SECURITY OP GARTNER SYMPOSIUM 2026

WAT JE TEAM MEE NAAR HUIS MOET NEMEN

Van het ON2IT-team in Barcelona, met duiding van **Tim Timmermans, CISO Nederland**

Je team blikt deze week waarschijnlijk terug op Barcelona. ON2IT was er ook. Wij liepen de security-track nog een keer door, zodat jullie nabespreking korter kan. Hieronder zes dingen die Gartner op het scherm zette, wat ze volgens ons betekenen en wat je maandagochtend kunt doen. De cijfers zijn zoals Gartner ze in de sessies presenteerde.

01 PATCHSNELHEID IS EEN CIJFER VOOR DE BÜHNE

Frontier-AI-modellen vinden kwetsbaarheden sneller en maken het aanvallers makkelijker. Legacy-systemen houden het updatetempo niet bij, en een kale CVSS-score houdt geen rekening met je bedrijfscontext. Gartner verschuift de vraag aan de board van "hoe snel patchen we?" naar "hoe lang accepteren we dat we openstaan voor een bekende kwetsbaarheid?"

MAANDAG

Kies je vijf meest kritieke systemen en spreek per systeem een exposure-based SLA af: hoe lang een bekende, misbruikbare fout maximaal bereikbaar mag blijven.

ONZE KIJK

Een fout die je vandaag niet kunt patchen, kun je wel onbereikbaar maken. Blootstelling is een ontwerpkeuze, niet alleen een kwestie van patchplanning.

02 EERST JE AI-AGENTS VINDEN, DAN PAS BELEID

In een Gartner-survey onder 251 bestuurders (juli 2026) draait 74% al productiviteitsagents op endpoints in productie, en 28% gebruikt AI-browsers. De meest gemaakte fouten: agents zonder authenticatie, en agents met veel meer rechten dan hun taak vraagt. Opstellingen met meerdere agents doorbreken ongemerkt de functiescheiding: twee agents samen kunnen bij wat geen enkele medewerker mag.

MAANDAG

Maak een lijst van je agents, met eigenaar, toepassing en rechten. Binnen 90 dagen: een beveiligingsbeleid en toegangsmodel voor agents. Binnen 12 maanden: adversarial testing, least privilege en detectie van intent drift.

ONZE KIJK

Dit is Zero Trust voor agents: elke agent een eigen identiteit, zo min mogelijk bevoegdheden en niets standaard vertrouwd. Mensen en agents hebben hetzelfde probleem: handelingsruimte.

03 SCHADUW-AI IS EERST EEN MENSENPROBLEEM

De mens blijft de belangrijkste aanvalsvector, en AI maakt phishing, deepfakes en helpdeskfraude goedkoper. Volgens Gartner gebruikt 57% van de medewerkers een persoonlijk GenAI-account voor hun werk, geeft 33% toe gevoelige werkinformatie in publieke of niet-goedgekeurde tools te stoppen en gebruikt 36% niet-goedgekeurde GenAI-apps op werkapparaten. Alles blokkeren drijft AI ondergronds. Gartner zoekt het midden tussen streng en ruim: eerst zicht, dan coachen op het moment zelf.

> **MAANDAG**
>
> Zoek uit welke AI-tools echt gebruikt worden, goedgekeurd of niet, voordat je het beleid schrijft.

04 AI IN DE SOC: VERSTERKEN, NIET VERVANGEN

Gartners 2026 Cybersecurity Technology Adoption Roadmap (142 securityleiders) laat zien dat AI voor security dreigt vast te lopen in de pilotfase: onvoorspelbare kosten, schaars talent en risico's in de leveranciersketen. Het levert wel op bij het verrijken van alerts, het herkennen van false positives, het prioriteren van kwetsbaarheden en input voor third-party risk. Het advies van Gartner: houd altijd een mens in de loop, investeer de tijd die je wint in vaardigheden, en bescherm de vaardigheden die je niet kwijt wilt raken, zoals threat modeling en het controleren van de false positives van de AI zelf.

> **MAANDAG**
>
> Kijk kritisch naar pilots die weinig opleveren. Bouw je securitytechnologiestrategie rond één hoofddoel: minder blootstelling, snellere incidentrespons of de laagste totale kosten.

05 CONSOLIDATIE SNIJDT AAN TWEE KANTEN

Platformen passen bij volwassen domeinen, maar te ver consolideren maakt een single point of failure. Gartner adviseert om leveranciers eerst te scoren met de Vendor Trust Index. De sessie over continuïteit was directer: extreme verstoring ontstaat als meerdere aannames tegelijk onderuitgaan (cloud, leverancier, geopolitiek). Winnen betekent dat je je minimaal levensvatbare organisatie draaiende houdt, en identiteit als eerste herstelt. Over soevereiniteit: een volledig soevereine stack is vandaag geen realistisch doel. Bouw je "soevereine technische schuld" af en spreid hem, in sprints van drie jaar.

> **MAANDAG**
>
> Breng je single points of failure in kaart, ook bij de leveranciers van je leveranciers. Oefen herstel als onderdeel van het gewone werk, niet één keer per jaar.

06 QUANTUM EN REGELGEVING: DE KLOK TIKT

De helft van de organisaties is nog niet begonnen met postquantum, terwijl aanvallers nu al versleutelde data verzamelen om die later te ontsleutelen. Bij AI-regelgeving schoof de EU AI Act op: de regels voor hoog risico gelden nu vanaf december 2027, de rest vanaf augustus 2028. Wereldwijd zijn er meer dan 1.800 AI-wetten, -regels en -richtlijnen. Gartner: "Het doel is niet langer compliance. Het is regulatory resilience."

> **MAANDAG**
>
> Begin met een inventarisatie van je cryptografie en van de plekken waar AI in je processen beslissingen neemt. Beide zijn stap één van elke roadmap die Gartner liet zien.

WAT GARTNER NIET ZEI

Een week vol slides over AI-governance, en op geen enkele stond: plak je wachtwoord niet in de AI-browser. Frameworks zijn de plattegrond. Gewoontes zijn het huis. Drie gewoontes die we zelf hanteren:

01
Niemand typt inloggegevens in een AI-browser of AI-assistent.

02
Geen agent draait op een geleend account of een serviceaccount. Elke agent krijgt een eigen identiteit.

03
Geen assistent krijgt rechten om te verwijderen of te versturen als hij die voor zijn ene taak niet nodig heeft.

"SLECHTE GOVERNANCE IS EEN BELASTING OP AI. GOEDE GOVERNANCE VERSNELT DE WAARDE."

Gartner, sessie Practical AI Governance

SPREEK DE AUTEUR

TWINTIG MINUTEN MET TIM TIMMERMANS

Wil je doorpraten met de expert die dit rapport schreef? We plannen twintig minuten met Tim Timmermans, onze CISO. Geen slides, geen productpitch.

Tim Timmermans, CISO Nederland, ON2IT

on2it.net/contact

PLAN HET GESPREK →

Bronnen: Gartner IT Symposium/Xpo 2026, Barcelona, sessies: Top Trends in Cybersecurity for 2026 (Akif Khan); Gartner's 2026 Cybersecurity Technology Adoption Roadmap for CIOs (Leigh McMullen, Christine Lee); The CIO 2027 Cybersecurity Radar (Leigh McMullen); AI Agents: Cybersecurity Strategies for Enterprise Protection (Dionisio Zumerle); Practical AI Governance (Nader Henein); European CIOs Sovereign Strategy Playbook (Nader Henein); Business Continuity Planning for Extreme Disruptions (Charlie Winckless). De cijfers zijn zoals Gartner ze presenteerde en niet onafhankelijk geverifieerd. De selectie, de interpretatie en "Onze kijk" zijn van ON2IT en niet onderschreven door Gartner.