STRATEGISCHE DREIGINGSANALYSE WEEK 10

Briefing Cyberspace | Digiweerbaar BV

Periode: 1 - 7 maart 2026 | Classificatie: TLP:AMBER

Kernboodschap: De scheiding tussen fysieke oorlogsvoering en digitale infrastructuur bestaat niet meer. Iraanse drones vernietigden AWS datacenters, een autonome AI compromitteerde zes grote repositories zonder menselijke sturing en het Nederlandse parlement eiste via vier moties actie op digitale soevereiniteit. Dit is een structurele verschuiving die directe gevolgen heeft voor uw continuiteitsplanning, uw leveranciersbeleid en uw compliance.

1. Fysieke Aanvallen op Digitale Infrastructuur ? NIEUW

Iraanse drones troffen drie AWS datacenters in de VAE en Bahrein als vergelding voor "Operation Epic Fury". Twee van drie Availability Zones vielen uit. Meer dan 60 diensten werden verstoord. Iran compromitteerde ook Hikvision en Dahua camera's voor doelcorrectie bij raketaanvallen via vijf bekende kwetsbaarheden.

Wat dit betekent voor uw organisatie: spreiding over meerdere cloudregio's is niet langer optioneel. AWS heeft bevestigd dat gelijktijdig verlies van meerdere Availability Zones niet in hun standaard architectuur was voorzien. Geopolitiek risico wordt een selectiecriterium voor datacenterlocatie onder NIS2.

2. AI Versnelt Beide Zijden van de Wapenwedloop ? NIEUW

De autonome bot "hackerbot-claw" opereerde een week zonder menselijke sturing, scande 47.000 repositories en bereikte bij vier grote projecten willekeurige uitvoering van code. Bij Trivy (32.000 sterren) werden alle 178 releases gewist. APT36 zette AI in om malware te produceren die traditionele detectie omzeilt. Aan de verdedigingskant vond geautomatiseerde analyse 22 kwetsbaarheden in Firefox en verminderde nieuwe tooling de ruis bij alerts met 84 procent.

Wat dit betekent voor uw organisatie: geautomatiseerde aanvallen opereren sneller dan menselijke verdedigers kunnen reageren. Controleer of uw CI/CD pipelines beschermd zijn tegen ongeautoriseerde pull requests. NIS2 vereist passende technische maatregelen, in 2026 betekent dat geautomatiseerde detectie.

3. Zes Benelux Organisaties Geraakt door Ransomware ? ESCALEERT

- Odido, 6,2 miljoen accounts (21 miljoen records volgens ShinyHunters), paspoort en IBAN nummers gepubliceerd. Medewerkers van ASML, Philips, ProRail, politie, Schiphol en ESA getroffen. Losgeld van 500.000 euro geweigerd
- AkzoNobel, Anubis ransomware, 170 GB data uit de Amerikaanse vestiging
- BK Group Amsterdam, Akira ransomware bij DNB geregistreerd trustkantoor
- Netwerk NV (Dordrecht), AiLock ransomware | Abutriek Service NV (Belgie), Qilin ransomware
- Brussels Airlines, winst gehalveerd mede door cyberaanval op Brussels Airport

Het misbruik van beheertools op afstand steeg met 277 procent (bron: Huntress). De meest misbruikte tools, ScreenConnect, AnyDesk en Atera, staan in veel Benelux organisaties standaard geinstalleerd.

Wat dit betekent voor uw organisatie: zes organisaties in een week is een patroon. Controleer of beheertools in uw omgeving via een allowlist zijn afgeschermd. Als u Odido als telecomprovider gebruikt, beoordeel dan of u een eigen melding moet doen bij de AP, medewerkers van grote organisaties zijn al doelwit van gerichte phishing.

4. Aanvalsinnovatie via de Toeleveringsketen ? ESCALEERT

Naast beheertools (sectie 3) zien we drie aanvullende routes: gekloonde softwarepagina's bovenaan in Google die malware verspreiden, het Chinese netwerk Funnull dat knooppunten in contentnetwerken vergiftigde (meer dan een miljoen gebruikers per dag), en de groep Velvet Tempest die 12 dagen onopgemerkt bleef in een omgeving met 3.000 endpoints.

Wat dit betekent voor uw organisatie: controleer of medewerkers software alleen via goedgekeurde kanalen downloaden. NIS2 artikel 21 verplicht u de beveiliging van uw toeleveringsketen te borgen. 12 dagen onopgemerkte aanwezigheid laat zien wat er misgaat zonder die borging.

5. Regelgeving en Digitale Soevereiniteit -> VERSNELT

Vier Kamermoties signaleren een kantelpunt: servers voor DigiD in Nederlandse handen, handelingskader voor slachtoffers van datalekken, nationaal basispakket digitale veiligheid en stresstest clouddiensten ministeries. De AP waarschuwde dat de Impactbarometer voor AI verslechtert. Het CBS meldde 2,5 miljoen slachtoffers van online criminaliteit in 2025.

Wat dit betekent voor uw organisatie: de politieke druk op digitale soevereiniteit groeit snel. Organisaties die nu afhankelijkheden van buitenlandse cloudleveranciers in kaart brengen, lopen vooruit op regelgeving die eraan komt.

Strategisch Raamwerk: Drie Verdedigingslagen

Laag 1 - Operationele Hygiene (deze en volgende week)

- Patch Cisco Secure Firewall Management Center (CVE-2026-20079, CVSS 10.0, geen workaround, root access)
- Patch Windows Server Update Service (CVE-2025-59287, CVSS 9.8, actief misbruikt sinds oktober 2025)
- Blokkeer WordPress User Registration exploits (CVE-2026-1492, 200+ pogingen per 24 uur)
- Audit Hikvision en Dahua camera's op vijf actief misbruikte kwetsbaarheden (bewezen inzet als wapen)
- Controleer Android devices op patches van maart (CVE-2026-21385 actief aangevallen)

Laag 2 - Architecturele Aanpassing (komende maanden)

- Allowlist voor beheertools, blokkeer ongeautoriseerd gebruik (les van 277 procent stijging)
- Cloudcontinuiteit evalueren bij verlies van meerdere Availability Zones (les van AWS incident)
- MFA voor alle authenticatiepaden (7 gedocumenteerde omzeilroutes deze week)
- CI/CD pipelines beveiligen tegen ongeautoriseerde pull requests (les van hackerbot-claw)

Laag 3 - Strategische Transformatie (komende kwartalen)

- Transitie naar AI ondersteunde detectie en respons, handmatige analyse kan de snelheid niet meer bijhouden
- Afhankelijkheden buitenlandse cloud in kaart brengen inclusief geopolitiek risico (versterkt door Kamermoties)
- Voorbereiding op aangescherpt beleid rond digitale soevereiniteit en compensatie bij datalekken

---

Slotverklaring

Drie AWS datacenters vernietigd door drones. Een autonome bot die zes grote repositories compromitteerde. Zes Benelux organisaties geraakt door ransomware. 6,2 miljoen Odido accounts op straat. Vier Kamermoties die het digitale beleid wijzigen. Dit is de week van 1 tot 7 maart 2026. Elke dag dat uw organisatie wacht met het aanpassen van continuiteitsplannen, leveranciersbeleid

en detectiecapaciteit, is een dag waarop dit risico onbeheerd blijft.

Bronnen: Cybercrimeinfo dagelijkse dreigingsrapportages 1-7 maart 2026, CISA KEV catalog, NCSC, Huntress 2026 Cyber Threat Report, Palo Alto Unit 42 (CVE-2025-59287), StepSecurity/Cybernews (hackerbot-claw), CNBC/Bloomberg/Fortune (AWS drone strikes), Tweede Kamer der Staten-Generaal, CBS Veiligheidsmonitor 2025

Rapport samengesteld door Digiweerbaar BV | digiweerbaar.nl