Digiweerbaar BV

# Briefing Cyberspace

## Weekoverzicht Week 10 | 1-7 maart 2026

| 6,5M | 15 | 8 | 4 |
|---|---|---|---|
| Odido slachtoffers | Kritieke CVE's | Staatshackergroepen | Ransomware NL/BE |

Classificatie: TLP:AMBER | Alleen voor geautoriseerde ontvangers

# Executive Summary - Top 3 Dreigingen

**KRITIEK** **Odido, het grootste datalek in de Nederlandse geschiedenis**

6,5 miljoen klanten getroffen. ID nummers, bankrekeningen, adressen gepubliceerd. 16.300 medewerkers van vitale bedrijven (NXP, Philips, ProRail, TenneT, politie, Schiphol, ASML) betrokken. Phishing op basis van gelekte data is actief.

**KRITIEK** **Ransomware golf in de Benelux, 4 slachtoffers in 1 week**

Akira trof BK Group Amsterdam (trustkantoor/DNB). Qilin claimde Abutriek (BE). AiLock publiceerde Netwerk NV Dordrecht. Anubis claimt 170 GB bij AkzoNobel.

**HOOG** **Staatshackers op alle fronten actief**

APT28 (Rusland) exploiteert actief twee Microsoft CVE's. APT41 (China) richt zich op Europese overheden. APT36 (Pakistan) gebruikt AI voor massaproductie malware. In totaal 8 groepen uit 5 landen.

# Patchoverzicht + Trending CVE's + KEV

## Kritieke patches deze week

| Product | CVE | CVSS | Status |
|---|---|---|---|
| Microsoft MSHTML | CVE-2026-21513 | 8.8 | **APT28** |
| Microsoft Office | CVE-2026-21509 | 7.8 | **APT28** |
| Cisco Firewall MC | CVE-2026-20079 | 10.0 | **Actief** |
| BeyondTrust | CVE-2026-1731 | 9.8 | **Ransomware** |
| Cisco SD-WAN | CVE-2026-20127 | 10.0 | **CISA KEV** |
| WordPress plugin | CVE-2026-1492 | 9.8 | **200+/24u** |

## NL/BE Top 5 misbruikt (CISA/NCSC)

| CVE | Product | EPSS |
|---|---|---|
| CVE-2026-1731 | BeyondTrust | **64.6%** |
| CVE-2026-20127 | Cisco SD-WAN | 2.6% |
| CVE-2022-20775 | Cisco SD-WAN | 0.5% |
| CVE-2026-22719 | VMware Aria | 7.4% |
| CVE-2026-2441 | Chromium | 0.1% |

**Weekcijfer:** 90 zerodays in 2025 (+15%). 48.196 CVE's, 132/dag. KEV +30% naar 241.

# Datalekken & Incidenten

| Organisatie | Wat is er gebeurd | Impact |
|---|---|---|
| **Odido** (NL) KRITIEK | Volledige dataset gepubliceerd door ShinyHunters | 6,5M klanten, ID's, bankrek., 16.300 vitale medewerkers |
| **BK Group** (NL) | Ransomware Akira, trustkantoor bij DNB | Financiele diensten, wealth management |
| **SkiWebShop** (NL) | Klantgegevens op darkweb te koop | 81.000 klantgegevens |
| **AkzoNobel** (NL) | Claim Anubis ransomware (niet bevestigd) | 170 GB, 169.000 bestanden |
| **Mall of NL** (NL) | Ongeautoriseerde databasetoegang | Loyaliteitsprogramma + nieuwsbrief data |
| **Netwerk NV** (NL) | AiLock ransomware, Dordrecht | Omvang onbekend |
| **Abutriek** (BE) | Qilin ransomware, Anzegem | Dubbele afpersing |
| **Brussels Airlines** (BE) | Cyberaanval halveerde winst 2025 | 9,1M passagiers, 1,6 mrd omzet |

**Nederland: 6 incidenten in 1 week.** Odido is het grootste datalek in de Nederlandse geschiedenis.

# Dreigingsactoren - Wie was actief

## Staatshackers (8 groepen, 5 landen)

| Actor | Land | Activiteit |
|---|---|---|
| APT28 | Rusland | CVE-2026-21513/21509, BadPaw + MeowMeow |
| APT41 | China | Cobalt Strike, Google Drive C2 |
| APT36 | Pakistan | AI malware in Nim, Zig, Crystal |
| APT37 | N-Korea | USB malware, air gapped systemen |
| CL-UNK-1068 | China | Telecom/energie espionage |
| UAT-9244 | China | Telecom Zuid-Amerika |
| Dust Specter | Iran | SPLITDROP, GHOSTFORM |
| Iraanse groepen | Iran | DDoS, ICS aanvallen |

## Ransomware in NL/BE

| Groep | Slachtoffer | Profiel |
|---|---|---|
| **Akira** | BK Group (NL) | 620+ slachtoffers, ~$244M |
| **Qilin** | Abutriek (BE) | 1.500+ slachtoffers |
| **AiLock** | Netwerk NV (NL) | Nieuw sinds begin 2025 |
| **Anubis** | AkzoNobel (NL) | Niet bevestigd |
| **ShinyHunters** | Odido (NL) | 1-10M losgeld geëist |

Trend: China domineert met 4 groepen. AI wordt ingezet voor malwareproductie (APT36).

# Awareness - Doorsturen naar teams

### Odido phishing (NL, actief)
Valse compensatieformulieren en neptelefontjes. Medewerkers worden gericht benaderd met echte naam en adres uit het datalek.

### ClickFix campagnes (wereldwijd)
Malvertising leidt naar valse CAPTCHA pagina's. Gebruikers voeren Windows Run commando uit dat malware installeert (Lumma Stealer, CastleRAT).

### Valse software updates
Nep Zoom/Teams/Adobe updates via gestolen EV certificaten. Passeren standaard beveiligingscontroles.

### Fake tech support (VS/EU)
Voice phishing leidt tot Quick Assist installatie, daarna RMM tools + Havoc C2 voor volledige toegang.

### Watergroep phishing (BE)
Valse compensatie e-mails (€124) in Zelzate. Echte vergoeding wordt automatisch verstrekt door Farys.

### Browser als aanvalsoppervlak
41% medewerkers gebruikt AI webtools. 46% voert gevoelige data in via persoonlijke accounts. Phishing domeinen gemiddeld 18 jaar oud.

# Sectorrisico's + Operationele Verstoringen

## Sectorrisico's

| Sector | Niveau | Dreiging |
|---|---|---|
| Telecom | KRITIEK | Odido 6,5M + Chinese APT's |
| Financieel | HOOG | BK Group (Akira), BeyondTrust KEV |
| Industrie | HOOG | AkzoNobel + Abutriek + Netwerk NV |
| Overheid | HOOG | EU politieaccounts, APT28, DigiD |
| Retail | VERHOOGD | Mall of NL + SkiWebShop |
| Luchtvaart | VERHOOGD | Brussels Airlines |
| OT/BMS | VERHOOGD | Honeywell controllers bypass |

## Operationele verstoringen

| Dienst | Impact |
|---|---|
| AWS ME-CENTRAL-1 | 109+ diensten down, drone aanvallen, meerdere dagen |
| Wikipedia | JS worm, 3.996 pagina's, hersteld (23 min) |
| Brussels Airlines | Vluchtverstoringen |
| Iran internet | 4% van normaal verkeer |

**Let op:** AWS incident toont kwetsbaarheid van fysieke cloudinfrastructuur voor kinetische aanvallen.

# Regelgeving & Compliance

## Nederlandse ontwikkelingen

### Kamermotie datalekken

Handelingskader voor slachtoffers. Breed gesteund (VVD, CDA, CU, D66, JA21).

### DigiD soevereiniteit

Motie aangenomen: servers en beveiliging moeten in Nederlandse handen blijven.

### Belastingdienst

Kamervragen over keuze voor Amerikaans bedrijf Fast Enterprises. Spionagerisico's.

## EU/Internationaal

### AP: AI Impactbarometer

Rode markers verdubbeld (2 naar 4). AI Verordening implementatie achterblijft. Deepfakes en AI fraude als nieuwe dreigingen.

### Leeftijdsverificatie

300+ wetenschappers uit 30 landen waarschuwen tegen privacy en datalekrisico's.

### Cyberverzekeringsmarkt

Claimfrequentie +150% (4,3% naar 10,6%). E-mail: 59,4% van claims. Ransomware 60% impactvoller.

# Aanbevolen Acties - Week 11

## Direct uitvoeren

- [ ] Communiceer Odido risico naar alle medewerkers. Waarschuw voor gerichte phishing met persoonlijke gegevens
- [ ] Controleer of Patch Tuesday februari volledig is uitgerold (APT28 kwetsbaarheden CVE-2026-21513/21509)
- [ ] Verifieer patchstatus BeyondTrust, Cisco en Ivanti (CISA KEV, actief in ransomware)
- [ ] Test backup en recovery procedures (4 ransomware aanvallen NL/BE deze week)

## Deze week plannen

- [ ] Evalueer browser isolatie en DLP beleid voor AI tools (41% medewerkers gebruikt AI webtools)
- [ ] Controleer Hikvision/Dahua camera firmware (CVE-2017-7921 nog steeds meest misbruikt wereldwijd)
- [ ] Bereid voor op Patch Tuesday 11 maart
- [ ] Blokkeer persoonlijke accounts op zakelijke apparaten. Centraliseer software updates

Vragen of meer informatie? Neem contact op via **info@digiweerbaar.nl** | **06-17236093**