www.CyberSecured.be

WEKELIJKSE CYBERDREIGINGSBRIEFING

Voor Belgische organisaties | Week van 20 februari 2026

KMO's • Ziekenhuizen • Overheden • Non-profits • Grote bedrijven

KRITIEK | HOOG | GEMIDDELD | LAAG

1. Openingsboodschap

De cijfers liegen er niet om: twee op drie Belgische bedrijven werd de afgelopen twee jaar getroffen door een cyberaanval. België staat in de wereldwijde top tien van meest getroffen landen voor ransomware. En het meest geviseerde doelwit op Belgische bodem? De gezondheidssector. Niet de banken, niet de techbedrijven — maar de organisaties die zorg verlenen aan mensen.

De vraag is niet langer of jouw organisatie aangevallen wordt, maar wanneer — en of je dan klaar bent. Een school in Berchem ontdekte dat de hard way: na een aanval waarbij leerlinggegevens, financiele informatie en vertrouwelijke zorgdata werden gestolen, weigerden ze terecht te betalen. De aanvallers richtten hun pijlen vervolgens op de ouders persoonlijk. Dat is een nieuw soort escalatie die ons allemaal raakt.

Tegelijkertijd heeft Microsoft deze week zes actief uitgebuite beveiligingslekken gepatcht — meer dan we normaal in een ronde zien. Jouw IT-team heeft op dit moment prioritaire patches te verwerken. Dit is een week om in actie te schieten, niet om te wachten.

2. BE Belgische dreigingen en bevestigde slachtoffers

OLV Pulhof Berchem — Aanval op school, ouders persoonlijk geviseerd

BEVESTIGD — VRT NWS, The Record, Cybernews

Het secundair onderwijs van het Onze-Lieve-Vrouwinstituut Pulhof in Berchem (Antwerpen) werd na de kerstvakantie getroffen door een aanval waarbij servers werden versleuteld en meer dan 45 GB data buitgemaakt. De gestolen data omvat leerlinggegevens (2016-2025), personeelsinformatie (2009-2025), financiele gegevens en vertrouwelijke geestelijke gezondheidsdata.

Toen de school weigerde te betalen (initieel 100.000 euro, later verlaagd naar 15.000 euro), contacteerden de aanvallers rechtstreeks de ouders van leerlingen met een eis van 50 euro per kind. Experts bevestigen dat de aanvallers zich ten onrechte voordeden als de LockBit-groep — het gaat om een imitator.

Impact voor jouw organisatie: De aanval toont dat criminelen bereid zijn naasten en klanten van slachtoffers rechtstreeks te chanteren. GDPR-meldplicht bij diefstal van persoonsgegevens is verplicht (72u). Reputatieschade en juridische kosten lopen hoog op.

- Bron: VRT NWS — 30 januari 2026
- Bron: The Record by Recorded Future
- Bron: Cybernews

www.CyberSecured.be

INGUS — Qilin ransomwaregroep claimt Belgisch slachtoffer

BEVESTIGD — Ransomware.live (2 februari 2026)

Op 2 februari 2026 publiceerde de Qilin-groep op haar darkweb-leksite een claim op INGUS. Verdere details over de omvang zijn niet publiek. Qilin is momenteel de actiefste ransomwaregroep ter wereld, met meer dan 1.000 bevestigde slachtoffers in 2025 en al 55+ nieuwe slachtoffers in de eerste weken van 2026. De groep richt zich uitdrukkelijk op zorg, onderwijs en overheid.

- Bron: Ransomware.live — INGUS/Qilin
- Bron: Barracuda: Qilin surges into 2026

UPDATE — Belgie consistent in top-ransomware-doelwitten

BEVESTIGD — Inetum rapport, Business AM, VBO-FEB

Uit het recentste dreigingsrapport van Inetum (10 februari 2026) blijkt dat Belgie op de tiende plaats staat wereldwijd voor ransomware-aanvallen. Belgische bedrijven verwerken gemiddeld 1.288 aanvallen per organisatie — een stijging van 14% tegenover 2024. De gezondheidssector is het meest geviseerde doelwit in Belgie, gevolgd door de financiele sector. Gemiddelde kost van een aanval voor KMO's: 1,2 miljoen euro.

- Bron: ICT Magazine — Inetum rapport
- Bron: VBO-FEB

3. Kwetsbaarheden — actie vereist van IT

NOODGEVAL: Microsoft Patch Tuesday februari 2026 — Zes actief uitgebuite zero-days

Microsoft heeft op 11 februari 2026 patches uitgebracht voor 58 kwetsbaarheden, waaronder zes die actief worden uitgebuit. Dit is uitzonderlijk — normaal zien we 1-2 zero-days per maand. CISA heeft alle zes toegevoegd aan het KEV-catalogus. Federale patching vereist voor 3 maart 2026.

Actief uitgebuite kwetsbaarheden:

- CVE-2026-21510 (CVSS 8.8): Windows Shell bypass — malafide link volstaat om SmartScreen te omzeilen. Bijzonder gevaarlijk in phishingcampagnes.
- CVE-2026-21513: MSHTML Framework bypass — een HTML-bestand kan beveiligingsprotocollen omzeilen.
- CVE-2026-21514: Microsoft Word OLE-bypass — kwaadaardig Word-document volstaat.
- CVE-2026-21519 (CVSS 7.8): Desktop Window Manager privilege-escalatie naar SYSTEM.
- CVE-2026-21533 (CVSS 7.8): Remote Desktop Services privilege-escalatie. CrowdStrike bevestigt actieve exploitatie.
- CVE-2026-21525 (CVSS 6.2): Windows RasMan Denial of Service.

- Bron: CCB Advisory — Microsoft Patch Tuesday februari 2026
- Bron: BleepingComputer — February 2026 Patch Tuesday
- Bron: CISA KEV Catalog

DRINGEND: SolarWinds Web Help Desk — Actief uitgebuit (CVSS 9.8)

CVE-2025-40551: Kritieke RCE-kwetsbaarheid zonder authenticatie. Huntress documenteerde op 7 februari 2026 concrete aanvallen waarbij aanvallers persistente toegang installeerden via Zoho ManageEngine tools en Cloudflare-tunnels. SolarWinds WHD wordt gebruikt bij overheden, zorginstellingen en grote bedrijven.

Actie: Update onmiddellijk naar versie 2026.1. Verwijder de web-interface van publiek internet of zet achter VPN.

- Bron: CCB Advisory — SolarWinds Web Help Desk
- Bron: BleepingComputer — SolarWinds WHD exploit

DRINGEND: F5 BIG-IP TMM — Denial-of-Service (CCB 19 feb 2026)

Het CCB waarschuwde op 19 februari 2026 voor een kwetsbaarheid in F5 BIG-IP TMM die tot volledige DienstOnBeschikbaarheid kan leiden. Organisaties die F5 BIG-IP gebruiken voor loadbalancing dienen onmiddellijk te patchen.

- Bron: CCB.be — F5 BIG-IP waarschuwing

DRINGEND: Dell RecoverPoint — Actief uitgebuit door APT-actor (CCB 18 feb 2026)

CVE-2026-22769: Kritieke kwetsbaarheid door hardcoded credentials. Mandiant en Google GTIG bevestigden actieve exploitatie door dreigingsactor UNC6201, met gebruik van malware zoals BRICKSTORM en GRIMBOLT. De aanvaller gebruikt 'Ghost NICs' voor onzichtbare netwerktoegang.

Actie: Upgrade naar versie 6.0.3.1 HF1 of voer DSA-2026-079 uit.

- Bron: CCB Advisory — Dell RecoverPoint

4. Europese en mondiale dreigingen relevant voor België

Qilin ransomware — Exponentieel groeiende dreiging voor Europa

Qilin is momenteel de meest actieve ransomwaregroep ter wereld. In 2024 veroorzaakten ze in het VK een aanval op Synnovis (NHS) met zware gevolgen voor patientenzorg. De groep richt zich uitdrukkelijk op West-Europa. Belgie heeft al meerdere bevestigde slachtoffers op de Qilin-leksite: identic.be, seabridge.eu, INGUS. Geen enkele sector is uitgesloten.

- Bron: Barracuda — Qilin surges into 2026
- Bron: SOCRadar — Dark Web Profile Qilin

UPDATE — Cyberaanval op Waalse administratie (november 2025, herstel lopend)

In november 2025 werd de Waalse administratie getroffen door een gesofisticeerde inbraak. Wallonie.be en het digitale loket Mon Espace lagen plat. De herkomst is niet publiek bevestigd. Het CCB, Microsoft en andere specialisten waren betrokken bij het herstel. Dit incident is een directe waarschuwing voor alle Belgische overheden en publieke diensten.

- Bron: ITdaily.be — Waalse administratie

www.CyberSecured.be

RTL Group — beweerde inbreuk (27.000+ medewerkers)

⚠ ONBEVESTIGD — Niet bevestigd door RTL Group

Een cybercrimineel claimt toegang te hebben tot het intranet van RTL Group met persoonsgegevens van meer dan 27.000 medewerkers (namen, e-mailadressen, telefoonnummers). RTL Group is actief in Belgie. De bewering is niet bevestigd noch ontkend door RTL Group zelf.

Bron: CyberCrimeInfo.nl

5. ☑ Wat kan je concreet doen

NOODGEVAL — Patches uitvoeren (deadline: deze week)

Vraag jouw IT-team of IT-partner vandaag nog: zijn de Microsoft-updates van 11 februari geinstalleerd? Is SolarWinds Web Help Desk bijgewerkt naar versie 2026.1? Is Dell RecoverPoint gepatcht? Is F5 BIG-IP bijgewerkt? Dit zijn geen routinepatches — zes zero-days worden actief uitgebuit.

Bron: CCB Patch Tuesday Advisory

DRINGEND — Controleer NIS2-registratie bij het CCB

Op 17 oktober 2024 trad de vernieuwde Belgische NIS2-wet in werking. Als jouw organisatie actief is in één van de in de wetgeving vermelde sectoren(energie, gezondheidszorg, transport, water, financien, ICT, overheidsdiensten,…) en niet geregistreerd is bij het CCB, loop je juridisch risico. Registratie geeft ook toegang tot gratis diensten zoals Quick Scan-rapporten en prioritaire kwetsbaarheidsmeldingen.

Bron: CCB — Registratie NIS2

HOOG — Sensibiliseer medewerkers voor phishing

46% van de cyberaanvallen op Belgische organisaties maakt misbruik van menselijke fouten. Herinner medewerkers aan de drie basisregels:

- Verdachte e-mails doorsturen naar verdacht@safeonweb.be
- Nooit klikken op links in onverwachte berichten — ook niet als ze van bekende namen afkomstig lijken
- Tweefactorauthenticatie (2FA) verplicht op alle externe toegangen

Bron: Safeonweb.be

HOOG — Beoordeel blootstelling van IT-beheertools aan internet

Producten als SolarWinds Web Help Desk, Remote Desktop Services en andere beheerstools worden actief uitgebuit. Controleer of dergelijke systemen rechtstreeks via het internet toegankelijk zijn, en beperk toegang onmiddellijk tot VPN of interne netwerken.

MEDIUM — Test het back-upproces

www.CyberSecured.be

Elke ransomware-aanval maakt back-ups tot prioriteit. Vraag jouw IT-team: wanneer is de laatste back-up getest? Zijn back-ups offline (air-gapped) bewaard? Hoelang duurt een volledige restore?

MEDIUM — KMO's: gebruik de gratis tools van het CCB

Het EU-gefinancierde SECURE-project biedt financiele ondersteuning aan KMO's die willen voldoen aan de Cyber Resilience Act. Het CCB biedt gratis tools zoals Safeonweb@work en de SME Security Scan.

Bron: https://ccb.belgium.be/ncc/secure-project

6. Dreigingsniveau-overzicht per categorie

Categorie	Niveau	Toelichting
Ransomware (algemeen)	Kritiek	Qilin en andere groepen extreem actief; BE in top 10 wereldwijd
Phishing & social engineering	Kritiek	46% van Belgische aanvallen via menselijke fout
Softwarekwetsbaarheden	Kritiek	6 actief uitgebuite zero-days; SolarWinds WHD in the wild
Gezondheidssector	Kritiek	Meest geviseerde sector in Belgie
Onderwijs	Hoog	OLV Pulhof; beperkte budgetten = hoog risico
Lokale besturen / overheden	Hoog	Waalse aanval; geopolitieke dreiging van pro-Russische actoren
KMO's	Hoog	Gem. 1,2M kost per incident; onderbeschermd
DDoS	Gemiddeld	Verhoogd door geopolitieke context
Supplychain-aanvallen	Gemiddeld	Groeiende dreiging via IT-dienstverleners

7. Technische bijlage (voor het IT-team)

Microsoft Patch Tuesday — februari 2026 — Actief uitgebuite CVE's

CVE	CVSS	Product	Type	Status
CVE-2026-21510	8.8	Windows Shell	Security Feature Bypass (SmartScreen)	Actief uitgebuit
CVE-2026-21513	~7.9	MSHTML Framework	Security Feature Bypass	Actief uitgebuit
CVE-2026-21514	~7.3	Microsoft Word	Security Feature Bypass (OLE)	Actief uitgebuit
CVE-2026-21519	7.8	Win Desktop Window Mgr	Privilege Escalation (SYSTEM)	Actief uitgebuit
CVE-2026-21533	7.8	Windows RDS	Privilege Escalation (Admin)	Actief uitgebuit (CrowdStrike)

www.CyberSecured.be

CVE	CVSS	Product	Type	Status
CVE-2026-21525	6.2	Windows RasMan	Denial of Service	Actief uitgebuit

Remediation: Installeer de cumulatieve beveiligingsupdates van februari 2026 via Windows Update / WSUS / SCCM. Prioriteit: systemen met directe internetblootstelling en RDP-toegang.

- Bron: MSRC — Security Update Guide
- Bron: CISA KEV Catalog

SolarWinds Web Help Desk — CVE-details

CVE	CVSS	Type	Status
CVE-2025-40551	9.8	Deserialization RCE (unauthenticated)	Actief uitgebuit — CISA KEV
CVE-2025-40552	9.8	Authentication Bypass	Gepatcht (WHD 2026.1)
CVE-2025-40553	9.8	Deserialization RCE	Gepatcht
CVE-2025-40554	9.8	Authentication Bypass	Gepatcht
CVE-2025-40536	8.1	Overig	Gepatcht
CVE-2025-40537	7.5	Hardcoded credentials	Gepatcht

IOC's (Huntress, 7 februari 2026):

- Zoho MSI SHA256: 897eae49e6c32de3f4bfa229ad4f2d6e56bcf7a39c6c962d02e5c85cd538a189
- Velociraptor C2: auth.qgtxtebl.workers.dev
- Proton Mail account: esmahyft@proton[.]me
- Verdacht proces: wrapper.exe -> java.exe -> cmd.exe -> PowerShell

Remediation: Update naar WHD 2026.1. Isoleer achter VPN/firewall. Reset alle admin credentials. Controleer logs op bovenstaande IOC's.

Dell RecoverPoint for Virtual Machines

CVE	CVSS	Type	Status
CVE-2026-22769	Kritiek	Hardcoded credential — RCE/laterale beweging	Actief uitgebuit (UNC6201/Mandiant)

Dreigingsactor UNC6201 (Mandiant/Google GTIG) maakt gebruik van BRICKSTORM, SLAYSTYLE en GRIMBOLT malware. Gebruikt Ghost NICs voor onzichtbare netwerktoegang en iptables voor Single Packet Authorization.

Remediation: Upgrade naar versie 6.0.3.1 HF1 of voer DSA-2026-079 uit. Systemen op versie 5.3 moeten eerst upgraden naar een ondersteunde versie.

www.CyberSecured.be

✉ Incidenten melden | Verdachte berichten

cert.be/report-incident | verdacht@safeonweb.be | +32 (0)2 501 05 60

Volgende briefing: 27 februari 2026