAR HET BEGIN

DE AANVALLER IS EEN MACHINE GEWORDEN

Cyberaanvallen waren altijd mensenwerk. Dat is voorbij. Deze zomer voerden AI-systemen voor het eerst volledig zelfstandig aanvallen uit: onvermoeibaar, razendsnel, zichzelf sturend. De aanvaller is een machine geworden.

Wie zich blijft verdedigen op menselijk tempo, elke organisatie voor zich, verliest die wedloop. Niet door onwil of onkunde, maar omdat geen mens de snelheid van een machine kan bijhouden.

Deze ontwikkeling treft de vitale sectoren het hardst. Dit zijn de bedrijven die onze samenleving draaiende houden. Deze bedrijven vallen onder de nieuwe Cyberbeveiligingswet die strengere eisen stelt aan digitale veiligheid. Maar hun veiligheid hangt niet alleen af van hun eigen maatregelen. Ze draaien op software, systemen en diensten van anderen, vaak diep verweven in digitale ketens. Eén fout kan daardoor honderden organisaties tegelijk raken.

Bestuurlijke bewustwording en toepassing van basis-maatregelen blijven noodzakelijk, maar we zien dat dit ondanks jarenlange oproepen door experts en autoriteiten te langzaam gaat. Nu de opkomst van krachtige AI cybermodellen de dreiging snel vergroot, is versnelling cruciaal.

Geen bedrijf, overheid of kennisinstelling lost dit alleen op. Daarom hebben twaalf publieke en private koplopers het initiatief genomen, onder de naam **PROMETHEUS**, geïnspireerd door de gelijknamige godheid uit de Griekse mythologie die bekendstaat als beschermer en helper van de mensheid.

AMBITIE

Onze ambitie is dat Nederland een gezamenlijke, marktneutrale verdedigingslaag krijgt die organisaties helpt software, systemen en digitale ketens te toetsen op kwetsbaarheden, te beoordelen en op te lossen. Steeds sneller en steeds minder handmatig. Van eigen bodem. In afstemming en samenwerking met Europa. Van en voor iedereen. Veiligheid die meegroeit met de technologie en de dreiging zelf.

Uiteindelijk willen we toe naar software en digitale infrastructuur die van zichzelf veiliger zijn: veiligheid die zoveel mogelijk is ingebouwd, in plaats van achteraf toegevoegd.

En er is ook een economische kans. Wie nu leert verdedigen op machinesnelheid, bouwt kennis, technologie en een positie op waar ook Europa behoefte aan heeft.

HET BEGIN

De ambitie is groot, maar we beginnen gericht. Prometheus start met het gezamenlijk bepalen, ontwikkelen en in de praktijk beproeven van nieuwe digitale verdedigingsmogelijkheden met en tegen AI.

De start van onze inzet richt zich op het sneller ontdekken, valideren en oplossen van kwetsbaarheden in software en digitale ketens. Daarbij beginnen we niet automatisch met iets nieuws bouwen. We brengen eerst in kaart wat organisaties nodig hebben, wat al in de markt beschikbaar is en waar aantoonbare witte vlekken bestaan. Alleen daar waar een collectieve aanpak daadwerkelijk meerwaarde heeft, ontwikkelen en beproeven we gezamenlijk nieuwe verdedigingsmiddelen.

Een eerste gezamenlijke pilot richt zich op AI-gedreven cybersecurity en wordt samen met gebruikers, cybersecuritybedrijven, technologiepartners en kennisinstellingen in de praktijk beproefd.

Organisaties uit industrie, overheid en andere sectoren brengen concrete praktijkgevallen en testomgevingen in. Cybersecuritybedrijven, technologiepartners en kennisinstellingen ontwikkelen en beproeven de benodigde verdedigingsmiddelen. Wat aantoonbaar werkt, nemen we in gebruik en schalen we verder op.

Deze eerste verdedigingsmiddelen zijn daarmee niet het eindpunt, maar het begin van een structurele manier van werken die blijft meegroeien met nieuwe mogelijkheden van AI en nieuwe dreigingen.

ONZE KEUZEN

01

Samen bouwen

Wij kiezen ervoor om samen te bouwen, niet alleen af te stemmen.
We ontwikkelen samen wat afzonderlijke organisaties niet met dezelfde schaal, snelheid of kwaliteit voor elkaar krijgen.

02

AI aan de verdedigende kant

Wij kiezen ervoor om AI op verantwoorde wijze aan de verdedigende kant in te zetten. Waar snelheid en schaal dat vereisen, automatiseren we, binnen kaders die mensen bepalen.
We bouwen een verdedigingslaag die sneller leert dan de aanvaller.

03

Collectief waar nodig

Wij kiezen voor collectief waar nodig en commercieel waar mogelijk.
De gezamenlijke basis blijft marktneutraal; marktpartijen kunnen daarop concurreren met producten en diensten.

04

Wat werkt gebruiken

En wij kiezen ervoor wat werkt daadwerkelijk te gebruiken en op te schalen. Een succesvolle pilot eindigt niet met een rapport, maar met toepassing in de praktijk, verspreiding van succesvol ingezette verdediging en volgende ontwikkelstappen.

Dit manifest is onze gezamenlijke reactie op cyberdreigingen door AI en een oproep om aan te sluiten bij de beweging die Nederland op machinesnelheid laat verdedigen.

WAT IS HIERVOOR NODIG

Om deze nieuwe generatie digitale verdediging te bouwen, moeten we goed begrijpen aan welke eisen organisaties en hun ketens willen dat zij voldoet.

DAARVOOR ZIJN VIER DINGEN NODIG:

1. relevante data
2. veilige testomgevingen
3. krachtige AI technologie
4. voldoende rekenkracht.

Zonder deze bouwstenen geen machinesnelheid.

We hebben ook verschillende typen deelnemers nodig: organisaties die het probleem ervaren en use cases inbrengen, bedrijven en kennisinstellingen die verdedigingsmiddelen kunnen ontwikkelen, ketenpartners die oplossingen kunnen helpen verspreiden en publieke partijen die het collectieve belang en de randvoorwaarden kunnen helpen borgen.

Prometheus staat daarin niet los van Europa. Het initiatief is bekend bij ENISA en sluit aan op het EU Action Plan on Cybersecurity and AI, waarin dezelfde urgentie wordt onderkend en onder meer wordt ingezet op AI-gedreven remediatie, testcapaciteit, compute en Europese cyber-AI-vermogens.

ONZE GEZAMENLIJKE BELOFTE

- **Wij bouwen wat gezamenlijk sterker kan dan afzonderlijk.**
- **Wij benutten wat al bestaat en ontwikkelen alleen collectief waar aantoonbare meerwaarde ligt.**
- **Wij brengen praktijk, technologie, kennis en publieke slagkracht bij elkaar.**
- **En wij laten ons uiteindelijk niet beoordelen op plannen of overleg, maar op wat daadwerkelijk wordt gebouwd, gebruikt en opgeschaald.**

MEEDOEN BETEKENT BIJDRAGEN

Dit manifest is onze gezamenlijke reactie op autonome cyberdreigingen en een oproep om mee te bouwen aan een digitale verdediging die Nederland ook in het AI-tijdperk weerbaar houdt.

Door het manifest te ondertekenen spreken wij de intentie uit om vanuit onze eigen rol actief bij te dragen aan de verdere ontwikkeling, beproeving en opschaling van AI-gedreven digitale verdediging.

Dat kan met bestuurlijk bewustzijn, mensen en middelen, kennis, technologie, data, infrastructuur, voldoende bereik en concrete use cases. En vooral door daadwerkelijk te gebruiken wat beschikbaar komt.

Met mijn ondertekening onderschrijf ik namens mijn organisatie de ambitie van Prometheus en de intentie om vanuit onze eigen rol actief bij te dragen aan de verdere ontwikkeling en beproeving ervan.

Samen sneller dan de dreiging

ACHTERGROND BIJ DIT MANIFEST

Nederland bouwt aan een collectieve digitale verdediging die meegroeit met AI.

HOE VOEREN WE HET MANIFEST UIT

De wezenlijke veranderingen door AI vragen om een fundamenteel andere aanpak van cybersecurity. Tegen een dreiging die met machinesnelheid en op landelijke schaal werkt, helpt namelijk maar één ding: een verdediging die óók op machinesnelheid en óók op landelijke schaal werkt. Die kan geen enkele organisatie alleen bouwen, geen bedrijf, geen ministerie, geen sector.

Het moet ergens beginnen. Wij bouwen niet meteen de hele verdedigingslaag: hoe die er precies uit moet zien, weten we namelijk nog niet. Daarom verkennen we, experimenteren we en beproeven we, met echte systemen en echte urgentie. Wat werkt, roept dit manifest organisaties op over te nemen en op te schalen. En dan beginnen we opnieuw, met wat de volgende stap in AI en in de dreiging van ons vraagt.

Wij richten ons op twee dingen tegelijk. We beperken de acute risico's: gezamenlijke voorzieningen die zwakke plekken in veelgebruikte software en configuratie van infrastructuur opsporen en helpen dichten, sneller dan aanvallers ze kunnen misbruiken. Tegelijkertijd bouwen aan intrinsieke veiligheid: een doorlopend programma van onderzoek en ontwikkeling, met als doel veiligheid die in systemen zelf zit ingebouwd, zodat de verdediging elk jaar meegroeit met wat AI kan, en niet één keer wordt ingehaald en daarna weer achteropraakt

> "We bouwen een verdedigingslaag die sneller leert dan de aanvaller."

WAT IS DE ROL VAN DE RIJKSOVERHEID

De Rijksoverheid onderschrijft de ambitie van dit manifest. Met de **Actieagenda Cybersecurity** Technologies, onderdeel van de Nationale Technologie Strategie (NTS) en gecoördineerd door Digital Holland, heeft zij een nationale agenda neergezet die onderzoekers, ondernemers en overheid verbindt om de digitale technologie van de toekomst te ontwikkelen. In Nederland, voor Nederland.

Door de opkomst van AI ontstaan in hoog tempo nieuwe cyberdreigingen. Die lossen we niet op met meer van hetzelfde maar door ook zelf te kijken naar mogelijkheden op het snijvlak van cyber- en AI-technologieën. Daarom bundelen we de krachten met de **Actieagenda AI & Data**. In Prometheus zetten we het beste van beide ecosystemen in.

Wij vragen het kabinet om deze gezamenlijke ambitie bestuurlijk te bekrachtigen en sporen de Rijksoverheid aan om dit initiatief structureel en langjarig te borgen.

< NAAR HET BEGIN

WIE VORMEN DE PUBLIEK-PRIVATE SAMENWERKING

De ambities van Prometheus vragen om een sterke samenwerking van betrokken partijen. Elk vanuit hun eigen positie en mogelijkheden. Daarom bouwen we de komende tijd aan een duurzaam samenwerkingsverband dat zowel de uitvoering van Prometheus ondersteunt en adoptie en opschaling van de opgeleverde verdedigingsmiddelen.

VRAAGZIJDE VAN GEBRUIKERS

NIS2-organisaties, industrie en relevante publieke organisaties brengen de concrete uitdagingen, randvoorwaardes en use-cases in. Zij helpen bepalen welke verdedigingsmiddelen prioriteit hebben, stellen praktijkomgevingen beschikbaar en toetsen of nieuwe oplossingen daadwerkelijk waarde leveren.

KETENPARTNERS

Softwareleveranciers, systeemintegratoren, IT- en OT-dienstverleners, MSP's en brancheorganisaties zorgen ervoor dat succesvolle verdedigingsmiddelen onderdeel kunnen worden van producten, diensten en digitale ketens. Zij zijn daarmee essentieel voor adoptie en schaal.

CAPABILITY-PARTNERS

Cybersecuritybedrijven, technologiebedrijven, kennisinstellingen en universiteiten brengen technologie, expertise, infrastructuur en onderzoekscapaciteit in. Zij ontwikkelen, integreren en beproeven nieuwe verdedigingsmiddelen en maken zichtbaar wat al bestaat en waar nog echte witte vlekken liggen.

PUBLIEKE PARTNERS

Rijksoverheid en andere publieke partijen helpen het collectieve belang te borgen. Zij kunnen bijdragen aan randvoorwaarden, financiering, beleid, verbinding met nationale en Europese programma's en waar passend optreden als gebruiker of eerste afnemer.

Naast deze vier categorieën kan op termijn een aparte uitvoerende- of orkestratierol nodig zijn voor de operationele organisatie van collectieve verdedigingsmiddelen. Hoe die rol structureel wordt ingevuld, hoeft in deze fase nog niet te worden vastgelegd.

COLLECTIEF WAAR NODIG, COMMERCIEEL WAAR MOGELIJK

Prometheus is niet bedoeld om bestaande cybersecuritybedrijven of technologie-leveranciers te vervangen.

Waar de markt goede oplossingen biedt, worden die benut. Gezamenlijke ontwikkeling is vooral relevant wanneer schaal, neutraliteit, gedeelde infrastructuur of publiek belang een collectieve aanpak rechtvaardigen. Marktpartijen kunnen bovendien voortbouwen op de gezamenlijke basis en daar eigen producten en diensten omheen ontwikkelen.

Prometheus moet daarmee niet naast de markt komen te staan, maar juist helpen om de markt en de collectieve digitale weerbaarheid tegelijk te versterken.

DIGITAL HOLLAND
where innovation starts

PROMETHEUS
samen sneller dan de dreiging