BRANDEFENSE COUNTRY REPORT · BELGIUM 2026

Brandefense Rapport over het Belgische cyberdreigingslandschap 2026

Blootstelling van identiteitsgegevens, gedeelde leveranciers en operationele continuïteit

Odin by Brandefense
Onderzoeksperiode: 1 januari–22 november 2026
Versie 1.0 · Publieke onderzoekseditie · TLP:CLEAR · 9–22 november 2026

63 van 250
geselecteerde organisatiedomeinen hadden bij controle een authenticatiegegeven te koop staan

1.025
afzonderlijke bewaarde forumberichten, met beperkte dekking buiten deze omgevingen

22
ransomwaregroepsnamen in de bewaarde Belgische vermeldingspopulatie

11 van 25
geselecteerde bank- en financiële domeinen hadden een actueel authenticatieaanbod

INHOUD

Inhoud

Translated with AI

Deze editie is met AI vertaald vanuit de Engelse hoofdtekst. Bij verschillen is de Engelse editie leidend.

01	Samenvatting	04
	Rapportkaart	08
	Inhoud en leeswijzer	09
02	De Belgische digitale en dreigingscontext	10
03	Nationale blootstelling: geselecteerde organisaties en domeinen	13
04	Wat we op het darkweb zien	22
05	Bevestigde incidenten en claims per sector	36
06	Hacktivisme, verstoring en operationele systemen	49
07	Dreigingsactoren en bewijsverbanden	53
08	De fraude-economie	61
09	Verdieping bankwezen en financiën	66
10	Regelgeving en nationale respons	69
11	Vooruitblik	74
12	Actieplan	77
A	Bijlage A. Methode en grenzen	83
B	Bijlage B. Bewijsregister	86
C	Bijlage C. Bronnen	87
D	Bijlage D. Begrippenlijst	90
	Over dit rapport	92

CISO en leiding	01 05 10 11 12
SOC en identiteit	03 04 07 09 A–B
Operations en inkoop	02 05 06 12
Financiën en klantbescherming	04 08 09
Privacy en communicatie	05 06 10 A–C

Over deze editie

Vertaald met AI. Bij verschillen heeft de Engelse editie voorrang.

Onderzoek en tekst met ondersteuning van AI. De bewijslabels en dekkingsbeperkingen gelden voor het hele rapport. Bij verschillen tussen vertalingen heeft de Engelse editie voorrang.

HOOFDSTUK 01

Samenvatting

01

DIT HOOFDSTUK BEANTWOORDT

Wat is in 2026 het belangrijkst voor Belgische organisaties en wat moet de leiding eerst doen?

4

beslissingen over identiteit, leveranciers, operations en incidentcommunicatie

Vier beslissingen voor de leiding 06

Het jaar in cijfers 06

HOOFDSTUK 01

Samenvatting

IN HET KORT

Het Belgische bewijs wijst op identiteitsbescherming en dienstencontinuïteit. Het CCB ontving tot 28 september 588 incidentmeldingen. Ransomwaresites bevatten 46 Belgische vermeldingen binnen de onderzoeksperiode. Bewaarde forumberichten boden klantgegevens, identiteitsmateriaal, toegang en fraudehulpmiddelen aan. Publieke incidenten raakten zorg, ledengegevens, onderwijs en administratieve diensten. Deze populaties meten verschillende zaken. Controleer actieve identiteiten, breng leveranciersafhankelijkheden in kaart, beperk operationele toegang op afstand en oefen meldings- en herstelbeslissingen.

Het rapport combineert ondergrondse waarnemingen, blootstellingsgegevens en gecontroleerde publieke berichtgeving. Brandefense Blackhole registreert 96.265 landgelabelde berichten over platforms. De bewaarde inhoud omvat 1.025 afzonderlijke forumberichten, waaronder 480 met een landlabel. Deze overlappende populaties beschrijven zichtbaarheid, geen nationale aanvalsaantallen. [S1][S2][S3]

1. **Officiële bronnen ondersteunen identiteitsbescherming het sterkst.** In zijn beoordeling van 9 november beschreef het CCB accountgerelateerde incidenten als ongeveer 30% van de gemelde incidenten tijdens de eerste twee kwartalen. Politieberichten beschrijven daarnaast hergebruikte mailboxgegevens, aangepaste facturen en bankimitatiefraude. Geen van beide bronnen meet de actuele blootstelling van elke Belgische organisatie. [S5][S31][S32]

2. **Afpersingsclaims zijn verspreid over veel groepsnamen.** Ransompedia registreerde binnen de periode 46 aanvaarde vermeldingen, verdeeld over 22 groepsnamen. Qilin is goed voor 9 en The Gentlemen voor 7. Het gedeeltelijke jaartotaal ligt boven de 42 vermeldingen uit heel 2025. Dit is geen jaarlijkse groeivoet of bewijs van 46 afzonderlijke inbraken. [S1]

3. **Gedeelde leveranciers maken technische incidenten tot dienstverleningsbeslissingen.** Onderwijs-, zorg- en gemeentelijke gevallen tonen hoe afhankelijkheid de communicatie, beschikbaarheid en gegevensbeoordeling kan beïnvloeden. Een klantenpopulatie is geen telling van getroffen slachtoffers. Vraag een impactverklaring voor de specifieke leverancier en klant. [S8][S13][S22]

4. **Advertenties mengen oude gegevens, actuele claims en ongeteste mogelijkheden.** Een telecomadvertentie verwijst naar juli 2025. Een aanbieder van een groot burgerbestand erkent dat de bron onbekend is. Recente berichten bieden ondersteuningstickets, bankimitatiehulpmiddelen en een casinogerichte klantenlijst aan. Ze tonen geen werkende toegang of afgeronde transacties aan. [S3]

5. **Operationeel herstel heeft een eigen verantwoordelijke nodig.** De verstoring van koelsystemen in november verschilt van een website-uitval. Publieke toeschrijving bleef betwist in de bewaarde berichtgeving. De directe verdedigingsvraag is hoe toegang op afstand wordt beheerst en apparatuur veilig wordt teruggezet. [S25][S26][S27]

6. Actuele aanbiedingen vereisen gerichte identiteitscontrole. 63 van 250 geselecteerde organisatiedomeinen hadden bij controle een authenticatiegegeven te koop staan. De nationale Atlas-waarde is 48 op 100. Minstens 296.591 apparaatassociaties en 26.236.674 authenticatierecords beschrijven overlappende blootstellingspopulaties, geen bevestigde inbraken. [S2]

Vier beslissingen voor de leiding

1. **Controleer identiteiten voordat u ingrijpende maatregelen voorschrijft.** Vraag identiteits- en SOC-verantwoordelijken onderscheid te maken tussen een oud authenticatiegegeven, een actief account en een verdachte sessie. Leg voor elke relevante bevinding een afhandeling vast.
2. **Koppel leveranciersafhankelijkheden aan gevolgen voor gegevens en diensten.** Vraag elke kritieke leverancier om afgebakende meldingsafspraken en een getest alternatief proces. Oefen een uitval terwijl de vertrouwelijkheidsbeoordeling nog onzeker is.
3. **Beheers operationele toegang op afstand.** Geef operations een gecontroleerde toegangslijst, een veilig lokaal proces en de bevoegdheid om leverancierstoegang zo nodig te beperken. Test herstel zonder de gewone toegangsroute op afstand.
4. **Bereid heldere meldingen en herstelbeslissingen voor.** Wijs privacy-, juridische, communicatie- en technische verantwoordelijken aan. Houd wettelijke termijnen apart van interne planningsdoelen en behoud onzekerheid in Franse en Nederlandse meldingen.

Het jaar in cijfers

Cijfer	Wat het is	Wat het niet is
588	Incidentmeldingen ontvangen door het CCB, 1 januari–28 september 2026 [S4]	Een volledig jaartotaal, unieke slachtoffers of een nationale prevalentieschatting
46	Aanvaarde Belgische ransomwaremeldingen binnen de onderzoeksperiode [S1]	Bevestigde versleuteling, afzonderlijke inbraken of gemeten verlies
22	Groepsnamen bij die vermeldingen [S1]	Geverifieerde afzonderlijke criminele organisaties
1.025	Afzonderlijke bewaarde forumberichten uit de verzamelde sets [S3]	Alle berichten over België of unieke incidenten
480	Berichten met een landlabel binnen die bewaarde populatie [S3]	Een extra populatie die bij 1.025 moet worden opgeteld
31	Bewaarde berichten gedateerd 9–22 november [S3]	Geen bevestigde nieuwe inbraken
250	Doelgericht geselecteerde kandidaatdomeinen [S2]	Een gerangschikte economische telling of representatieve nationale steekproef

Cijfer	Wat het is	Wat het niet is
245	Kandidaatdomeinen met een DNS-antwoord op de waarnemingsdatum [S2]	Geverifieerde onafhankelijke rechtspersonen of een beveiligingsscore
63	Geselecteerde organisatiedomeinen met een actueel authenticatieaanbod [S2]	Werkende toegang, actieve accounts of bevestigde inbraken
48	Nationale Atlas-waarde voor de 250 geselecteerde domeinen [S2]	Nationale prevalentie of sectorscore
96.265	Landgelabelde berichten over platforms [S3]	Bevestigde Belgische doelwitten, criminele relevantie of nationale incidenten

KERNPUNTEN

01

Geef accountcontrole en herstelbare diensten voorrang.

02

Houd advertenties, vermeldingen en bevestigde incidenten als afzonderlijke populaties.

03

Wijs verantwoordelijken aan voor leveranciers, operations en meldingsbeslissingen.

Rapportkaart

Begin bij uw eigen beslissing en volg daarna het bewijs en zijn grenzen.

CISO en leiding	Financier identiteit, continuïteit en meldingswerk	01 05 10 11 12
SOC en identiteit	Controleer advertenties, sessies en actuele activiteit	03 04 07 09 A–B
Operations en inkoop	Behoud veilige diensten tijdens een leveranciersincident	02 05 06 12
Financiën en klantbescherming	Onderbreek imitatie en betalingswijzigingen	04 08 09
Privacy en communicatie	Behoud bewijsreikwijdte en meldingsplichten	05 06 10 A–C

Inhoud en leeswijzer

Hoofdstuk	Vraag
1 Samenvatting	Welke beslissingen moet de leiding eerst nemen?
2 Context	Welke afhankelijkheden bepalen het Belgische beeld?
3 Nationale blootstelling	Wat toont het onderzoek van de geselecteerde domeinen aan?
4 Darkweb	Wat werd aangeboden en wat blijft onbevestigd?
5 Incidenten	Welke gevolgen voor diensten en gegevens worden ondersteund?
6 Verstoring	Hoe verschillen claims van operationele gevolgen?
7 Actoren	Welke verbanden worden door bewijs ondersteund?
8 Fraude	Hoe kan blootgestelde informatie misleiding ondersteunen?
9 Banksector	Wat moeten identiteits- en fraudeteams controleren?
10 Regelgeving	Welke verplichtingen en mijlpalen gelden?
11 Vooruitblik	Welke voorwaardelijke scenario's verdienen een oefening?
12 Actieplan	Wie is verantwoordelijk voor de volgende 30/60/90 dagen?
Bijlagen A–D	Reikwijdte, bewijsregister, bronnen en begrippenlijst

De leiding kan beginnen met hoofdstukken 1, 5, 10 en 12. SOC- en identiteitsteams lezen bij voorkeur hoofdstukken 3, 4, 7 en 9. Operations, inkoop en klantbescherming kunnen hoofdstukken 5, 6 en 8 gebruiken.

Waargenomen betekent dat een bewaarde advertentie, vermelding of publieke verklaring bestaat. **Geclaimd** geeft weer wat een adverteerder zegt, zonder de uitkomst te bevestigen. **Beoordeeld** benoemt een evenredige interpretatie, de alternatieve verklaring en de actie die deze ondersteunt.

HOOFDSTUK 02

De Belgische digitale en dreigingscontext

02

DIT HOOFDSTUK BEANTWOORDT

Welke Belgische kenmerken zijn belangrijk voor incidentrespons en welke conclusies moeten verdedigers vermijden?

588

incidentmeldingen ontvangen door het CCB tot 28 september, geen nationale slachtoffertelling

2.1 Een digitale afhankelijkheid kan meerdere grenzen overschrijden 11

2.2 Officiële rapporten wijzen op identiteit en systeemblootstelling 11

2.3 Leveranciers creëren dienstenafhankelijkheden 12

2.4 Politiek geduide activiteit vraagt zorgvuldige toeschrijving 12

HOOFDSTUK 02

De Belgische digitale en dreigingscontext

IN HET KORT

Belgische openbare diensten, commerciële platformen en leveranciers delen digitale afhankelijkheden over organisatie- en landsgrenzen heen. Het CCB ontving tot 28 september 588 incidentmeldingen. Zijn identiteitsrapport van november plaatst accountbescherming centraal in de respons. De gevallen tonen ook waarom een leveranciersonderbreking een klantendienstprobleem kan worden. Bepaal welke account-, leveranciers- en operationele afhankelijkheden uw organisatie nodig heeft om te blijven werken.

2.1 Een digitale afhankelijkheid kan meerdere grenzen overschrijden

Het officiële Belgische portaal beschrijft een federale staat met drie gemeenschappen en drie gewesten. Nederlands, Frans en Duits zijn officiële talen. Dit zijn bestuurlijke feiten, geen verklaringen voor beveiligingsprestaties. [S6]

Voor verdedigers is de nuttige vraag wie een dienst en zijn gegevens beheert. Een centraal contract kan meerdere lokale besturen ondersteunen. Een buitenlands platform kan Belgische klantrecords bewaren. Een platformincident toont geen inbraak aan in het eigen netwerk van elke Belgische klant.

Het rapport onderscheidt daarom binnenlandse organisatie-incidenten, incidenten bij gedeelde diensten en context rond buitenlandse diensten. Het rangschikt taalgemeenschappen, gewesten of besturen niet naar beveiliging. De geselecteerde domeinwaarnemingen ondersteunen zulke vergelijkingen niet.

Communicatie moet de getroffen gebruikers volgen. Bereid duidelijke meldingen voor in de talen van uw dienst. Houd reikwijdte, onzekerheid en beschermingsadvies gelijk tussen edities. Een vertaling mag mogelijke openbaarmaking niet veranderen in bevestigde diefstal.

2.2 Officiële rapporten wijzen op identiteit en systeemblootstelling

Het CCB ontving tussen 1 januari en 28 september 2026 588 incidentmeldingen, tegenover 556 tijdens heel 2025. De perioden verschillen. De vergelijking toont dat het eerdere volledige jaartotaal werd overschreden; ze is geen jaarlijkse groeivoet. [S4]

De kwartaalrapporten beschrijven veranderende incidentmixen. Het eerste kwartaal telde 154 cyberincidenten; het tweede telde 188 cyberincidenten binnen een bredere meldingspopulatie. Deze cijfers zijn niet uitwisselbaar met alle meldingen. [S7][S8]

Het derdekwartaalrapport benadrukt systeeminbraken en blootgestelde kwetsbaarheden. Volgens de identiteitsbeoordeling van het CCB in november betroffen accounts ongeveer 30% van de gemelde incidenten tijdens de eerste twee kwartalen. Elk cijfer behoudt zijn meldingspopulatie en periode. [S9][S5]

Dit ondersteunt twee parallelle werkstromen. Identiteitsteams moeten sessies, herstelroutes en bevoorrechte toegang controleren. Infrastructuurteams moeten weten welke blootgestelde systemen dringende maatregelen vereisen. Geen team kan zijn werk afsluiten door alleen de controlelijst van het andere team af te werken.

2.3 Leveranciers creëren dienstenafhankelijkheden

Het tweedekwartaalrapport van het CCB bespreekt softwareketens die België raken. Publieke gevallen betreffen zorgsoftware, leerplatformen en een dienst voor digitale handtekeningen die lokale besturen gebruiken. Hun gemeenschappelijke kenmerk is afhankelijkheid, geen bewijs van één gecoördineerde aanvaller. [S8][S13][S22]

Voor leveranciers is de eerste nuttige oplevering een klantspecifieke impactverklaring. Voor klanten is dat een overzicht van de gegevens, accounts en processen die van die leverancier afhangen. Het klantenaantal van een leverancier telt niet hoeveel klanten gegevens verloren.

Houd bedrijfscontinuïteit apart van vertrouwelijkheid. Een dienst kan onbeschikbaar zijn doordat hij bewust werd geïsoleerd. Een andere dienst kan beschikbaar blijven terwijl persoonsgegevens worden blootgesteld. Hoofdstuk 5 registreert deze uitkomsten afzonderlijk.

2.4 Politiek geduide activiteit vraagt zorgvuldige toeschrijving

Het CCB noemt door staten gesteunde activiteit en geopolitiek hacktivisme relevante dreigingen. Die beoordeling schrijft niet elk Belgisch incident aan een staat toe. Het publieke dossier over de koelcampagne toont waarom dit onderscheid telt. [S8][S9][S26]

Reuters meldde op 13 november verschillende ministeriële beoordelingen. De minister van Binnenlandse Zaken noemde Iraanse betrokkenheid zeer waarschijnlijk. De minister van Buitenlandse Zaken vond de beschikbare informatie onvoldoende voor officiële toeschrijving. Het onderzoek liep nog. [S26]

Dit rapport doet geen zelfstandige toeschrijving voor die campagne. Het neemt geen standpunt in over overheidsbeslissingen, internationale geschillen, taalpolitiek of historische relaties. Actorretoriek toont geen motief, technische verantwoordelijkheid of impact aan.

EU-instellingen verschijnen alleen als publieke context. Een Brusselse locatie, een EU-gerelateerd merk of een meertalig bericht maakt een incident op zichzelf geen deel van de Belgische binnenlandse organisatiepopulatie.

KERNPUNTEN

01

Koppel elk officieel cijfer aan zijn eigen meldingspopulatie en periode.

02

Koppel leveranciersafhankelijkheden aan de werkelijk getroffen dienst en gegevens.

03

Behoud onzekerheid bij toeschrijving en vertaling van een melding.

HOOFDSTUK 03

Nationale blootstelling: geselecteerde organisaties en domeinen

DIT HOOFDSTUK BEANTWOORDT

Wat betekenen de gemeten blootstellingssignalen voor de geselecteerde organisaties?

63 van 250

geselecteerde organisatiedomeinen hadden bij controle een authenticatiegegeven te koop staan

3.1 Populatiekaart 14
3.2 Blootstellingssignalen per sector 15
3.3 Apparaten en authenticatiegegevens 17
3.4 Omgaan met een actuele identiteitsbevinding 18
3.5 E-mail- en webcontroles 19

HOOFDSTUK 03

Nationale blootstelling: geselecteerde organisaties en domeinen

IN HET KORT

63 van 250 geselecteerde organisatiedomeinen hadden bij controle een authenticatiegegeven te koop staan. De nationale Atlas-waarde is 48 op 100. De portefeuille bevat minstens 296.591 apparaatassociaties en 26.236.674 authenticatierecords. Deze overlappende waarnemingen tonen geen unieke personen, actieve accounts of bevestigde inbraken aan. Passieve controles omvatten 245 van deze domeinen. Controleer actuele aanbiedingen, onderzoek aan werknemers gekoppelde apparaten en verifieer herstelroutes.

3.1 Populatiekaart

Kenmerk	Reikwijdte
Populatie	250 geselecteerde primaire domeinen in tien sectoren; 245 met passieve waarnemingen
Eenheid	Een primair domein; DNS toont geen onafhankelijkheid of eigendom van rechtspersonen aan
Selectie	Publieke en economische functies; doelgerichte portefeuille, geen gerangschikte nationale telling
Blootstellingsdatum	Cumulatieve apparaat-, authenticatie-, aanbod- en documentwaarnemingen: 21 november 2026
Overige perioden	Vermeldingen: 365 dagen tot en met 22 november 2026; gelijkende domeinen: 30 dagen; passieve waarnemingen: 22 november 2026
Overlap	Records kunnen overlappen tussen bronnen, domeinen, apparaten en personen; totalen tellen geen unieke gebruikers
Interpretatie	Bevindingen beschrijven geselecteerde domeinen, geen nationale prevalentie of alle organisatie-assets

De nationale reikwijdte maakt de portefeuille niet representatief. Een domein kan werknemers, studenten, klanten of meerdere bedrijfseenheden bedienen. Domeinassociaties tonen geen apparaateigendom of inbraak in het bedrijfsnetwerk aan. [S2]

3.2 Blootstellingssignalen per sector

De nationale Atlas-waarde voor de 250 geselecteerde domeinen is 48 op een schaal van 0–100. Hogere waarden beschrijven meer waargenomen externe blootstelling in deze portefeuille. De tabel geeft aantallen signalen per sector. [S2]

Actuele aanbiedingen, werknemerassociaties en documentverwijzingen beschrijven verschillende populaties

Elke cel toont domeinen met het signaal van 25 geselecteerde domeinen per sector. Actuele authenticatieaanbiedingen staan in koraal.

	Actueel aanbod	Aanbodgeschiedenis	Werknemersapparaten	Documentverwijzing
Bankwezen en financiën	11/25	11/25	18/25	18/25
Overheid en publieke diensten	3/25	3/25	11/25	11/25
Lokaal bestuur	2/25	2/25	23/25	18/25
Onderwijs en onderzoek	6/25	6/25	21/25	19/25
Gezondheid en zorg	2/25	2/25	19/25	13/25
Energie en nutsbedrijven	2/25	2/25	16/25	9/25
Transport en logistiek	8/25	8/25	18/25	13/25
Industrie en bedrijfsleven	2/25	2/25	20/25	20/25
Detailhandel en consumentendiensten	18/25	18/25	16/25	14/25
Telecom, technologie en media	9/25	9/25	17/25	18/25

Bron: blootstellingswaarnemingen voor 250 geselecteerde organisatiedomeinen, 21 november 2026. Cumulatieve, overlappende relaties; geen bevestigde inbraken of nationale prevalentie [S2].

Sector	Domeinen	Actueel aanbod	Aanbodhistorie	Met werknemersapparaten	Met documenten
Banken en financiën	25	11	11	18	18
Overheid en openbare diensten	25	3	3	11	11
Lokaal bestuur	25	2	2	23	18

Sector	Domeinen	Actueel aanbod	Aanbodhistorie	Met werknemersap-paraten	Met documenten
Onderwijs en on-derzoek	25	6	6	21	19
Gezondheid en zorg	25	2	2	19	13
Energie en nuts-voorzieningen	25	2	2	16	9
Transport en lo-gistiek	25	8	8	18	13
Industrie en be-drijfsleven	25	2	2	20	20
Handel en consu-mentendiensten	25	18	18	16	14
Telecom, techno-logie en media	25	9	9	17	18
Alle geselecteerde domeinen	250	63	63	179	153

De laatste twee kolommen tellen domeinen met een werknemerassociatie of documentverwijzing, geen apparaten of documenten. Elke sector bevat 25 geselecteerde domeinen. Een actuele aanbieding ondersteunt accountcontrole, maar toont niet aan dat het account werkt. [S2]

3.3 Apparaten en authenticatiegegevens

Apparaat- en authenticatieassociaties verschillen tussen de geselecteerde sectoren



Bron: blootstellingswaarnemingen voor 250 geselecteerde organisatiedomeinen, 21 november 2026. Cumulatieve, overlappende relaties; geen bevestigde inbraken of nationale prevalentie [S2].

Sector	Domeinen	Apparaten, minstens	Werknemersapparaten	Authenticatierecords
Banken en financiën	25	13.221	156	190.956
Overheid en openbare diensten	25	11.202	53	44.270
Lokaal bestuur	25	4.119	336	137.471

Sector	Domeinen	Apparaten, minstens	Werknemersapparaten	Authenticatierecords
Onderwijs en onderzoek	25	21.825	2.833	652.567
Gezondheid en zorg	25	8.484	138	85.104
Energie en nutsvoorzieningen	25	25.718	93	32.333
Transport en logistiek	25	46.548	1.849	658.184
Industrie en bedrijfsleven	25	4.545	1.294	404.814
Handel en consumentendiensten	25	65.121	118	41.710
Telecom, technologie en media	25	95.808	14.023	23.989.265
Alle geselecteerde domeinen	250	296.591	20.893	26.236.674

De portefeuille bevat minstens 296.591 apparaatassociaties, waaronder 20.893 met werknemersclassificatie. Authenticatierecords bestaan uit 9.869.372 datalekrecords, 1.488.704 stealerlogrecords en 14.878.598 combolistrecords. Deze bronnen overlappen; hun totaal telt geen unieke accounts. [S2]

Sommige apparaattotalen zijn ondergrenzen. Een werknemersclassificatie is een onderzoekssignaal, geen bevestigde arbeidsrelatie of apparaateigendom. Gedeelde onderwijs- en klantdomeinen vereisen rolcontrole voordat accountmaatregelen volgen.

De portefeuille bevat ook 38.774 kandidaatdomeinen met merkgelijkenis en 1.333 blootgestelde documentverwijzingen. Gelijkenis toont geen kwaadwillig gebruik aan; een documentverwijzing bewijst geen vertrouwelijk datalek. Darkchatvermeldingen betreffen 39 domeinen en darkwebvermeldingen 31. Zichtbaarheid toont geen vijandigheid aan. [S2]

3.4 Omgaan met een actuele identiteitsbevinding

Wijs een bevinding toe aan een verantwoordelijke voor identiteit. Controleer of het account bestaat, actief is en al werd beveiligd. Vergelijk de ouderdom van de bevinding met recente authenticatie- en herstelactiviteit.

Trek een bevestigde verdachte actuele sessie in en onderzoek blijvende toegang, geregistreerde authenticatiemethoden en mailboxwijzigingen. Leg de afhandeling vast als het record historisch en inactief is. Bewaar bewijs voordat u een account verwijdert of opnieuw instelt.

De 63 actuele authenticatieaanbiedingen betreffen de geselecteerde domeinportefeuille. Forumvragen en advertenties over mogelijkheden zijn afzonderlijke waarnemingen. Een actueel aanbod of koopvraag toont geen werkende toegang of bevestigde organisatie-inbraak aan. [S2][S3]

3.5 E-mail- en webcontroles

Waarneming	Aantal	Noemer
DMARC reject of quarantine	188	245
DMARC-monitoringbeleid	46	245
Geen geldig DMARC-beleid waargenomen	11	245
SPF waargenomen	234	245
DKIM-informatie waargenomen	204	245
DS-record (delegation signer) waargenomen	65	245
TLS-certificaat gevalideerd	240	245
TLS-certificaatfout	1	245
TLS-resultaat onbepaald	4	245
Antwoord van startpagina verkregen	213	245
HSTS (HTTP Strict Transport Security) in verkregen antwoord	164	213
CSP (Content Security Policy) in verkregen antwoord	91	213

Een gepubliceerd DMARC-beleid beschrijft hoe ontvangers worden gevraagd niet-geauthenticeerde berichten te behandelen. Een monitoringbeleid verschilt van handhaving. Zelfs handhaving bewijst niet dat elke legitieme verzender correct aansluit of dat elke ontvanger het beleid toepast. [S2]

SPF en DKIM ondersteunen e-mailauthenticatie, maar hun aanwezigheid vormt geen volledige e-mailbeveiligingsbeoordeling. Een niet-waargenomen ondertekeningsconfiguratie bewijst niet dat geen geldige ondertekeningsconfiguratie bestaat. Beheerders moeten hun werkelijke verzenddiensten controleren.

Een waargenomen DS-record is geen volledige DNSSEC-validatie. Een geslaagde TLS-waarneming betreft de onderzochte host op dat tijdstip. Een mislukte of ontbrekende waarneming moet worden onderzocht voordat ze als configuratiefout van een organisatie wordt beschreven. [S2]

Homepageheaders beschrijven het vastgelegde antwoord, niet elke applicatie of elk pad. Een ontbrekende header kan een configuratiecontrole rechtvaardigen. Hij toont geen misbruikbaarheid, blootstelling van gevoelige gegevens of geslaagde inbraak aan.

E-mailwaarnemingen betreffen de geselecteerde domeinpopulatie

	DMARC reject / quarantine	SPF	TLS
Bankwezen en financiën	23/25	25/25	25/25
Overheid en publieke diensten	21/25	20/25	24/25
Lokaal bestuur	20/23	22/23	22/23
Onderwijs en onderzoek	13/24	23/24	24/24
Gezondheid en zorg	16/24	21/24	23/24
Energie en nutsbedrijven	21/25	25/25	25/25
Transport en logistiek	16/24	23/24	24/24
Industrie en bedrijfsleven	22/25	25/25	23/25
Detailhandel en consumentendiensten	19/25	25/25	25/25
Telecom, technologie en media	17/25	25/25	25/25

Bron: passieve waarnemingen, 22 november 2026. Elke cel toont waargenomen/beoordeelde domeinen; gepubliceerde beleidsregels bewijzen geen handhaving voor elk bericht [S2].

Sector	Waargenomen	DMARC reject/quarantine	SPF waargenomen	TLS geldig
Banken en financiën	25	23	25	25
Overheid en openbare diensten	25	21	20	24
Lokaal bestuur	23	20	22	22
Onderwijs en onderzoek	24	13	23	24
Gezondheid en zorg	24	16	21	23
Energie en nutsvoorzieningen	25	21	25	25
Transport en logistiek	24	16	23	24
Industrie en bedrijfsleven	25	22	25	23

Sector	Waargenomen	DMARC reject/quarantine	SPF waargenomen	TLS geldig
Handel en consumentendiensten	25	19	25	25
Telecom, technologie en media	25	17	25	25

KERNPUNTEN

01

Controleer actuele aanbiedingen en werknemerassociaties met hun eigenaren.

02

Houd overlappende records apart van personen en bevestigde inbraken.

03

Beoordeel passieve controles volgens het onderzochte domein en de datum.

HOOFDSTUK 04

Wat we op het darkweb zien

04

DIT HOOFDSTUK BEANTWOORDT

Wat tonen bewaarde advertenties aan over de vraag naar Belgische gegevens, toegang en fraudemateriaal?

1.025

afzonderlijke bewaarde forumberichten, met beperkte dekking buiten deze omgevingen

4.1 Populatiekaart 23
4.2 Volume en taal 25
4.3 De aangeboden producten 27
4.4 Casestudies 27
4.5 Aanvullende bewijskaarten 33
4.6 Recente activiteit in de bewaarde forums 35
4.7 Wat de forums toevoegen 35

HOOFDSTUK 04

Wat we op het darkweb zien

IN HET KORT

De bewaarde forums tonen een markt voor klantrecords, identiteitsbeelden, toegang en fraudehulpmiddelen. Sommige advertenties verwijzen uitdrukkelijk naar oudere incidenten. Andere erkennen onzekere herkomst of beschrijven voorgestelde gegevensstructuren. De laatste weken voegen claims over ondersteuningstickets, banktemplates en casinogegevens toe. Het waargenomen feit is de advertentie. Controleer relevantie, actualiteit en toegang met betrouwbaar organisatiebewijs voordat u een aanbod als actueel incident behandelt.

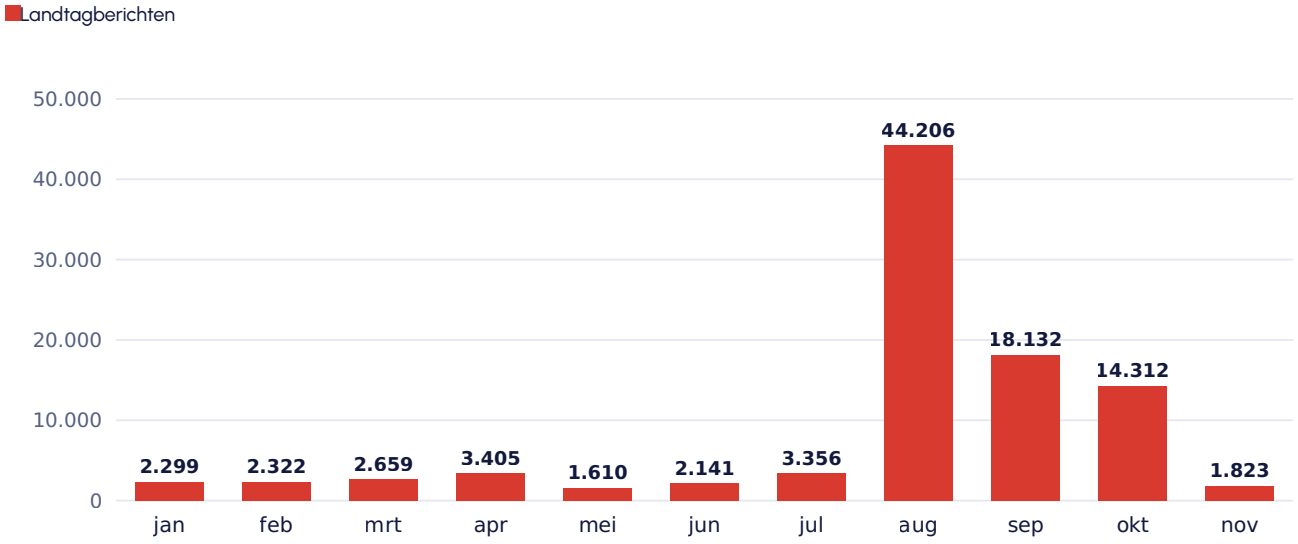
4.1 Populatiekaart

Kenmerk	Reikwijdte
Periode	Berichtdatums 1 januari–22 november 2026
Bewaarde populatie	1.025 afzonderlijke berichten in het bewaarde forummateriaal
Deel met landlabel	480 berichten, opgenomen in de bewaarde populatie
Recent deel	31 berichten gedateerd 9–22 november, eveneens opgenomen in de bewaarde populatie
Omgeving	Bewaarde inhoud komt uit forums; gelabelde aantallen omvatten ook andere platforms
Eenheid	Een bericht, geen uniek bestand, verkoper, aankoop, slachtoffer of incident
Dekkingsgrens	Sommige aangekondigde records blijven onbeschikbaar; gelabelde totalen en bewaarde forumberichten zijn afzonderlijke populaties

De bewaarde sets overlappen. Hun totalen mogen niet worden opgeteld. Landlabels en verwijzingen naar België bevestigen niet zelfstandig targeting, herkomst of de nationaliteit van een slachtoffer. [S3]

Brandefense Blackhole registreert 96.265 landgelabelde berichten over platforms binnen de rapportperiode. Een landlabel toont geen Belgische doelwitselectie, criminele relevantie of incident aan. Deze aantallen omvatten discussie en advertenties; ze staan apart van de 1.025 bewaarde forumberichten. [S3]

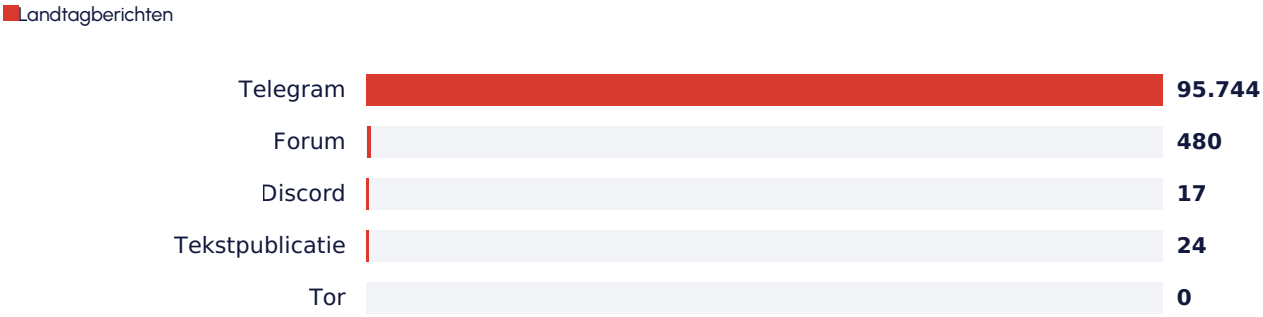
Maandelijkse landlabels meten vastgelegde zichtbaarheid, geen aanvalsfrequentie



Bron: Brandefense Blackhole, 1 januari-22 november 2026; november onvolledig. Landtagberichten en bewaarde forumberichten zijn afzonderlijke populaties, geen bevestigde incidenten [S3].

Maand	Landgelabelde berichten
2026-01	2.299
2026-02	2.322
2026-03	2.659
2026-04	3.405
2026-05	1.610
2026-06	2.141
2026-07	3.356
2026-08	44.206
2026-09	18.132
2026-10	14.312
2026-11	1.823

Platformaantallen beschrijven zichtbaarheid, geen slachtoffers



Bron: Brandefense Blackhole, 1 januari-22 november 2026; november onvolledig. Landtagberichten en bewaarde forumberichten zijn afzonderlijke populaties, geen bevestigde incidenten [S3].

Platform	Landgelabelde berichten
telegram	95.744
forum	480
discord	17
paste	24
tor	0

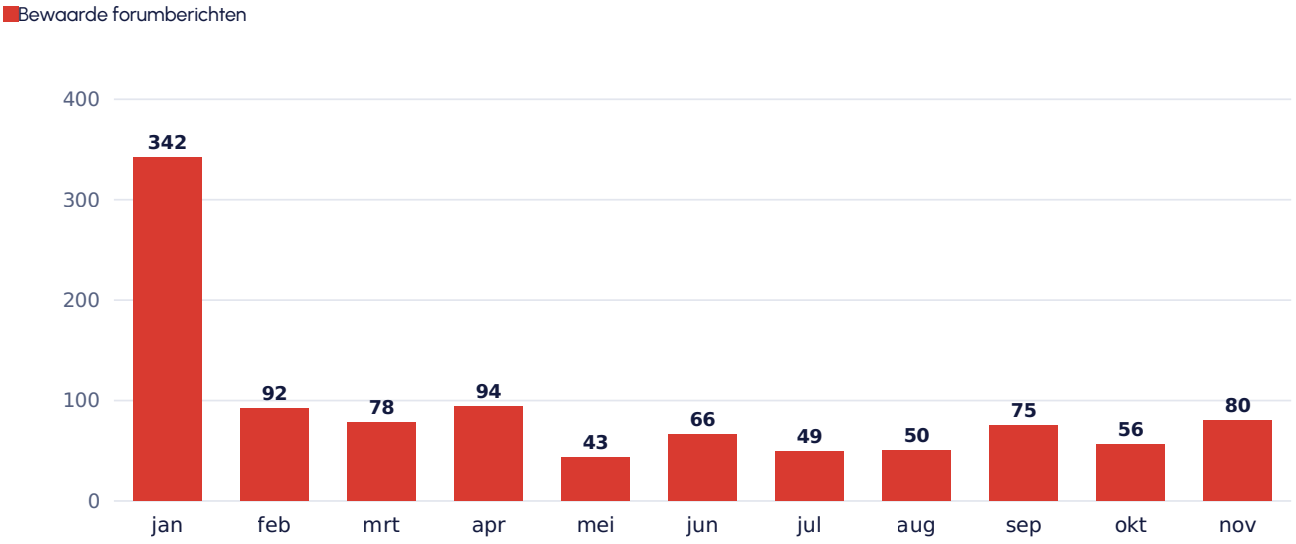
Telegram omvat 95.744 van de 96.265 gelabelde berichten. Bewaard casusbewijs komt uit forums; berichtenplatforms zijn hier door aantallen vertegenwoordigd. Die aantallen bevestigen geen advertentieclaims of aanvalsfrequentie. De foruminhoud kan geen aandelen van misdaadcategorieën over alle platforms aantonen. [S3]

4.2 Volume en taal

Maand	Bewaarde berichten
2026-01	342
2026-02	92
2026-03	78
2026-04	94
2026-05	43
2026-06	66
2026-07	49
2026-08	50

Maand	Bewaarde berichten
2026-09	75
2026-10	56
2026-11	80

Maandcijfers beschrijven bewaarde forumberichten, niet de nationale aanvalsfrequentie



Bron: Brandefense Blackhole, 1 januari-22 november 2026; november onvolledig. Landtagberichten en bewaarde forumberichten zijn afzonderlijke populaties, geen bevestigde incidenten [S3].

De maandcijfers beschrijven deze bewaarde populatie. Ze tonen niet aan dat Belgische dreigingsactiviteit steeg of daalde met het aantal berichten. Advertenties, herplaatsingen, discussie en zichtbaarheid kunnen elk de telling beïnvloeden. [S3]

Het onderzoek omvatte Engelse, Franse, Nederlandse en Russische berichtgeving, met aanvullende relevante regionale context. De taal van een advertentie bepaalt niet de nationaliteit van de adverteerder of de taal van getroffen gebruikers.

4.3 De aangeboden producten

Categorie	Wat het bewaarde materiaal toont	Wat het niet aantoont
Klant- en burgergegevens	Aanbiedingen rond telecom, opleidingen, juridische diensten en consumenten	Authenticiteit, unieke personen of een nieuwe inbraak
Identiteitsdocumenten	Vragen naar Belgische identiteitsbeelden	Een geleverd document of geslaagde onboarding
Toegang en sessies	Claims over beheertoegang en vraag naar cookies	Geldige actuele toegang of een afgeronde aankoop
Bankrekeningidentificatoren	Aangeboden identificatoren en vraagprijzen	Accountcontrole of betalingsbevoegdheid
Fraudehulpmiddelen	Advertenties voor bankspecifieke phishingtemplates	Een werkend hulpmiddel, ingezette campagne of geslaagde onderschepping van authenticatie

Dit zijn waargenomen thema's, geen wederzijds uitsluitende incidentcategorieën of aandelen van een nationale ondergrondse economie. Een advertentie kan meerdere producten noemen. Een weergegeven prijs toont nog geen transactie aan. [S3]

4.4 Casestudies

A

CASUS A

Een telecomadvertentie verwijst naar 2025

Bewijskaart B01 | 24 jan 2026 | Lekforum | Telecommunicatie

Claim niet geverifieerd

CLAIM	De adverteerder biedt een klantgegevensvoorbeeld aan dat meer dan 300k personen zou bevatten. Hij dateert het oorspronkelijke incident uitdrukkelijk op juli 2025.
TIJDLIJN	De bewaarde advertentie dateert van 24 januari 2026. Vergelijkbare titels en latere herplaatsingen bewijzen niet dat de bestanden identiek zijn.
VASTGESTELD	De advertentie en de historische verwijzing zijn bewaard. Aantal, bron en echtheid van de gegevens zijn niet geverifieerd.
ANDERE VERKLARING	Ouder materiaal kan worden gekopieerd, hernoemd of doorverkocht. Een bericht uit 2026 bewijst geen nieuwe inbraak.

AANPAK	Controleer betrokken accounts en eerdere herstelmaatregelen voordat u een nieuw incident beschrijft. Geef evenredig advies als oude persoonsgegevens opnieuw circuleren. [S3]

Conclusie

Een advertentie uit januari noemt een eerdere incidentdatum en biedt een voorbeeld van klantgegevens aan.

Bewijskaart B01 — 24 jan 2026

kazutlg | Lekforum | Forum | English

ORIGINEEL

At the end of July 2025, [a telecom operator] detected a cyberattack on one of its IT systems [...] Here is a sample from this parsed database containing over 300k individuals.

VERTALING

Eind juli 2025 ontdekte [een telecomoperator] een cyberaanval [...] Hier is een voorbeeld uit deze databank met meer dan 300k personen.

Vastgesteld
Een advertentie uit januari noemt een eerdere incidentdatum en biedt een voorbeeld van klantgegevens aan.

Niet vastgesteld
Het aantal of de echtheid van gegevens, een nieuwe inbraak in 2026 of een verkoop.

B

CASUS B

Een aanbieder van burgergegevens kent de bron niet

Bewijskaart B02 | 21 jan 2026 | Lekforum | Burgergegevens

Claim niet geverifieerd

CLAIM	Een account adverteert 3,1M Belgische burgerrecords en suggereert een overheidsbron, maar erkent dat de bron onbekend is.
TIJDLIJN	Een reactie op het bericht van 21 januari wijst op oudere socialemediagegevens. Het oorspronkelijke account aanvaardt dat als mogelijkheid.
VASTGESTELD	De onzekerheid staat in de discussie. Noch de oorspronkelijke claim, noch de reactie valideert de gegevensbron.
ANDERE VERKLARING	Oudere socialemediagegevens, openbare bronnen en hernoemde gegevens blijven mogelijk. De discussie bewijst geen toegang tot een overheidsdatabank.

AANPAK	Vraag gevalideerde herkomst en relevante voorbeelden voordat u de vermeende bronorganisatie waarschuwt. Een groot getal met een landenlabel vervangt die controle niet. [S3]

Conclusie

Een forumbericht claimt een grote bevolkingsdatabank en erkent tegelijk dat de bron onbekend is.

Bewijskaart B02 21 jan 2026

xmlrpc Lekforum Forum English

ORIGINEEL

Today, I leak data from 3.1M Belgian citizens. I don't have a source for this database [...] It's probably a government department scrape.

VERTALING

Vandaag publiceer ik gegevens van 3,1M Belgische burgers. Ik heb geen bron voor deze databank [...] Waarschijnlijk zijn ze bij een overheidsdienst verzameld.

Vastgesteld

Een forumbericht claimt een grote bevolkingsdatabank en erkent tegelijk dat de bron onbekend is.

Niet vastgesteld

Herkomst bij de overheid, het aantal unieke personen of een inbraak bij een overheidsdienst in 2026.

C

CASUS C

Een opleidingsaanbod kan ouder materiaal opnieuw verspreiden

Claim niet geverifieerd

Bewijskaart B03 2 okt 2026 Lekforum Opleiding

CLAIM	De adverteerder biedt meer dan 700K personen en +85 K IBAN aan en beweert ook toegang te verkopen. Dat zijn afzonderlijke beweringen.
TIJDLIJN	Het bewaarde aanbod dateert van 2 oktober. Reacties uit februari en een ander pakket uit oktober noemen hetzelfde doelwit. Berichtgeving beschrijft afzonderlijk herpublicatie. [S20]
VASTGESTELD	De advertentie is bewaard. Het aantal unieke personen en huidige toegang zijn niet onafhankelijk vastgesteld.
ANDERE VERKLARING	Een ouder pakket kan opnieuw of door een ander account worden aangeboden. Een vergelijkbare naam bewijst geen identieke bestanden of afzonderlijke oktoberinbraak.

AANPAK	Controleer huidige accounttoegang los van historische gegevensblootstelling. Waarschuw gebruikers voor nieuwe imitatiepogingen wanneer de organisatie de relevantie heeft vastgesteld. [S3]

Conclusie

Een advertentie uit oktober claimt gegevens en toegang. Reacties uit februari verwijzen al naar hetzelfde onderwerp.

Bewijskaart B03 2 okt 2026

yneov18 Lekforum Forum English

ORIGINEEL

I am selling the complete [vocational-training network] database from belgium containing more than 700K different people and +85 K IBAN [...] also selling the access.

VERTALING

Ik verkoop de volledige databank [van een beroepsopleidingsnetwerk] uit België met meer dan 700K verschillende personen en +85 K IBAN [...] ik verkoop ook toegang.

Vastgesteld
Een advertentie uit oktober claimt gegevens en toegang. Reacties uit februari verwijzen al naar hetzelfde onderwerp.

Niet vastgesteld
Het aantal unieke personen, nog geldige toegang of een nieuwe inbraak in oktober.

D

CASUS D

Een toegangsaanbod noemt herhaaldelijk voorgestelde tabellen

Claim niet geverifieerd

Bewijskaart B04 | 8 nov 2026 | Lekforum | Digitale identiteit

CLAIM	Een verkoper claimt beheerderstoegang tot een identiteitscontroledienst, ongeveer 412k records en een prijs van USD 4.550.
TIJDLIJN	Het aanbod dateert van 8 november. De beschrijvingen noemen de contact-, identiteitscontrole- en hersteltabellen herhaaldelijk voorgesteld.
VASTGESTELD	De structuurbeschrijvingen en toegangsclaim zijn bewaard. Ze tonen geen gevalideerd account, klantomgeving of databank.
ANDERE VERKLARING	De structuren kunnen hypothetisch, gekopieerd of synthetisch zijn. De formulering roept vragen op, maar bewijst niet zelfstandig dat alles verzonnen is.
AANPAK	Controleer een relevante klantomgeving via vertrouwde leverancierskanalen. Bewaar beheerdersactiviteit en herstelgegevens voordat u brede accountresets voorschrijft. [S3]

Conclusie

Het aanbod en de beschrijvingen bestaan. De titel claimt ongeveer 412k records.

Bewijskaart B04 — 8 nov 2026

DataJava | Lekforum | Forum | English

ORIGINEEL

Access: full admin account in [identity-verification portal] [...] Proposed contact table [...] Proposed identity verification case table [...] Proposed account recovery case table [...] Price: $4,550

VERTALING

Toegang: volledig beheerdersaccount in [een identiteitscontroleportaal] [...] Voorgestelde contacttabel [...] Voorgestelde identiteitscontroletabel [...] Voorgestelde accountthersteltabel [...] Prijs: $4.550

Vastgesteld

Het aanbod en de beschrijvingen bestaan. De titel claimt ongeveer 412k records.

Niet vastgesteld

Geldige toegang, werkelijk opgeslagen gegevens, het aantal, een verkoop of een incident bij een leverancier.

E

CASUS E

Een phishingadvertentie noemt banksjablonen

Bewijskaart B05 | 20 nov 2026 | Lekforum | Bankfraude

Claim niet geverifieerd

CLAIM	De SALTA3-advertentie biedt sjablonen voor specifieke banken, waaronder Belgische merken, en claimt interactieve authenticatiefuncties.
TIJDLIJN	Het bericht van 20 november valt in de laatste twee weken. Het is gereedschapsreclame, geen bewaard aanvalsspoor.
VASTGESTELD	De advertentie en geclaimde merkdekking bestaan. Een bankmerk in een sjablonenlijst is een imitatiethema, geen bewijs van toegang tot banksystemen.
ANDERE VERKLARING	Functies kunnen overdreven of gekopieerd zijn. Het materiaal bewijst geen werking, inzet of geslaagde authenticatieonderschepping.
AANPAK	Oefen klantmeldingen en de afhandeling van ongebruikelijke apparaatregistraties of betalingsgoedkeuringen. Beoordeel phishingbestendige authenticatie en blijf reclame onderscheiden van waargenomen aanvallen. [S3]

Conclusie

Een advertentie van 20 november biedt bankspecifieke sjablonen, waaronder Belgische merken, en claimt interactieve functies.

Bewijskaart B05 20 nov 2026

0xcasper Lekforum Forum English

ORIGINEEL

SALTA3 is a live panel phishing kits customized to target specific banks [...] OTP/TAN/2FA support including QR Codes and PhotoTAN method.

VERTALING

SALTA3 is een live phishingpaneel met kits voor specifieke banken [...] ondersteuning voor OTP/TAN/2FA, waaronder QR-codes en PhotoTAN.

Vastgesteld
Een advertentie van 20 november biedt bankspecifieke sjablonen, waaronder Belgische merken, en claimt interactieve functies.

Niet vastgesteld
Een werkende kit, geslaagde onderschepping, inzet, slachtoffers, toegang tot banksystemen of betalingsverlies.

F

CASUS F

Een leveranciersclaim omvat supporttickets en bijlagen

Bewijskaart B06 | 13 nov 2026 | Lekforum | Bedrijfstechnologie

Claim niet geverifieerd

CLAIM	Een account claimt alle supporttickets en bijlagen te bezitten en adverteert 6.028 gebruikers. Beweringen over klanten en eerder contact zijn niet geverifieerd.
TIJDLIJN	Het bericht dateert van 13 november. Geen bewaard bewijs bevestigt onafhankelijk het geclaimde eerdere contact met de leverancier.
VASTGESTELD	De bewering is bewaard. Ze bewijst niet dat elke bijlage aanwezig is of dat een specifieke klant getroffen is.
ANDERE VERKLARING	Het materiaal kan gedeeltelijk, historisch, gekopieerd of verzonnen zijn. Een klantnaam in een advertentie bevestigt geen klantimpact.
AANPAK	Vraag een verklaring over uw eigen organisatie. Beperk gevoelige supportbijlagen en beoordeel beheerderstoegang tot portalen met operationele informatie. [S3]

Conclusie

Een actor claimt supporttickets en bijlagen. Het bericht adverteert 6.028 gebruikers.

Bewijskaart B06 13 nov 2026

updap Lekforum Forum English

ORIGINEEL

some random internet group has your every support ticket and every attachment [...] We urge your customers to review what they shared with you.

VERTALING

Een willekeurige internetgroep heeft elk supportticket en elke bijlage [...] Wij vragen uw klanten na te gaan wat zij met u hebben gedeeld.

Vastgesteld
Een actor claimt supporttickets en bijlagen. Het bericht adverteert 6.028 gebruikers.

Niet vastgesteld
Bezit van alle tickets, getroffen klanten, huidige toegang of technische gevolgen.

4.5 Aanvullende bewijskaarten

De overige kaarten tonen advertenties voor identificatoren, vraag naar identiteitsbeelden, het kopen van sessies en een recent casinogericht aanbod. De oorspronkelijke fragmenten komen uit bewaarde advertenties en bevatten geen identificerend materiaal. Ze zijn geen instructies of gevalideerde productbeschrijvingen. [S3]

Bewijskaart B07 13 apr 2026

[alias withheld] Lekforum Forum English

ORIGINEEL

I SELL 40K+ BELGIUM IBANS PRICE : 1000 IBANS = 1,75$ (USD) ALL IBANS = 70,19$ (USD)

VERTALING

IK VERKOOP 40K+ BELGISCHE IBAN-NUMMERS PRIJS: 1.000 IBAN = 1,75$ (USD) ALLE IBAN-NUMMERS = 70,19$ (USD)

Vastgesteld
Een verkoper biedt bankrekeningidentificatoren met een Belgisch label en vraagprijzen aan.

Niet vastgesteld
Rekeningtoegang, betalingsbevoegdheid, een bankincident of een verkoop.

Bewijskaart B08 24 feb 2026

Crazy88 Lekforum Forum English

ORIGINEEL

Hello i'm looking for a seller that can provide belgium ids i need a lot of them 500+

VERTALING

Hallo, ik zoek een verkoper die Belgische identiteitsdocumenten kan leveren, ik heb er veel nodig, 500+

Vastgesteld
Een koopvraag naar Belgische identiteitsdocumenten.

Niet vastgesteld
Een geleverd document, aankoop, geslaagde identiteitscontrole of de bron van gestolen documenten.

Bewijskaart B09 3 nov 2026

buylogs Lekforum Forum English

ORIGINEEL

I will buy requests from your logs EXPENSIVELY - cookies with active email [...] 250-2500 (fixed and percentage possible)

VERTALING

Ik koop DUUR gegevens uit uw logs: cookies met actieve e-mail [...] 250-2.500 (vast bedrag en percentage mogelijk)

Vastgesteld
Een koopvraag noemt logistieke platformen en actieve e-mailcookies, met een prijsbereik.

Niet vastgesteld
Een antwoord, gekochte sessies, geldige accounts, een verkoop of een platforminbraak.

Bewijskaart B10 21 nov 2026

WSdatabase Lekforum Forum English

ORIGINEEL

Belgium Casino User Database 2026

VERTALING

Belgische casinogebruikersdatabank 2026

Vastgesteld
De advertentie van 21 november en een getoond contactvoorbeeld met geclaimde stortingsvelden.

Niet vastgesteld
Het broncasino, actualiteit, juiste stortingen, huidige accounttoegang of een nieuwe inbraak.

Een IBAN-aanbod vermeldt USD 1,75 voor 1.000 identificatoren en USD 70,19 voor het volledige aangeboden pakket. De hoeveelheden vormen geen exact gecontroleerde inventaris. Een IBAN geeft geen bevoegdheid om geld te verplaatsen. [S3]

Een koopvraag voor logistieke sessies vermeldt een bereik van USD 250–2.500. Dit toont vraag en een prijsbereik aan, geen accountgeldigheid of afgeronde handel. De verdedigingswaarde ligt in sessieherstel en onafhankelijke controle van betalingswijzigingen. [S3]

4.6 Recente activiteit in de bewaarde forums

Berichtdatum	Kaart	Advertentie	Grens
2026-11-13	B06	Ondersteuningstickets en bijlagen van een leverancier	Klantnamen in een claim tonen geen gevolgen voor klanten aan
2026-11-20	B05	Bankspecifieke phishingtemplates	Marketing bewijst geen inzet of incident in banksystemen
2026-11-21	B10	Casinogerichte klantgegevens	Vergelijkbare advertenties in september tonen geen identieke bestanden of nieuw incident aan

Het identiteitsdienstenaanbod in B04 dateert van 8 november en valt buiten de recente periode. De nabijheid van latere meldingen legt geen verband daartussen. Er wordt geen gezamenlijke beheerder of gemeenschappelijk incident afgeleid. [S3]

Een advertentie van 22 november bood opnieuw bankimitatiesjablonen aan en claimde interactieve authenticatiefuncties. Een andere multinationale advertentie nam België in de prijslijst op. Deze waarnemingen tonen geen werkende toegang, geldige kaarten of nieuwe bankinbraak aan. [S3]

4.7 Wat de forums toevoegen

De forums maken de bewoording en timing van claims zichtbaar. Een aanbieder van burgergegevens erkent onzekerheid over de herkomst. Een telecomadverteerder geeft een oudere incidentdatum. Een toegangsverkoper noemt zijn tabellen herhaaldelijk voorgesteld.

Die details helpen onderzoekers betere vragen te stellen. Ze beslissen niet over authenticiteit. Een titel, rijtelling of schema kan gekopieerd, deels juist, verouderd of verzonnen zijn. Het rapport behoudt deze alternatieven in plaats van alle advertenties als gelijkwaardige inbreuken te behandelen.

KERNPUNTEN

01

Berichtdatums geven advertentietijdstippen aan, geen inbraakdatums.

02

Controleer herkomst en werkende toegang afzonderlijk.

03

Recente marketing voor fraudehulpmiddelen ondersteunt voorbereiding, geen claim over geslaagde aanvallen.

HOOFDSTUK 05

Bevestigde incidenten en claims per sector

05

DIT HOOFDSTUK BEANTWOORDT

Welke uitkomsten zijn vastgesteld en welke cijfers blijven van een claimant?

3

afzonderlijke vragen: beschikbaarheid, gegevensblootstelling en toeschrijving

5.1 Het incidentregister lezen 37

5.2 Zorg- en leerdiensten 38

5.3 Gemeentelijke en gedeelde openbare diensten 40

5.4 Leden-, klant- en operationele gegevens 42

5.5 Andere geregistreerde incidenten en gemelde claims 44

5.6 Aanvullende zakelijke, onderzoeks- en lokale dienstverleningsgevallen 45

5.7 Wat deze gevallen aantonen 47

HOOFDSTUK 05

Bevestigde incidenten en claims per sector

IN HET KORT

Het Belgische publieke dossier omvat onderbroken zorg, blootgestelde ledengegevens, onderwijsplatformen, gemeentelijke systemen en gedeelde leveranciers. Meerdere organisaties bevestigden een incident zonder het aantal getroffen personen vast te stellen. Herstel en beoordelingen van gegevensverlies veranderden soms op verschillende datums. De casuskaarten behouden die verschillen. Gebruik het meest vergelijkbare operationele voorbeeld om uw eigen beheersings-, klantmeldings- en herstelbeslissingen te testen.

5.1 Het incidentregister lezen

Een bevestigd incident bevestigt niet elke bijbehorende criminele claim. Het register onderscheidt rechtstreekse organisatieverklaringen, officiële waarschuwingen, toegeschreven berichtgeving en ondergrondse advertenties. De onderstaande gevallen zijn geselecteerde dossiers, geen nationale telling.

Sommige buitenlandse diensten bewaren gegevens van Belgische gebruikers. Ze horen bij het afhankelijkheidsbeeld, maar een wereldwijd gebruikersaantal is geen Belgisch getroffen aantal. Herhaalde advertenties en verwante federatiemeldingen zijn niet automatisch onafhankelijke incidenten.

Namen verschijnen alleen wanneer officiële bevestiging en bredere berichtgeving ze ondersteunen. Andere organisaties krijgen brede rolomschrijvingen. Zo'n omschrijving beschermt de identiteit; ze mag onzekerheid over de gebeurtenis zelf niet verbergen.

5.2 Zorg- en leerdiensten

CASUS G

G

Een ziekenhuis isoleert systemen in januari

Gezondheidszorg

Toegeschreven openbaar verslag

GEBEURTENIS	Een Belgisch ziekenhuisnetwerk ontdekte op 13 januari een ernstige IT-verstoring. Zijn in de berichtgeving geciteerde verklaring beschreef een preventieve uitschakeling op zijn campussen. [S10]
CHRONOLOGIE	Geplande zorg werd onderbroken en kritieke patiënten werden overgebracht. Het bewaarde januariverslag toont geen losgeldbetaling, genoemde aanvaller of volledige omvang van gegevensverlies aan.
VASTGESTELD	Klinische continuïteit hing af van kunnen werken zonder beschikbare digitale systemen. Een uitschakelingsbeslissing kan systemen beschermen en tegelijk directe operationele kosten veroorzaken.
ALTERNATIEVEN EN GRENZEN	Dienstverstoring alleen maakt geen onderscheid tussen versleuteling, beheersing of een andere technische oorzaak. Latere criminele claims vereisen eigen bewijs.
RESPONS	De klinische leiding moet handmatige documentatie, patiëntentransfers en communicatie met naburige zorgverleners oefenen. Leg vast welke systemen moeten zijn hersteld voordat normale planning hervat.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS H

H

Basic-Fit bevestigt een grensoverschrijdend klantgegevensincident

Consumentendiensten

Toegeschreven openbaar verslag

GEBEURTENIS	Safeonweb gaf op 13 april de bedrijfsbevestiging door dat Belgische leden betrokken waren bij een klantgegevensincident. Reuters meldde eveneens de bedrijfsverklaring. [S11][S12]
CHRONOLOGIE	De bekendmaking beschreef informatie over leden in meerdere landen. Het cijfer van ongeveer één miljoen betreft de bredere internationale populatie, niet alleen België.

VASTGESTELD	Mogelijk getroffen gegevens omvatten contact-, geboortedatum- en bankinformatie. Het bedrijf zei dat wachtwoorden en identiteitsdocumenten niet waren buitgemaakt. [S11]
ALTERNATIEVEN EN GRENZEN	Een bankrekeningidentificator bewijst geen toegang tot de bankrekening van de houder. De bewaarde bronnen stellen geen Belgisch aantal getroffen personen vast.
RESPONS	Waarschuw klanten voor berichten die echte lidmaatschapsgegevens noemen. Ondersteuningsteams moeten identiteit via een afzonderlijk betrouwbaar proces controleren voordat ze contact- of betalingsinformatie wijzigen.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS I

Een leerplatformincident roept Belgische afhankelijkheidsvragen op

Onderwijs

Toegeschreven openbaar verslag

GEBEURTENIS	Safeonweb beschreef op 6 mei een door de leverancier bevestigd incident bij een online leerplatform dat in België wordt gebruikt. De leveranciersbevestiging dateerde van 1 mei. [S13]
CLAIM	Een criminele groep adverteerde met een wereldwijde populatie van 275 miljoen gebruikers. Safeonweb noemde dat aantal uitdrukkelijk onbevestigd. Het is geen Belgisch aantal.
VASTGESTELD	Mogelijke gegevenscategorieën waren namen, e-mailadressen, studentidentificatoren en berichten. De leverancier meldde toen geen aanwijzingen voor betrokkenheid van wachtwoorden, geboortedatums, officiële identificatoren of financiële gegevens.
ALTERNATIEVEN EN GRENZEN	Een platformbrede claim toont niet aan welke records van een bepaalde instelling zijn buitgemaakt. Instellingsmeldingen en dienstenherstel beantwoorden verschillende vragen.
RESPONS	Onderwijsaanbieders moeten een afgebakende impactverklaring vragen, studentenmeldingen voorbereiden en ondersteuningsprocessen voor medewerkers controleren. Behandel onverwachte opleidingsberichten als een kwestie van klantbescherming.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

Het tweedekwartaalrapport van het CCB bespreekt ook een zorgsoftwareleveranciersincident dat relevant is voor België. Dit toont een afhankelijkheidsvraagstuk aan; het bewijst niet dat elk klantziekenhuis gegevens verloor. [S8]

5.3 Gemeentelijke en gedeelde openbare diensten

J

CASUS J

Machelen wijzigt de gegevensverliesbeoordeling na het eerste incident

Lokaal bestuur

Toegeschreven openbaar verslag

GEBEURTENIS	De gemeente ontdekte op 11 september een cyberincident. Volgens haar eigen update bevestigde verdere analyse op 22 september diefstal van persoonsgegevens. [S15][S16]
CHRONOLOGIE	Digitale diensten werden getroffen. Volgens de vastgelegde gemeentelijke melding werkten de diensten weer, met mogelijke vertragingen, terwijl het onderzoek naar gegevensverlies doorging.
VASTGESTELD	Incidentdatum, bevestigingsdatum en hersteltoestand zijn verschillende feiten. De eerste onzekerheid verhinderde de gemeente niet om latere updates te geven.
CLAIM	Een latere afpersingsvermelding staat in de ransomwarepopulatie van het rapport. Die vermelding toont niet zelfstandig de volledige dataset, aanvalsmethode of identiteit van de indringer aan. [S1]
RESPONS	Onderhoud een updatepagina met gedateerde wijzigingen. Geef inwoners praktisch beschermingsadvies en leg uit welke gegevenscategorieën en getroffen personen nog worden onderzocht.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

L

CASUS L

Een digitalehandtekeningleverancier raakt lokale werkprocessen

Gedeelde openbare diensten

Toegeschreven openbaar verslag

GEBEURTENIS	Berichtgeving op 26 oktober citeerde een leveranciersdirecteur over ongeoorloofde toegang tot een digitalehandtekeningdienst. Verdachte activiteit was op 23 oktober ontdekt. [S22]

CHRONOLOGIE	De leverancier haalde de dienst offline en herstelde hem de volgende avond met beperkingen. Klantspecifieke impactbeoordelingen werden voorbereid.
VASTGESTELD	De leverancier zei dat vooral metadata betrokken waren en dat geen frauduleuze handtekeningen waren aangemaakt. Dit zijn toegeschreven bedrijfsverklaringen, geen onafhankelijke forensische conclusie.
ALTERNATIEVEN EN GRENZEN	Meer dan 120 lokale besturen gebruikten de module. Die klantenpopulatie telt niet de getroffen besturen. Een afzonderlijke integratiepopulatie mag er niet bij worden opgeteld.
RESPONS	Vraag naar de gevolgen voor uw eigen documenten, identiteiten en integraties. Controleer vervangen toegangsrechten en test betalingsmeldingen via een bekend officieel kanaal.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

M

CASUS M

Federale belastingdiensten herstellen applicaties in fasen

Overheid

Toegeschreven openbaar verslag

GEBEURTENIS	SPF Finances/FOD Financiën bevestigde een cyberaanval op 28 oktober. Volgens zijn herstelmelding beheerste de dienst het incident binnen enkele uren en werden applicaties tijdelijk offline gehaald. [S23][S24]
CHRONOLOGIE	Belangrijkste diensten keerden terug op 31 oktober. Een functie voor roerende voorheffing keerde terug op 6 november en e604 op 12 november. Dit zijn herstelmijlpalen, geen afzonderlijke inbraken.
VASTGESTELD	Volgens de autoriteit vond haar onderzoek geen gegevensexfiltratie of aanvallerscontrole over applicaties. Schrijf die conclusie toe aan de autoriteit en haar onderzoek. [S23]
ALTERNATIEVEN EN GRENZEN	Een preventieve uitschakeling heeft echte beschikbaarheidsgevolgen. Ze bewijst geen gegevensdiefstal, en herstel alleen zou de afwezigheid daarvan niet aantonen.
RESPONS	Oefen gefaseerd herstel en communiceer welke functies onbeschikbaar blijven. Houd technische beheersing, gebruikersimpact en vertrouwelijkheidsbevindingen in afzonderlijke delen van het incidentdossier.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

5.4 Leden-, klant- en operationele gegevens

CASUS K

K Een fitnessketenincident en een grotere criminele personentelling

Consumentendiensten

Toegeschreven openbaar verslag

GEBEURTENIS	Een fitnessketen erkende een incident met ledeninformatie. De berichtgeving citeerde haar woordvoerder over records die betrekking hadden op hoogstens 31 van haar 85 Belgische clubs. [S18]
CLAIM	Het veel herhaalde cijfer van 150.000 leden werd toegeschreven aan de aanbieders van de gegevens. Het mag geen door het bedrijf bevestigd getroffen aantal worden.
VASTGESTELD	Gemelde categorieën omvatten identiteits-, contact- en lidmaatschapsgegevens en sommige bankrekeningidentificatoren. Het bedrijf zei dat wachtwoorden en gezondheidsgegevens niet betrokken waren. [S18]
ALTERNATIEVEN EN GRENZEN	Clubs, leden, potentiële klanten en geadverteerde records zijn verschillende eenheden. Een geclaimd personenaantal delen door het clubaantal toont geen blootstelling per club aan.
RESPONS	Informeer de personen die het bedrijfsonderzoek identificeert en bereid u voor op gerichte imitatie. Authenticeer een beller niet alleen omdat die een lidmaatschaps- of bankrekeninggegeven kent.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS N

N Koelverstoring maakt toegang op afstand een operationele kwestie

Winkelactiviteiten

Toegeschreven openbaar verslag

GEBEURTENIS	Officiële waarschuwingen en publieke berichtgeving beschrijven een novemberincident met winkelkoeling. Gewijzigde werkingsomstandigheden hadden gevolgen voor winkels en voorraden. [S25][S27]
CHRONOLOGIE	Belgische verstoring werd gemeld op 2 november. Daarna volgden technisch advies en toegeschreven verklaringen. Verschillende verslagen telden winkels, apparatuur en klantenpopulaties van leveranciers.

VASTGESTELD	Operationele teams moeten toegang op afstand beheersen en veilige instellingen kunnen herstellen. De publieke bronnen rechtvaardigen niet dat alle genoemde apparatuur- en winkelaantallen worden opgeteld.
TOESCHRIJVING	Reuters meldde op 13 november tegenstrijdige ministeriële beoordelingen. Dit rapport beslecht dat meningsverschil niet en schrijft de campagne niet zelfstandig toe. [S26]
RESPONS	Verwijder onmiddellijk rechtstreekse publieke internettoegang tot beheerinterfaces van koelinstallaties. Operations en beveiliging moeten veilige continuïteit en beschermd onderhoud op afstand coördineren, accounts tot goedgekeurde behoeften beperken en een veilige lokale modus oefenen. Controleer veilige instellingen en bewaar bewijs dat de interfaces niet meer rechtstreeks bereikbaar zijn. [S25]

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS O

Een recente melding van een geschenkbonnendienst

Consumentendiensten

Toegeschreven openbaar verslag

GEBEURTENIS	Safeonweb waarschuwde op 20 november voor ongeoorloofde toegang tot een geschenkbonnenplatform. De melding gaf de bedrijfsbevinding door en vermeldde dat het onderzoek doorging. [S29]
VASTGESTELD	Namen en e-mailadressen zijn mogelijk ingezien. Volgens het bedrijf waren wachtwoorden en betaalkaartgegevens op dat moment niet getroffen.
ALTERNATIEVEN EN GRENZEN	De melding gaf geen Belgisch aantal getroffen klanten. Overtuigende vervolgberichten zijn een aannemelijk risico, geen bewijs dat een bepaalde fraude deze records al gebruikte.
RESPONS	Klantenteams moeten via de gewone dienstkanalen een korte waarschuwing publiceren. Adviseer gebruikers de officiële app of website rechtstreeks te openen bij controle van een onverwacht bericht.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

5.5 Andere geregistreerde incidenten en gemelde claims

Deze rijen behouden aanvullende incidentdekking zonder elk persverslag als gecontroleerde technische bevinding te behandelen.

Periode	Brede rol	Bewijs en grens	Gevolg voor verdedigers
Juni	Een gevoelige overheidsdienst	Berichtgeving beschreef een mobielbeheerincident tussen 2025 en voorjaar 2026; officiële bevestiging en toeschrijving bleven onopgelost [S14]	Onderzoek beheertoegang zonder aan te nemen dat het interne inlichtingennetwerk werd bereikt
september	Een sportfederatie	Berichtgeving citeerde bevestiging van een ledendatabase-incident; de volledige omvang werd niet onafhankelijk vastgesteld [S17]	Bereid ledenmeldingen voor en controleer uitbestede administratie
september	Een verwante sportledenadministratie	Een federatie en haar vleugel werden samen besproken; aangeboden recordaantallen blijven claims [S17]	Houd één campagnedossier wanneer het bewijs verwante systemen betreft
Oktober	Een scholengroep	Een directeur bevestigde een incident met leerlingen en medewerkers; 3.550 plus 650 is 4.200 personen in de gemelde populatie [S19]	Controleer medewerkerstoegang en ondersteuning, inclusief gevoeligheid van thuisadressen
Oktober	Een beroepsopleidingsnetwerk	Berichtgeving beschreef herpublicatie van gegevens uit een februari-incident; 700.000 records en 85.000 bankgegevens waren gemelde cijfers [S20]	Een herplaatsing kan phishingrisico vernieuwen zonder een nieuwe inbraak aan te tonen
Oktober	Een publiek e-learningplatform	Berichtgeving beschreef een dienstsluiting en een afzonderlijke geadverteerde gegevenstelling [S21]	Behandel beschikbaarheid en de gegevensclaim als afzonderlijke controletaken

Periode	Brede rol	Bewijs en grens	Gevolg voor verdedigers
november	Een betaaldienst voor personeelsvoordelen	Officiële waarschuwing beschreef mogelijke accountgegevensblootstelling; het bedrijf had geen betaalproblemen of verdachte transacties vastgesteld [S28]	Waarschuw accounthouders zonder onbevestigde betalingsverliezen te beschrijven
April	Een onlineboekingsdienst	Safeonweb meldde mogelijke toegang tot reserveringsgegevens en gewijzigde reserveringspincodes; het bedrijf zei dat financiële gegevens niet waren ingezien [S11]	Geen Belgisch totaal van getroffen gebruikers vastgesteld

5.6 Aanvullende zakelijke, onderzoeks- en lokale dienstverleningsgevallen

CASUS R

R

Een onderzoeksinstituut bevestigt gekopieerde gegevens terwijl diensten doorgaan

Medisch onderzoek

Toegeschreven openbaar verslag

OFFICIEEL VERSLAG

Een gespecialiseerd medisch en onderzoeksinstituut beschrijft ongeoorloofde toegang tot en kopiëren uit een database na ontdekking op 12 oktober. De melding werd bijgewerkt op 10 november. [S49]

VASTGESTELD

Volgens het instituut was het merendeel van de gekopieerde informatie gecodeerd en een kleiner deel rechtstreeks identificeerbaar. De actuele bevindingen toonden geen gevolgen voor andere systemen; zorg en onderwijs gingen door.

GRENZEN

Gecodeerde gegevens zijn niet automatisch anoniem. Een afzonderlijk gemeld aantal geïnformeerde personen meet niet de volledige gekopieerde database. Het rapport geeft geen gecombineerd totaal van getroffen personen.

RESPONS

Onderzoeks- en privacyteams moeten coderings- en identificatierisico samen beoordelen. Bepaal wie de koppelinformatie bezit, documenteer de getroffen projecten en bereid evenredige deelnemerscommunicatie voor.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS S

S De contactpopulatie van een beroepsorganisatie vraagt een precieze noemer

Professionele diensten

Toegeschreven openbaar verslag

OFFICIEEL VERSLAG	Een juridische beroepsorganisatie zegt in haar update van 6 november dat ze op 29 oktober over het incident werd geïnformeerd. Ze beschrijft toegang via een administratieve applicatie en aangeboden contactinformatie. [S50]
VASTGESTELD	De update noemt ongeveer 27.500 contacten die geen advocaten zijn, naast advocatenrecords. Ze geeft geen volledig getroffen totaal.
GRENZEN	Volgens de organisatie vond haar analyse geen bankgegevens of bijzondere persoonsgegevens in de getroffen populatie. Dit is haar beoordeling, geen onafhankelijke controle van elk aangeboden bestand.
RESPONS	Houd beroeps- en externe contactpopulaties apart. Waarschuw ontvangers voor berichten met echte contactgegevens en controleer de scope voordat u een groter advertentieaantal overneemt.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

De volgende aanvullende gevallen verbreden het dienstenbeeld. Ze tonen niet allemaal gegevensdiefstal of ransomware aan.

Periode	Brede rol	Wat de bron ondersteunt	Grens
april	Een gemeente	De burgemeester beschreef verstoring en gegevensdiefstal; herstel verliep geleidelijk [S53]	Oorspronkelijke gemeentelijke verklaring niet bewaard; geen volledig getroffen personenaantal
Mei	Een chemische fabrikant	De eigen verduidelijking beschrijft ongeoorloofde toegang; forensisch onderzoek vond volgens het bedrijf geen exfiltratie- of ransomwarebewijs [S47]	Latere publiciteit betreft dezelfde meigebeurtenis
Mei	Een recyclageparkbeheerder	Het vervolgbericht beperkt het incident tot een externe leverancierscomputer; activiteiten werden uit voorzorg geïsoleerd [S48]	Geen exfiltratieaanwijzingen in het genoemde onderzoek
Juli	Externe klantgegevensleverancier van een supermarkt	Berichtgeving citeert een bedrijfsverklaring over contactgegevens op een afzonderlijke leveranciersserver [S51]	Niet veralgemenen naar betaalsystemen of elke klant

Periode	Brede rol	Wat de bron ondersteunt	Grens
Augustus	Een meubelhandelaar	Een woordvoerder beschreef korte verstoring en toegang tot klantcontact- en bestelinformatie [S52]	Criminele toeschrijving blijft een claim
Oktober	Een reisorganisatie	Een woordvoerder bevestigde een gegevensincident en klantenwaarschuwing [S56]	Herkomst van gepersonaliseerde fraudeberichten bleef onopgelost
Oktober, gemeld in november	Een edelmetaalhandelaar	Berichtgeving citeert bevestiging van klantensysteemtoegang [S54]	Een voorgesteld verband met inbraken in woningen werd niet vastgesteld
november	Een gemeentelijke publieke website	Een burgemeester beschreef websitetoegang en mogelijke blootstelling van medewerkersaccounts [S55]	Geen bevinding van burgergegevensblootstelling of toegang tot afzonderlijke gemeentediensten

Een laadaccountdienst biedt recente grensoverschrijdende context. Zijn eigen FAQ beschrijft een aanval op 8 november, ontdekking op 10 november en herstelmaatregelen op 12 november. Gebruikers werden geïnformeerd op 18 november. Een Belgisch getroffen aantal is niet vastgesteld. [S46]

VRT meldt meer dan 3,5 miljoen gebruikers in Europa; die populatie is geen aantal getroffen accounts. [S71] Het bedrijf noemt account- en profielinformatie, waaronder wachtwoordhashes, en sluit in zijn melding meerdere andere categorieën uit. Individuele Belgische dienstverleners moeten hun eigen afhankelijkheid en gebruikers controleren. [S46]

5.7 Wat deze gevallen aantonen

Het sterkst terugkerende pad is een verschil tussen dienstgrens en organisatiegrens. Leden gebruiken een platform, medewerkers vertrouwen op een leverancier en inwoners hangen af van een administratieve applicatie. Incidentrespons moet de werkelijke afhankelijkheid identificeren.

De gevallen tonen ook waarom heldere berichtgeving belangrijk is. Een bevestiging kan een criminele claim beperken zonder elk risico weg te nemen. Een herstelmelding kan gebruikers helpen hervatten terwijl het gegevensonderzoek doorgaat.

Het rapport telt klantenaantallen, geclaimde records, organisaties en winkelaantallen niet op tot één hoofdcijfer. Zo'n totaal zou niets samenhangends meten. Leiders moeten vragen welke dienst, gegevenscategorie en persoon nu actie nodig heeft.

KERNPUNTEN

01

Houd herstel, gegevensblootstelling en toeschrijving als afzonderlijke bevindingen.

02

Klantenpopulaties van leveranciers zijn geen totalen van getroffen slachtoffers.

03

Herplaatste gegevens kunnen frauderisico vernieuwen zonder een nieuwe inbraak te bewijzen.

HOOFDSTUK 06

Hacktivisme, verstoring en operationele systemen

06

DIT HOOFDSTUK BEANTWOORDT

Wat werd waargenomen, wat werd geclaimd en hoe blijven diensten bruikbaar tijdens verstoring?

9–22 november

de recente periode binnen de bredere jaarperiode

6.1 Tijdlijn 50

6.2 Claim tegenover publiek verslag 51

6.3 Een website-incident is geen apparatuurincident 51

6.4 Recente activiteit: 9–22 november 52

6.5 Beslissingen tijdens een korte verstoring 52

HOOFDSTUK 06

Hacktivisme, verstoring en operationele systemen

IN HET KORT

Het publieke dossier ondersteunt voorbereiding op websiteverstoring en operationele gevolgen. Het CCB meldde geen hacktivistische DDoS-incidenten in het eerste kwartaal en een beperkte terugkeer in het tweede. Koelincidenten in november tonen een ander continuïteitsprobleem. Actorverklaringen en politieke verklaringen tonen geen technische impact aan. Bereid statuscommunicatie, alternatieve diensten en beheerste toegang op afstand voor op de volgende verstoring.

6.1 Tijdlijn

13 jan 2026	**Ziekenhuisverklaring, geciteerd in berichtgeving** Preventieve systeemuitschakeling en onderbroken zorg [S10]
22 apr 2026	**CCB-kwartaalrapport** Geen hacktivistische DDoS-incidenten gemeld voor het eerste kwartaal [S7]
15 jul 2026	**CCB-kwartaalrapport** Beperkte terugkeer van DDoS-activiteit gedurende één dag in het tweede kwartaal [S8]
11 sep 2026	**Gemeentelijke incidentmelding** Digitale dienstonderbreking, gevolgd door latere bevestiging van gegevensdiefstal [S15]
28 okt 2026	**Federale belastingadministratie** Applicaties tijdelijk offline na een incident [S23]
2 nov 2026	**Berichtgeving over winkelkoeling** Verstoring van Belgische apparatuur gemeld [S25][S27]
9 nov 2026	**CCB-identiteitsbeoordeling** Accountbescherming blijft een prioriteit [S5]
10 nov 2026	**Medisch onderzoeksinstituut** Incidentverklaring bijgewerkt; geen nieuwe inbraak vastgesteld [S49]
12 nov 2026	**Federale belastingadministratie** Herstelupdate voor e604 [S23]
13 nov 2026	**Reuters** Verschillende ministeriële beoordelingen van koeltoeschrijving [S26]
17 nov 2026	**Safeonweb** Waarschuwing voor valse aanbiedingen van pellets en brandhout [S45]
18 nov 2026	**Laadaccountdienst**

Gebruikers geïnformeerd na eerdere ontdekking en herstel; Belgisch getroffen aantal onbekend [S46]

20 nov 2026 **Safeonweb**
Waarschuwing over geschenkbonnendienst vermeldt lopend onderzoek [S29]

Een officiële rij benoemt de bron van het verslag. Dit betekent niet dat de bron elke genoemde aanvallersverklaring onafhankelijk controleerde. Een doorgifterij benoemt berichtgeving, geen oorspronkelijk actorbericht.

6.2 Claim tegenover publiek verslag

Punt	Claim of interpretatie	Officieel verslag	Beoordeling
Websitebeschikbaarheid	Een actor kan een site als onbeschikbaar adverteren	CCB-rapporten beschrijven hun eigen waargenomen incidentpopulatie [S7][S8]	Een schermafbeelding of bericht toont geen uitvalduur of nationale impact aan
Uitschakeling belastingsystemen	Onbeschikbaarheid kan als geslaagde toegang worden beschreven	Volgens de autoriteit werden applicaties geïsoleerd en geen exfiltratie of applicatiecontrole gevonden [S23]	Schrijf de bevindingen toe aan haar onderzoek
Verantwoordelijkheid koelincidenten	In politiek commentaar kan een staat worden genoemd	Reuters registreert verschillende ministeriële beoordelingen en een lopend onderzoek [S26]	Toeschrijving blijft in dit rapport onopgelost
Omvang koelincidenten	Apparatuur, winkels en klanten verschijnen in verschillende verslagen	Officiële waarschuwingen beschrijven het operationele risico [S25][S27]	Combineer geen onverenigbare noemers

6.3 Een website-incident is geen apparatuurincident

Een website kan onbeschikbaar zijn terwijl interne activiteiten doorgaan. Een operationele interface kan apparatuurgedrag veranderen terwijl de bedrijfswebsite online blijft. Telemetrie, verantwoordelijken en herstelbeslissingen verschillen.

Spreek voor publieke websites af hoe verkeersbeperking wordt aangevraagd en hoe legitieme gebruikers toegang behouden. Bewaar beschikbaarheidsmetingen en de tijdzone. Vermijd uitspraken die gegevenstoegang afleiden uit een DDoS-claim.

Verwijder voor koelapparatuur onmiddellijk rechtstreekse publieke internettoegang tot beheerinterfaces. Operations en beveiliging moeten veilige continuïteit en beschermd onderhoud op afstand coördineren. Controleer dat beheerinterfaces niet meer rechtstreeks bereikbaar zijn. [S25]

Betrek voor operationele apparatuur het team dat veilige instellingen beheert. Test wat er gebeurt als de externe leveranciersroute wordt verwijderd. Controleer dat het lokale herstelproces veilig blijft en noodtoegang wordt geregistreerd.

Het koelgeval toont niet aan dat alle verbonden huishoudapparaten dezelfde blootstelling hebben. Safeonweb maakt in zijn publieke advies onderscheid tussen algemene apparaatbescherming en de specifieke commerciële incidenten. [S27]

6.4 Recente activiteit: 9–22 november

De recente periode is een waarnemingsperiode, geen voorspelling. Het CCB-identiteitsrapport van 9 november beschrijft actuele verdedigingsprioriteiten met eerdere meldingspopulaties. De publicatiedatum verplaatst de onderliggende incidenten niet naar november. [S5]

Op 12 november meldde de belastingadministratie herstel van nog een applicatie na het oktoberincident. Op 13 november registreerde Reuters toeschrijvingsonzekerheid rond koeling. Geen van beide vormt een nieuwe onafhankelijke aanvalstelling. [S23][S26]

De Safeonweb-waarschuwing over geschenkbonnen van 20 november voegt een klantgegevensrisico toe. Ze meldt mogelijke openbaarmaking en lopend onderzoek, zonder Belgisch personenaantal. Gebruik dit als aanleiding voor afgebakende klantcommunicatie. [S29]

Het recente ondergrondse bewijs wordt afzonderlijk in hoofdstuk 4 beoordeeld. Een nieuwe advertentie kan oude gegevens betreffen. Ze kan ook een hulpmiddel promoten waarvan werkelijk gebruik niet is vastgesteld. Berichtdatums meten advertenties, niet de onderliggende incidenten. [S3]

6.5 Beslissingen tijdens een korte verstoring

Spreek af welke minimuminformatie nodig is om verkeersbescherming te activeren, een leveranciersintegratie te isoleren of handmatig te gaan werken. Wachten op toeschrijving kan verstoring verlengen zonder de eerste beheersingsbeslissing te verbeteren.

Gebruik één publiek statuskanaal met expliciete tijdstempels. Zeg welke diensten werken, welke niet en wat gebruikers moeten doen. Beschrijf gegevenstoegang alleen wanneer bewijs dit ondersteunt.

Behoud het verschil tussen voorzorg en bevinding. Een organisatie kan een systeem isoleren omdat ze risico nog niet kan uitsluiten. Dat betekent niet dat elk verbonden systeem is getroffen.

KERNPUNTEN

01

Meet dienstenbeschikbaarheid afzonderlijk van criminele claims.

02

Operationele teams moeten veilig apparatuurherstel beheren.

03

Recente publicatiedatums maken oudere incidenten geen nieuwe aanvallen.

HOOFDSTUK 07

Dreigingsactoren en bewijsverbanden

07

DIT HOOFDSTUK BEANTWOORDT

Welke actornamen worden waargenomen en welk verband ondersteunt elk bewijsstuk werkelijk?

22

ransomwaregroepsnamen in de bewaarde Belgische vermeldingspopulatie

7.1 Hoe het bewijs samenhangt 54

7.2 Afpersing: een verspreide vermeldingspopulatie 55

7.3 Advertentiepersona's 59

7.4 Spionage en onopgeloste inbraakberichtgeving 59

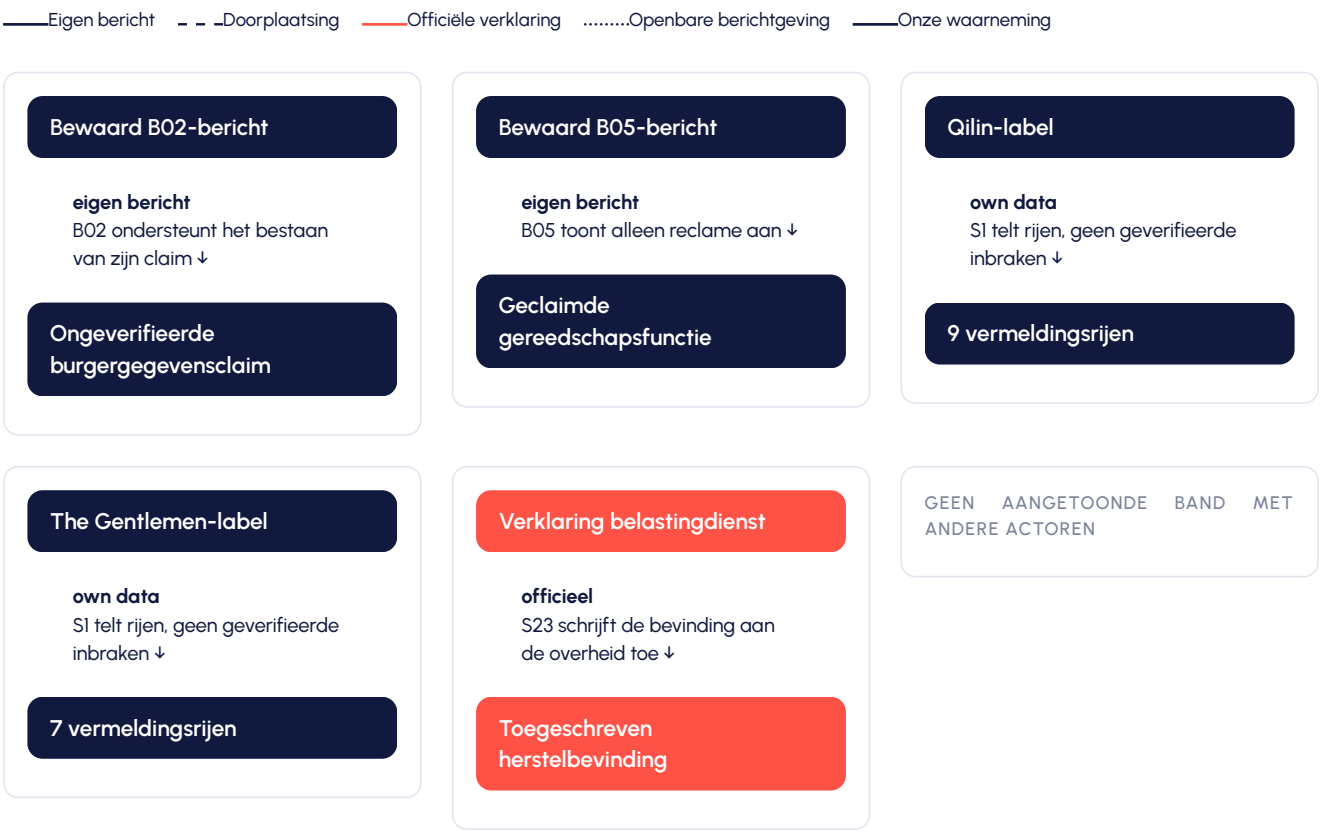
HOOFDSTUK 07

Dreigingsactoren en bewijsverbanden

IN HET KORT

Het bewijs bevat afpersingsnamen, advertentiepersona's en door autoriteiten beschreven campagnes. Dit zijn verschillende soorten identiteit. Een gemeenschappelijke sector, taal of politiek thema verbindt geen beheerders. De verbandkaart koppelt bewijs aan een stelling in plaats van ongerelateerde groepen te verbinden. Baseer respons op bevestigde toegang, dienstimpact en herstelbehoeften; gebruik toeschrijving wanneer ze die beslissingen verbetert.

7.1 Hoe het bewijs samenhangt



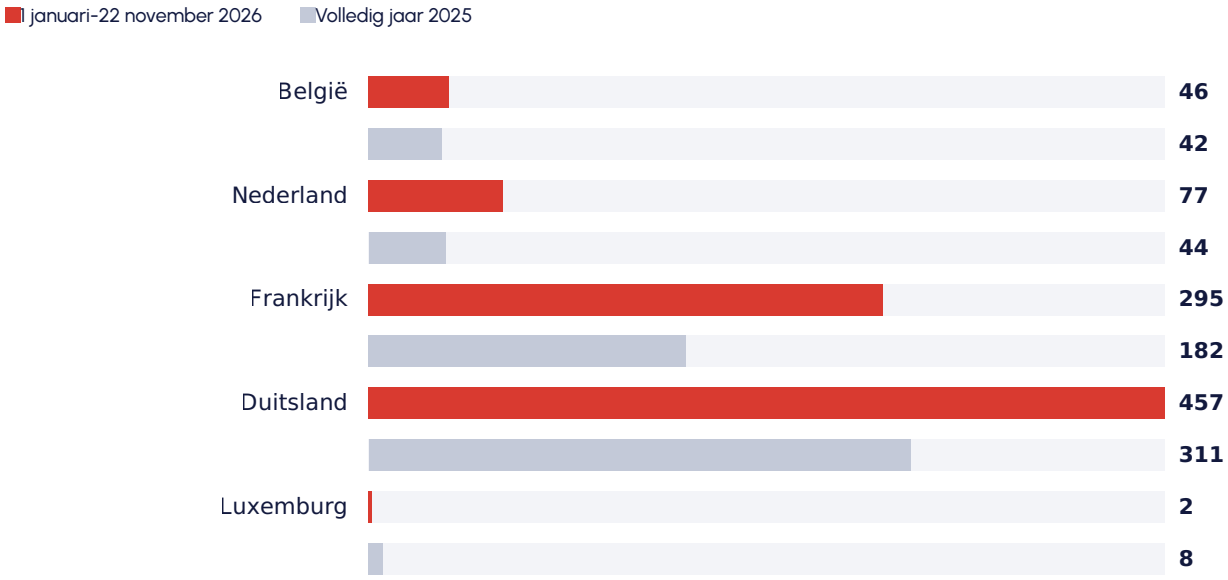
De kaart toont een bewaarde advertentie die haar eigen claim ondersteunt, een vermelding die een afpersingsclaim ondersteunt en publieke bronnen die een beschreven uitkomst ondersteunen. Ze leidt geen gezamenlijke beheerder tussen die populaties af.

Overeenkomende titels kunnen vergelijkbare advertenties aantonen. Een herhaalde alias kan gebruik van die persona aantonen. Geen van beide toont identieke bestanden, een afgeronde overdracht of de persoon achter het account aan. Uit deze overeenkomsten wordt geen gemeenschappelijke criminele organisatie afgeleid. [S3]

Het verband tussen hergebruikte authenticatiegegevens, accountmisbruik en fraude is een analytisch model van een mogelijk pad. De politie beschrijft dat pad in specifieke onderzoeken. Dit betekent niet dat de forumverkopers uit dit rapport aan die campagnes leverden. [S31][S32]

7.2 Afpersing: een verspreide vermeldingspopulatie

België telt 46 vermeldingen in de gedeeltelijke jaarperiode, met verschillende totalen bij vier regionale vergelijkingslanden



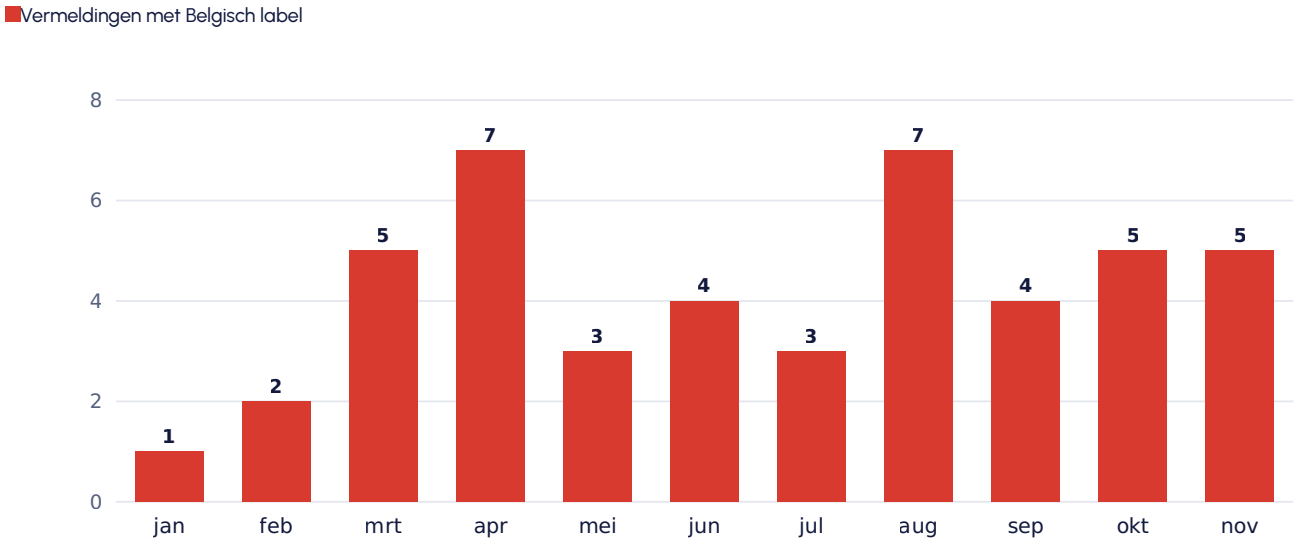
Ongelijke perioden; geen nationale risicorangschikking. Bron: aanvaarde Ransompedia-vermeldingen met landenlabel, 1 januari-22 november 2026; november onvolledig. Vermeldingsdatums zijn geen incidentdatums [S1].

De vergelijkingslanden zijn uitsluitend als voorbeelden gekozen om context te bieden; hun selectie houdt geen rangschikking of politieke beoordeling in.

Land	Periode 2026	Volledig 2025	Vergelijkingsgrens
België	46	42	Vermeldingen, geen bevestigde inbraken
Nederland	77	44	Naburige logistieke en Nederlandstalige markt
Frankrijk	295	182	Naburige Franstalige en zakelijke markt
Duitsland	457	311	Naburige industriële en handelseconomie
Luxemburg	2	8	Naburige financiële markt met een kleine vermeldingspopulatie

Alle cijfers voor 2026 betreffen dezelfde onderzoeksperiode. Ze zijn niet gecorrigeerd voor bedrijvenpopulatie, economische omvang, meldingsbereidheid of bronzichtbaarheid. De tabel kan niet aantonen dat een Belgische organisatie veiliger of meer blootgesteld is dan een vergelijkbare organisatie. [S1]

Belgische vermeldingen verschijnen door het jaar heen, niet alleen in één maand

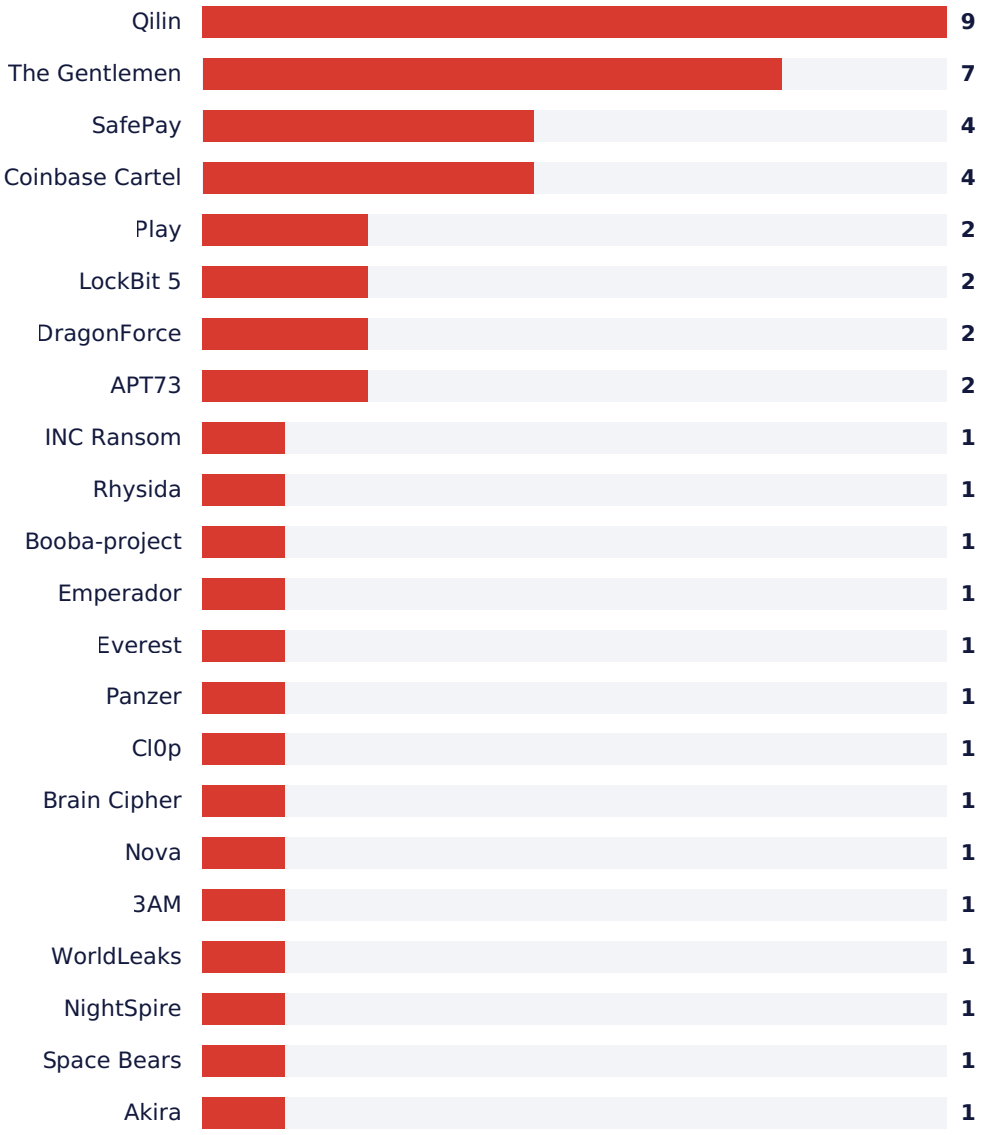


Bron: aanvaarde Ransompedia-vermeldingen met landenlabel, 1 januari–22 november 2026; november onvolledig. Vermeldingsdatums zijn geen incidentdatums [S1].

De maandelijkse aantallen zijn 1, 2, 5, 7, 3, 4, 3, 7, 4, 5 en 5 van januari tot de novemberafsluiting. De som is 46. Een gedeeltelijke novembermaand mag niet met een volledige maand worden vergeleken als trendvoorspelling. [S1]

Vier groepsnamen zijn goed voor 24 van de 46 Belgische vermeldingen





Bron: aanvaarde Ransompedia-vermeldingen met landenlabel, 1 januari–22 november 2026; november onvolledig. Vermeldingsdatums zijn geen incidentdatums [S1].

Qilin telt 9 vermeldingen, The Gentlemen 7, SafePay 4 en Coinbase Cartel 4. Samen vormen zij 24 van 46 vermeldingen. De resterende 22 zijn verdeeld over 18 andere namen. [S1]

Qilin

Label van afpersingsvermeldingen | Geen staat toegeschreven

IN BELGIË, 2026

2026

9 · Belgisch gelabelde vermeldingen binnen de rapportperiode; geen bevestigde inbraken

GECLAIMDE DOELWITTEN

Sector- en landenlabels vereisen controle; geen slachtofferlijst gepubliceerd

IN OPENBARE BERICHTGEVING

[S1] Bewaard vermeldingenoverzicht, geen onafhankelijke actorattributie

ONZE BEOORDELING

Bereid herstel voor en controleer claims zonder op het actorlabel te vertrouwen

ZEKERHEID

Hoge zekerheid over het bewaarde aantal rijen; inbraakuitkomsten niet geverifieerd

The Gentlemen

Label van afpersingsvermeldingen | Geen staat toegeschreven

IN BELGIË, 2026

2026

7 · Belgisch gelabelde vermeldingen binnen de rapportperiode; geen bevestigde inbraken

GECLAIMDE DOELWITTEN

Sector- en landenlabels vereisen controle; geen slachtofferlijst gepubliceerd

IN OPENBARE BERICHTGEVING

[S1] Bewaard vermeldingenoverzicht, geen onafhankelijke actorattributie

ONZE BEOORDELING

Bereid herstel voor en controleer claims zonder op het actorlabel te vertrouwen

ZEKERHEID

Hoge zekerheid over het bewaarde aantal rijen; inbraakuitkomsten niet geverifieerd

Het landlabel blijft een kenmerk van de vermelding, geen aanvaard bewijs van binnenlandse juridische bevoegdheid. De populatie bevat herhaalde merkomschrijvingen en een buitenlandse bedrijfseenheid. Mogelijke organisatieoverlap blijft als afzonderlijke vermeldingsrijen staan; er wordt geen uniek slachtoffertotaal gegeven. [S1]

7.3 Advertentiepersona's

Persona	Kaarten	Waargenomen stelling	Grens
kazutlg	B01	Telecomgerichte klantgegevensadvertentie	De adverteerder dateert het incident zelf op 2025
xmlrpc	B02	Burgergegevensclaim met erkende brononzekerheid	Overheidsherkomst onbevestigd
yneov18	B03	Claims over opleidingsnetwerkgegevens en toegang	Actuele toegang en uniek personenaantal onbevestigd
DataJava	B04	Geclaimd beheer van een identiteitsdienst	Voorgestelde tabelbeschrijvingen bevestigen geen toegang
0xcasper	B05	Marketing voor een banktemplate-phishingpaneel	Werkende mogelijkheden en inzet onbevestigd
updap	B06	Claim over ondersteuningstickets van een leverancier	Klantimpact en volledig bezit onbevestigd

Dit zijn bewaarde accountaliassen. Het zijn geen geïdentificeerde personen en hun namen authenticeren geen advertentie. Een alias met één juist bericht zou niet elke latere claim bevestigen. [S3]

7.4 Spionage en onopgeloste inbraakberichtgeving

Het CCB bespreekt door staten gesteunde spionage als deel van de dreigingsomgeving. Een gemeld incident bij een gevoelige overheidsdienst is niet onafhankelijk bevestigd in het bewaarde officiële dossier. Daarom gebruikt het rapport een brede rol en schrijft het verslag toe aan berichtgeving. [S8][S9][S14]

Het CCB-rapport over het derde kwartaal beschrijft afzonderlijke activiteit die het aan Rusland, China en Iran koppelt. Het meldt ook een Teams-spearphishingcampagne die in België is waargenomen. Dit zijn beoordelingen van de autoriteit. [S9]

De publieke leveranciers- en NVD-records voor twee mobielbeheerkwetsbaarheden tonen een productrisico aan. Ze bepalen niet welke kwetsbaarheid, actor of gegevensuitkomst bij dat gemelde Belgische incident hoorde. [S41] [S42][S43]

Record	Getroffen scope	Opgeloste leveranciersversies	Grens
CVE-2026-1281	NVD noemt versies tot en met 12.5.0.0 en specifieke latere kwetsbare builds, waaronder 12.5.1.0, 12.6.0.0, 12.6.1.0 en 12.7.0.0	Zie het versieregister hieronder	Controleer producttak en actuele leveranciersrichtsnoeren
CVE-2026-1340	NVD noemt getroffen EPMM-versies tot en met 12.7.0.0	Zie het versieregister hieronder	Geen afleiding over een individuele Belgische installatie

Herstelde Ivanti EPMM-versies volgens de leverancier [S41]:

`12.6.1.1, 12.7.0.1, 12.8.0.1`

Ivanti beschrijft beide in zijn advies als risico's op code-injectie zonder authenticatie. De productuitzonderingen omvatten Sentry en zijn cloudproduct voor mobielbeheer. Een herstelbeslissing moet passen bij het geïnstalleerde product en de producttak. Beide NVD-records zijn voor dit rapport gecontroleerd. [S41][S42][S43]

Voor het onbevestigde overheidsverslag wordt geen incidentspecifieke ATT&CK-matrix gegeven. Een algemene techniekmapping zou productmogelijkheden kunnen veranderen in een waargenomen Belgisch aanvalsverloop.

KERNPUNTEN

01

Groepsnamen en persona's zijn geen geverifieerde beheerdersidentiteiten.

02

Regionale vermeldingstotalen meten geen vergelijkende aanvalskans.

03

Productkwetsbaarheden schrijven een gemeld Belgisch incident niet zelfstandig toe.

HOOFDSTUK 08

De fraude-economie

08

DIT HOOFDSTUK BEANTWOORDT

Hoe kunnen aangeboden gegevens, documenten en toegang fraude ondersteunen en waar kunnen verdedigers ingrijpen?

2

politiecampagnegevallen met concrete responslessen

8.1 Van juiste gegevens naar een valse instructie 62

8.2 Politiecampagnes als casuskaarten 62

8.3 Identiteitsbeelden, sessies en onboarding 64

8.4 Betaalkaartmateriaal in berichten: een beperkte kijk 64

8.5 Prijzen zijn vraagprijzen 64

8.6 Publieke campagnewaarschuwingen door het jaar heen 65

HOOFDSTUK 08

De fraude-economie

IN HET KORT

Bewaarde advertenties bieden identificatoren, identiteitsbeelden, sessies en bankgerichte hulpmiddelen aan. Politie en Safeonweb beschrijven fraudepaden met imitatie, aangepaste facturen en schadelijke applicaties. Die publieke campagnes worden niet aan de forumpersona's toegeschreven. Betaalkaart-waarnemingen blijven een zeer beperkte kijk. Bescherm herstel, betalingswijzigingen en klantcommunicatie via onafhankelijke controle en een duidelijke route voor dringende fraudemeldingen.

8.1 Van juiste gegevens naar een valse instructie

Echte persoonsgegevens kunnen een frauduleus bericht geloofwaardig maken. Ze authenticeren de afzender niet. De opleidings-, lidmaatschaps- en leveranciersgevallen verklaren waarom klantondersteuning en financiën bescherming nodig hebben, ook wanneer wachtwoorden volgens meldingen niet waren getroffen. [S13][S18][S22]

De meiwaarschuwing van de politie beschrijft criminelen die eerder gelekte mailboxgegevens gebruiken, binnenkomende berichten volgen en facturen aanpassen. Ze schrijft toenemende automatisering toe aan het waargenomen fraudepatroon. Dit rapport meet het AI-aandeel daarin niet onafhankelijk. [S31]

De doorslaggevende controle is onafhankelijke verificatie van de instructie. Gebruik een al bekende contactroute voordat u een gewijzigde begunstigde of noodoverschrijving aanvaardt. Een bekende mailbox, juist factuurbedrag of correcte klantnaam volstaat op zichzelf niet.

8.2 Politiecampagnes als casuskaarten

P

CASUS P

Een onderzoek richt zich op een phishingpaneelleverancier

Fraudediensten

Toegeschreven openbaar verslag

OFFICIEEL VERSLAG	De Federale Politie kondigde op 22 april een onderzoek aan naar een verdachte die phishingpanelen zou maken en verkopen. De verklaring beschrijft gebruik bij fraude in België en andere Europese landen. [S30]
CHRONOLOGIE	De politie beschreef een huiszoeking in januari en een overdracht van de verdachte aan België in april. Die procedurele datums verschillen van de aankondigingsdatum.

VASTGESTELD	De verklaring ondersteunt een crimineel dienstenpad: een leverancier biedt hulpmiddelen aan die andere criminelen kunnen gebruiken. Ze verbindt de verdachte niet met B05 of een persona uit de bewaarde forums.
GRENZEN	Een arrestatie en politiebeschuldigingen zijn geen veroordeling. Leid uit dit individuele onderzoek geen nationaal slachtoffer- of verliestotaal af.
RESPONS	Neem phishingbestendige authenticatie en betalingscontrole op in dezelfde fraudeoefening. Leg vast hoe een gebruiker een onderschepte authenticatie-interactie kan melden.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

CASUS Q

Q ■ Valse bankmedewerkers combineren berichten, oproepen en externe toegang

Toegeschreven openbaar verslag

Bankimitatie

OFFICIEEL VERSLAG	Een verklaring van de Federale Politie van 2 juli beschrijft een onderzoek met tientallen Belgische slachtoffers en vermeende opbrengsten boven EUR 500.000. Het onderzoek liep nog. [S32]
CHRONOLOGIE	Volgens de politie begon het onderzoek in maart en werd een hoofdverdachte op 29 juni gearresteerd. De julipublicatie is niet het begin van elk gemeld misdrijf.
PAD	Het officiële verslag beschrijft berichten die overheidsdiensten imiteren, een daaropvolgende oproep van een valse bankmedewerker en overreding om afstandsbedieningssoftware te installeren.
GRENZEN	De opbrengst is een vermeend bedrag, geen nationale fraudeverliesschatting. Een gezamenlijke beheerder met de ondergrondse advertenties uit dit rapport is niet vastgesteld.
RESPONS	Klantenteams moeten gebruikers adviseren onverwachte oproepen te beëindigen en zelf de bank te contacteren. Fraudeteams hebben een dringende escalatieroute nodig voor externe toegang en nieuwe begunstigden.

Conclusie

Hanteer de vermelde reikwijdte en behoud de openstaande vragen.

8.3 Identiteitsbeelden, sessies en onboarding

De vraag in B08 betreft meer dan 500 Belgische identiteitsbeelden. Ze toont alleen vraag aan. Ze bewijst geen leveranciersreactie, geslaagde identiteitscontrole of diefstal uit een overheidsregister. [S3]

De vraag in B09 betreft actieve sessies voor logistieke diensten. Sessies kunnen een ander responsprobleem vormen dan een wachtwoord alleen. Controleer actieve sessies en herstelroutes wanneer de organisatie een relevante bevinding heeft bevestigd. [S3]

Maak documentbezit niet het enige identiteitsbewijs. Onboarding- en herstelteams moeten testen wanneer een echt documentbeeld, contactadres of oude accountidentificator misbruikt kan worden. Leg een escalatieroute vast voor onzekere gevallen.

8.4 Betaalkaartmateriaal in berichten: een beperkte kijk

REIKWIJDTE VAN DE KAARTCIJFERS

Deze beperkte waarnemingen ramen geen totale kaartdiefstal, actieve kaarten, inbraak in banksystemen of fraudeverlies.

Het bewaarde materiaal koppelt 3 afzonderlijke betaalkaartnummers aan België, verspreid over 9 berichten en 17 verschijningen. Voor deze drie kaarten is geen toeschrijving aan een genoemde Belgische uitgever vastgesteld. Herhaalde verschijningen zijn geen extra kaarten. [S3]

Deze waarnemingen tonen niet aan of een kaart nog actief was of een betalingspoging slaagde. Uitgevers moeten hun eigen fraudebewijs gebruiken voordat ze blokkering of vervanging adviseren. De kaartpopulatie mag niet bij authenticatie- of klantrecordtellingen worden opgeteld.

8.5 Prijzen zijn vraagprijzen

Aangeboden product	Weergegeven prijs	Bewijsgrens
Bankrekeningidentificatoren	USD 1,75 per 1.000; USD 70,19 voor het aangeboden pakket	Hoeveelheid, herkomst en betalingsbevoegdheid onbevestigd
Geclaimd beheer van een identiteitsdienst	USD 4.550	Werkende toegang en geadverteerde recordpopulatie onbevestigd
Logistiekgerelateerde sessies	USD 250–2.500	Een koopbereik, geen afgeronde transactie

De prijzen beschrijven de bewaarde advertenties. Ze tonen geen transactieprijzen, inkomsten, winstgevende activiteit of omvang van een Belgische ondergrondse markt aan. Verschillen in geclaimde scope verhinderen een eenvoudige prijsvergelijking. [S3]

8.6 Publieke campagnewaarschuwingen door het jaar heen

Periode	Officiële waarschuwing	Ondersteunde beslissing
Januari	Imitatie rond prominente uitnodigingen en sponsoring [S65]	Controleer verzoeken via een bestaande zakelijke contactpersoon
Februari	Imitatie van overheidsaanmeldingen [S62]	Open de officiële dienst rechtstreeks
Maart	Valse compensatie- en herstelberichten [S63]	Stuur geen identiteitsdocumenten naar een ongecontroleerd herstelcontact
Juni	Hotelberichten met juiste reserverings-gegevens [S61]	Controleer betalingsverzoeken onafhankelijk bij de accommodatie
september	Directie-imitatie via samenwerkingssoftware [S60]	Behandel een bekende organisatie-identiteit als een te controleren claim
september	Schadelijke apps en mobiele kaartrelay-fraude [S59]	Weiger ongevraagde appinstallatie en neem afzonderlijk contact op met de bank
Oktober	Koppelen van berichtenaccounts via valse stemverzoeken [S64]	Controleer onverwachte verzoeken, ook van een bekende contactpersoon
november	Valse winterbrandstofwinkels en vooruitbetalingsaanbiedingen [S45]	Controleer verkopersidentiteit en betalingsvoorwaarden vóór bestelling

Dit zijn preventie- en campagnemeldingen. Het zijn geen acht gescheiden slachtofferpopulaties. De hotelwaarschuwing toont bijvoorbeeld niet aan dat het eerdere boekingsplatformincident de gebruikte informatie leverde. [S61]

KERNPUNTEN

01

Juiste persoonsgegevens authenticeren geen betalingsverzoek.

02

Een hulpmiddeladvertentie staat los van een waargenomen fraudecampagne.

03

Kaartverschijningen en vraagprijzen meten geen verliezen of afgeronde handel.

HOOFDSTUK 09

Verdieping bankwezen en financiën

09

DIT HOOFDSTUK BEANTWOORDT

Welke identiteits- en klantbeschermingssignalen moet de bankportefeuille eerst controleren?

11 van 25

geselecteerde bank- en financiële domeinen hadden een actueel authenticatieaanbod

9.1 Wat het bewijs wel en niet zegt 67

9.2 Scheid account-, sessie- en betalingsbeslissingen 67

9.3 Leveranciers en regelgevingscoördinatie 68

HOOFDSTUK 09

Verdieping bankwezen en financiën

IN HET KORT

11 van 25 geselecteerde bank- en financiële domeinen hadden een actueel authenticatieaanbod. De sector bevat minstens 13.221 apparaatassociaties, waaronder 156 met werknemersclassificatie, en 190.956 authenticatierecords. De drie kaarten uit berichten zijn niet aan een genoemde uitgever toegeschreven. Deze waarnemingen meten verschillende populaties. Coördineer identiteit, fraude en klantondersteuning rond gecontroleerde accounts, sessies en betalingsactiviteit.

9.1 Wat het bewijs wel en niet zegt

Populatie	Beschikbaar resultaat	Interpretatie
Geselecteerde bank- en financiële domeinen	25	Inclusief financiële diensten; geen telling van vergunninghoudende kaartuitgevers
Apparaatassociaties	Minstens 13.221; 156 met werknemersclassificatie	Classificatie toont geen eigendom of bedrijfsinbraak aan
Authenticatierecords	190.956	Overlappende historische bronnen, geen unieke actieve accounts
Actuele authenticatieaanbiedingen	11 van 25 domeinen	Controleer actualiteit, accountgeldigheid en eerdere maatregelen
Subset van uitgeversdomeinen	7 gekoppelde domeinen; 6 met actueel aanbod	86 werknemer- en 4.306 overige apparaatassociaties; subset van de sector
Banktemplateadvertenties	Waargenomen in B05	Een claim over een imitatieproduct, geen bankinbraak
Kaartmateriaal	3 kaarten; 9 berichten; 17 verschijningen	Geen toeschrijving aan een genoemde uitgever of schatting van verliezen of inbraken

Geen bewaarde kaart is aan een genoemde uitgever toegeschreven. Dit toont niet aan dat gestolen kaarten ontbreken. Niet-werknemerassociaties tonen geen klanteigendom aan. [S2][S3]

9.2 Scheid account-, sessie- en betalingsbeslissingen

Een blootgestelde identificator kan een oproep persoonlijker maken. Een geldige sessie kan accountactiviteit ondersteunen. Een betalingsinstructie kan alleen binnen het relevante autorisatieproces geld verplaatsen. Onderzoek die stellingen afzonderlijk in plaats van één als bewijs van alle drie te behandelen.

Stuur meldingen over afstandsbedieningssoftware of onverwachte authenticatieverzoeken snel door van fraudemedewerkers naar accountbescherming. Controleer nieuwe begunstigden en herstelwijzigingen via een onafhankelijk bekend kanaal. Bewaar de beslissing en ondersteunende activiteitsregistraties. [S32]

De advertentie in B05 claimt bankspecifieke templates en interactieve authenticatiefuncties. Ze bewijst niet dat die functies werken of dat controles van een bank zijn omzeild. De praktische waarde is het testen van de frauderespons op een imitatiescenario. [S3]

9.3 Leveranciers en regelgevingscoördinatie

DORA geldt sinds 17 januari 2025 voor een brede populatie financiële entiteiten. De NBB beschrijft toezicht op ICT- en cyberrisico, waaronder incidentinformatie, tests en afhankelijkheden van derden. [S38]

Identificeer voor elke essentiële bankdienst de identiteitsleverancier, telecommunicatieroute, kernleverancier en herstelafhankelijkheid. Een algemene herstelmelding van een leverancier toont niet aan dat uw eigen dienst veilig, volledig en gereconcilieerd is.

Onderhoud één incidentchronologie en afzonderlijke beslissingen voor operationele melding, privacy, klantcommunicatie en frauderespons. De aanwezigheid van één meldingsregime sluit de beoordeling onder een ander niet automatisch af. [S36][S37][S38]

KERNPUNTEN

01

Handel actuele aanbiedingen af via accountcontrole.

02

Onderzoek identificatoren, sessies en betalingsautorisatie afzonderlijk.

03

Houd uitgeverssubsets, sectorassociaties en kaarten uit berichten apart.

HOOFDSTUK 10

Regelgeving en nationale respons

10

DIT HOOFDSTUK BEANTWOORDT

Welke meldingsplichten en toezichtsmijlpalen moeten Belgische leiders al operationeel hebben?

18 april 2027

de conformiteitsmijlpaal uit de CCB-mededeling van augustus

10.1 Regels die nu gelden 70
10.2 NIS2-conformiteit: bewijs en herstelmaatregelen 71
10.3 Sancties en uitzonderingen vragen de juiste reikwijdte 71
10.4 Persoonsgegevens melden is een afzonderlijke beslissing 72
10.5 Nationale crisiscoördinatie 72

HOOFDSTUK 10

Regelgeving en nationale respons

IN HET KORT

Belgische NIS2-verplichtingen zijn al van kracht. Het bewijscheckpoint van april 2026 en de toezichtsmededeling van augustus vragen praktische voorbereiding, geen wachten op een nieuwe wet. Persoonsgegevensincidenten vereisen daarnaast een afzonderlijke AVG-beoordeling. Financiële entiteiten moeten het toepasselijke DORA-regime bepalen. Productfabrikanten hebben sinds september CRA-meldingsplichten. Wijs voor elk regime een verantwoordelijke aan en oefen de eerste melding voordat een incident plaatsvindt.

10.1 Regels die nu gelden

De volgende tabel onderscheidt aanleiding, termijnen en toezicht. Ze is een planningshulpmiddel, geen juridisch advies. De bevoegde autoriteit en reikwijdte hangen af van de entiteit, activiteit en het incident. [S33][S35][S36][S37][S38][S39]

Regime	Geldt voor	Termijn	Bevoegde route
Belgische NIS2-wet	Essentiële en belangrijke entiteiten binnen het toepassingsgebied; significante incidenten bij gedekte diensten	Zonder onredelijke vertraging na kennisname van een significant incident: vroegtijdige waarschuwing uiterlijk binnen 24 uur; incidentmelding uiterlijk binnen 72 uur. Eindverslag binnen één maand na de melding, tenzij het incident voortduurt (zie hieronder)	Nationaal CSIRT bij het CCB; voor vertrouwensdienstverleners geldt een uitzondering van 24 uur voor incidentmelding
AVG	Verwerkingsverantwoordelijken bij een persoonsgegevensinbreuk, tenzij risico voor rechten en vrijheden van personen onwaarschijnlijk is	Zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur na kennisname	Bevoegde gegevensbeschermingsautoriteit; APD/GBA is niet voor elke sector bevoegd
DORA	Financiële entiteiten binnen het toepassingsgebied van de verordening	Van toepassing sinds 17 januari 2025; gebruik de relevante incidentclassificatie en meldingsprocedure	Toepasselijke financiële toezichthouder en meldingskanaal
CRA-melding	Fabrikanten van producten met digitale elementen en meldingsplichtige kwetsbaarheden of ernstige incidenten	Verplichtingen begonnen op 11 september 2026. Na kennisname van een actief misbruikte kwetsbaarheid of ernstig incident: vroegtijdige waarschuwing binnen 24 uur en melding binnen 72 uur	Europees Single Reporting Platform, relevant CSIRT en ENISA

Duurt het incident na één maand nog voort, dien dan op die mijlpaal een voortgangsverslag in. Dien het eindverslag in binnen één maand na de definitieve afhandeling van het incident. [S36]

De CRA-termijnen voor eindverslagen verschillen. Voor een actief misbruikte kwetsbaarheid noemt het CCB 14 dagen nadat een corrigerende of beperkende maatregel beschikbaar wordt. Voor een ernstig incident noemt het één maand na de melding. [S39]

Pas een termijn uit één regime niet op elk incident toe. Melding aan een leverancier, verzekeraar of politie is niet automatisch melding aan de bevoegde toezichthouder. Bewaar een kennisnametijdstip en een afzonderlijk beslisdocument voor elke toepasselijke verplichting.

10.2 NIS2-conformiteit: bewijs en herstelmaatregelen

De wet van 26 april 2024 trad in werking op 18 oktober 2024. De aprilmededeling van het CCB beschreef het bewijs dat essentiële entiteiten tegen 18 april 2026 moesten aanleveren. De inhoud hing af van de gekozen conformiteitsroute. [S33][S36]

Voor CyberFundamentals beschreef het CCB verificatie of een actief traject daarnaartoe, inclusief een ondertekende beoordelingsovereenkomst. Voor ISO/IEC 27001 vroeg het documentatie over reikwijdte, toepasselijkheid en interne audit. Rechtstreekse inspectie vereiste zelfbeoordeling en ondersteunend bewijs. [S33]

De augustusmededeling betreft de mijlpaal van 18 april 2027. Essentiële entiteiten die geen maatregelen gelijkwaardig aan het niveau Essential kunnen aantonen, moeten bewijs gelijkwaardig aan Important en een herstelplan richting Essential tegen 18 april 2028 indienen. [S34]

Een herstelplan is niet vereist als de entiteit tegen 18 april 2027 maatregelen gelijkwaardig aan Essential aantoont of op basis van haar risicoanalyse een lager gelijkwaardig zekerheidsniveau rechtvaardigt. [S34]

Het CCB zegt uitdrukkelijk dat deze aanpak de wettelijke verplichtingen of termijnen niet verandert. Behandel de mededeling als toezichtsvereiste om een geloofwaardig traject te documenteren, geen algemene verlenging. Registreer route, beoordelingsscope, bewijsverantwoordelijke en onopgeloste hiaten. [S34]

10.3 Sancties en uitzonderingen vragen de juiste reikwijdte

Artikel 59 onderscheidt meerdere overtredingen van de Belgische NIS2-wet. Voor risicobeheer en incidentmelding gelden verschillende sanctiebanden voor essentiële en belangrijke entiteiten. Andere tekortkomingen hebben afzonderlijke banden. [S36]

Bepaling	Wettelijke band	Reikwijdte
Belangrijke entiteiten	EUR 500 tot EUR 7.000.000 of 1,4% van de wereldwijde jaaromzet van de onderneming in het vorige boekjaar, waarbij het hoogste bedrag geldt	Relevante verplichtingen voor risicobeheer of incidentmelding
Essentiële entiteiten	EUR 500 tot EUR 10.000.000 of 2% van de wereldwijde jaaromzet van de onderneming in het vorige boekjaar, waarbij het hoogste bedrag geldt	Relevante verplichtingen voor risicobeheer of incidentmelding
Herhaling	De administratieve boete verdubbelt voor dezelfde feiten binnen drie jaar	De wettelijke voorwaarden voor herhaling moeten vervuld zijn
Sector overheid	Artikel 62 sluit deze entiteiten uit van de administratieve boetes en maatregelen onder artikelen 59–60	Beoordeel toepasselijke cyberbeveiligings- en meldingsplichten afzonderlijk [S36]

Dit zijn wettelijke banden, geen boetevoorspelling. De wet bevat ook sectorspecifieke uitzonderingen en samenhang met gelijkwaardige EU-regels. De financiële bepalingen moeten naast DORA worden gelezen; een algemene NIS2-controlelijst volstaat niet. [S36][S38]

10.4 Persoonsgegevens melden is een afzonderlijke beslissing

De APD/GBA verwijst verwerkingsverantwoordelijken naar haar portaal. Volgens haar richtsnoeren moet de melding in een landstaal gebeuren; technische bijlagen mogen ook in het Engels. Voor bepaalde domeinen, waaronder politie-informatie, noemt ze andere bevoegde federale autoriteiten. [S37]

Bereid het portaalaccount en de bevoegdheidsbeoordeling voor op een incident. Leg vast wat bekend is, wat onzeker blijft en wanneer de volgende update komt. Een ontbrekend definitief slachtofferaantal vraagt uitleg over onzekerheid, geen uitstel van elke meldingsbeslissing.

Het incidentteam moet privacymedewerkers een beknopte impactverklaring geven. Vermeld gegevenscategorieën, getroffen verwerkingen, mogelijke ontvangers, beschermingsmaatregelen en het bewijs voor elke conclusie. Houd criminele recordclaims apart van de eigen beoordeling van de verwerkingsverantwoordelijke.

10.5 Nationale crisiscoördinatie

Het CCB beschrijft een herzien nationaal cybercrisiskader. Volgens zijn publieke richtsnoeren geldt het bijgewerkte plan sinds 7 mei 2026. Het coördineert bevoegde autoriteiten zonder hun mandaten te vervangen. De operationele details zijn niet openbaar. [S40]

Een organisatie moet nog steeds haar eigen beslisketen kennen. Wijs bevoegdheden toe om een dienst te isoleren, externe hulp te vragen, handmatige werking te activeren en een statusbericht te publiceren. Test dit met een onbeschikbare leverancier en onzeker gegevensverlies.

KERNPUNTEN

01

Houd NIS2-, privacy-, financiële en productmeldingsbeslissingen afzonderlijk.

02

De herstelbenadering van het CCB schrapt geen wettelijke termijnen.

03

Bereid meldingstoegang, bewijsverantwoordelijken en crisisbeslissingen voor op de eerste waarschuwing.

HOOFDSTUK 11

Vooruitblik

11

DIT HOOFDSTUK BEANTWOORDT

Welke planningsaannames worden ondersteund en welke signalen zouden ze veranderen?

3

voorwaardelijke scenario's voor continuïteit, identiteit en leveranciersrespons

11.1 Belangrijkste beoordelingen 75

11.2 Wat de beoordeling zou veranderen 75

11.3 Voorwaardelijke scenario's 76

HOOFDSTUK 11

Vooruitblik

IN HET KORT

Identiteitsbescherming, leverancierszekerheid en herstelbare diensten hebben de sterkste basis voor planning. Officiële berichtgeving en de gevallen ondersteunen deze prioriteiten, zonder de kans op een toekomstig incident vast te stellen. Afpersingsvermeldingen blijven over veel groepsnamen verspreid. Recente operationele verstoring maakt beheersing van toegang op afstand dringender. Gebruik de scenario's om beslissingen te testen en herzie ze wanneer uw eigen bewijs verandert.

11.1 Belangrijkste beoordelingen

Beoordeling	Vertrouwen	Basis	Grens
Accountbescherming verdient directe aandacht	Hoog voor de prioriteit	CCB-identiteitsbeoordeling en politieberichten over fraude [S5][S31][S32]	Meet geen blootstelling bij een individuele werkgever
Leveranciersproblemen kunnen lokale diensten verstoren	Hoog voor het pad	Onderwijs-, zorg- en handtekeninggevallen [S8][S13] [S22]	Een gedeelde afhankelijkheid betekent niet dat elke klant is getroffen
Afpersingsvoorbereiding moet meerdere actornamen omvatten	Hoog voor de zichtbare vermeldingsmix	46 vermeldingen verdeeld over 22 namen [S1]	Vermeldingen tonen geen afzonderlijke inbraken of verliezen aan
Operationele toegang op afstand verdient controle	Hoog voor de controleprioriteit	Koelverstoring en officieel advies [S25][S27]	Bepaalt niet de oorzaak van elke gemelde storing

Vertrouwen geldt voor deze stellingen. Het bevestigt niet de eerlijkheid van een actor, de volledige catalogus van een verkoper of de authenticiteit van elk bestandsrecord.

11.2 Wat de beoordeling zou veranderen

Een geverifieerd actueel bevoorrecht account zou de identiteitsrespons van een organisatie dringender maken. Een oud inactief authenticatiegegeven met gedocumenteerde maatregelen zou de scope beperken. Accountgeldigheid en recente activiteit zijn relevant, niet het advertentievolume.

Een gecontroleerd klantspecifiek impactrapport van een leverancier kan de getroffen gegevenspopulatie verkleinen of vergroten. Een algemene herstelverklaring kan beschikbaarheid aantonen terwijl vertrouwelijkheid onopgelost blijft. Documenteer beide toestanden afzonderlijk.

Een officieel onderzoek of reproduceerbaar technisch bewijs kan de toeschrijving van de koelcampagne veranderen. Herhaalde beschuldigingen, schermafbeeldingen en politieke timing volstaan op zichzelf niet. Pas de beoordeling pas aan wanneer de stelling zelf sterker wordt ondersteund.

11.3 Voorwaardelijke scenario's

Deze scenario's zijn planningsaannames. Het zijn geen voorspellingen over aanvalsfrequentie, financieel verlies of waarschijnlijke daders.

Scenario	Aanleiding	Eerste beslissing	Afrondingsbewijs
Een actuele identiteit wordt misbruikt	Een actief account en verdachte sessie zijn bevestigd	Identiteitsverantwoordelijke trekt sessies in en bewaart toegangsregistraties	Accounteigenaar bevestigt herstel; toegangs- en herstelroutes gecontroleerd
Een gedeelde leverancier isoleert zijn platform	Een dienstmelding past bij een gedocumenteerde afhankelijkheid	Diensteigenaar activeert het geteste alternatief en vraagt een afgebakende impactverklaring	Handmatige dienst werkt; getroffen records en meldingsbeslissingen gedocumenteerd
Apparatuur op afstand gedraagt zich onverwacht	Operations bevestigt een instellingswijziging of controleverlies	Operationele verantwoordelijke gebruikt het veilige lokale proces en beperkt toegang op afstand	Veilige toestand bevestigd; externe accounts en wijzigingshistoriek gecontroleerd

KERNPUNTEN

01

Behandel scenario's als beslissingstests, geen voorspellingen.

02

Herzie identiteitsurgentie op basis van accountgeldigheid en actuele activiteit.

03

Verander toeschrijving pas wanneer sterker bewijs die stelling ondersteunt.

HOOFDSTUK 12

Actieplan

12

DIT HOOFDSTUK BEANTWOORDT

Wie moet eerst handelen en welk bewijs toont dat het werk klaar is?

30/60/90

dagen om identiteiten te controleren, afhankelijkheden te oefenen en herstel te verifiëren

12.1 De eerste 30/60/90 dagen 78

12.2 Verantwoordelijkheden per rol 80

12.3 Hoe Brandefense kan helpen 80

HOOFDSTUK 12

Actieplan

IN HET KORT

Begin met feiten die uw organisatie kan controleren: actieve accounts, blootgestelde diensten, leveranciersafhankelijkheden en herstelvermogen. Geef elke actie een verantwoordelijke en een afsluitingsdocument. Betrek privacy, klantondersteuning, financiën en operations bij de oefening. Het doel is een herstelbare dienst en een team dat kan uitleggen wat gebeurde. Beoordeel de voortgang met het onderstaande bewijs tijdens elke leidinggevende vergadering.

12.1 De eerste 30/60/90 dagen

1Onmiddellijk

Verwijder rechtstreekse publieke internettoegang tot beheerinterfaces van koelinstallaties; coördineer veilige continuïteit en beschermd onderhoud op afstand

VERANTWOORDELIJKE

Operationele en beveiligingsverantwoordelijken met onderhoudsleveranciers

AFRONDINGSBEWIJS

Bereikbaarheidstests bevestigen geen rechtstreekse publieke toegang; veilige instellingen en beschermd onderhoud gecontroleerd [S25]

230 dagen

Als een actueel authenticatiegegeven of een sessie aan uw dienst is gekoppeld, controleer het account, trek verdachte sessies in en controleer herstelroutes

VERANTWOORDELIJKE

Identiteits- en SOC-verantwoordelijken

AFRONDINGSBEWIJS

Accountafhandeling, activiteitsbeoordeling en hersteldocument

Identificeer extern bereikbare beheertoegang en bedrijfskritieke applicaties; prioriteer dringende door leveranciers bevestigde oplossingen

VERANTWOORDELIJKE

Infrastructuurverantwoordelijke

AFRONDINGSBEWIJS

Inventaris met eigenaars, patchbewijs en gedocumenteerde uitzonderingen

Koppel kritieke leveranciers aan gegevens, beheertoegang en dienstprocessen

VERANTWOORDELIJKE

Inkoop en diensteigenaars

AFRONDINGSBEWIJS

Afhankelijkheidsregister met incidentcontact en alternatief proces

Bereid één incidentbeslisdocument voor met meldingsaanleidingen en kennisnametijdstippen

VERANTWOORDELIJKE

Juridische dienst, privacy en incidentleider

AFRONDINGSBEWIJS

Geteste toegang tot verplichte meldingskanalen en benoemde vervangers

360 dagen

Oefen een leveranciersuitval met onzekere gevolgen voor klantgegevens

VERANTWOORDELIJKE

Continuïteits- en privacyverantwoordelijken

AFRONDINGSBEWIJS

Werkend alternatief, conceptgebruikersmelding en afzonderlijke regelgevingsbeslissingen

Test controle van betalingswijzigingen via een al bekend contactkanaal

VERANTWOORDELIJKE

Financiële en fraudeverantwoordelijken

AFRONDINGSBEWIJS

Steekproef van terugbelregistraties en afhandeling van afwijkende begunstigdengegevens

Controleer accounts en toegangspaden voor apparatuur op afstand met onderhoudsleveranciers

VERANTWOORDELIJKE

Operationele verantwoordelijke

AFRONDINGSBEWIJS

Goedgekeurde toegangslijst, veilig lokaal proces en bewijs van wijzigingscontrole

490 dagen

Herstel één essentiële dienst uit beschermde back-ups onder realistische afhankelijkheidsbeperkingen

VERANTWOORDELIJKE

Herstelverantwoordelijke

AFRONDINGSBEWIJS

Gemeten herstelresultaat, gegevensvalidatie en afgesloten oefenpunten

Test detectie van verdachte sessies, nieuwe authenticatiemethoden en ongeoorloofd doorsturen van mailboxberichten

VERANTWOORDELIJKE

SOC- en identiteitsverantwoordelijken

AFRONDINGSBEWIJS

Beoordeelde waarschuwingen, benoemde responsverantwoordelijke en bewaard oefenbewijs

Presenteer conformiteitsroute, leveranciershiaten en oefenresultaten aan het management

VERANTWOORDELIJKE	AFRONDINGSBEWIJS
CISO	Ondertekende beslissingen, gefinancierde maatregelen en datums voor open punten

De termijnen zijn organisatorische planningsdoelen. Ze vervangen geen wettelijke meldingstermijnen, dringende beheersing of onmiddellijke respons op een actief incident.

12.2 Verantwoordelijkheden per rol

Beveiligingsleiding. Vraag bewijs van herstel en identiteitscontrole in plaats van een lijst aangekochte hulpmiddelen. Verduidelijk eigenaarschap wanneer een applicatie, leverancier en operationele dienst meerdere teams raken. Registreer aanvaarde restrisico's met een vervaldatum.

SOC en incidentrespons. Begin met het account, de getroffen dienst en het bewijstype. Bewaar de oorspronkelijke melding en een duidelijke chronologie. Controleer het verschil tussen een verdachte advertentie, een geldige identiteit en een waargenomen sessie voordat u een uitkomst beschrijft.

IT en infrastructuur. Controleer of dringende updates het werkelijke blootgestelde systeem bereikten. Een geslaagde uitroltaak bewijst niet dat elke appliance, meegeleverde runtime of secundaire server is gedekt. Houd hersteltoegang apart van normaal beheer.

Privacy en communicatie. Schrijf korte meldingen met wat bekend is, wat onzeker blijft en wat gebruikers moeten doen. Bereid waar relevant Franse en Nederlandse versies samen voor. Gebruik voor latere updates een stabiel officieel kanaal.

Financiën en klantbescherming. Controleer nieuwe betalingsinstructies onafhankelijk. Train ondersteuningsteams voor bellers die echte persoonsgegevens noemen. Juiste klantgegevens maken een fraudepoging overtuigender; ze authenticeren de beller niet.

Operations en leveranciers. Bepaal een veilige lokale modus voordat toegang op afstand wordt beperkt. Spreek af wie instellingen mag wijzigen, noodtoegang goedkeurt en herstel bevestigt. Controleer leverancierstoegang na personeels- of contractwijzigingen.

12.3 Hoe Brandefense kan helpen

Brandefense biedt externe dreigingsinformatie en monitoring van digitale risico's. De dienst kan onderzoek naar blootgestelde authenticatiegegevens, gelekte gegevens en merkimitatie ondersteunen. Een waarschuwing moet de controle- en responsprocedure uit dit rapport ingaan. [S44]

Breng de domeinen, merken en diensten die u mag onderzoeken mee naar een Brandefense-demonstratie. Vraag hoe een bevinding een verantwoordelijke bereikt, hoe onzekerheid wordt weergegeven en welk bewijs een zaak afsluit. [S44]

KERNPUNTEN

01

Geef elke actie een verantwoordelijke en een controleerbaar afrondingsdocument.

02

Test herstel zonder de leveranciers- en identiteitsafhankelijkheden.

03

Houd organisatorische planningsdoelen apart van directe incident- en meldingsplichten.

BIJLAGEN

Bijlagen

A–D

DIT HOOFDSTUK BEANTWOORDT

Hoe moet een lezer het bewijs interpreteren zonder populaties te verwarren?

4

bewijssoorten: waarneming, claim, publieke bevestiging en beoordeling

Bijlage A. Methode en grenzen 83

Bijlage B. Bewijsregister 86

Bijlage C. Bronnen 87

Bijlage D. Begrippenlijst 90

Bijlage A. Methode en grenzen

De vergelijkingslanden zijn uitsluitend als voorbeelden gekozen om context te bieden; hun selectie houdt geen rangschikking of politieke beoordeling in.

A.1 Periode en betekenis van tijdstempels

Het rapport bestrijkt 1 januari–22 november 2026. Ondergrondse waarnemingen gebruiken berichtdatums, geen veronderstelde inbraakdatum. Eigen blootstellingswaarnemingen dateren van 21 november; forum- en passieve waarnemingen dateren van 22 november. De afsluiting op de huidige dag weerspiegelt informatie bij vastlegging, niet latere uren van die datum.

Recente activiteit draagt het label 9–22 november. Een officieel rapport dat dan verschijnt, kan oudere gebeurtenissen beschrijven. Een herstelupdate, herpublicatie en nieuw aangeboden historisch bestand zijn niet automatisch nieuwe inbraken.

A.2 Bewijspopulaties

Populatie	Eenheid	Dekkingsgrens
Bewaard ondergronds materiaal	Afzonderlijk bericht	1.025 bewaarde forumberichten; gelabelde aantallen afzonderlijk vermeld
Forumdeel met landlabel	Bericht	480, opgenomen in de bewaarde populatie
Ransomwarematериaal	Aanvaarde vermeldingsrij	46 Belgisch gelabelde rijen; voorzichtigheid nodig bij land- en entiteitsscope
Domeininventaris	Primair kandidaatdomein	250 geselecteerd; 245 met een DNS-antwoord
Publieke incidenten en campagnes	Bewijsdossier	Organisatieverklaringen, officiële waarschuwingen en toegeschreven berichtgeving; geen nationale telling
Betaalkaartmateriaal	Afzonderlijke kaart en verschijningen	3 kaarten, 17 verschijningen, 9 berichten; geen genoemde uitgever

De publieke grafiekbestanden bevatten aggregaten. Publieke bewijskaarten bewaren korte geredigeerde fragmenten zonder persoonsvoorbeelden, slachtofferidentificatoren of criminele contactroutes. Een actoralias identificeert een forumpersona, geen geverifieerde persoon.

A.3 Waarnemingen van geselecteerde domeinen

De domeinset omvat openbare diensten en brede economische rollen. De selectie is doelgericht en toont geen ranglijst van de grootste onafhankelijke Belgische organisaties aan. DNS-antwoorden bevestigen geen juridisch eigendom, organisatorische onafhankelijkheid of beveiligingsprestaties.

Passieve e-mail- en webwaarnemingen betreffen de onderzochte domeinen op de waarnemingsdatum. Ontbrekende of mislukte waarnemingen blijven onderscheiden van vastgestelde configuratiebevindingen.

Atlas omvat alle 250 geselecteerde domeinen. De nationale waarde is 48 op 100. Apparaat-, authenticatie-, document- en actuele aanbodwaarnemingen dateren van 21 november 2026. Dit zijn cumulatieve records, niet uitsluitend gebeurtenissen uit 2026.

Vermeldingen beslaan 365 dagen tot en met 22 november 2026; gelijkende domeinen beslaan 30 dagen. Organisatie- en sectorscores worden niet gepubliceerd. De waarnemingen tonen geen actieve accounts, unieke personen of bevestigde inbraken aan. [S2]

A.4 Ransomwarevergelijkingen

Vermeldingen op ransomwareleksites zijn criminele beweringen. Een vermelding toont geen versleuteling, geslaagde diefstal, betaling, verlies of unieke rechtspersoon aan. Herhaalde merkomschrijvingen en buitenlandse eenheden kunnen landenvergelijkingen bemoeilijken.

De vier regionale vergelijkingslanden grenzen aan België en bieden relevante logistieke, taal-, industrie- of financiële context. Ruwe vermeldingstotalen zijn geen gecorrigeerde nationale risicocijfers. Gedeeltelijke totalen voor 2026 en volledige voor 2025 blijven uitdrukkelijk apart.

A.5 Betaalkaartscope

Deze beperkte waarnemingen ramen geen totale kaartdiefstal, actieve kaarten, inbraak in banksystemen of fraudeverlies.

De 3 afzonderlijke kaarten werden niet toegeschreven aan genoemde Belgische uitgevers. Zeventien verschijningen zijn geen zeventien kaarten. De drie kaarten vormen één populatie; er is geen extra populatie van genoemde banken om daarbij op te tellen.

A.6 Publieke bronnen en naamgebruik

Publieke broncategorieën omvatten de nationale cyberautoriteit, Safeonweb, de gegevensbeschermingsautoriteit, politie, organisatieverklaringen en berichtgeving in relevante talen. Elke geciteerde feitenbron werd voor de ondersteunende passage gelezen. Controledatums registreren de beoordeling, niet de incidentdatum.

Genoemde slachtoffers vereisen officiële bevestiging en bredere berichtgeving. Andere organisaties krijgen brede rolomschrijvingen. Wanneer een artikeladres een niet-genoemde organisatie identificeert, geeft het publieke bronnenregister de hoofdsite van de uitgever en laat het artikeladres weg.

Een onbeschikbare oorspronkelijke verklaring beperkt naamgebruik en bevestiging. Een gerapporteerd citaat blijft toegeschreven aan spreker en uitgever. Het wordt niet stilzwijgend een onafhankelijk gecontroleerde forensische uitkomst.

A.7 Vertrouwen en alternatieven

Er kan hoog vertrouwen zijn in het bestaan van een bewaarde advertentie, terwijl vertrouwen in de geclaimde inhoud laag blijft. Dit zijn verschillende stellingen. Elke casus vermeldt wat bewaard is, wat onopgelost blijft en een alternatieve verklaring.

Analytische modellen zijn gelabeld. Gemeenschappelijke taal, geografie, sector, politieke retoriek of publicatietiming volstaat niet om actoren te verbinden. Het rapport leidt uit die overeenkomsten geen gezamenlijke beheerder af.

A.8 Wat het rapport uitsluit

Het rapport geeft geen telling van alle Belgische cybercriminaliteit, nationaal getroffen personentotaal, financiële verliesschattingen of actorkansen. Meerdere publieke meldingen betreffen preventie of oude gebeurtenissen. Ze tellen niet als nieuwe aanvallen alleen omdat ze in 2026 verschenen.

Een preventieve website-uitschakeling in oktober en ziekenhuisuitval in november zonder aanwijzingen voor een externe aanval zijn bijvoorbeeld uitgesloten als bevestigde cyberaanvallen. Ze tonen waarom onbeschikbaarheid alleen onvoldoende is. [S66][S67]

Juridische uitspraken blijven beperkt tot de geciteerde autoriteit en tekst. Het rapport is geen juridisch advies. Publicatie- en regelgevingsdatums verschillen van incidentdatums; een bestuurlijke beslissing kan gedrag uit een eerder jaar betreffen.

Bijlage B. Bewijsregister

Kaart	Datum	Locatie	Alias	Taal	Hoofdstuk
B01	2026-01-24	Lekforum	kazutlg	Engels	4
B02	2026-01-21	Lekforum	xmlrpc	Engels	4
B03	2026-10-02	Lekforum	yneov18	Engels	4
B04	2026-11-08	Lekforum	DataJava	Engels	4
B05	2026-11-20	Lekforum	0xcasper	Engels	4
B06	2026-11-13	Lekforum	updap	Engels	4
B07	2026-04-13	Lekforum	[alias withheld]	Engels	4
B08	2026-02-24	Lekforum	Crazy88	Engels	4
B09	2026-11-03	Lekforum	buylogs	Engels	4
B10	2026-11-21	Lekforum	WSdatabase	Engels	4

Casussen A–F beoordelen de bewaarde forumstellingen. Casussen G–O en R–S beoordelen publieke incidentverslagen. Casussen P–Q beoordelen officiële politiecampagneverklaringen. Het zijn casusdossiers, geen wederzijds uitsluitende nationale incidenteenheden.

Bijlage C. Bronnen

S1: Odin by Brandefense ransomware-listing aggregate. https://brandefense.io/. Geverifieerd op 2026-11-22. Bewaarde rapportgegevens; de URL beschrijft de dienst en publiceert de onderliggende records niet.

S2: Atlas exposure ratings, Brandefense Blackhole domain associations and selected-domain passive observations. https://brandefense.io/. Geverifieerd op 2026-11-22. Bewaarde rapportgegevens; de URL beschrijft de dienst en publiceert de onderliggende records niet.

S3: Brandefense Blackhole country-tagged post counts and retained forum and card-material observations. https://brandefense.io/. Geverifieerd op 2026-11-22. Bewaarde rapportgegevens; de URL beschrijft de dienst en publiceert de onderliggende records niet.

S4: CCB, Figures show a steady rise in incidents. https://ccb.belgium.be/news/figures-show-steady-rise-incidents-ccb-urges-enterprises-act-immediately. Geverifieerd op 2026-11-22.

S5: CCB, The growing threat of identity compromise. https://ccb.belgium.be/news/growing-threat-identity-compromise. Geverifieerd op 2026-11-22.

S6: Belgian federal portal, Belgium, a federal state. https://www.belgium.be/en/about_belgium/government/federale_staat. Geverifieerd op 2026-11-22.

S7: CCB, Quarterly Cyber Threat Report Q1 2026. https://ccb.belgium.be/nl/open-media/1237/download?inline. Geverifieerd op 2026-11-22.

S8: CCB, Quarterly Cyber Threat Report Q2 2026. https://ccb.belgium.be/open-media/1427/download?inline. Geverifieerd op 2026-11-22.

S9: CCB, Quarterly Cyber Threat Report Q3 2026. https://ccb.belgium.be/open-media/1470/download?inline. Geverifieerd op 2026-11-22.

S10: Security Affairs, hospital service disruption and quoted statement. https://securityaffairs.com/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S11: Safeonweb, company-confirmed fitness and booking-service incidents. https://safeonweb.be/nl/actueel/opgelet-klantgegevens-gelekt-bij-basic-fit-en-bookingcom. Geverifieerd op 2026-11-22.

S12: Reuters, Basic-Fit customer-data incident. https://www.reuters.com/business/basic-fit-says-data-breach-exposes-details-200000-members-netherlands-2026-04-13/. Geverifieerd op 2026-11-22.

S13: Safeonweb, learning-platform incident and phishing warning. https://safeonweb.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S14: RTBF, reported mobile-management incident at a public agency. https://www.rtbf.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S15: Machelen, municipal incident updates. https://www.machelen.be/cyberincident. Geverifieerd op 2026-11-22.

S16: VRT, municipal confirmation of personal-data theft. https://www.vrt.be/vrtnws/nl/2026/09/23/dan-toch-persoonsgegevens-gestolen-bij-cyberaanval-op-gemeentebe/. Geverifieerd op 2026-11-22.

S17: RTBF/Belga, sports membership incident accounts. https://www.rtbf.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S18: RTBF, fitness-chain company statement and criminal claim. https://www.rtbf.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S19: VRT, school-group incident and director statement. https://www.vrt.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S20: VRT, vocational-training data republication. https://www.vrt.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S21: L'Avenir, reported public e-learning platform incident. https://www.lavenir.net/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S22: VRT, digital-signature supplier statement and customer-scope distinction. https://www.vrt.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S23: SPF Finances/FOD Financiën, recovery updates. https://finances.belgium.be/fr/Actualites/eservices-disponibles-apres-cyberattaque. Geverifieerd op 2026-11-22.

S24: VRT, federal tax administration incident. https://www.vrt.be/vrtnws/nl/2026/10/28/cyberaanval-bij-fod-financien/. Geverifieerd op 2026-11-22.

S25: CCB, refrigeration-controller security advisory. https://ccb.belgium.be/advisories/warning-six-new-danfoss-vulnerabilities-refrigeration-controllers-risk-immediate-action. Geverifieerd op 2026-11-22.

S26: Reuters, differing ministerial assessments of refrigeration attribution. https://www.reuters.com/world/belgian-ministers-odds-over-irans-alleged-role-refrigerator-cyberattacks-2026-11-13/. Geverifieerd op 2026-11-22.

S27: Safeonweb, refrigeration incidents and connected-device advice. https://safeonweb.be/nl/actueel/na-de-incidenten-met-koelkasten-warenhuizen-kan-jouw-slimme-koelkast-een-eigen-leven-gaan. Geverifieerd op 2026-11-22.

S28: Safeonweb, possible benefits-service data exposure. https://safeonweb.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S29: Safeonweb, possible gift-voucher customer-data exposure. https://safeonweb.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S30: Federal Police, alleged phishing-panel supplier investigation. https://www.police.be/5998/fr/actualites/crime-as-a-service-arrestation-dun-fournisseur-de-panneaux-de-phishing. Geverifieerd op 2026-11-22.

S31: Federal Police, automated invoice-fraud warning. https://www.police.be/5998/fr/actualites/factures-falsifiees-la-police-judiciaire-federale-danvers-tire-la-sonnette-dalarme. Geverifieerd op 2026-11-22.

S32: Federal Police, phishing and fake-bank-employee investigation. https://www.police.be/5998/fr/actualites/un-chef-dune-bande-dhameconneurs-arrete-son-retour-de-dubai. Geverifieerd op 2026-11-22.

S33: CCB, NIS2 evidence milestone in April 2026. https://ccb.belgium.be/news/nis2-18-april-2026-deadline-what-essential-entities-must-have-place. Geverifieerd op 2026-11-22.

S34: CCB, New communication for NIS2 essential entities. https://ccb.belgium.be/news/new-communication-nis2-essential-entities. Geverifieerd op 2026-11-22.

S35: CCB, NIS2 Notifications – Howto?. https://ccb.belgium.be/cert/report-incident/nis2-notifications-howto. Geverifieerd op 2026-11-22.

S36: Justel, Belgian NIS2 law, consolidated text. https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel. Geverifieerd op 2026-11-22.

S37: APD/GBA, Notifier et gérer une violation de données. https://www.autoriteprotectiondonnees.be/professionnel/actions/violation-de-donnees-personnelles. Geverifieerd op 2026-11-22.

S38: National Bank of Belgium, ITA team and DORA. https://www.nbb.be/en/financial-supervision/digital-resilience-and-cyber-risk/ita-team. Geverifieerd op 2026-11-22.

S39: CCB, CRA reporting obligations take effect. https://ccb.belgium.be/news/cyber-resilience-act-european-reporting-obligations-take-effect. Geverifieerd op 2026-11-22.

S40: CCB, National Cyber Emergency Plan. https://ccb.belgium.be/vital-sectors/national-cyber-emergency-plan. Geverifieerd op 2026-11-22.

S41: Ivanti, EPMM security advisory and resolved versions. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340. Geverifieerd op 2026-11-22.

S42: NVD, CVE-2026-1281. https://nvd.nist.gov/vuln/detail/CVE-2026-1281. Geverifieerd op 2026-11-22.

S43: NVD, CVE-2026-1340. https://nvd.nist.gov/vuln/detail/CVE-2026-1340. Geverifieerd op 2026-11-22.

S44: Brandefense, Request a demo. https://brandefense.io/request-a-demo/. Geverifieerd op 2026-11-22.

S45: Safeonweb, fake pellet and firewood offers. https://safeonweb.be/nl/actueel/pellets-brandhout-kopen-laat-je-niet-misleiden-door-valse-aanbiedingen. Geverifieerd op 2026-11-22.

S46: Charging-account service, company incident FAQ. https://help.chargemap.com/nl/articles/11583170. Geverifieerd op 2026-11-22.

S47: Chemical manufacturer, clarification of the May incident. https://www.christeyns.com/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S48: Recycling operator, forensic follow-up. https://www.iok.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S49: Medical research institute, statement updated in November. https://www.itg.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S50: Professional legal body, scope update. https://www.avocats.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S51: ITdaily, supermarket supplier incident. https://itdaily.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S52: Wonen360, furniture-retailer company statement. https://www.wonen360.nl/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S53: Télésambre, municipal incident and restoration reporting. https://www.telesambre.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S54: La Libre, precious-metals customer-data incident. https://www.lalibre.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S55: DH, municipal website incident and scope. https://www.dhnet.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S56: HLN/VTM, travel-operator statement and customer messages. https://www.hln.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S59: Safeonweb, malicious-app and NFC-relay warning. https://safeonweb.be/nl/actueel/pas-op-voor-frauduleuze-telefoontjes-waarin-je-wordt-gevraagd-een-app-te-installeren-en-je. Geverifieerd op 2026-11-22.

S60: Safeonweb, executive impersonation on Teams. https://safeonweb.be/nl/actueel/pas-op-voor-ceo-fraude-microsoft-teams. Geverifieerd op 2026-11-22.

S61: Safeonweb, false hotel and B&B reservation messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-whatsapp-berichten-over-hotel-en-bb-boekingen. Geverifieerd op 2026-11-22.

S62: Safeonweb, government sign-in impersonation. https://safeonweb.be/nl/actueel/phishing-naam-van-csam. Geverifieerd op 2026-11-22.

S63: Safeonweb, fraudulent compensation and recovery messages. https://safeonweb.be/nl/actueel/opgelet-voor-fake-dossier-voor-schadevergoeding-na-fraude. Geverifieerd op 2026-11-22.

S64: Safeonweb, false voting and account-linking messages. https://safeonweb.be/nl/actueel/opgelet-voor-valse-stemwedstrijden-whatsapp. Geverifieerd op 2026-11-22.

S65: Safeonweb, high-profile invitation impersonation. https://safeonweb.be/nl/actueel/opgepast-voor-berichten-die-van-het-koningshuis-lijken-te-komen. Geverifieerd op 2026-11-22.

S66: Safeonweb, preventive PHP patching outage. https://safeonweb.be/nl/actueel/php-crisis-waarom-waren-verschillende-websites-niet-bereikbaar. Geverifieerd op 2026-11-22.

S67: Numerikare/Belga, hospital outage without external-attack indications. https://www.numerikare.be/ (artikel-URL weggelaten). Geverifieerd op 2026-11-22.

S68: IETF, RFC 6797: HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html. Geverifieerd op 2026-11-22.

S69: W3C, Content Security Policy Level 3, abstract. https://www.w3.org/TR/CSP3/. Geverifieerd op 2026-11-22.

S70: IETF, RFC 4034: Resource Records for the DNS Security Extensions, section 5. https://www.rfc-editor.org/rfc/rfc4034.html. Geverifieerd op 2026-11-22.

S71: VRT, charging-account service incident and European user population. https://www.vrt.be/vrtnws/nl/2026/11/18/charge-map-cyberaanval/. Geverifieerd op 2026-11-22.

Bijlage D. Begrippenlijst

Begrip	Eenvoudige betekenis
Accountherstel	Toegang herstellen nadat authenticatiegegevens of -methoden verloren zijn
Authenticatiegegeven	Informatie om te authenticeren, zoals een wachtwoord of authenticatiegeheim
Apparaatassociatie	Een record dat een apparaatwaarneming aan een domein koppelt; eigendom vereist controle
DMARC	Een e-mailbeleid dat ontvangers helpt berichten met een domeinidentiteit te beoordelen
DKIM	Een digitale e-mailhandtekening gecontroleerd tegen gepubliceerde verificatie-informatie van een domein
DNSSEC	Een systeem om ondertekende DNS-informatie te valideren
DS-record	Een delegation signer-record koppelt een bovenliggende DNS-zone aan de ondertekeningssleutel van een onderliggende zone; waarneming ervan valideert niet de volledige DNSSEC-keten [S70]
HSTS	HTTP Strict Transport Security verplicht browsers HTTPS te gebruiken voor een site; één waargenomen header beoordeelt niet elke applicatie [S68]
CSP	Content Security Policy bepaalt welke bronnen een pagina mag laden of uitvoeren; één waargenomen beleid bewijst geen volledige applicatiebeveiliging [S69]
Exfiltratie	Ongeoorloofd kopiëren van gegevens uit een systeem
Handelaar in initiële toegang	Een verkoper die toegang tot organisatiesystemen aanbiedt; elke toegangsclaim vereist controle
Metadata	Informatie over een ander record, zoals titel, auteur of verwerkingstijd
NFC-relay	Korteafstandscommunicatie van kaarten doorsturen naar een andere locatie tijdens een frauduleuze transactie
OAuth-toestemming	Toestemming waarmee een applicatie onder een account toegang krijgt tot bepaalde middelen
Pseudonimisering	Directe identificatoren vervangen met behoud van een mogelijke koppeling tussen records en personen
Sessie	Een geauthenticeerde interactie die na de eerste aanmelding bruikbaar kan blijven

Begrip	Eenvoudige betekenis
SPF	Een in DNS gepubliceerde verklaring over bevoegde verzend-diensten voor een e-maildomein
TLS	Het protocol voor bescherming van netwerkcommunicatie en authenticatie van een dienst

Over dit rapport

Opgesteld door Odin by Brandefense. Brandefense Country Report · Belgium 2026. Versie 1.0, waarnemingsafsluiting 22 november 2026. TLP:CLEAR.

Het rapport houdt advertenties, vermeldingen, officiële verslagen en beoordeling apart. Het neemt geen politiek standpunt in en doet geen zelfstandige staatstoeschrijving. Aanbevelingen beschrijven acties die een organisatie moet controleren; ze stellen niet dat een genoemde organisatie deze heeft nagelaten.

Franse en Nederlandse edities zijn met AI vertaald vanuit de Engelse hoofdtekst. Bij verschillen heeft de Engelse editie voorrang. Onafhankelijke publicatiebeoordeling, opmaak en vrijgave zijn afzonderlijke stappen.

© 2026 Brandefense. Alle rechten voorbehouden.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO