Salesforce Position Paper

Rondetafelgesprek Cyberveiligheid en informatiebeveiliging 20 mei 2026

Salesforce deelt graag dit position paper ten behoeve van het rondetafelgesprek Cyberveiligheid van 20 mei 2026. Wij waarderen het initiatief van de commissie voor Digitale Zaken om dit cruciale onderwerp op de agenda te zetten. Als wereldwijde technologiepartner van duizenden organisaties in alle sectoren over de hele wereld, hopen we dan ook dat onze ervaring nuttige inzichten biedt voor de beleidsontwikkeling van de commissie.

Over Salesforce

Salesforce, opgericht in 1999 in San Francisco, is een wereldwijde marktleider op het gebied van cloud-bedrijfssoftware voor klantrelatiebeheer (CRM) en levert Software-as-a-Service (Saas) en Platform-as-a-Service (PaaS) oplossingen aan bedrijven en overheidsorganisaties wereldwijd.

Bij Salesforce is vertrouwen onze belangrijkste waarde. Al meer dan 25 jaar ondersteunen we onze klanten bij elke grote technologische verschuiving: van cloud naar mobiel naar voorspellende en generatieve AI, en vandaag de dag naar Agentic AI. Salesforce zet zich in voor de ontwikkeling en implementatie van ethische, transparante en betrouwbare AI. Onze klanten verwachten het hoogste niveau van privacy, veiligheid, eerlijkheid en nauwkeurigheid bij het gebruik van onze producten, inclusief onze AI-oplossingen.

Salesforce houdt zich al meer dan tien jaar bezig met AI-onderzoek en de verantwoorde ontwikkeling van AI. Met onze nieuwste AI-innovatie, Agentforce, geeft Salesforce vorm aan de volgende fase van de samenwerking tussen mens en AI: naadloze integratie met menselijke teams, waarbij AI-agenten zelfstandig complexe taken uitvoeren om bedrijfsdoelstellingen te realiseren. Meer informatie over onze strategie voor verantwoorde AI is te vinden in ons Trusted AI Impact Report.

Met twintig jaar ervaring in Nederland fungeert Salesforce als een betrouwbare katalysator voor de digitale toekomst van het land. Dankzij ons diepgaand marktaandeel, dat bijna twee derde van de AEX25 omvat en een omvangrijke voetafdruk in het MKB heeft, zijn wij een belangrijke partner in het ecosysteem dat de Nederlandse nationale strategieën voor de digitale economie en e-overheid kan versnellen. Trouw aan onze kernwaarden gaat deze digitale transformatie hand in hand met maatschappelijk welzijn. Salesforce ondersteunt de Nederlandse sociale

sector actief door technologie te leveren aan meer dan 800 non-profitorganisaties en instellingen voor hoger onderwijs, aangevuld met bijna 6 miljoen dollar aan lokale donaties en 105.000 vrijwilligersuren van medewerkers. Deze voortdurende inzet voor mensen en de maatschappij is de reden waarom Salesforce al acht jaar op rij door Great Place to Work is erkend als een van de beste werkgevers in Nederland.

Het dreigingslandschap evolueert

De cybersecurity-bedreigingen en -ontwikkelingen waarmee Nederlandse organisaties in 2026 worden geconfronteerd, versnellen op een manier die we nog niet eerder hebben gezien. Zoals aangegeven in het rapport Threat Landscape 2025 van ENISA, nemen het aantal en de complexiteit van aanvallen sterk toe, terwijl aanvallers zich met de snelheid van machines voortbewegen en daarmee de detectie- en reactiemogelijkheden van veel organisaties te boven gaan.

Bovendien heeft AI de drempel voor geavanceerde aanvallen verlaagd. Ons eigen State of IT: Security-rapport, waarvoor meer dan 4.000 IT-leiders wereldwijd (waaronder meer dan 2.000 beveiligings- en compliance-specialisten) zijn ondervraagd, laat zien dat 80% van de IT-beveiligingsmanagers zowel het transformatieve potentieel van AI voor cyberbeveiliging inziet, als de nieuwe risico's die het met zich meebrengt, zoals data poisoning, model inversion en privacylekken. 75% van de organisaties verwacht hun beveiligingsbudgetten te verhogen als reactie op frequentere en geavanceerdere AI-gedreven bedreigingen. Tegelijkertijd zegt 75% van de IT-beveiligingsmanagers dat AI-aangedreven bedreigingen zich waarschijnlijk sneller zullen ontwikkelen dan traditionele cyberbeveiligingstools.

Het regelgevingslandschap is versplinterd

De Nederlandse Cyberbeveiligingswet (Cbw), die op 15 april 2026 door de Tweede Kamer is aangenomen en momenteel in behandeling ligt bij de Eerste Kamer, vormt een belangrijke stap voorwaarts bij de omzetting van NIS2 in nationale wetgeving. Het bredere Europese regelgevingslandschap ontwikkelt zich echter met wisselende mate van coördinatie:

- De implementatie van de NIS2-richtlijn verloopt nog steeds zeer ongelijkmatig binnen de EU. Sommige lidstaten (België, Italië, Denemarken) hebben wetgeving aangenomen; andere (Duitsland, Frankrijk) zijn hier nog mee bezig.
- De Europese AI-wet zal binnenkort volledig van kracht worden. Dit neemt een op risico gebaseerde nalevingsplicht met zich mee, die direct raakt aan cyberbeveiliging van AI-systemen die in kritieke sectoren worden ingezet.
- DORA is sinds januari 2025 van kracht en stelt verplichte eisen aan operationele weerstand, specifiek voor ICT-aanbieders in de financiële sector.

Deze wildgroei aan – vaak overlappende – kaders zorgt voor een reële compliance-last, vooral voor organisaties die grensoverschrijdend opereren. Het Nederlandse Cybersecurity Assessment 2025 (CSAN) vermeldt dat voor de gemiddelde organisatie de prioriteit moet liggen bij primaire digitale hygiëne en veerkracht. De complexiteit van het regelgevingslandschap dreigt echter de aandacht en middelen af te leiden van deze basisprincipes. Eigen onderzoek van Salesforce bevestigt deze druk: IT-beveiligingsmanagers zien de complexiteit van de regelgeving als een van de grootste operationele uitdagingen.

Agentic AI: de volgende grens

Agentic AI biedt zowel aanzienlijke kansen als een nieuw aandachtsgebied op het gebied van cyberbeveiliging. Het potentieel voor alle bedrijven en overheidsinstanties om complexe werkprocessen te automatiseren, de dienstverlening te verbeteren en de operationele lasten te verminderen, is reëel. Tegelijkertijd betekent het autonome en multisysteemkarakter van deze technologie dat beveiligingskaders die zijn ontworpen voor traditionele software of zelfs eerdere generaties van AI mogelijk niet toereikend zijn. Ervoor zorgen dat agentic AI binnen duidelijk omschreven grenzen functioneert, met passende toezichtmechanismen, is een gedeelde verantwoordelijkheid van technologieleveranciers, implementerende organisaties en toezichthouders.

Toezichthouders beginnen hierop te reageren. In februari 2026 lanceerde het Amerikaanse National Institute of Standards and Technology (NIST) haar ‘AI Agent Standards Initiative’, gericht op kaders voor identiteitsverificatie en authenticatie voor AI-agenten. In mei 2026 publiceerden cyberbeveiligingsinstanties uit de VS, Australië, Canada, Nieuw-Zeeland en het Verenigd Koninkrijk gezamenlijke richtlijnen voor de veilige implementatie van agentic AI. Nederland moet zich actief inzetten voor deze opkomende internationale normen.

De beveiligingsarchitectuur van Salesforce

De beveiligingsaanpak van Salesforce, die wordt geleid door onze kernwaarde ‘vertrouwen’, is gebaseerd op een fundamenteel principe: **cyberbeveiliging is een gedeelde verantwoordelijkheid van klanten en hun technologieleveranciers.**

Hoewel Salesforce beveiliging in al onze activiteiten integreert en de nodige tools en middelen biedt om klantgegevens te beschermen, werken we ook samen met onze klanten om hen te helpen bij het implementeren van beveiligingsmaatregelen en best practices. Zo versterken we gezamenlijk de beveiliging van hun Salesforce-omgeving.

Het platform van Salesforce is ontworpen met beveiliging in elke laag van onze architectuur, inclusief versleuteling, netwerkbeveiliging en zero-trust-principes. Belangrijke technische en organisatorische maatregelen, uiteengezet in onze publiekelijk beschikbare Security, Privacy and Architecture (SPARC)-documentatie, omvatten:

- **Versleuteling in rust en tijdens verzending:** met opties voor door de klant beheerd extern sleutelbeheer via in de EU gevestigde providers.
- **Bring Your Own Key (BYOK) en External Key Management (EKMS):** klanten behouden de cryptografische controle.
- **Situaties monitoren en veld audittrail:** onveranderlijke logboeken van elke gebruikersactie, die rechtstreeks kunnen worden geëxporteerd naar de SIEM-systemen van klanten voor realtime detectie van afwijkingen en nalevingsrapportage.
- **Security Health Check:** een standaardplatformfunctie die beveiligingsconfiguraties analyseert aan de hand van basisnormen en bruikbare aanbevelingen doet.
- **trust.salesforce.com**: een openbaar, realtime transparantieportaal dat de systeemstatus, incidentgeschiedenis en beschikbaarheidsprestaties wereldwijd weergeeft.

Naleving en certificeringen

Salesforce beschikt over een uitgebreid portfolio aan certificeringen, die allemaal up-to-date worden gehouden en jaarlijks door onafhankelijke derde partijen worden gecontroleerd. Deze zijn te raadplegen via compliance.salesforce.com.

Daarnaast hebben we complianceprogramma's voor alle belangrijke Europese regelgeving, waaronder de **AVG/GDPR**, **DORA** en de **EU Data Act**.

Aanbevelingen aan beleidsmakers

Salesforce doet de volgende aanbevelingen aan de commissie, gebaseerd op onze ervaring in het werken met ondernemingen en organisaties in de publieke sector in Nederland en Europa. Deze zijn erop gericht bij te dragen aan een samenhangend, toekomstbestendig nationaal cyberbeveiligingskader, dat effectief inspeelt op het snel evoluerende cyberbeveiligingslandschap dat we hierboven hebben beschreven:

- **Zet in op een consistente implementatie van NIS2 in de hele EU.** Uiteenlopende nationale interpretaties versnipperen de Europese beveiligingsperimeter en creëren onevenredige compliance-lasten voor organisaties die grensoverschrijdend opereren, waardoor middelen worden onttrokken aan daadwerkelijke beveiligingsverbeteringen. Nederland is goed gepositioneerd om het voortouw te nemen bij de harmonisatie en wederzijdse erkenning van certificeringen.
- **Werk samen met internationale partners.** Nederland moet proactief aansluiten bij de opkomende richtlijnen van NIST, ENISA en CISA op het gebied van agentische AI-beveiliging. Door, nauw samen te werken met technologieleveranciers kunnen nationale kaders risicogebaseerd en resultaatgericht worden geactualiseerd. Hierbij moeten prescriptieve technische voorschriften, die snel verouderd raken naarmate het dreigingslandschap evolueert, worden vermeden.
- **Investeer in publiek-private samenwerking om de landelijke weerstand te versterken.** Het dreigingslandschap verandert sneller dan welke toezichthouder dan ook in zijn eentje kan bijhouden. Een gestructureerde, op vertrouwen gebaseerde dialoog tussen het NCSC, de Autoriteit Persoonsgegevens en vertrouwde technologieleveranciers, naar het voorbeeld van de kaders voor informatie-uitwisseling die in de financiële sector al onder DORA functioneren, zou de nationale veerkracht aanzienlijk versterken zonder dat er nieuwe wetgeving nodig is.
- **Pak het tekort in cyberbeveiligingsvaardigheden aan.** Met een tekort van ongeveer 300.000 cyberbeveiligingsprofessionals in de hele EU zal geen enkel regelgevingskader slagen zonder de mensen om het uit te voeren. De overheid, de academische wereld en de technologiesector moeten gezamenlijk investeren in opleidingsprogramma's, onder meer via publiek-private partnerschappen op het gebied van opleiding en certificering.

Conclusie

Effectieve cyberbeveiliging in 2026 kan niet op één enkele actor rusten. Het vereist een model van gedeelde verantwoordelijkheid tussen de overheid, technologieleveranciers en eindgebruikersorganisaties. De aanpak van Salesforce weerspiegelt onze belangrijkste waarde, namelijk vertrouwen, en onze overtuiging dat technologieleveranciers verantwoordelijke, transparante en controleerbare partners moeten zijn in de nationale cyberweerbaarheid.