STRATEGISCHE DREIGINGSANALYSE WEEK 16

Briefing Cyberspace | Digiweerbaar BV

Periode: 11 - 17 april 2026 | Classificatie: TLP:AMBER

Kernboodschap: Nederland en België verankerden deze week tegelijkertijd de Europese NIS2 richtlijn in nationaal recht. De Tweede Kamer stemde in met de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, wat betekent dat meer dan 8.000 Nederlandse organisaties binnen afzienbare tijd een wettelijke zorgplicht krijgen, in België liep op 18 april de deadline voor 2.410 essentiële entiteiten af. Tegelijk bevestigde ChipSoft diefstal van patiëntgegevens en publiceerden Britse onderzoekers de langetermijnimpact van de Synnovis ransomwareaanval van juni 2024, 161.560 vertraagde pathologierapporten, 122 patiëntveiligheidsincidenten en een patiëntoverlijden waarbij de cyberaanval als bijdragende factor werd aangemerkt. De derde lijn is de industrialisering van SaaS gerichte afpersing door ShinyHunters, met bevestigde slachtoffers McGraw Hill (13,5 miljoen gebruikers), Amtrak (2,1 miljoen e-mailadressen), Hallmark (1,7 miljoen) en Rockstar Games via een inbreuk bij cloud leverancier Anodot. Organisaties die hun leveranciersketen niet kunnen aantonen, kunnen volgende maand niet aantonen dat zij voldoen.

1. NIS2 wordt wettelijke werkelijkheid in Nederland en België ? NIEUW

De Nederlandse Tweede Kamer stemde deze week in met de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke). De Cbw implementeert de Europese NIS2 richtlijn en vervangt de huidige Wbni, de Wwke implementeert de Critical Entities Resilience richtlijn. Het werkterrein van het Nationaal Cyber Security Centrum groeit hiermee naar meer dan 8.000 organisaties, waaronder zorgaanbieders, luchthavens, kredietinstellingen en energieleveranciers. De wetsvoorstellen gaan naar de Eerste Kamer, inwerkingtreding wordt verwacht in het tweede kwartaal van 2026. In België liep op 18 april de NIS2 deadline voor essentiële entiteiten af, waarbij 2.410 organisaties uit kritieke sectoren actie ondernamen in wat het Cyber Security Centre Belgium beschrijft als de grootste cybersecurity operatie ooit in het land. Nederland is hiermee trager dan België, dat samen met Kroatië als enige de oorspronkelijke oktober 2024 deadline haalde.

Parallel kondigde de Autoriteit Persoonsgegevens preventieve controles aan bij ICT leveranciers, een expliciete beleidsverschuiving van reactief toezicht naar proactieve handhaving. Dit sluit aan bij de Kamervragen van D66 en GroenLinks-PvdA over de marktconcentratie van EPD leveranciers naar aanleiding van ChipSoft.

Wat dit betekent voor uw organisatie: de overgangsperiode is voorbij. Als uw organisatie onder de definities van NIS2 of CER valt, bent u binnen maanden onderhevig aan zorgplicht, meldplicht en registratieplicht. De aangekondigde preventieve controles van de Autoriteit Persoonsgegevens betekenen dat toezichthouders niet wachten op een incident maar actief beoordelen of uw leveranciersrisicobeheer op orde is. Bestuursaansprakelijkheid is expliciet in NIS2 verankerd, dit is niet langer een IT vraagstuk maar een juridisch en bestuurlijk risico.

2. ChipSoft escaleert van incident naar systeemcrisis ? ESCALEERT

Week 15 toonde elf Nederlandse ziekenhuizen die hun patiëntportalen uit voorzorg offline haalden. Week 16 voegt twee kwalitatieve verschuivingen toe. ChipSoft bevestigde diefstal van patiëntgegevens en medische gegevens, de Autoriteit Persoonsgegevens ontving datalekmeldingen van meerdere ziekenhuizen. Volgens Tweakers gebruiken circa vijftien Nederlandse ziekenhuizen de getroffen dienst. De patiëntportalen bleven dagenlang offline, wachttijden in ziekenhuizen liepen op. Parallel publiceerde het Verenigd Koninkrijk de langetermijnimpact van de Synnovis ransomwareaanval van juni 2024, 161.560 pathologierapporten zijn vertraagd in patiëntendossiers vanaf januari 2026, 122 patiëntveiligheidsincidenten werden geregistreerd en King's College Hospital registreerde een patiëntoverlijden waarbij de cyberaanval als bijdragende factor werd aangemerkt.

De politieke respons was vrijwel direct. D66 en GroenLinks-PvdA (Kamerleden Bushoff en Kathmann) stelden vragen over de marktconcentratie waarbij één leverancier circa 70 procent van het Nederlandse ziekenhuislandschap bedient. Het Ministerie van Binnenlandse Zaken adviseerde Odido slachtoffers eerder al hun paspoort niet te vernieuwen, wat de langetermijnimpact van dit type incidenten onderstreept.

Wat dit betekent voor uw organisatie: Synnovis toont wat ChipSoft kan worden als het onderzoek zich de komende maanden verdiept. Een ransomwareaanval van juni 2024 leidt achttien maanden later tot geregistreerde patiëntveiligheidsincidenten en een patiëntoverlijden. Wanneer uw organisatie afhankelijk is van één dominante leverancier voor een kernproces, moet u niet alleen continuïteitsplannen hebben maar ook de juridische positie opnieuw waarderen. Artikel 28 AVG maakt u mede aansprakelijk wanneer uw verwerker onvoldoende beveiligd blijkt. De Kamervragen tonen dat marktconcentratie zelf een politiek risico is geworden, diversificatie van kritieke leveranciers wordt een compliance onderwerp, niet alleen een operationeel.

3. Benelux incidenten via SaaS toeleveringsketens bereiken sectorbreedte ? ESCALEERT

Binnen één week raakten in de Benelux Basic-Fit (200.000 Nederlandse leden plus een onbekend aantal Belgische leden, met naam, adres, bankgegevens en geboortedatum), de Dienst Justitiële Inrichtingen (hack van de Ivanti EPMM server met medewerkerdata, staatssecretaris Van Bruggen bevestigde aanvullend risico op chantage en afpersing) en Booking.com (onbevoegde derden toegang tot boekingsgegevens, verhoogd AI phishing risico). Internationaal claimde ShinyHunters deze week Rockstar Games (via een inbreuk bij Anodot, een SaaS leverancier voor cloudkostenmonitoring die vertrouwde Snowflake tokens hield), Hallmark (1,7 miljoen e-mails), McGraw Hill (bevestigd 13,5 miljoen gebruikers via een Salesforce misconfiguratie, 100 gigabyte gepubliceerd) en Amtrak (2,1 miljoen e-mailadressen). De Franse Basketbalfederatie FFBB verloor data van 1,9 miljoen leden en circa 800.000 ouders aan dreigingsactor HexDex, inclusief gegevens van minderjarigen en medische certificaten.

Het patroon is expliciet. Niet de organisatie zelf maar een SaaS leverancier, een cloudintegratie of een Salesforce configuratie vormt het primaire toegangspunt. Payouts King, een ransomwaregroep gelieerd aan voormalige BlackBasta affiliates, verkreeg initiële toegang via blootgestelde SonicWall en Cisco SSL VPN's en tunnelde via QEMU emulators om detectie te omzeilen.

Wat dit betekent voor uw organisatie: elke SaaS integratie is nu een potentieel toegangspunt tot uw hele organisatie. Een ketenrisicoanalyse die beperkt blijft tot directe leveranciers mist het pad Anodot - Snowflake - Rockstar. Artikel 21 lid 2d van NIS2 vereist expliciet beveiliging van de toeleveringsketen inclusief indirecte afhankelijkheden. De combinatie van Basic-Fit, DJI, Booking.com en Basic-Fit in één week toont dat geen enkele sector immuun is. Voor verwerkingsverantwoordelijken onder AVG artikel 28 betekent dit dat het auditen van uw verwerkers een terugkerend proces moet worden, niet een eenmalige oefening.

4. AI industrialiseert als aanvalsinstrument ? NIEUW

Deze week verschenen vier afzonderlijke bewijzen van AI gedreven aanvallen die de commercialiseringslijn tonen. Een valse Anthropic website verspreidde PlugX malware via een bestand genaamd Claude-Pro-windows-x64.zip, verspreid door spamcampagnes Kingmailer en CampaignLark. Een ethisch hacker demonstreerde dat een complete phishingpagina kan worden gegenereerd in minder dan dertig minuten via Claude AI. Het vishing platform ATHR werd geïdentificeerd op underground forums voor 4.000 dollar plus tien procent commissie, met geautomatiseerde telefonische aanvallen op acht diensten waaronder Google, Microsoft, Coinbase en Binance. Parallel werd de Digital Age Verification App van de Europese Commissie binnen twee minuten na lancering op 14 april gekraakt door onderzoekers die een volledige authenticatie bypass demonstreerden, inclusief pincode bypass, rate limit bypass en biometrische bypass. Deze laatste combinatie toont dat ook overheidssoftware niet is gevrijwaard van snelle aanvalsontwikkeling.

Wat dit betekent voor uw organisatie: AI is niet langer alleen een verdedigingsinstrument dat uw Security Operations Center ondersteunt, maar een commercieel aanvalsinstrument dat elke medewerker rechtstreeks kan raken. Een telefoontje dat overtuigend klinkt, een e-mail met perfecte grammatica in de stijl van uw leverancier, een phishingpagina die niet van echt te onderscheiden is, dat is deze week standaard geworden. Uw awareness programma moet worden herzien, visuele afwijkingen en spelfouten zijn niet langer betrouwbare signalen. Verplichte terugbelprocedures voor financiële en beveiligingsgerelateerde verzoeken worden de minimumstandaard. De kraak van de EU leeftijdsverificatie app toont dat ook software met overheidsvalidatie niet automatisch betrouwbaar is.

5. Handhaving synchroniseert tussen landen en sectoren ? ESCALEERT

De Nederlandse Autoriteit Persoonsgegevens kondigde preventieve controles aan bij ICT leveranciers, een structurele verschuiving van reactief naar proactief toezicht. De Europese wetshandhaving rondde een nieuwe fase van Operatie PowerOFF af waarbij meer dan 75.000 DDoS gebruikers werden geïdentificeerd en 53 domeinen werden uitgeschakeld, Europol gaat nu de preventiefase in met bewustmakingscampagnes gericht op jongeren. Het Nederlandse kabinet investeert 3,7 miljoen euro in digitale weerbaarheid voor het midden- en kleinbedrijf via Cybersecurity learning communities en het CYRCLE project. De Toezichthouder Inlichtingen en Veiligheidsdiensten rapporteerde dat AIVD en MIVD inzet in 2025 voor 1,3 procent van de gevallen onrechtmatig was, wat neerkomt op ongeveer één incident per week, de overige 96 procent was rechtmatig. De Kamervragen van D66 en GroenLinks-PvdA over ChipSoft koppelen de ransomwareaanval aan een bredere discussie over marktconcentratie van EPD leveranciers.

De verschuiving is significant. Toezichthouders wachten niet langer op incidenten, zij controleren proactief. Wetshandhaving beweegt van opsporing naar preventie. Het parlement koppelt techniek aan marktordening.

Wat dit betekent voor uw organisatie: de toezichtlogica verschuift fundamenteel. Tot nu toe kon een organisatie wachten tot een incident of melding voordat de Autoriteit Persoonsgegevens aandacht gaf, de preventieve controles maken dat uw beveiligingsdocumentatie op elk moment beschikbaar moet zijn. NIS2 compliance moet aantoonbaar zijn, niet verklaarbaar achteraf. De 75.000 geïdentificeerde DDoS gebruikers tonen dat ook uw medewerkers en klanten in beeld komen bij internationale wetshandhavingsacties, een awareness component die verder gaat dan alleen phishing. De combinatie van handhaving, opsporing en parlementaire aandacht betekent dat cybersecurity bestuurlijk toezicht krijgt in meerdere dimensies tegelijk.

Strategisch Raamwerk: Drie Verdedigingslagen

Laag 1 - Operationele Hygiene (deze en volgende week)

- Patch Marimo naar versie 0.23.0 onmiddellijk of blokkeer `/terminal/ws` op netwerkniveau (CVE-2026-39987, CVSS 9.3, actief misbruikt binnen tien uur na openbaarmaking)
- Patch Microsoft SharePoint (CVE-2026-32201, actief misbruikt, CISA KEV), Cisco Secure Firewall Management Center (CVE-2026-20131, zero day Interlock ransomware) en SAP Business Planning en Warehouse (CVE-2026-27681, CVSS 9.9)
- Audit alle Salesforce en Snowflake integraties op misconfiguratie en niet geauthenticeerde toegangspunten (les van ShinyHunters week met Rockstar, Hallmark, McGraw Hill, Amtrak)
- Verifieer blootstelling van SonicWall en Cisco SSL VPN instanties (Payouts King gebruikt deze als primaire initiële toegang)
- Instrueer medewerkers over de valse Claude installer, itsme vishing en nep DPD SMS campagnes, update het awareness programma met AI gegenereerde voorbeelden

Laag 2 - Architecturele Aanpassing (komende maanden)

- Bouw een ketenrisicoregister dat indirecte SaaS afhankelijkheden in kaart brengt, Anodot toont dat vertrouwde cloud kostenmonitoring het pad kan zijn naar de Snowflake omgeving van een speluitgever (les van Rockstar Games via Anodot)
- Implementeer verplichte terugbelprocedures voor financiële en beveiligingsverzoeken, de combinatie van itsme fraude en ATHR vishing platform maakt stemauthenticatie onvoldoende (les van Safeonweb waarschuwing België)
- Plan een NIS2 gap analyse die ook de Wwke criteria omvat als uw organisatie essentiële diensten levert, wacht niet op de Eerste Kamer (les van BE 2.410 entiteiten die actie ondernamen voor de deadline)
- Herzie uw dataclassificatie bij educatieve uitgevers, platformaanbieders en detailhandel met loyaliteitsprogramma's, 13,5 miljoen records van McGraw Hill en 200.000 Basic-Fit leden tonen dat secundaire databases evenveel impact hebben als primaire (les van ShinyHunters focus op marketing datasets)

Laag 3 - Strategische Transformatie (komende kwartalen)

- Herpositioneer leveranciersbeheer als bestuurlijk agendapunt met kwartaalrapportage, de Kamervragen over ChipSoft maken marktconcentratie tot politiek onderwerp en beïnvloeden inkoopbeleid (les van Tweede Kamer D66 en GroenLinks-PvdA)
- Bereid uw organisatie voor op Autoriteit Persoonsgegevens controles die geen aanleiding nodig hebben, documentatie moet op elk moment beschikbaar zijn en extern verifieerbaar (les van aangekondigde preventieve ICT controles)
- Investeer in AI weerbaarheid aan zowel aanvals- als verdedigingszijde, het vishing platform ATHR voor 4.000 dollar en PlugX via valse Claude installer tonen dat de drempel voor AI gedreven aanvallen is gedaald naar midden segment criminaliteit (les van FBI IC3 rapport 2025 met 893 miljoen dollar AI gefaciliteerde fraude)
- Herdefinieer cyberweerbaarheid als meetbaar en rapporteerbaar bestuurlijk kader analoog aan financiële controle, NIS2 en Wwke maken dit niet alleen wenselijk maar wettelijk verplicht vanaf het tweede kwartaal 2026

Slotverklaring

13,5 miljoen McGraw Hill gebruikers bevestigd. 2,1 miljoen Amtrak e-mailadressen gepubliceerd. 200.000 Basic-Fit leden met bankgegevens in verkeerde handen. 161.560 Synnovis pathologierapporten achttien maanden na de aanval nog vertraagd, met een patiëntoverlijden waarbij de cyberaanval als bijdragende factor werd aangemerkt. 2.410 Belgische entiteiten die op 18 april aan NIS2 moesten voldoen. 8.000 plus Nederlandse organisaties die binnen maanden dezelfde verplichting krijgen. Dit is de werkelijkheid van de week van 11 tot 17 april 2026. De tijd dat cybersecurity een technische specialisatie was binnen de IT afdeling is deze week juridisch en feitelijk afgesloten. Het verschil tussen de organisaties die volgende maand compliant zijn en de organisaties die dat niet zijn, is de beslissing die vandaag op het bestuursniveau wordt genomen.

Bronnen: Rijksoverheid en Tweede Kamer (Cyberbeveiligingswet en Wwke aangenomen), CCB België (NIS2 deadline 18 april 2.410 entiteiten), Autoriteit Persoonsgegevens (preventieve ICT leveranciercontroles), Tweakers en NOS (ChipSoft vijftien ziekenhuizen en bevestigde datadiefstal), South London and Maudsley NHS Foundation Trust (Synnovis 161.560 vertraagde rapporten en 122 veiligheidsincidenten), King's College Hospital (patiëntoverlijden aanmerking), Have I Been Pwned (McGraw Hill 13,5 miljoen, Amtrak 2,1 miljoen, Hallmark 1,7 miljoen), Rijksoverheid (DJI staatssecretaris Van Bruggen), Basic-Fit persbericht, Sysdig en NVD (CVE-2026-39987 Marimo), CISA KEV catalogus (CVE-2026-32201, CVE-2026-20131, CVE-2026-34621), Cybercrimeinfo (HexDex FFBB monitoring), Europol (Operatie PowerOFF 75.000 DDoS gebruikers), Kamervragen D66 en GroenLinks-PvdA (ChipSoft marktconcentratie), Sophos en onderzoeksrapporten (ATHR vishing platform, valse Claude installer, EU Digital Age Verification App kraak)

Rapport samengesteld door Digiweerbaar BV | digiweerbaar.nl