BRANDEFENSE COUNTRY REPORT · NETHERLANDS 2026

Brandefense Rapport over het Nederlandse cyberdreigingslandschap 2026

Identiteitsdiefstal, gedeelde software en dienstcontinuïteit in een verbonden economie

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

84 van 250
geselecteerde vermeldingen hadden bij controle een inloggegeven te koop staan

5.160
bewaarde berichten binnen de genoemde reikwijdte, geen nationaal aanvalstotaal

77
geaccepteerde Nederlandse ransomwarevermeldingen in de momentopname van de onderzoeksperiode

21 van 25
geselecteerde financiële domeinen met gepubliceerd DMARC-quarantine- of rejectbeleid

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	09
02	De Nederlandse digitale en institutionele context	10
03	Blootstelling van geselecteerde domeinen en openbare technische waarnemingen	13
04	Wat de bewaarde ondergrondse berichten aantonen	22
05	Bevestigde incidenten, leveranciersafhankelijkheden en recente activiteit	41
06	Verbonden systemen, verstoring en operationele continuïteit	53
07	Actoren, campagnes en de grenzen van toeschrijving	58
08	De fraude-economie en schade na openbaarmaking	69
09	Bankwezen en financiën: onderscheid instelling, klant en leverancier	77
10	Regelgeving en de nationale respons	81
11	Vooruitblik: beslissingen veranderen met het bewijs	85
12	Een 90-dagenplan met afrondingsbewijs	89
A	Bijlage A. Reikwijdte, bewijs en interpretatie	97
B	Bijlage B. Bewijsregister van berichten	100
C	Bijlage C. Bronnen	102
D	Bijlage D. Begrippenlijst	107
	Over dit rapport	109

Bestuur en directie	01 05 10 11 12
CISO en diensteigenaren	03 04 05 06 10 12
SOC en dreigingsinformatie	04 06 07 12 A B
Fraude en klantoperatie	04 08 09 12
Privacy, juridische zaken en communicatie	05 08 10 12 A

Over deze editie

Vertaald met AI

Bij verschillen tussen deze vertaling en de Engelse editie is de Engelse tekst leidend.

Opgesteld door Odin by Brandefense op basis van Brandefense Blackhole, Ransompedia, Atlas, openbare technische waarnemingen en geverifieerde openbare berichtgeving. Analyse en eerste versies door AI-agenten; beoordeling door een analist is vereist vóór uitgave. Bijlage A beschrijft de reikwijdte en beperkingen.

De gedocumenteerde Nederlandse gevallen verbinden identiteit, gedeelde software en dienstcontinuïteit. Ze vragen om afzonderlijke beslissingen over toegang, gegevens, fysieke bedrijfsvoering en meldingen.

5.160

bewaarde berichten, geen unieke incidenten [S1]

77

geaccepteerde ransomwareclaims op leksites, geen bevestigde inbraken [S3]

249

waargenomen kandidaatdomeinen uit een geselecteerde lijst van 250 [S2]

24

bewijskaarten van berichten met expliciete grenzen aan de conclusies [S1]

HOOFDSTUK 01

Samenvatting

01

DIT HOOFDSTUK BEANTWOORDT

Wat moeten Nederlandse organisaties als eerste besluiten na de in 2026 gedocumenteerde incidenten en campagnes?

4

beslissingen over identiteit, leveranciers, continuïteit en incidentmeldingen

Vier beslissingen voor bestuurders 06

Het jaar in cijfers 07

HOOFDSTUK 01

Samenvatting

IN HET KORT

Nederlandse meldingen tonen hoe klantgegevens, gedeelde software en vertrouwde accounts beveiligingsproblemen verbinden met dagelijkse diensten. Gevolgen zijn onderbroken zorgkoppelingen, gestolen verenigingsgegevens en bedreigingen na diefstal van bankgegevens. Officiële berichten beschrijven ook spionage tegen persoonlijke accounts en verbonden apparatuur. Ransomwarevermeldingen tonen afzonderlijk criminele claims. Begin bij accountherstel, leverancierstoegang en dienstafhankelijkheden en oefen vervolgens de vereiste meldingsbeslissingen.

Dit rapport combineert verschillende bewijsverzamelingen. Brandefense Blackhole levert Nederland-gerelateerde berichten en nauw afgebakende waarnemingen van betaalkaarten. Ransompedia levert geaccepteerde vermeldingen op leksites. Atlas-blootstellingsrelaties en openbare technische waarnemingen beschrijven een geselecteerde lijst van kandidaatdomeinen. Bedrijfsverklaringen, overheden en technische onderzoekers bevestigen specifieke gebeurtenissen en geven context. Deze verzamelingen hebben verschillende eenheden, perioden en beperkingen. Ze worden niet opgeteld tot een nationaal aanvalstotaal. [S1][S2][S3][S4]

1. Diefstal van klantgegevens vraagt meer dan wachtwoordherstel. De bevestigde Odido-zaak verbindt het nabootsen van een collega met interne toegang en latere publicatie van klantinformatie. Politieberichtgeving over Revolut koppelt gestolen identificerende gegevens aan een poging tot geweld. Het verdedigingsdoel omvat daarom accountbeveiliging, klantcommunicatie en een meldroute voor zorgen over persoonlijke veiligheid. De zaken tonen geen gemeenschappelijke dader of nationaal schadepercentage aan. [S15][S75]

2. Eén gedeelde leverancier kan de werkdag van veel organisaties veranderen. ChipSoft, leerplatform Canvas en AllUnited illustreren verschillende afhankelijkheden: patiëntkoppelingen, onderwijssystemen en verenigingsadministratie. Een leveranciersmelding toont geen gelijke gevolgen bij alle klanten aan. Iedere afhankelijke organisatie moet haar eigen getroffen gegevens, dienststatus en meldplichten vaststellen. Hoofdstukken 5 en 12 vertalen dit onderscheid naar leveranciersvragen en herstelbewijs. [S44][S49][S68]

3. Een geslaagde patch sluit eerdere toegang niet uit. Het NCSC documenteerde misbruik van systemen voor mobiel beheer in Nederland. Het maakt onderscheid tussen waargenomen binnendringing en latere herstelmaatregelen. Toets daarom twee zaken afzonderlijk: is de kwetsbaarheid verholpen en had een aanvaller al toegang gekregen? Een patchregistratie beantwoordt de eerste vraag; onderzoek en indamming beantwoorden de tweede. [S21]

4. Spionage omvat persoonlijke accounts en kleine verbonden apparaten. De AIVD en MIVD beschreven berichten- en cameracampagnes met banden met de Russische staat. De AIVD meldde Nederlandse slachtoffers van een malwarecampagne van Iraanse actoren. Dit zijn toeschrijvingen van de diensten. Ze rechtvaardigen niet dat elke criminele claim, anderstalig bericht of kwetsbaar apparaat aan een staat wordt toegeschreven. Bescherm herstel van berichtenaccounts en verbonden apparatuur naast bedrijfssystemen. [S36][S58][S61]

5. November veranderde vóór deze peildatum de operationele prioriteiten. Updates van AllUnited, een internationale malwareverstoring, een incident met een browserscript van derden en het Revolut-onderzoek vragen verschillende reacties. Een gelijktijdige cloudstoring raakte ook de continuïteit, maar volgens het NCSC waren er geen aanwijzingen voor een hack. Het overzicht van recente activiteit onderscheidt meldingen, opsporing, afhankelijkheden en preventie; niet elk bericht is een aanval. [S68][S71][S74][S75][S73]

6. Blootstellingssignalen vragen verschillende validatieverantwoordelijken. Bij 250 geselecteerde vermeldingen hadden 84 bij controle een inloggegeven te koop staan. De nationale Atlas-hoofdwaarde is 50 op 100. Apparaatrelaties bedragen minstens 312.644, waaronder 16.435 relaties met werknemersapparaten; inloggegevensrecords bedragen 4.736.932. Deze overlappende records ondersteunen account- en apparaatvalidatie, geen nationale incidentschatting. [S2]

Vier beslissingen voor bestuurders

1. **Maak accountherstel een geautoriseerd proces.** Vereis een onafhankelijk geverifieerde route voor wijzigingen van wachtwoorden, MFA en herstel van berichtenaccounts. Controleer actieve sessies en gekoppelde apparaten bij een relevant signaal. Een overtuigende beller mag niet met interne woordenschat een nieuwe vertrouwde route kunnen creëren (§6–§7).

1. **Vraag leveranciers afzonderlijk naar gegevens en diensten.** Stel vast welke tenant, koppeling, geëxporteerde gegevens en herstelafhankelijkheden betrokken zijn. Vereis een vaste contactpersoon, een bruikbare melding en bewijs dat heraansluiting ondersteunt. Een hersteld systeem bewijst niet dat gestolen informatie is verdwenen (§5).

1. **Controleer verbonden besturingen en browserafhankelijkheden.** Beoordeel beheer op afstand van koeling, camera's en andere fysieke systemen. Beoordeel daarnaast scripts van derden die in klantbrowsers draaien. Wijs een operationeel eigenaar aan die de afhankelijkheid kan isoleren zonder naar de bedrijfsgevolgen te gissen (§5.8, §6).

1. **Oefen de meldtermijnen die daadwerkelijk gelden.** Koppel de Cyberbeveiligingswet, AVG en financiële-sectorvereisten aan de organisatie. Leg bewustwording, classificatie, beslissingen en ontvangers vast in één incidentdossier. Een algemene instructie om alles binnen 72 uur te melden dekt deze verschillende plichten niet (§10).

Het jaar in cijfers

250

Doelgericht geselecteerde kandidaatdomeinen verdeeld over 12 sectorcategorieën

WAT HET NIET IS

Geen 250 onafhankelijke Nederlandse organisaties of nationale prevalentiesteekproef

84 van 250

Geselecteerde vermeldingen met een inloggegeven te koop bij controle

WAT HET NIET IS

Geen werkende accounts of bevestigde inbraken [S2]

50 op 100

Nationale Atlas-hoofdwaarde voor de geselecteerde portefeuille

WAT HET NIET IS

Geen sectorbeoordelingen of nationale prevalentie [S2]

77

Geaccepteerde Nederlandse ransomwarevermeldingen in de bewaarde momentopname van de onderzoeksperiode

WAT HET NIET IS

Geen 77 onafhankelijk bevestigde inbraken of unieke slachtoffers [S3]

478

Verenigingen in de collectieve AP-melding van AllUnited waarover op 18 november werd bericht

WAT HET NIET IS

Geen definitief slachtoffertotaal of aantal getroffen personen [S68]

178

Organisaties wereldwijd in het onderzoek van Report URI naar een script van derden

WAT HET NIET IS

Geen 178 Nederlandse slachtoffers [S29]

15 augustus 2026

Datum van inwerkingtreding genoemd in het Cyberbeveiligingsbesluit

WAT HET NIET IS

Niet de uiterste termijn voor iedere afzonderlijke incidentmeldplicht [S10]

5.160

Bewaarde Nederland-gerelateerde berichten binnen de onderzoeksreikwijdte

WAT HET NIET IS

Geen unieke aanbiedingen, transacties of aanvallen [S1]

249 van 250

Domeinen met passieve waarnemingen; beschikbaarheid verschilt per onderdeel

WAT HET NIET IS

Geen gevalideerde rangschikking van organisatiebeveiliging [S2]

36

Betaalkaarten zichtbaar als leesbare tekst in de bewaarde berichten

WAT HET NIET IS

Geen nationale kaartdiefstal of fraudeverliezen [S4]

REIKWIJDTE VAN DE KAARTCIJFERS

Kaartcijfers betreffen uitsluitend betaalkaarten die als leesbare tekst zichtbaar zijn in de bewaarde berichten. Brandefense detecteert gestolen kaarten ook met andere methoden buiten dit rapport. Deze waarnemingen meten geen nationale kaartdiefstal, actieve kaarten, prevalentie per uitgever of fraudeverliezen.

Bestuurders kunnen hoofdstukken 1, 5, 10 en 12 volgen. Beveiligingsteams moeten ook de blootstellingsreikwijdte, bronkaarten en actorverschillen lezen. Fraudeverantwoordelijken verbinden hoofdstukken 8 en 9 met de klantoperatie. De rapportkaart toont de volledige leesroutes.

Rapportkaart

Twaalf hoofdstukken, vijf leesroutes. Elk hoofdstuk opent met de beantwoorde vraag; hoofdstukken 2–12 sluiten met drie kernpunten.

Bestuur en directie	Welke beslissingen vragen eigenaarschap, middelen en afrondingsbewijs?	01 05 10 11 12
CISO en diensteigenaren	Welke signalen, afhankelijkheden en technische maatregelen beïnvloeden onze respons?	03 04 05 06 10 12
SOC en dreigingsinformatie	Wat staat vast, wat blijft een claim en welke campagne-indelingen gelden?	04 06 07 12 A B
Fraude en klantoperatie	Hoe maakt informatie benaderingen overtuigend en hoe verifiëren we ingrijpende verzoeken?	04 08 09 12
Privacy, juridische zaken en communicatie	Welke reikwijdte en termijnen gelden en hoe communiceren we onzekerheid?	05 08 10 12 A

01 Samenvatting
Wat bestuurders als eerste moeten besluiten

02 Context
Waarom herstel, gedeelde gegevens en institutionele rollen van belang zijn

03 Blootstelling van geselecteerde domeinen
Wat afgebakende openbare waarnemingen kunnen ondersteunen

04 Ondergrondse berichten
Welke claims validatie verdienen en welke zijn uitgesloten

05 Incidenten
Wat organisaties en overheden vaststelden, inclusief recente activiteit

06 Verbonden systemen
Hoe verstoring te verifiëren en de fysieke of afhankelijke dienst te beschermen

07 Actoren
Welke toeschrijvingen en relaties de bronnen ondersteunen

08 Fraude-economie
Hoe records en aangeboden diensten verband houden met fraude- en veiligheidsrespons

09 Bankwezen en financiën
Hoe bewijs over instelling, klant en leverancier verschilt

10 Regelgeving
Welke aanleidingen, ontvangers en termijnen beslissingen vereisen

11 Vooruitblik
Welke signalen de beoordeling zouden veranderen

12 Actieplan
Wie wat doet en hoe afronding wordt aangetoond

HOOFDSTUK 02

De Nederlandse digitale en institutionele context

02

DIT HOOFDSTUK BEANTWOORDT

Welke kenmerken van het bewijs veranderen hoe Nederlandse organisaties zich moeten voorbereiden?

12

sectorcategorieën in de geselecteerde domeinverzameling, elk met minstens vijf domeinen

2.1 Digitaal werken maakt identiteit en herstel operationele beslissingen 11

2.2 Gedeelde gegevens vragen een dienstenkaart, naast een leverancierslijst 11

2.3 Het technische aanspreekpunt veranderde gedurende het jaar 12

2.4 Nieuwe wetgeving vervangt bestaande meldingsbeslissingen niet 12

2.5 Politieke context vraagt brongebonden toeschrijving 12

HOOFDSTUK 02

De Nederlandse digitale en institutionele context

IN HET KORT

Het bewijs raakt klanten, werkgevers, verenigingen, dienstverleners en overheden. Een gestolen account kan gegevens van een andere organisatie blootstellen. Isolatie van een leverancier kan werk onderbreken zonder te bewijzen dat iedere klant is getroffen. Ook Nederlandse instellingen veranderden in 2026, met een versterkt NCSC en de inwerkingtreding van de Cyberbeveiligingswet. Verbind gegevens, diensten en verantwoordelijke eigenaren in een inventaris en bepaal vervolgens de toepasselijke regels per relatie.

2.1 Digitaal werken maakt identiteit en herstel operationele beslissingen

Het CBS publiceerde in februari 2026 zijn hoofdstuk over ICT bij bedrijven, op basis van gegevens uit 2025. Bij bedrijven met minstens tien werknemers gebruikte 82% van het personeel internet. Verder ondersteunde 80% van de bedrijven thuiswerken en had 61% van het personeel op afstand toegang tot documenten of software. Dit zijn gebruikscijfers, geen metingen van aanvallen in 2026. [S6]

Het beveiligingsgevolg is een inschatting voor de planning. Thuiswerken vereist dat een werknemer toegang kan herstellen wanneer een apparaat, wachtwoord of tweede factor uitvalt. Herstel verdient daarom dezelfde ontwerpaandacht als normaal inloggen. De vertrouwde beller, het supportticket en de nooduitzondering horen bij het beheersysteem.

Dit raakt zowel continuïteit als het voorkomen van inbraken. Een proces dat fraude voorkomt maar medewerkers niet laat werken, zet druk op informele omwegen. Meet beide uitkomsten in een geautoriseerde oefening: wordt de imitator tegengehouden en krijgt de echte gebruiker toegang via de goedgekeurde route?

2.2 Gedeelde gegevens vragen een dienstenkaart, naast een leverancierslijst

De bevestigde zaken in hoofdstuk 5 betreffen verschillende gedeelde systemen. Het gemeenschappelijke beheervraagstuk is wie de relevante gegevens heeft en wie de dienst veilig kan herstellen. Dit is onze synthese van die zaken. Het bewijst niet dat elke Nederlandse leverancier dezelfde zwakte heeft.

Een gebruikelijke inkooplijst kan de juridische wederpartij aanwijzen en toch een operationele afhankelijkheid missen. Een lokaal team kan afhankelijk zijn van een federatieve koppeling, leerplatformintegratie of patiënten-portaal dat via die wederpartij wordt beheerd. De incidentverantwoordelijke moet de relatie tussen die onderdelen kennen, inclusief wie ze kan onderbreken en herstellen.

De bruikbaarste kaart heeft twee weergaven. De gegevensweergave benoemt informatiecategorieën, bevoegde ontvangers, exports en bewaarplichten. De dienstenweergave benoemt welk proces stopt wanneer een verbinding wordt uitgeschakeld, de terugvaloptie en het benodigde hervattingsbewijs. Elke weergave beantwoordt vragen die de andere niet kan beantwoorden.

Een aanbieder kan een koppeling herstellen voordat de volledige omvang van het gegevensverlies bekend is. Omgekeerd kan een beperkt gegevensincident tot een brede voorzorgssluiting leiden. Communiceer beide toestanden afzonderlijk. Klanten moeten weten of ze een dienst kunnen gebruiken en of ze beschermende maatregelen voor hun informatie moeten nemen.

2.3 Het technische aanspreekpunt veranderde gedurende het jaar

Een NCSC-bericht van 6 januari meldt dat het Digital Trust Center per 1 januari 2026 is opgegaan in het NCSC. Het beschrijft een versterkt nationaal aanspreekpunt voor de digitale weerbaarheid van organisaties. Deze organisatorische wijziging verandert niet automatisch de wettelijke plichten van iedere entiteit. [S5]

Een CISO moet advies, technische coördinatie, wettelijke melding en aangifte onderscheiden. Deze activiteiten kunnen één incident ondersteunen, maar contact met één instantie vervult op zichzelf niet elke verplichting. De meldkaart moet per contact het doel, de benodigde informatie en de dossierverantwoordelijke benoemen.

2.4 Nieuwe wetgeving vervangt bestaande meldingsbeslissingen niet

Het nationale overzicht meldt dat de Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten op 15 augustus 2026 in werking traden. Het noemt registratie-, zorg- en meldplichten voor significante incidenten, naast bestuurstraining. Hoofdstuk 10 onderscheidt deze cyberwettelijke plichten van privacy- en financiële meldingen. [S8]

Bij groepen met meerdere entiteiten kan één technisch incident meer dan één meldingsrelatie opleveren. Het responsplan moet een gedeelde feitelijke tijdlijn bewaren, met ruimte voor verschillende juridische beoordelingen. Zo worden dubbele speculatie en de onjuiste aanname vermeden dat een groepsmelding iedere entiteit dekt.

2.5 Politieke context vraagt brongebonden toeschrijving

Dit rapport gebruikt verklaringen van de AIVD en MIVD om staatsgerelateerde activiteit te beschrijven. Het leidt geen verantwoordelijkheid af uit een alias, taal of vestigingsland van een infrastructuuraanbieder. Het concrete campagnebewijs staat in hoofdstukken 6 en 7. [S36][S58][S61][S62]

KERNPUNTEN

01

Ontwerp accountherstel met dezelfde aandacht als inloggen.

02

Breng gegevens- en dienstafhankelijkheden afzonderlijk in kaart, zodat herstel de blootstelling niet verhult.

03

Stel institutionele contacten en wettelijke toepasselijkheid vast voordat het volgende incident begint.

HOOFDSTUK 03

Blootstelling van geselecteerde domeinen en openbare technische waarnemingen

DIT HOOFDSTUK BEANTWOORDT

Welke blootstellingswaarnemingen moeten eigenaren eerst valideren binnen de geselecteerde Nederlandse portefeuille?

84 van 250

geselecteerde vermeldingen hadden bij controle een inloggegeven te koop staan

3.1 Populatiekaart 14
3.2 Blootstellingssignalen per sector 15
3.3 E-mailauthenticatie vraagt een inventaris van bevoegde afzenders 18
3.4 Webcontinuïteit en beveiligingswaarnemingen beantwoorden verschillende vragen 19
3.5 Advertenties, gelijkende domeinen, documenten en vermeldingen vragen verschillende validatie 20
3.6 Maak van de waarneming een taak met een verantwoordelijke 20

HOOFDSTUK 03

Blootstelling van geselecteerde domeinen en openbare technische waarnemingen

IN HET KORT

Binnen de geselecteerde portefeuille hadden 84 van 250 vermeldingen bij controle een inloggegeven te koop staan. De nationale Atlas-hoofdwaarde is 50 op 100. Minstens 312.644 apparaatrelaties en 4.736.932 inloggegevensrecords ondersteunen afzonderlijke validatietaken. Deze overlappende waarnemingen beschrijven geselecteerde domeinen, waaronder merken en groepen, geen onafhankelijke organisaties of nationale prevalentie. Valideer actuele accounts, onderzoek signalen over werknemersapparaten en wijs eigenaren toe aan bevestigde tekortkomingen in e-mailbeleid.

3.1 Populatiekaart

Onderdeel	Definitie
Populatie	250 kandidaatdomeinen geselecteerd vanwege publieke, commerciële of systemische relevantie
Sectorcategorieën	Overheid 40; financiën 25; verzekeringen 15; onderwijs 25; zorg 25; energie 20; transport 25; telecom en technologie 25; industrie 20; handel 15; horeca 10; media 5
Eenheid	Een geselecteerd primair domein van een instelling, operationeel merk of groep
Interpretatie	Eén domein is niet noodzakelijk één onafhankelijke rechtspersoon of organisatie
Selectie	Doelgericht, niet willekeurig en geen officiële nationale ranglijst
Blootstellingsmomentopname	Apparaat-, inloggegevens-, document- en advertentiewaarnemingen gelezen op 21 november 2026; cumulatieve records, geen nieuwe incidenten uit 2026
Andere perioden	Vermeldingswaarnemingen beslaan 365 dagen tot 22 november 2026; waarnemingen van gelijkende domeinen beslaan 19 oktober–18 november 2026
Passieve momentopname	Openbare technische waarnemingen voor 249 van 250 kandidaten bij de afsluiting; elke maatregel gebruikt zijn eigen noemer
Overlap	Records kunnen overlappen tussen bronnen, domeinen en personen; merken en moedergroepen kunnen tussen vermeldingen overlappen

Onderdeel	Definitie
Reikwijdte	Externe blootstellingsrelaties plus openbare e-mail-, DNS-, certificaat- en webheaderwaarnemingen waar beschikbaar
Nationale Atlas-hoofdwaarde	50 op 100 voor deze geselecteerde portefeuille; sector- en organisatiebeoordelingen worden niet gepubliceerd

[S2]

De lijst is een vertrekpunt voor gerichte vragen van eigenaren. Zij bewijst niet dat elke vermelding dezelfde verantwoordelijkheden, verkeersvolumes, gegevensgevoeligheid of operationele zelfstandigheid heeft. Het openbare domein van een vervoerder en een groepsmerk kunnen heel andere relaties hebben met de systemen die hun diensten leveren.

Ook de registratiepopulatie van een toezichthouder verschilt van de financiële categorie in dit rapport. Het bankenregister van DNB omvat Nederlandse vergunninghouders en buitenlandse instellingen met een Europees paspoort. De geselecteerde categorie omvat daarnaast andere financiële activiteiten. Beschrijf haar niet als 25 Nederlandse vergunninghoudende banken of 25 kaartuitgevers. [S7]

3.2 Blootstellingssignalen per sector

De nationale Atlas-hoofdwaarde is 50 op een schaal van 0 tot 100. Hogere waarden wijzen op meer waargenomen externe blootstelling, geen geschatte kans op binnendringing. Zij beschrijft deze geselecteerde portefeuille en schat geen Nederlandse nationale prevalentie. De tabel toont hoeveel geselecteerde vermeldingen elk signaal hebben; de apparaat- en documentkolommen tellen vermeldingen, geen afzonderlijke records.

Sector	Kandidaten	Actuele advertenties	Werknemersapparaten	Documenten
Banken en financiën	25	11	16	13
Onderwijs	25	12	22	23
Energie en nutsbedrijven	20	10	12	11
Overheid	40	5	35	33
Zorg	25	2	21	13
Horeca en toerisme	10	10	8	5
Verzekeringen	15	3	10	10
Productie en industrie	20	4	14	13
Media en entertainment	5	2	4	2
Detailhandel en handel	15	9	12	11

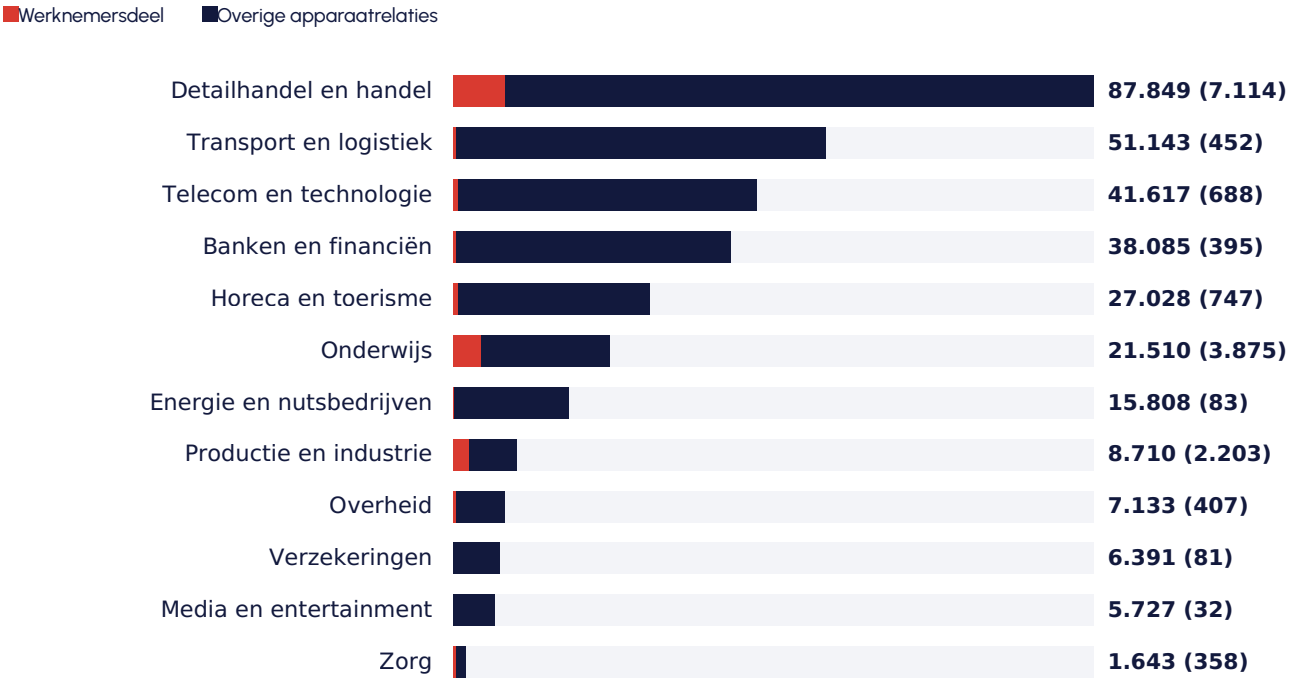
Sector	Kandidaten	Actuele advertenties	Werknemersapparaten	Documenten
Telecom en technologie	25	9	15	19
Transport en logistiek	25	7	21	17
Alle geselecteerde domeinen	**250**	**84**	**190**	**170**

[S2]

Alle tien horecavermeldingen hebben een actuele advertentie voor inloggegevens; de overheid heeft er vijf bij 40 geselecteerde vermeldingen. Deze aantallen ondersteunen accountvalidatie binnen de geselecteerde portefeuille. Zij tonen niet aan of een inloggegeven werkt, of MFA het beschermt of dat een instelling een inbraak ondervond.

De apparaat- en inloggegevensvolumes beschrijven een andere populatie dan de aantallen vermeldingen hierboven.

Handel en transport hebben de grootste aantallen apparaatrelaties binnen de geselecteerde portefeuille



Bron: Brandefense-blootstellingsrelaties, 250 geselecteerde kandidaatdomeinen, gelezen op 21 november 2026. Records zijn cumulatief en kunnen overlappen [S2].

Sector	Apparaatrelaties	Werknemersdeel	Inloggegevensrecords
Banken en financiën	38.085	395	178.904
Onderwijs	21.510	3.875	1.287.262

Sector	Apparaatrelaties	Werknemersdeel	Inloggegevensrecords
Energie en nutsbedrijven	15.808	83	88.963
Overheid	7.133	407	424.906
Zorg	1.643	358	276.856
Horeca en toerisme	27.028	747	163.266
Verzekeringen	6.391	81	120.004
Productie en industrie	8.710	2.203	438.927
Media en entertainment	5.727	32	9.451
Detailhandel en handel	87.849	7.114	1.173.918
Telecom en technologie	41.617	688	341.992
Transport en logistiek	51.143	452	232.483
Alle geselecteerde domeinen	**312.644**	**16.435**	**4.736.932**

[S2]

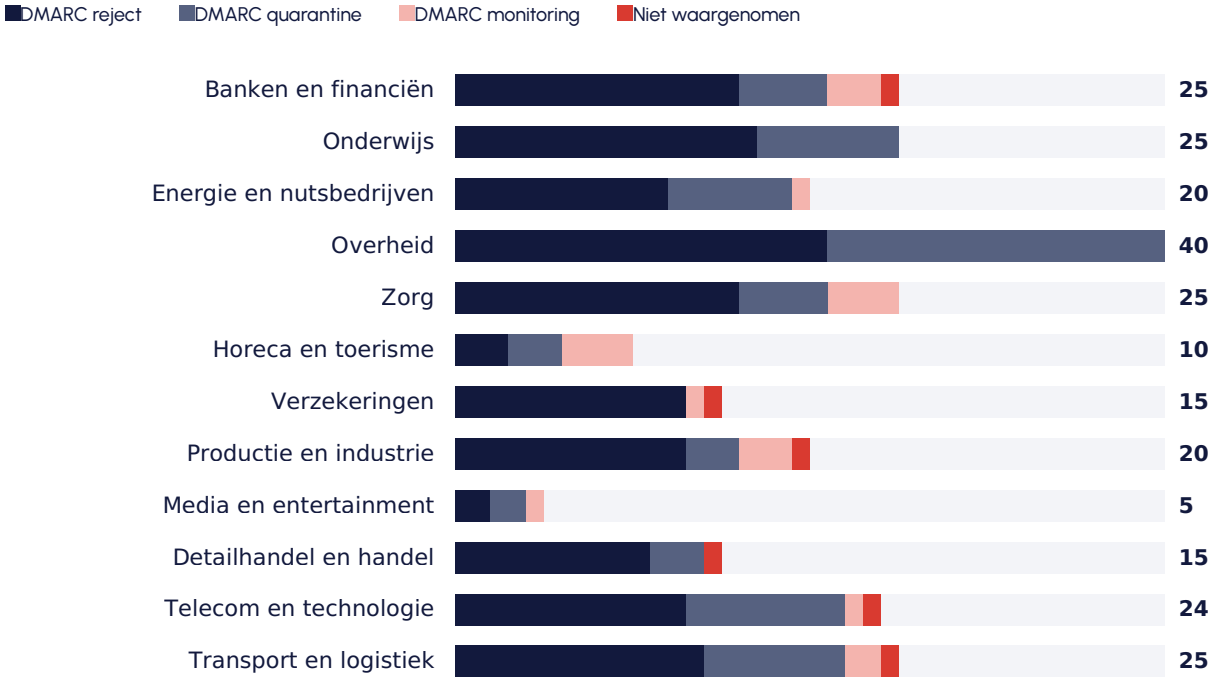
Apparaattotalen zijn ondergrenzen. Relaties met werknemersapparaten zijn opgenomen in het apparaattotaal en worden er niet bij opgeteld. Een apparaat dat met een klantendienst is verbonden, kan van een klant of andere externe gebruiker zijn. De relatie alleen toont geen toegang tot interne systemen van de instelling aan.

Inloggegevensrecords bestaan uit 2.263.427 records uit datalekdatabases, 454.417 stealerlogrecords en 2.019.088 records met combinaties van inloggegevens. Deze populaties kunnen overlappen en historisch materiaal bevatten. Handel levert 7.114 relaties met werknemersapparaten en onderwijs 3.875; accounteigendom vereist nog validatie, ook bij studenten- en klantaccounts. [S2]

De noemer maakt deel uit van het resultaat. Blootstellingswaarnemingen beslaan 250 geselecteerde vermeldingen; de passieve momentopname beslaat 249. De niet-beschikbare passieve kandidaat geldt niet als een falende maatregel. Een resultaat voor de ene populatie wordt niet stilzwijgend de noemer voor een andere.

3.3 E-mailauthenticatie vraagt een inventaris van bevoegde afzenders

DMARC-aantallen tonen gepubliceerd handhavingsbeleid in de geselecteerde sectorcategorieën



Bron: openbare technische waarnemingen voor 249 geselecteerde domeinen op de peildatum. Elke controle gebruikt haar eigen waarnemingsnoemer [S2].

Van de 249 waargenomen domeinen publiceren 151 een rejectbeleid, 72 een quarantinebeleid en 20 een monitoringbeleid; bij zes is geen beleid waargenomen. Handhaving is dus zichtbaar bij 223 waargenomen domeinen. Alle geselecteerde overheids- en onderwijsdomeinen publiceren handhavingsbeleid, tegenover zes van de tien horecadomeinen. Dit zijn resultaten voor geselecteerde domeinen, geen sectorprevalentie. [S2]

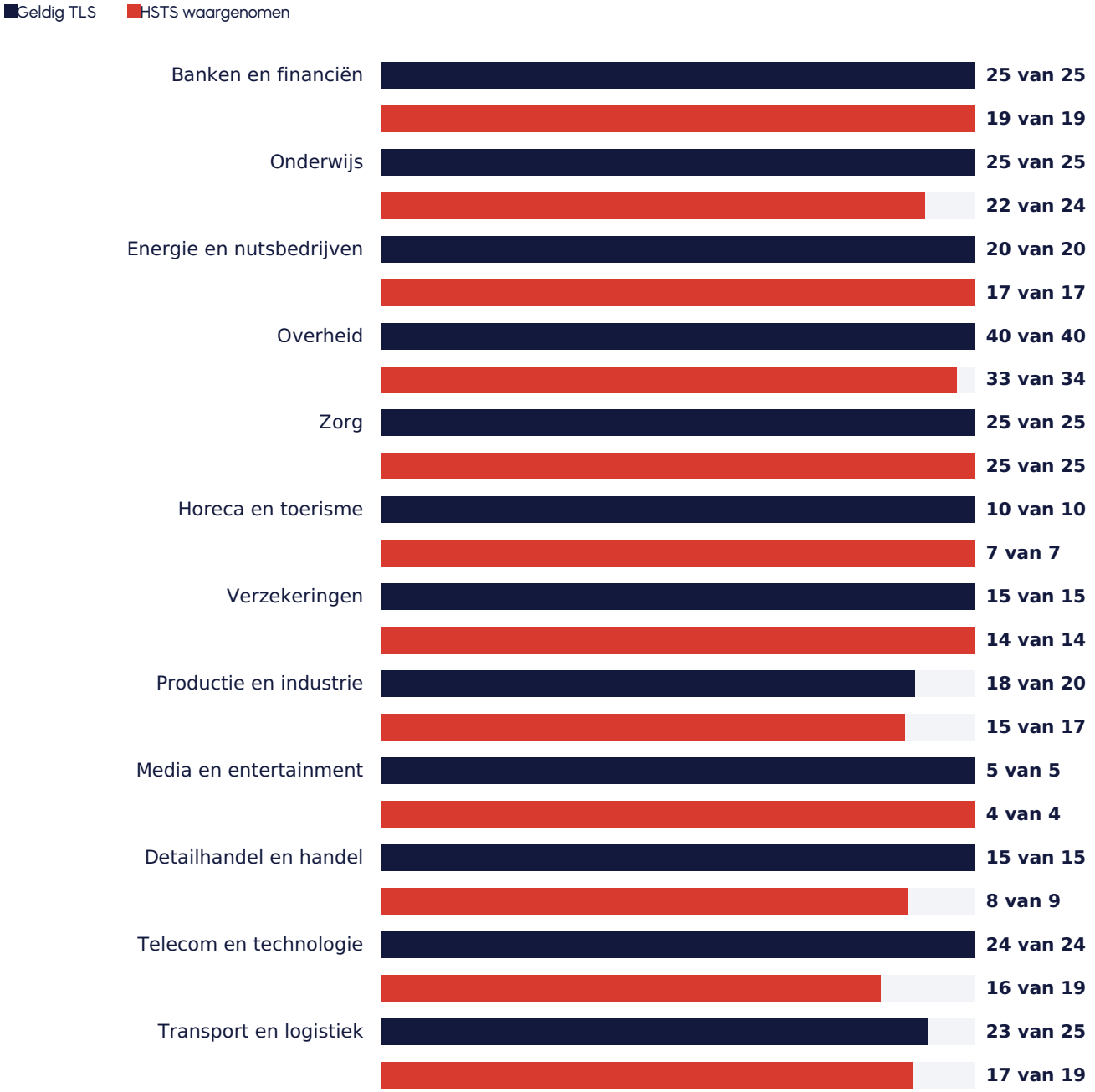
In dit rapport geldt een gepubliceerd quarantine- of rejectbeleid als waargenomen DMARC-handhaving. Monitoring is een andere toestand. [S85] Handhavingsbeleid bewijst niet dat elke legitieme afzender correct is ingesteld, ontvangers het altijd toepassen of andere imitatievormen worden voorkomen.

De beslissing voor de e-mailverantwoordelijke is daarom specifieker dan een beleidslabel wijzigen. Bepaal welke diensten namens het domein mogen verzenden en welke correct zijn uitgelijnd. Spreek een test en terugdraaiprocedure af voordat handhaving wordt uitgebreid. Een maatregel die legitieme dienstberichten afwijst, kan het beschermde bedrijfsproces schaden.

Het gevolg voor incidentrespons is even specifiek. Een klant met een overtuigend bericht kan te maken hebben met een gelijkende naam, een getroffen legitiem account of een telefonische benadering. Sterke authenticatie van het eigen domein maakt zulke meldingen niet irrelevant. Bewaar het bericht en stuur het naar de juiste onderzoeksroute.

3.4 Webcontinuïteit en beveiligingswaarnemingen beantwoorden verschillende vragen

TLS- en HSTS-waarnemingen gebruiken de domeinen waarvoor elk resultaat beschikbaar was



Bron: openbare technische waarnemingen voor 249 geselecteerde domeinen op de peildatum. Elke controle gebruikt haar eigen waarnemingsnoemer [S2].

De momentopname bevat 245 geldige TLS-resultaten, 2 mislukte resultaten en 2 onbesliste resultaten. De laatste categorieën tonen geen specifiek certificaatgebrek aan. Van de 208 waargenomen homepages hebben 197 HSTS. SPF verschijnt bij 238 waargenomen domeinen, DKIM bij 215 en een DS-record bij 182. [S2]

Certificaatgeldigheid is relevant voor de beoogde versleutelde verbinding van een gebruiker. Een resultaat moet een waargenomen ongeldig certificaat onderscheiden van een domein zonder bruikbaar resultaat. De eigenaar moet de dienst en certificaatketen bevestigen voordat het resultaat als productiegebrek wordt behandeld.

HSTS is een browserinstructie voor toekomstig HTTPS-gebruik. [S88] Waarneming op een bereikbare homepage beschrijft niet elke applicatie, elk subdomein of elk eerste bezoek. Een homepageheader is geen volledige beoordeling van de transportbeveiliging van een organisatie.

Niet-waargenomen DKIM bewijst niet dat het domein nooit e-mail ondertekent. SPF gaat over de bevoegdheid van verzendende hosts, niet over de legitimiteit van elk bericht. [S86][S87]

Ook DNSSEC vraagt precieze termen. Een DS-record bij een delegatie bewijst op zichzelf niet dat de volledige vertrouwensketen valideert. Houd bij een delegatieresultaat de waarneming en de validatieconclusie gescheiden. Een netwerkverantwoordelijke kan de bedoelde configuratie via het normale wijzigingsproces bevestigen.

3.5 Advertenties, gelijkende domeinen, documenten en vermeldingen vragen verschillende validatie

De 84 actuele advertenties beschrijven bij controle aangeboden inloggegevens, geen unieke personen of bevestigde inbraken. Valideer eigendom, ouderdom, accountstatus en sessieactiviteit via bevoegde incidentafhandeling. Historische records kunnen na herstel zichtbaar blijven; een actuele advertentie toont niet aan dat toegang nog werkt.

De momentopname bevat ook 36.644 waarnemingen van gelijkende domeinen en 1.888 relaties met blootgestelde documenten. Gelijkende namen kunnen losstaan van een merk; openbare documenten kunnen bewust gepubliceerd zijn. Geen van beide totalen telt bevestigde phishingsites of vertrouwelijke bestanden. Merk- en gegevenseigenaren moeten relevantie, toestemming en gevoeligheid vaststellen voordat zij handelen. [S2]

Vermeldingswaarnemingen beschrijven discussie en verspreiding, geen gevalideerde toegang of gemeenschappelijke operator. Beoordeel de onderliggende context en ondersteunend bewijs voordat u een vermelding aan een incident verbindt. Houd deze waarnemingen gescheiden van ransomwarevermeldingen en de berichtenpopulaties in hoofdstuk 4.

3.6 Maak van de waarneming een taak met een verantwoordelijke

Een bruikbaar kwestieregister benoemt het domein, de waargenomen toestand, de verantwoordelijke dienst, het validatieresultaat en de beslissing. Gevalideerde punten kunnen worden hersteld of als goedgekeurde uitzondering vastgelegd. Onduidelijk eigendom moet worden geëscaleerd; behandel het domein niet stilzwijgend als onaangetast.

KERNPUNTEN

01

De kandidaatdomeinlijst is een doelgerichte selectie met merk- en groepsoverlap.

02

Elke maatregel vereist een eigen bruikbare waarnemingsnoemer en validatie door de eigenaar.

03

Valideer actuele advertenties en signalen over werknemersapparaten zonder relaties als bevestigde inbraken te behandelen.

HOOFDSTUK 04

Wat de bewaarde ondergrondse berichten aantonen

DIT HOOFDSTUK BEANTWOORDT

Welke Nederland-gerelateerde aanbiedingen verdienen onderzoek en wat laat een bericht onbeslist?

5.160

bewaarde berichten binnen de genoemde reikwijdte, geen nationaal aanvalstotaal

4.1 Afbakeningskaart 23
4.2 Volume, platforms en taal 24
4.3 Thema's in de bewaarde deelverzameling 26
4.4 Zes gerichte berichtzaken 27
4.5 Doorplaatsingen en onderwijsclaims vragen data en inhoud 33
4.6 Aankondigingen van inloggegevens en vraagsignalen 37
4.7 Voorbeelden uitgesloten van Nederlandse incidentconclusies 39

HOOFDSTUK 04

Wat de bewaarde ondergrondse berichten aantonen

IN HET KORT

De bewaarde berichten bieden klantgegevens, vermeende toegang, identiteitsmateriaal en financiële accounts aan. Hun waarde ligt in een toetsbare bewering, niet alleen in het landlabel. Doorplaatsingen, materiaal over meerdere landen en onbewezen herkomst beperken de interpretatie. Lees iedere bewijskaart met haar beperkingen. Valideer de relevante gegevens, het account of de dienst voordat u beslist over incidentrespons, openbare reacties of klantbescherming.

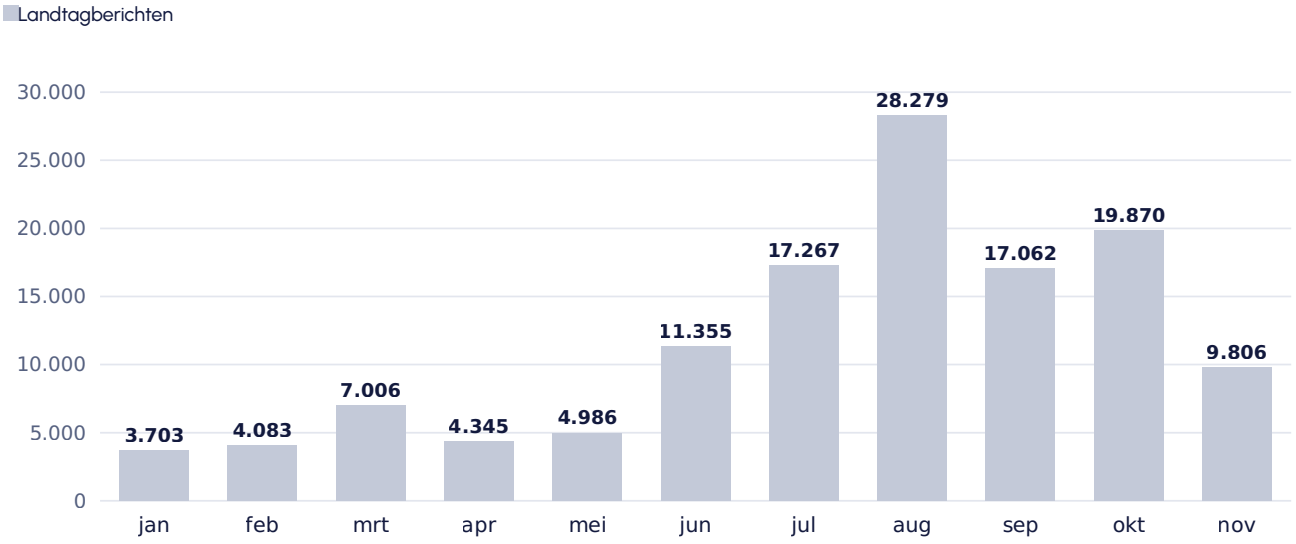
4.1 Afbakeningskaart

Onderdeel	Definitie
Periode	1 januari–22 november 2026, tot de momentopname op de peildatum
Landverband	Materiaal over Nederland, met een vermelding van Nederland of met een geclaimde band met Nederland
Bewaarde populatie	5.160 bewaarde berichten; 329 vallen in de recente periode van 8–22 november
Populatie met landtag	127.762 berichten in de tagtotalen; 3.286 bewaarde berichten dragen die tag
Basis voor thema en taal	De 3.286 bewaarde berichten met landtag; niet de volledige getagde populatie
Basis voor platform	De gezamenlijke verzameling van 5.160 bewaarde berichten
Eenheid	Een bericht, geen unieke verkoper, gegevensverzameling, transactie of incident
Beperking	Terloopse verwijzingen en producten met een landlabel tonen geen Nederlandse slachtoffers aan

[S1]

4.2 Volume, platforms en taal

Landtagtotalen beschrijven het maandelijkse berichtvolume; november is onvolledig

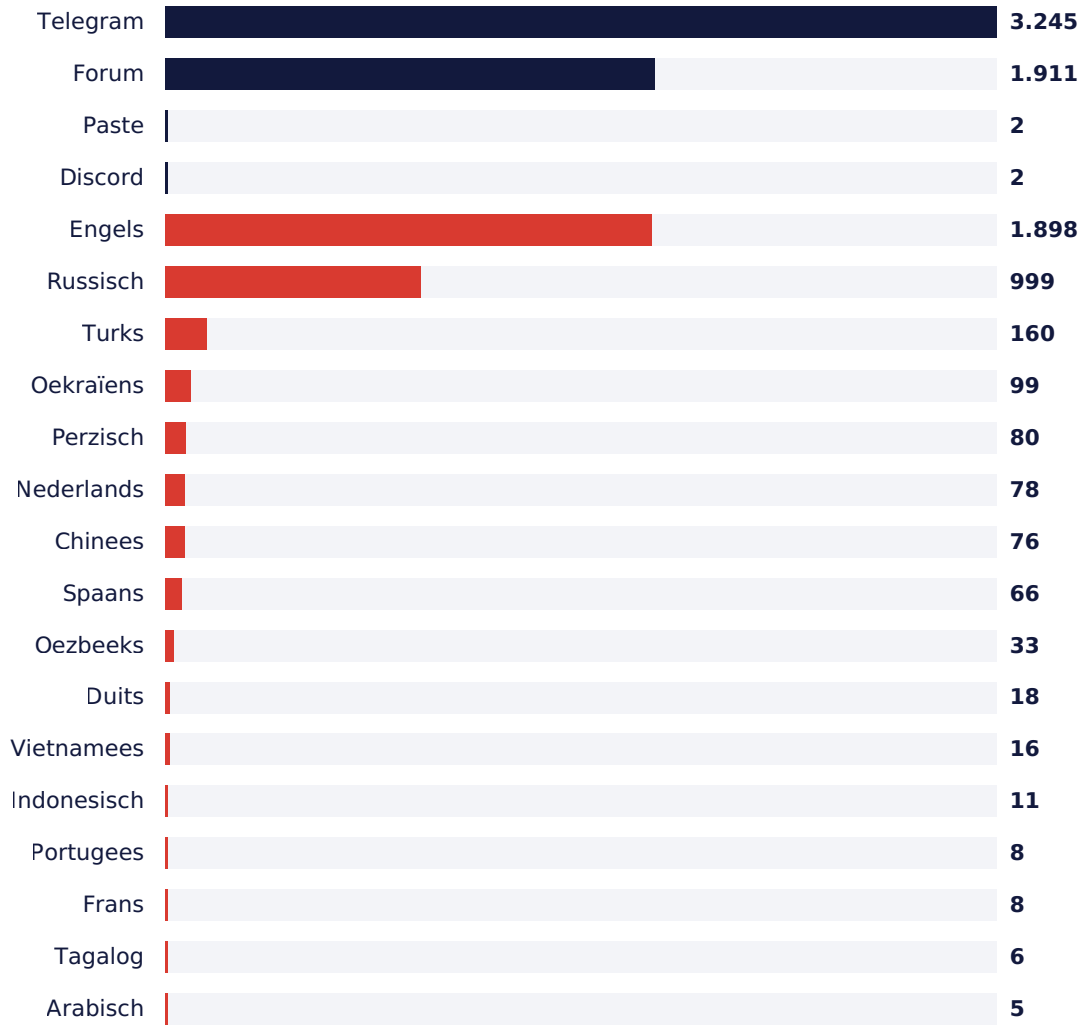


Bron: Brandefense Blackhole, 1 januari-22 november 2026; november onvolledig [S1].

Tagtotalen lopen van 3.703 in januari tot 28.279 in augustus; november is onvolledig. De bewaarde deelverzameling is geen volledige maandelijkse telling. Het verschil tussen deze populaties is geen aantal niet-criminele berichten. De tagreeks meet ook geen aanvalstrend. [S1]

Platforms en talen beschrijven de bewaarde deelverzameling, niet de Nederlandse bevolking





Bron: Brandefense Blackhole, 1 januari-22 november 2026; november onvolledig [S1].

Dimensie	Bewaard resultaat	Basis en beperking
Telegram	3.245	Van 5.160 bewaarde berichten
Forums	1.911	Van 5.160 bewaarde berichten
Paste / Discord	2 / 2	Van 5.160 bewaarde berichten
Engels	1.898	Van 3.286 bewaarde berichten met landtag
Russisch	999	Dezelfde basis; taal toont geen nationaliteit aan
Turks / Nederlands	160 / 78	Dezelfde basis; taaltoewijzingen kunnen overlappen

[S1]

4.3 Thema's in de bewaarde deelverzameling

Thema's beschrijven geadverteerde activiteit in 3.286 bewaarde tagberichten; categorieën overlappen



Basis: 3.286 bewaarde landtagberichten; categorieën kunnen overlappen. Bron: Brandefense Blackhole, 1 januari–22 november 2026; november onvolledig [S1].

Thema	Berichten	Thema	Berichten
Handel in financiële accounts	1.000	Identiteit en verificatie	432
Phishing en fraude	443	Kaartmateriaal	431
Gegevens- en databaseaan-biedingen	343	Verwijzingen naar malware/ kwetsbaarheden	198
Combinaties van inloggege-vens	83	Toegangsaanbiedingen	76
Verwijzingen naar stealerlogs	50	Verwijzingen naar DDoS/ hacktivisme	14
Ransomwareverwijzingen	5		

[S1]

Categorieën kunnen overlappen en terloopse landvermeldingen blijven mogelijk. Ze mogen niet worden opgeteld tot unieke incidenten of geëxtrapoleerd naar een Nederlands markttotaal. Een geadverteerd product is ook niet noodzakelijk afkomstig uit een datalek. Een contactlijst met een banknaam kan van een partner, openbaar materiaal of een ongerelateerde oudere gegevensverzameling komen.

4.4 Zes gerichte berichtzaken

A

CASE A

Een identiteitsgegevensaanbod met telecomlabel

Bewijskaart B01 | 19 feb 2026 | Forumdiscussie | Telecommunicatie

Claim niet geverifieerd

CLAIM	Een verkoper biedt op 19 februari een gegevensverzameling met het label van een Nederlandse telecomaanbieder aan: 5,8 miljoen records en 1,3 miljoen scans van identiteitsdocumenten. De velden bevatten identificerende, contact- en financiële informatie.
VASTGESTELD	De advertentie bestaat. De aantallen komen van de verkoper en zijn geen bevestigde getroffen populatie. Dit rapport koppelt het aanbod niet aan een bij naam genoemd, bevestigd telecomincident.
ALTERNATIEVEN EN BEPERKINGEN	Echt materiaal, samenvoeging, hergebruikte gegevens of onjuiste beschrijving blijven mogelijk. Herkomst, ouderdom, unieke personen, beschikbaarheid van documenten en een verkoop zijn niet geverifieerd.
REACTIE	Laat de bevoegde gegevenseigenaar een geloofwaardig signaal beoordelen. Klantmedewerkers moeten identiteit via een bestaande route verifiëren, niet via de kennis van basisgegevens van de beller.

Conclusie

Controleer de genoemde gegevensvelden en accounts voordat een advertentie als nieuw incident wordt behandeld.

Bewijskaart B01 19 feb 2026

Verkoper van gegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

[Dutch telecom provider] DATALEAK NL 5.8 MIL & 1.3 MIL ID/PASSPORT SCANS [...] -Full Name -Address -DOB -Phonen -[email field] -IBAN -BSN [...] [contact removed]

VERTALING

[Nederlandse telecomaanbieder] DATALEK NL 5,8 MILJOEN & 1,3 MILJOEN SCANS VAN IDENTITEITSBEWIJZEN/PASPOORTEN [...] -Volledige naam -Adres -Geboortedatum -Telefoonnummer -[e-mailveld] -IBAN -BSN [...] [contactgegevens verwijderd]

Opmerking. De geadverteerde aantallen verschillen tussen latere berichten. Het zijn claims van de verkoper, geen bevestigd aantal getroffen personen.

Vastgesteld
Een aanbod dat een Nederlandse telecomaanbieder noemt en identiteitsgegevens en aantallen claimt.

Niet vastgesteld
Echtheid, herkomst, verzamelingsdatum, aantal unieke personen, beschikbaarheid van documenten, een verkoop of een bevestigd datalek.

CASE B

B

Patiënttabellen en vermeende beheerderstoegang

Bewijskaart B02 8 nov 2026 Forumdiscussie Zorg

Claim niet geverifieerd

CLAIM	Op 8 november biedt een verkoper drie gekoppelde tabellen aan met patiëntcontacten, afspraakverzoeken en factureringsaccounts, naast vermeende beheerderstoegang en een vraagprijs van USD 4.650.
VASTGESTELD	Het bericht beschrijft een aanbod. Consolebeelden bewijzen niet onafhankelijk de genoemde dienstrelatie, geldige toegang, omvang van de gegevensverzameling of gevolgen voor de zorg.
ALTERNATIEVEN EN BEPERKINGEN	Een ongerelateerde dienst, gedeeltelijke export, oude toegang of vervalst bewijs blijven mogelijk. Een verkoop of geslaagde controle over een zorgdienst is niet vastgesteld.
REACTIE	Valideer de dienst- en gegevensrelatie voordat u gevolgen voor patiënten bekendmaakt. Betrek de gegevenseigenaar en het incidentteam zonder de technische beschrijving van de adverteerder als juist aan te nemen.

Conclusie

Controleer de relatie met de dienst en het accountbewijs; tabellen met patiëntgegevens tonen geen gevolgen voor de zorg aan.

Bewijskaart B02 8 nov 2026

Verkoper van zorggegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

The file I'm selling came out of [healthcare service domain]. It covers Patient Contacts, Patient Appointment Requests and Patient Billing Accounts and is split across 3 tables. [...] Price: $4,650 [...] [contact removed]

VERTALING

Het bestand dat ik verkoop is afkomstig van [domein van een zorgdienst]. Het bevat contactgegevens van patiënten, afspraakverzoeken en factureringsaccounts van patiënten, verdeeld over 3 tabellen. [...] Prijs: $4.650 [...] [contactgegevens verwijderd]

Vastgesteld
Op 8 november biedt een verkoper drie gekoppelde tabellen met patiëntgegevens, vermeende beheerderstoegang en een vraagprijs aan.

Niet vastgesteld
De relatie tussen de genoemde dienst en het bedrijf, echtheid van de consolebeelden, herkomst, geldigheid van de toegang, omvang van de gegevensverzameling, gevolgen voor de zorg of een verkoop.

CASE C

C

Een online-retailexport met walletvelden

Bewijskaart B03 | 18 okt 2026 | Forumdiscussie | Detailhandel

Claim niet geverifieerd

CLAIM	Een bericht van 18 oktober met het label Nederland biedt contact-, account-, bestel- en walletvelden aan, met vermeende voorbeeldrijen.
VASTGESTELD	De veldlijst en advertentie zijn zichtbaar. Een veld voor een walletsaldo toont geen bruikbare wallettoegang of volledige klantgegevensverzameling aan.
ALTERNATIEVEN EN BEPERKINGEN	Openbare of partnergegevens, oudere exports en synthetische records blijven alternatieven. Het bericht toont geen unieke klanten, actualiteit of herkomst bij de winkel aan. Een verband met het bevestigde retailincident in hoofdstuk 5 is niet vastgesteld.
REACTIE	Vergelijk een geloofwaardig signaal via geautoriseerde kanalen met bekende schema's en eerdere incidenten. Behandel toegang tot betaalaccounts als een afzonderlijke bewering die eigen bewijs vereist.

Conclusie

Namen van walletvelden tonen niet aan dat iemand geld kan verplaatsen.

Bewijskaart B03 18 okt 2026

Verkoper van retailgegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

[online retailer] Netherlands [...] user_id,full_name, email, contact_phone, street_address, city, postal_code [...] orders_count [...] wallet_balance_minor [...] [sample rows removed]

VERTALING

[onlinewinkel] Nederland [...] user_id, full_name, email, contact_phone, street_address, city, postal_code [...] orders_count [...] wallet_balance_minor [...] [voorbeeldrijen verwijderd]

Vastgesteld

Een bericht over retailgegevens met het label Nederland biedt velden voor contactgegevens, accounts, bestellingen en wallets aan, met vermeende voorbeeldrijen.

Niet vastgesteld

Herkomst, echtheid, volledigheid, aantal unieke klanten, actualiteit, toegang tot wallets of de vraag of de gegevens van de winkel afkomstig zijn.

D

CASE D

RDWEB-toegang in de softwaresector

Bewijskaart B04 | 3 apr 2026 | Forumdiscussie | Softwarediensten

Claim niet geverifieerd

CLAIM	Een aanbod van 3 april noemt Nederland, softwareoplossingen en RDWEB-toegang, met onbekende omzet en een prijs waarvoor biedingen welkom zijn.
VASTGESTELD	Er bestaat een toegangsaanbod. De zichtbare beschrijving bewijst geen organisatie-identiteit, werkende sessie of bevoegdheidsniveau.
ALTERNATIEVEN EN BEPERKINGEN	Verouderde, gedeeltelijke, onbevoegde of verzonnen toegang blijven mogelijk. De toegangsroute en een verkoop zijn onbekend.
REACTIE	Controleer eigen gateways voor beheer op afstand, bevoegde gebruikers en actuele toegangssignalen. Een aanbeveling voor sterke authenticatie bewijst niet dat het ongenoemde doelwit die miste.

Conclusie

Controleer de aangeboden toegang en de autorisatie voordat een anoniem landenlabel wordt opgeschaald.

Bewijskaart B04 3 apr 2026

Verkoper van toegang (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Country: Netherlands Revenue: Unknown Industry: Software Solutions access: RDWEB price: $$$ open for offers [...] [contact removed]

VERTALING

Land: Nederland Omzet: onbekend Sector: softwareoplossingen Toegang: RDWEB Prijs: $$$ biedingen welkom [...] [contactgegevens verwijderd]

Vastgesteld
Een aanbod noemt expliciet Nederland, softwareoplossingen en RDWEB-toegang. Biedingen zijn welkom.

Niet vastgesteld
Identiteit van de organisatie, toestemming, werkende toegang, bevoegdheidsniveau, actualiteit, toegangsroute of een verkoop.

CASE E

E

Forex-contactleads met financiële velden

Bewijskaart B05 | 30 jul 2026 | Forumdiscussie | Financiële contactgegevens

Claim niet geverifieerd

CLAIM	Een bericht van 30 juli biedt een forex-contactlijst met Nederlands label en 230.000 rijen aan voor USD 350, met contact-, valuta- en stortingsvelden.
VASTGESTELD	De verkoper geeft een voorgesteld product een label en prijs. De velden bewijzen geen werkelijke saldi of gegevensverlies bij een achterliggende broker.
ALTERNATIEVEN EN BEPERKINGEN	Samengevoegde marketinggegevens, oudere records of onjuiste labels blijven mogelijk. Unieke personen, echtheid, herkomst en afgeronde verkoop zijn onbeslist. Het latere crypto-aanbod in hoofdstuk 8 is niet vastgesteld als hetzelfde bestand.
REACTIE	Fraudeteams moeten rekening houden met benaderingen op basis van vermeende financiële interesses. Valideer wel de specifieke gegevensverzameling voordat de herkomst wordt toegeschreven.

Conclusie

Contactvelden en informatie over stortingen kunnen misleiding ondersteunen; herkomst en saldi blijven ongeverifieerd.

Bewijskaart B05 30 jul 2026

Verkoper van leadgegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Netherland Forex Consumer Database 230k Price $350 [...] COUNTRY CURRENCY EMAIL NAME PHONE DEPOSITES AMOUNT [...] [sample rows removed]

VERTALING

Nederlandse forex-consumentendatabase 230.000 Prijs $350 [...] LAND VALUTA E-MAIL NAAM TELEFOON STORTINGSBEDRAG [...] [voorbeeldrijen verwijderd]

Vastgesteld
Een aanbod bestempelt een forex-consumentenlijst met 230.000 rijen als Nederlands en noemt $350 en financiële en contactvelden.

Niet vastgesteld
Echtheid van de records, de achterliggende broker, verzamelingsdatum, aantal unieke personen, rechtmatige herkomst, saldi of een afgeronde verkoop.

CASE F

F

Een lijst met camera-inloggegevens met Nederlands label

Bewijskaart B06 | 23 aug 2026 | Forumdiscussie | Verbonden camera's

Claim niet geverifieerd

CLAIM	Een discussie uit augustus biedt inloggegevens en momentopnamelinks aan voor 474 camera's die in Nederland zouden staan.
VASTGESTELD	Het bericht toont een claim met een aantal. Het bewijst geen locaties, eigendom, huidige bereikbaarheid of werkende inloggegevens.
ALTERNATIEVEN EN BEPERKINGEN	Oude, onjuist gelokaliseerde of ongeldige records blijven mogelijk. Fysieke gevolgen en toegang tot industriële besturingen zijn niet vastgesteld. Het bericht is niet gekoppeld aan de officiële cameracampagne in hoofdstuk 7.
REACTIE	Een eigenaar met een geloofwaardig, apparaatspecifiek signaal moet dit valideren en beheer op afstand controleren. Leid uit een ongeverifieerde lijst geen nationaal incident met besturingssystemen af.

Conclusie

Een advertentie met camerainloggegevens toont geen industriële besturing of fysieke gevolgen aan.

Bewijskaart B06 — 23 aug 2026

Uploader op een forum (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

474 cameras in Netherlands IP:PORT,USER,PASS with snapshot links [...]

VERTALING

474 camera's in Nederland IP:POORT,GEBRUIKER,WACHTWOORD met links naar momentopnamen [...]

Vastgesteld
Een forumdiscussie claimt een lijst met inloggegevens voor Nederlandse camera's, links naar momentopnamen en een aantal van 474.

Niet vastgesteld
Locaties of eigendom van camera's, huidige bereikbaarheid, geldige inloggegevens, fysieke gevolgen of een inbraak in industriële besturingssystemen.

4.5 Doorplaatsingen en onderwijsclaims vragen data en inhoud

B07 verspreidt een databasebeschuldiging over een technologiebedrijf; herhaling van een vergelijkbaar thema toont geen nieuwe inbraak aan. B24 dateert de onderliggende broncodebeschuldiging expliciet op oktober 2025, hoewel het bericht uit augustus 2026 komt. Behandel verspreidingsdatum en inbraakdatum afzonderlijk. [S1]

Bewijskaart B07 1 jun 2026

Doorplaatser op een forum (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Today i am leaking [technology company domain] ~154 DB's. [...] The files will be in .SQL extensions [...] The compromissed data are: - Disk Encryption keys - users - software, and etc. - devices [...]

VERTALING

Vandaag lek ik ongeveer 154 databases van [domein van een technologiebedrijf]. [...] De bestanden hebben de extensie .SQL [...] De buitgemaakte gegevens zijn: - schijfversleutelingssleutels - gebruikers - software, enzovoort - apparaten [...]

Opmerking. Een vergelijkbaar databasethema komt voor in eerder bewaarde berichten. Herhaling toont geen nieuw incident aan.

Vastgesteld
Een forumposter verspreidt een databaseclaim over een technologiebedrijf, met een vermeend aantal bestanden en gegevenscategorieën.

Niet vastgesteld
Echtheid, eerste publicatie, verzamelingsdatum, geldigheid van sleutels, getroffen systemen of een nieuwe inbraak in 2026.

Bewijskaart B24 21 aug 2026

Doorplaatser op een forum (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Today I have uploaded [software company] Data Breach for you to download [...] In October 2025, [software company] suffered a data breach and had their source code [...] [links removed]

VERTALING

Vandaag heb ik het datalek van [softwarebedrijf] geüpload zodat jullie het kunnen downloaden [...] In oktober 2025 kreeg [softwarebedrijf] te maken met een datalek en werd de broncode [...] [links verwijderd]

Opmerking. Het bericht dateert het vermeende incident op oktober 2025. Het toont latere verspreiding aan, geen nieuwe gebeurtenis in 2026.

Vastgesteld
Een forumbericht uit augustus 2026 verspreidt opnieuw een broncodeclaim over een softwarebedrijf en dateert die expliciet op oktober 2025.

Niet vastgesteld
Echtheid, oorspronkelijke publicatie, inhoud, een nieuw incident in 2026 of een verband met andere broncodeaanbiedingen.

Ook onderwijsmateriaal verschilt. B08 biedt materiaal aan onder een universitaire broncode-/lektitel, zonder de bestandsinhoud vast te stellen. B09 noemt onderwijsrecords relevant voor 2023. B10 beschrijft professionele adresvelden die niet zelfstandig een inbraak aantonen. Geen van deze berichten kan eenvoudig bij de bevestigde Canvas-zaak worden opgeteld. [S1]

Bewijskaart B08 — 31 jan 2026

Uploader op een forum (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Today I have uploaded [university domain] data breach for you to download [...] [data-description label] Tree Download [...] [links removed]

VERTALING

Vandaag heb ik het datalek van [universiteitsdomein] geüpload zodat jullie het kunnen downloaden [...] [label met gegevensbeschrijving] Download van de boomstructuur [...] [links verwijderd]

Opmerking. Het zichtbare bericht toont niet aan wat de bestanden bevatten.

Vastgesteld
Een forumdiscussie noemt een Nederlandse universiteit en biedt materiaal aan onder een titel over broncode of een lek.

Niet vastgesteld
Inhoud van de bestanden, exfiltratie, echtheid van de broncode, datum van de inbraak of getroffen gebruikers.

Bewijskaart B09 — 1 feb 2026

Verkoper van onderwijsgegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Data includes: ID;Voornaam;Voorletters;Tussenvoegsel;Naam;GeboorteDatum [...] BIC;IBAN [...] OuderEmail [...] BSNouder [...] Records: 1.338.803 [...] Relevance: 2023 [...] [sample rows removed]

VERTALING

Gegevens omvatten: ID;Voornaam;Voorletters;Tussenvoegsel;Naam;GeboorteDatum [...] BIC;IBAN [...] OuderEmail [...] BSNouder [...] Records: 1.338.803 [...] Relevant voor: 2023 [...] [voorbeeldrijen verwijderd]

Opmerking. De verkoper noemt het materiaal relevant voor 2023. Een publicatiedatum in 2026 is geen nieuwe incidentdatum.

Vastgesteld
Een forumaanbod uit 2026 biedt onderwijsgerelateerde persoonsgegevens en ouder- en accountvelden aan en vermeldt expliciet dat de gegevens relevant zijn voor 2023.

Niet vastgesteld
Herkomst, echtheid, aantal unieke personen, samenhang tussen de geadverteerde aantallen records en e-mailadressen of een nieuw datalek in 2026.

Bewijskaart B10 — 10 mei 2026

Forumposter (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

BEWARE OF FAKE CLAIMS/FAKE ACCOUNTS [...] Target: [research organisation] Type: Academic / Research Institution User Database Fields: UID, Email, Title, Initials, Prefix, Surname, Function, Telephone, Discipline, Organisation, Department, Address [...] [sample rows removed]

VERTALING

PAS OP VOOR VALSE CLAIMS/NEPACCOUNTS [...] Doelwit: [onderzoeksorganisatie] Type: database van een academische instelling/onderzoeksinstelling Gebruikersvelden: UID, e-mail, titel, initialen, tussenvoegsel, achternaam, functie, telefoon, vakgebied, organisatie, afdeling, adres [...] [voorbeeldrijen verwijderd]

Vastgesteld
Een bericht biedt een adressenbestand met het label van een onderzoeksorganisatie en professionele contactvelden aan.

Niet vastgesteld
Het aantal uit de titel, of de velden uit een openbare adressenlijst komen, herkomst, actualiteit of een inbraak.

Het retailaanbod voor Nederland en België in B11 stelt een andere grens. De geadverteerde tabelvelden tonen geen bruikbare betaaltokens of verdeling van unieke klanten tussen landen aan. Landlabels en veldnamen ondersteunen een onderzoeksvraag, niet het antwoord. [S1]

Bewijskaart B11 — 3 mei 2026

Verkoper van retailgegevens (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

[online retailer] [~530k Netherlands and Belgium exports] [...] The dataset is organized into six main sections [...] user_id, account_ref, email, phone_mask [...] order_id, user_id, order_date [...] payment_id, order_id, payment_token [...] [contact removed]

VERTALING

[onlinewinkel] [ongeveer 530.000 exports uit Nederland en België] [...] De gegevensverzameling is ingedeeld in zes hoofdonderdelen [...] user_id, account_ref, email, phone_mask [...] order_id, user_id, order_date [...] payment_id, order_id, payment_token [...] [contactgegevens verwijderd]

Vastgesteld
Een verkoper biedt een retailexport voor Nederland en België aan met tabelvelden voor accounts, bestellingen en betalingen.

Niet vastgesteld
Echtheid, bruikbaarheid van tokens, aantal unieke Nederlandse klanten, verdeling per land, herkomst of datum van de inbraak.

4.6 Aankondigingen van inloggegevens en vraagsignalen

B12 kondigt een bestand met 328 regels gecombineerde inloggegevens aan en noemt een marktplaats. B13 kondigt twee webmailregels aan. Geen van beide bewijst geldige accounts, een diefstalmethode of een inbraak bij de genoemde dienst. B14 is een koopverzoek voor logs en cookies uit meerdere landen; vraag bewijst geen aanbod of werkende sessies. [S1]

Bewijskaart B12 — 11 aug 2026

Geautomatiseerde uploader (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

[marketplace domain]-results Uploaded by [automated uploader] [...] Total Lines: 328 Content Type: Email / Password Combo Date Uploaded: 2026-08-11 [...] [credential sample removed]

VERTALING

[marktplaatsdomein]-resultaten Geüpload door [geautomatiseerde uploader] [...] Totaal aantal regels: 328 Inhoudstype: combinatie van e-mail en wachtwoord Uploaddatum: 2026-08-11 [...] [voorbeeld met inloggegevens verwijderd]

Vastgesteld
Een geautomatiseerde forumuploader kondigt een bestand met 328 regels aan dat een Nederlandse marktplaatsdienst noemt.

Niet vastgesteld
Geldigheid of ouderdom van de inloggegevens, aantal unieke accounts, oorspronkelijke diefstalmethode of een inbraak bij de dienst zelf.

Bewijskaart B13 — 26 jun 2026

Geautomatiseerde uploader (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

[webmail domain] Uploaded by [automated uploader] [...] Total Lines: 2 Content Type: URL / Email / Password Combo Date Uploaded: 2026-06-26 [...] [credential sample removed]

VERTALING

[webmaildomein] Geüpload door [geautomatiseerde uploader] [...] Totaal aantal regels: 2 Inhoudstype: combinatie van URL, e-mail en wachtwoord Uploaddatum: 2026-06-26 [...] [voorbeeld met inloggegevens verwijderd]

Vastgesteld
Een geautomatiseerde forumuploader kondigt twee regels met URL, gebruikersnaam en wachtwoord aan die een Nederlandse webmailinlog noemen.

Niet vastgesteld
Geldigheid, ouderdom, eigendom van accounts, diefstalmethode, aantal unieke personen of een datalek bij de mailaanbieder.

Bewijskaart B14 2 sep 2026

Koper van logs (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Buying [marketplace] logs. I pay well and on time. [...] Interested in the following GEOs: [...] Netherlands [...] If anyone can recommend reliable suppliers of [marketplace] logs,cookies, I'll also reward you financially. [...] [contact removed]

VERTALING

Ik koop logs van [marktplaats]. Ik betaal goed en op tijd. [...] Geïnteresseerd in de volgende landen: [...] Nederland [...] Als iemand betrouwbare leveranciers van logs en cookies van [marktplaats] kan aanbevelen, geef ik daar ook een financiële beloning voor. [...] [contactgegevens verwijderd]

Vastgesteld
Een koper zoekt expliciet logs en cookies van een marktplaats voor meerdere landen, waaronder Nederland.

Niet vastgesteld
Aanbod, verworven logs, geldige sessies, getroffen gebruikers of een inbraak bij de aanbieder.

4.7 Voorbeelden uitgesloten van Nederlandse incidentconclusies

B22 heeft een titel met Nederlands label maar een onsamenhangend identificatorfragment; het landverband is niet vastgesteld. B23 beschrijft een buitenlands adviesbureau als onder Nederlandse leiding, wat geen Nederlands slachtoffer aantoont. Beide blijven zichtbaar om de grens uit te leggen en tellen niet mee in Nederlandse incidentconclusies. [S1]

Bewijskaart B22 2 mei 2026

Forumposter (alias weggelaten) Forumdiscussie Forum

Indonesisch origineel; bewaarde Engelse vertaling geciteerd

ORIGINEEL

DATABASE [technology company] (NETHERLANDS) [...] NIK (National Identification Number) [...] [sample identifiers removed]

VERTALING

DATABASE [technologiebedrijf] (NEDERLAND) [...] NIK (nationaal identificatienummer) [...] [voorbeeldidentificatoren verwijderd]

Opmerking. Het fragment is een bewaarde Engelse vertaling van een Indonesischtalig bericht. Het verband met Nederland is niet vastgesteld; het bericht telt niet mee als Nederlands incident.

Vastgesteld

Een forumtitel koppelt de naam van een technologiebedrijf aan Nederland; het zichtbare voorbeeld is slechts een fragment met identificatoren onder het label NIK.

Niet vastgesteld

Een verband tussen die identificatoren en het genoemde bedrijf, herkomst van de gegevens, een Nederlandse populatie of een inbraak.

Bewijskaart B23 9 nov 2026

Verkoper van toegang (alias weggelaten) Forumdiscussie

Forum Engels

ORIGINEEL

Target Organization: [overseas consultancy] [...] [nationality descriptor removed] [...] based in [location outside Netherlands] [...] Environment: [file-transfer platform] Teams Dashboard [...] Access Parameters: Active verified session. [...] Available Assets: 112.8 GB [...] Fixed Price: $400 USD [...] [contact removed]

VERTALING

Doelorganisatie: [adviesbureau in het buitenland] [...] gevestigd buiten Nederland [...] Omgeving: Teams Dashboard van [platform voor bestandsoverdracht] [...] Toegangsparameters: actieve geverifieerde sessie. [...] Beschikbaar materiaal: 112,8 GB [...] Vaste prijs: $400 USD [...] [contactgegevens verwijderd]

Opmerking. Dat een organisatie in het buitenland als onder Nederlandse leiding wordt beschreven, toont geen Nederlands incident aan. Dit bericht telt daarin niet mee.

Vastgesteld

Een toegangsaanbod van 9 november beschrijft een adviesbureau in de VAE als onder Nederlandse leiding en biedt een cloudsessie en bestanden aan.

Niet vastgesteld

Geldige toegang, een Nederlands slachtoffer of Nederlandse gegevens, rechtmatig eigendom, omvang van de gegevens of een geslaagde verkoop.

Medewerkers moeten verdacht materiaal via bevoegde beveiligingsprocessen doorgeven, in plaats van verkopers te benaderen of zomaar gevoelige bestanden te verkrijgen. De politiewaarschuwing van november raadt deelname aan criminele handelsplatforms af. Dat is preventiecontext, geen aantal getroffen gebruikers. Openbare kaarten laten contactroutes, persoonsgegevens en werkende indicatoren weg. [S70]

KERNPUNTEN

01

Een bericht toont eerder een aanbod of claim aan dan een incident.

02

Stuur elke bewering naar de eigenaar die de gegevens, het account of de dienst kan valideren.

03

Doorplaatsingen, gemengde landaanbiedingen en onbewezen landlabels vereisen expliciete grenzen en beoordelingen.

HOOFDSTUK 05

Bevestigde incidenten, leveranciersafhankelijkheden en recente activiteit

DIT HOOFDSTUK BEANTWOORDT

Wat stelden organisaties of overheden vast en welke beslissingen blijven specifiek voor iedere getroffen dienst?

12

uitgewerkte incident- en campagnezaken in hoofdstukken 5, 6 en 8

5.1 Wat als bevestiging geldt 42
5.2 Telecommunicatie: het account en het klantrecord 43
5.3 Openbaar bestuur: misbruik, toegang en indamming 44
5.4 Zorg: heraansluiting is ook een klinische beslissing 46
5.5 Reizen en horeca: een echte boeking kan een vals betaalverzoek ondersteunen 47
5.6 Onderwijs: het leveranciersincident en de universitaire reactie 48
5.7 Retail, websites en andere onbesliste grenzen 49
5.8 Recente activiteit: 8–22 november 49

HOOFDSTUK 05

Bevestigde incidenten, leveranciersafhankelijkheden en recente activiteit

IN HET KORT

Het bevestigde bewijs omvat klantgegevensdiefstal, toegang bij overheden, zorg- en onderwijsafhankelijkheden, verenigingssoftware en blootgestelde besturingen. Elke zaak heeft een andere reikwijdte en herstelvraag. Onderzoek, leveranciersverklaringen of gepubliceerde aanvallersclaims bewijzen niet ieder vervolgeffect. Lees bevestigde feiten en open vragen afzonderlijk. Stel de eigen gegevens- en dienstgevolgen vast voordat u een andere incidentbeschrijving overneemt of een gedeelde koppeling herstelt.

5.1 Wat als bevestiging geldt

Een bevestigd incident vereist hier een verklaring van de organisatie of een overheid die een aanval of onbevoegde toegang vaststelt. Alleen een crimineel bericht of een vermelding blijft een claim. Naamgeving vereist daarnaast officiële bevestiging en brede berichtgeving; zonder die voorwaarde blijven algemene beschrijvingen passend.

De uitgewerkte zaken zijn geen nationaal incidentaantal. Een campagne kan meerdere organisaties treffen en een update kan maanden later dezelfde gebeurtenis beschrijven. Leveranciersincidenten kunnen meerdere klantmeldingen opleveren. Daarom vermeldt dit hoofdstuk relaties en data zonder ze op te tellen tot unieke slachtoffers.

De zaken scheiden ook indamming van schade. Het loskoppelen van een systeem toont een verdedigende handeling aan. Het bewijst niet dat het systeem versleuteld was, alle gekoppelde klanten gegevens verloren of nog geen gegevens waren verdwenen. Elke conclusie vereist eigen ondersteunend bewijs.

5.2 Telecommunicatie: het account en het klantrecord

CASE G

G

Odido-klantcontactgegevens

Telecommunicatie

Bedrijfs- en politieberichten

WAT IS BEVESTIGD	Odido beschreef op 12 februari onbevoegde toegang tot een klantcontactsysteem. Het meldde dat de dienstverlening niet was geraakt en benoemde informatie buiten de eerste reikwijdte. NOS meldde aanvankelijk 6,2 miljoen accounts; dit zijn niet noodzakelijk unieke personen. [S13][S35]
LATERE BESCHRIJVING	De bijgewerkte bedrijfs-FAQ dateert de activiteit op 5–6 februari en schrijft deze toe aan ShinyHunters. De politie beschreef een beller die zich voordeed als IT-collega en latere publicatie van gegevens over meer dan zes miljoen klanten. De toeschrijving blijft die van het bedrijf. [S14][S15]
WAT HIER ONBESLIST BLIJFT	Dit rapport reconstrueert niet iedere inbraakstap, verzoent niet alle latere populatieaantallen en stelt niet vast welke individuele records bruikbaar blijven. De eerste melding en latere updates beantwoorden verschillende vragen.
REACTIE	Oefen verificatie bij support en bereid u voor op vervolgfraude met echte klantgegevens. Vertrouw niet op de geheimhouding van basisaccountinformatie als identiteitsbewijs.

Conclusie

Bescherm klantcommunicatie en herstelprocessen naast wachtwoorden.

Het toezichthoudende onderzoek staat in hoofdstuk 10. Behandel het niet als een afgerond aansprakelijkheidsoordeel of onafhankelijk bewijs voor iedere criminele claim.

5.3 Openbaar bestuur: misbruik, toegang en indamming

CASE H

H

Misbruik van mobiel beheer en de AP/Rvdr-voorbeelden

Openbaar bestuur

Officiële campagnebevestiging

CAMPAGNE	Het NCSC bevestigde misbruik van Ivanti EPMM bij meerdere Nederlandse organisaties en beschreef in updates waargenomen databasekopieën of exfiltratie. De latere tijdlijn omvat geslaagd misbruik in Nederland vanaf 29 januari en achteraf vastgestelde eerdere activiteit. [S31][S21]
BENOEMDE VOORBEELDEN	Een regeringsbrief bevestigde misbruik bij de Autoriteit Persoonsgegevens en Raad voor de rechtspraak. Er was onbevoegde inzage in zakelijke contactinformatie van AP-medewerkers. De Rvdr deed een voorlopige datalekmelding; de gedetailleerde AP-velden gelden niet automatisch voor iedere Rvdr-medewerker. [S32][S33]
BEPERKING	Deze voorbeelden vallen binnen de campagne. Ze worden niet opnieuw als apart nationaal campagnetotaal opgeteld. Alleen productgebruik bewijst niet dat een andere organisatie is getroffen.
REACTIE	Bevestig herstelmaatregelen, onderzoek eerdere toegang en beoordeel beheerdersinloggegevens of vertrouwensrelaties die de oorspronkelijke kwetsbaarheid kunnen overleven.

Conclusie

Het verhelpen van een kwetsbaarheid en het onderzoeken van eerdere toegang zijn afzonderlijke controles.

CASE I

I

Systeemtoegang bij het ministerie van Financiën

Rijksoverheid

Ministerie bevestigde toegang

WAT IS BEVESTIGD	Het ministerie ontdekte onbevoegde toegang op 19 maart en blokkeerde toegang op 23 maart. De melding betrof systemen voor meerdere processen van het beleidsdepartement. Volgens het ministerie waren belasting-, douane- en toeslagendiensten aan burgers en bedrijven niet geraakt. [S37] [S38]

BEPERKING	De eerste verklaring stelde geen aanvaller, toegangsmethode, omvang van gestolen gegevens of definitieve groep getroffen systemen vast. Vul deze gaten niet met feiten uit andere overheidsincidenten.
REACTIE	Bepaal welke processen afhankelijk zijn van de geïsoleerde systemen, houd een operationele terugvaloptie beschikbaar en bewaar bewijs voor verklaringen over niet-getroffen diensten.

Conclusie

Onderscheid geraakte beleidssystemen van niet geraakte publieksdiensten in de communicatie.

J

CASE J

Bestandsdiefstal in Epe en veranderende reikwijdte

Lokaal bestuur

Gemeente meldde diefstal

WAT IS BEVESTIGD	Epe dateert in zijn doorlopende overzicht de toegang op 10 maart, het downloaden van bijna 552.000 bestanden op 12 maart en de eerste openbare melding op 14 maart. Later onderzoek stelde dat waarschijnlijk persoonsgegevens van vrijwel alle inwoners waren gestolen. Het noemde 845 geldige identiteitsdocumentkopieën. [S41]
CHRONOLOGIE EN BEPERKING	Eerdere berichtgeving noemde een ander aantal identiteitsdocumenten. Geldige kopieën zijn niet uitwisselbaar met alle kopieën of getroffen personen. De gedateerde gemeentelijke verklaring dat gegevens niet op bekende leksites waren verschenen, bewijst geen verwijdering en voorkomt geen later misbruik. [S42]
REACTIE	Houd definities en updatedata expliciet, geef voorrang aan advies over gevoelige documenten en maak de vragenroute voor inwoners bruikbaar.

Conclusie

Behoud de betekenis en de datum van veranderende omvangcijfers.

Een bestandenaantal is een onderzoeksmaat, geen aantal personen. Eén persoon kan in meerdere records voorkomen en één bestand kan meerdere personen bevatten. Leg in de openbare melding uit wat de organisatie over getroffen personen kan vaststellen. Laat gebruikers bestanden niet zelf door de bevolking delen.

Een afzonderlijk phishingincident bij de politie. Op 25 maart beschreef de politie snelle ontdekking en onderbreking van phishinggerelateerde toegang. Volgens de eerste verklaring waren burgergegevens en opsporingsinformatie niet zichtbaar of toegankelijk geweest. De bron noemde de vermoedelijke gevolgen beperkt en nog in onderzoek. Dit staat los van het politie-incident uit 2024. [S39][S40]

5.4 Zorg: heraansluiting is ook een klinische beslissing

CASE K

K

ChipSoft-ransomware en klantkoppelingen

Zorgsoftware

Bevestigd door leverancier en CERT

WAT IS BEVESTIGD	De Z-CERT-update van 17 april dateert de ransomware op 7 april en bevestigt diefstal van persoonlijke en medische patiëntgegevens bij enkele Nederlandse klanten. Ze onderscheidt getroffen gehoste koppelingen van zelfbeheerde of door derden beheerde software buiten die reikwijdte. [S44][S45]
HERSTEL	ChipSoft beschreef gefaseerd herstel en vrijwel volledige heraansluiting van patiëntenportalen op 12 mei, met doorlopend herstel in juni. De verklaring over gegevensvernietiging steunde op aan beveiligingsexperts toegeschreven verzekeringen; dit rapport kan niet garanderen dat alle kopieën verdwenen zijn. [S18]
BEPERKING	Een uitgeschakelde of herstelde klantverbinding bewijst op zichzelf niet de omvang van de gegevensdiefstal bij die klant. De aangehaalde primaire bronnen noemen geen actor.
REACTIE	Vereis vóór heraansluiting zowel goedkeuring voor klinische continuïteit als beveiligingsgoedkeuring, met een afgesproken terugdraaiprocedure en route voor patiëntcommunicatie.

Conclusie

Herstel iedere afhankelijkheid met de eigenaar; toezeggingen over verwijdering tonen niet aan dat alle kopieën verdwenen zijn.

5.5 Reizen en horeca: een echte boeking kan een vals betaalverzoek ondersteunen

L

CASE L

Toegang tot gastinformatie van Booking.com

Reistechnologie

Bevestigd in bedrijfsrapportage

WAT IS BEVESTIGD	Een latere rapportage van Booking Holdings bevestigt onbevoegde toegang door derden tot boekingsinformatie van bepaalde gasten in april, herstelmaatregelen en samenwerking met overheden. Berichtgeving van 13 april beschreef klantmeldingen en geresette reserveringspincodes. Het aandeel Nederlandse inwoners werd niet vastgesteld. [S46][S47]
BEPERKING	Dit bewijst niet dat elke boeking, elk hotel of elke Nederlandse reiziger is geraakt. Het rapport stelt geen gemeenschappelijke oorzaak vast met het afzonderlijke hotelonderzoek hieronder.
REACTIE	Geef klanten een onafhankelijke manier om betaalverzoeken te verifiëren en controleer welk vertrouwen supportmedewerkers aan reserveringsdetails ontlenen.

Conclusie

Behandel kennis van een boeking als phishingrisico, niet als bevoegdheid om betaling te vragen.

R

CASE R

Een treinpasmelding met een inbraakdatum in 2025

Treinpasdiensten

Melding in 2026; incident in 2025

WAT IS BEVESTIGD	Eurails eerste melding dateerde van 10 januari 2026. [S105] De februari-update beschreef databasekopieën en later verkoopgerelateerd materiaal. Een bij een toezichthouder ingediende bedrijfskennisgeving dateert bestandsoverdracht op 26 december 2025. Dit is een melding uit 2026, geen nieuwe inbraak in 2026. [S103][S104]
BEPERKING	Gewone directe kopers en DiscoverEU-deelnemers hebben verschillende gegevenscategorieën. Brede programmaspecifieke velden mogen niet aan iedere koper worden toegeschreven. Hier is geen totaal van Nederlandse inwoners vastgesteld.

REACTIE	Bepaal op welke dienst en klantcategorie een melding betrekking heeft voordat u advies geeft. Houd gebeurtenisdatum, meldingsdatum en latere verspreiding apart in het responsdossier.

Conclusie

Onderscheid gewone klanten, programmadata, incidentdata en meldingsdata van elkaar.

Een persoon kan één klantmerk gebruiken zonder te weten welk programma de informatie bewaart. Supportmedewerkers moeten via een bestaande route de relevante dienstrelatie kunnen vaststellen. Advies moet die relatie volgen, niet de uitgebreidste veldlijst die voor een klantcategorie is gemeld.

Een afzonderlijk juni-onderzoek betrof hotelgasten met gerichte reserverings- of betaalberichten. NOS meldde een brancheschatting van minstens 100 Nederlandse hotels; oorzaak en volledige omvang bleven onbeslist. De eigen pagina van de branchedeelnemer beschreef een inventarisatie. Geen van beide bewijst dat de deelnemer zelf de getroffen leverancier was. [S53][S54]

5.6 Onderwijs: het leveranciersincident en de universitaire reactie

M

CASE M

Canvas en universitaire continuïteit

Onderwijstechnologie

Universiteit meldde leveranciersincident

WAT IS BEVESTIGD	De doorlopende UvA-melding vermeldt formele leverancierskennisgeving uiterlijk op 7 mei, met volgens de leverancier namen, e-mailadressen en mogelijk identificatienummers. Ze beschreef zeven universiteiten. Koppelingen werden op 8 mei onderbroken; UvA herstelde Canvas op 13 mei. [S49] [S50]
BEPERKING	Eén universiteitsmelding rechtvaardigt niet het benoemen van iedere getroffen instelling of het toekennen van gelijke reikwijdte. Een verklaring van de leverancier dat gegevens zijn verwijderd, is geen onafhankelijk vastgestelde verwijdering van elke kopie.
REACTIE	Test een alternatieve onderwijs- en inleverroute, bepaal veilige heraansluitcriteria en stem informatie uit het tijdelijke proces af.

Conclusie

Een gedeeld platform vereist afzonderlijke beslissingen over klantimpact en herstel.

Onderwijscontinuïteit vraagt naast technische toegang ook beslissingen over deadlines. Als lesmateriaal, beoordeling of inlevering van een gedeeld platform afhangt, moeten facultaire verantwoordelijken weten wie alternatieven kan goedkeuren en communiceren. Alleen een inlogpagina herstellen lost die onderwijsbeslissingen niet op.

5.7 Retail, websites en andere onbesliste grenzen

Ahold Delhaize beschreef op 19 oktober kwaadwillige activiteit en het uit voorzorg stilleggen van enkele websites of apps, terwijl winkels openbleven. Het kwartaalrapport schatte gevolgen voor omzet en operationele winst in het vierde kwartaal. Het rapport van 4 november schatte een omzetdaling van EUR 200–250 miljoen en een operationele winstdaling van EUR 75–100 miljoen. Dit zijn groepsschattingen, geen definitieve of uitsluitend Nederlandse verliezen. Er wordt geen actortoeschrijving overgenomen. [S19][S20]

Een verwerkingsverantwoordelijke voor een retailwebshop meldde ook een klantgegevensincident in september. De naam blijft hier weggelaten. De melding ondersteunt de afgebakende incidentbeschrijving, geen conclusie over de bredere omgeving van de verantwoordelijke. [S30]

Dustins septemberchronologie bevestigt toegang tot interne systemen, tijdelijk stilleggen en gefaseerd herstel. De latere FAQ beschrijft getroffen administratie-/supportgegevens en beperkte zakelijke contact- of gebruikersinformatie bij bepaalde beheerdienstklanten. Andere berichtgeving geeft claims over Nederlandse klanten weer; die zijn geen officiële bevestiging van inbraken in hun eigen netwerken. [S101][S102]

Voor websites in bredere zin waarschuwde de AP in augustus voor misbruikte WordPress-kwetsbaarheden, datalekmeldingen en gebrekkige risicocommunicatie. Ze gaf geen aantal beheerders. Dit mag niet bij een wereldwijd besmette-websitetotaal van een andere campagne worden opgeteld of als één gemeten nationale golf gelden. [S60]

Een gemeld incident met interne mappen bij een luchtvaartgroep blijft hier algemeen beschreven. Een nieuwsbericht citeerde het bedrijf over onbevoegde toegang. In die fase waren volgens het bedrijf geen gevoelige gegevens of gevolgen voor klantdiensten vastgesteld. De verantwoordelijkheidsclaim van een afzonderlijke groep wordt niet overgenomen. De precieze incidentdag en volledige omvang blijven onbeslist. [S64]

Deze voorbeelden rechtvaardigen controles van webbeheer, bevoorrechte toegang en klantmeldingen. Ze bewijzen geen gedeelde actor of één toegangsroute. Het NCSC meldde in oktober expliciet toen geen reden te zien om de besproken voedselsectorincidenten als gerelateerd te beschouwen. [S63]

5.8 Recente activiteit: 8–22 november

De recente periode bevat gebeurtenissen die verschillende operationele reacties vereisen. De onderstaande data onderscheiden de gebeurtenis van de openbare update. Een update telt niet als een nieuwe inbraak; een preventieoefening telt niet als een crimineel slachtofferincident.

CASE O

AllUnited en reikwijdte per vereniging

Verenigingsadministratie

Bedrijf bevestigde diefstal

WAT IS BEVESTIGD	AllUnited meldt gegevensdiefstal op 9 november en herstel van een softwarefout na ontdekking. De update van 18 november meldde een collectieve AP-melding voor 478 verenigingen. De update van 20 november noemde nog uitgeschakelde bondskoppelingen. [S68]
BEPERKING	Het getal 478 telt deelnemende verenigingen in die collectieve melding. Het is geen definitief aantal getroffen personen, alle klanten of alle meldingen. De koppelingsstatus bewijst niet dat iedere genoemde bond is getroffen. Eerdere persaantallen beschrijven eerdere berichtgeving. [S69]
REACTIE	Iedere vereniging moet vaststellen welke records ze aan de dienst heeft toevertrouwd, haar eigen communicatiebesluit nemen en bepalen welke koppelingen veilig bruikbaar zijn.

Conclusie

Deelnemers aan een melding vormen geen definitief slachtoffertotaal; controleer de omvang per vereniging.

CASE Q

Een script van derden bereikt de klantbrowser

Browserafhankelijkheden

Leveranciersincident: lokaal bereik onduidelijk

WAT IS BEVESTIGD	Het advies van de experimentplatformaanbieder, bijgewerkt op 19 november, bevestigt misbruik van een fout in de aanmeldprocedure op 16 november, accountimitatie en kwaadaardige JavaScript-injectie. Volgens de aanbieder werd minder dan 5% van de klanten geraakt en vond herstel die dag plaats. [S74]
EXTERNE WAARNEMING	Report URI beschreef 178 organisaties wereldwijd in zijn onderzoek. Dat is een wereldwijd onderzoeksaantal, geen Nederlands slachtofferaantal. Klantnamen blijven weggelaten in afwachting van de vereiste bevestiging; het aangehaalde bewijs rechtvaardigt hier geen identificatie van Nederlandse klanten. [S29]
REACTIE	Breng scripts in klantbrowsers in kaart, bepaal welke accounts ze mogen wijzigen en test hoe een getroffen afhankelijkheid kan worden uitgeschakeld.

Conclusie

Wereldwijde aantallen geraakte websites tonen geen Nederlands slachtoffertotaal aan.

Een browserafhankelijkheid kan buiten het team vallen dat de hoofdapplicatie patcht. Beveiligingsverantwoordelijkheid moet aansluiten op wie uitvoerbare inhoud kan wijzigen, ook binnen marketing- of experimentbeheer. Oefen of de organisatie de afhankelijkheid kan vinden, beheerderstoegang kan intrekken en haar kan uitschakelen zonder essentiële klantfuncties te verliezen.

Openbare datum	Onderwerp	Interpretatie en directe beslissing
9 november	Politiewaarschuwing over criminele onlineplatforms [S70]	Preventiecontext; stuur verdacht materiaal via bevoegde beveiligingsprocessen door
12 november	Update Operation Endgame [S71][S72]	Internationale opsporing; onderzoek relevante meldingen en eerdere inbraken, zoals besproken in §7.5
12 november	Berichtgeving over leveranciersgerelateerde enquêtegegevens [S94]	Bedrijfsonderzoek zoals gemeld; e-mailadressen zijn geen unieke personen
13 november	Door het NCSC beschreven cloudmailstoring [S73]	Continuïteitsincident; in die beschrijving geen aanwijzing voor een hack; test onafhankelijke communicatie
16 november	RDI-bericht over GPS-onderzoek [S98]	Gebeurtenis op 9 november; oorzaak onbeslist, apart van conclusies over netwerkinbraken
18–20 november	AllUnited-updates over reikwijdte en koppelingen [S68]	Update van het incident van 9 november; bepaal gegevens- en dienststatus per vereniging
19 november	Revolut-onderzoek gemeld door de politie [S75]	Diefstal in september, later openbaar gemeld; persoonlijke veiligheid en fraude respons in Case P (§8.3)
21 november	Gesimuleerde webshopcampagne van de politie [S77]	Preventieoefening, geen klantverliezen door een criminele inbraak

Een afzonderlijk bericht van 12 november citeerde een consumentenmerk dat leveranciersgerelateerde blootstelling van 128.000 e-mailadressen en andere enquêtegegevens onderzocht. De mate van inzage, kopiëren of misbruik bleef onduidelijk. Namen blijven hier weggelaten. Een verband met het latere browserscriptincident is niet vastgesteld. [S94]

Het RDI-bericht van 16 november stelt een andere grens. Het betreft verstoring van vliegtuig-GPS op 9 november, 18:15–18:30. Volgens de toezichthouder beschermden secundaire systemen de luchtvaartveiligheid. Het onderzoek stelde geen opzettelijke verstoring, herkomst of verantwoordelijkheid vast. Dit bewijst geen inbraak in luchthavensystemen. [S98]

De cloudmailbeschrijving betreft beschikbaarheid zonder vastgestelde kwaadwillige oorzaak. De relevantie is continuïteit, geen nieuw aanvalsaantal. [S73]

KERNPUNTEN

01

Bevestig gegevens- en dienstgevolgen afzonderlijk per organisatie en leverancier.

02

Doorlopende updates, campagnevoorbeelden en collectieve meldingen mogen niet worden opgeteld tot unieke slachtoffers.

03

Recente activiteit maakt verenigingsreikwijdte, browserafhankelijkheden en onafhankelijke communicatie directe oefenprioriteiten.

HOOFDSTUK 06

Verbonden systemen, verstoring en operationele continuïteit

DIT HOOFDSTUK BEANTWOORDT

Welke verstoringsclaims vragen technische verificatie en wanneer wordt een verbonden systeem een operationele prioriteit?

2 november

NCSC-bericht dat cyberaanvallen op koelsystemen met gevolgen in Nederland bevestigt

6.1 Een tijdlijn met expliciete bewijstypen 54
6.2 Koelinstallaties en wijzigingen op afstand 55
6.3 Een cameralijst is geen incident met industriële besturingen 56
6.4 DigiD-beschikbaarheid en de grens van de bewaarde berichten 56
6.5 Continuïteitsoefeningen moeten beveiligingshulpmiddelen omvatten 57

HOOFDSTUK 06

Verbonden systemen, verstoring en operationele continuïteit

IN HET KORT

Het sterkste bewijs over verbonden besturingen is hier een officieel bericht over koelsystemen. Dat verschilt van een claim over camera-inloggegevens, een websitebeschikbaarheidsclaim of een cloudstoring. Deze gebeurtenissen vragen ander bewijs en andere eigenaren. Stel vast of een fysiek proces is geraakt, bewaar lokaal bewijs en isoleer onveilige externe toegang via een bevoegd besluit. Bereid onafhankelijke communicatie voor voordat de normale samenwerkingsdienst uitvalt.

6.1 Een tijdlijn met expliciete bewijstypen

9 mrt 2026	**AIVD en MIVD** Beschrijven een campagne tegen berichtenaccounts en Nederlandse overheidsslachtoffers; de toeschrijving is van de diensten [S36]
1 apr 2026	**NCSC** Waarschuwt voor kwaadaardige softwarepakketten; Nederlandse slachtofferaantallen zijn niet vastgesteld [S43]
28 mei 2026	**Politie en NCSC** Beschrijven een internationale botnetverstoring met in Nederland gehoste infrastructuur [S52]
30 jun 2026	**AIVD en MIVD** Beschrijven phishing naar herstelsleutels als ontwikkeling binnen de berichtencampagne [S57]
10 jul 2026	**AIVD en MIVD** Bevestigen gehackte camera's langs Nederlandse militaire logistieke routes, zonder eigenaren te benoemen [S58]
23 aug 2026	**Adverteerder van inloggegevenslijst** Biedt cameramateriaal aan; echtheid, locatie en toegang blijven ongeverifieerd (B06)
7 okt 2026	**Kamerantwoord** Beschrijft terugkerende DDoS-pogingen tegen DigiD en grotere beschikbaarheidsgevolgen gedurende 2026 [S96]
13 okt 2026	**NCSC** Ziet op dat moment geen reden om de besproken voedselsectorincidenten als gerelateerd te beschouwen [S63]
2 nov 2026	**NCSC** Bevestigt cyberaanvallen op koelsystemen in Europa, waaronder Nederland [S66]

12 nov 2026	**Politie** Kondigt verdere verstoring via Operation Endgame aan; internationale cijfers en cijfers over locaties in Nederland vragen afzonderlijke lezing [S71]
13 nov 2026	**NCSC** Beschrijft een cloudmailstoring, zonder aanwijzing voor een hack in dat bericht [S73]
16 nov 2026	**RDI** Meldt onderzoek naar GPS-verstoring op 9 november; oorzaak en verantwoordelijkheid onbeslist [S98]
16 nov 2026	**Leveranciersadvies en technisch onderzoek** Browserscriptinci- dent bevestigd; onderzoeksaantal is wereldwijd en klantidentiteiten blijven weggelaten [S74][S29]

6.2 Koelinstallaties en wijzigingen op afstand

CASE N

N

Koelinstallaties en wijzigingen op afstand

Koelinstallaties

Officiële campagnemelding

WAT IS BEVESTIGD	Het NCSC-bericht van 2 november beschrijft cyberaanvallen op koelinstallaties in meerdere Europese landen, waaronder Nederland. Zwakke of standaardwachtwoorden maakten wijzigingen op afstand mogelijk. Het advies is directe internetblootstelling te verwijderen. [S66]
ANDERE BERICHTGEVING	Een Anadolu-bericht, met NOS als bron, noemde minstens 17 Nederlandse bedrijven. Dit is gedateerde persberichtgeving, geen door het NCSC aangeleverd aantal. Het bewijs stelt geen enkele leverancier, actor of gemeten bederfschade op iedere locatie vast. [S67]
REACTIE	Bepaal de routes voor beheer op afstand en hun eigenaren. Controleer fysieke meetwaarden, beperk onveilige toegang en behoud een lokale hersteloptie voordat u publiekelijk over gevolgen spreekt.

Conclusie

Stem beperkingen op externe toegang af met de eigenaar van het fysieke proces.

Punt	Te vermijden gevolgtrekking	Ondersteunde grens	Beslissing van de beheerder
Reikwijdte	Ieder product van één leverancier was geraakt	Geen volledige leveranciers-populatie vastgesteld	Bepaal de werkelijke afhankelijkheid van afstandsbediening
Besturing	Een scherm toont fysieke schade aan	Lokaal procesbewijs blijft nodig	Controleer meetwaarden en lokale registraties
Toeschrijving	Eén actor coördineerde iedere gebeurtenis	Hier is geen gemeenschappelijke dader vastgesteld	Dam de geverifieerde toegang in zonder naar verantwoordelijkheid te gissen
Populatie	Een persschatting is een nationale telling	Het NCSC geeft geen Nederlands totaal	Stel de eigen installatiereikwijdte vast

[S66][S67]

Een noodbesluit mag niet afhangen van het achterhalen wie de verbinding installeerde. Facilitair beheer, koeltechnische aannemers, IT en bedrijfsvoering moeten afspreken wie toegang kan uitschakelen, apparatuur controleert en noodonderhoud voortzet. Leg die rollen vóór het incident vast, in plaats van te onderhandelen terwijl een proces afwijkt.

6.3 Een cameralijst is geen incident met industriële besturingen

Het camerabericht in Case F is ondergronds bewijs van een advertentie. Het stelt niet het land van ieder apparaat, werkende toegang, eigendom, echtheid of een wijziging van een fysiek proces vast. Het mag niet worden opgewaardeerd tot een geverifieerde campagne tegen industriële besturingen. [S1]

6.4 DigiD-beschikbaarheid en de grens van de bewaarde berichten

Een op 7 oktober ontvangen Kamerantwoord bevestigt dagelijkse DDoS-pogingen tegen DigiD en grotere beschikbaarheidsgevolgen gedurende 2026. Het beschrijft steeds complexere, gerichte aanvallen. Landelijke berichtgeving citeerde Logius over een nieuwe aanval op 30 oktober. Dit zijn ondersteunende gebeurtenissen binnen een terugkerende campagne, geen afzonderlijke datalekaantallen. [S96][S97]

Bij een dienst die van digitale authenticatie afhangt, moet de terugvaloptie aangeven wat gebruikers zonder inloggen kunnen doen. Een statusbericht moet de getroffen functie en volgende update uitleggen. Alleen een beschikbaarheidsincident bewijst geen diefstal van authenticatiegegevens.

De thematabel bevat DDoS- of hacktivismeverwijzingen, maar het bewaarde materiaal stelde geen Nederlandse DDoS-campagne of geverifieerde industriële-besturingsclaim vast. Dit is een beperking van het bewijs, geen bewijs dat Nederlandse organisaties zulke activiteit niet meemaakten. [S1]

Alleen een niet-reagerende website toont geen oorzaak, duur of operationele gevolgen aan. Een actor kan een claim publiceren terwijl een site om een andere reden onbereikbaar is. Vergelijk eigen diensttelemetrie, leveranciersstatus en incidentbewijs voordat u de beschrijving van de actor overneemt.

6.5 Continuïteitsoefeningen moeten beveiligingshulpmiddelen omvatten

De recente cloudstoring in §5.8 toont waarom beveiliging van gewone dienstbeschikbaarheid afhangt. Een incidentteam moet weten welke waarschuwingen, beheerdersgoedkeuringen en communicatie dezelfde dienst gebruiken. Een terugvaloptie met dezelfde uitgevallen identiteits- of berichtenafhankelijkheid kan tegelijk falen.

KERNPUNTEN

01

Verifieer het fysieke proces en de eigenaar van externe toegang voordat u operationele gevolgen concludeert.

02

Houd ondergrondse cameraclaims gescheiden van officieel spionage- en koelsysteembewijs.

03

Test communicatie en beveiligingsbeslissingen terwijl de normale clouddienst onbeschikbaar is.

HOOFDSTUK 07

Actoren, campagnes en de grenzen van toeschrijving

DIT HOOFDSTUK BEANTWOORDT

Welke actoren ondersteunt het bewijs en welke relaties moeten verdedigers niet afleiden?

77

geaccepteerde Nederlandse ransomwarevermeldingen in de momentopname van de onderzoeksperiode

7.1 Een relatiekaart met bewijs op iedere lijn 59
7.2 Ransomwarevermeldingen en regionale context 60
7.3 ShinyHunters en bedrijfsspecifieke toeschrijving 63
7.4 Drie officiële campagnelijnen 64
7.5 Opsporing verandert infrastructuur, niet de geschiedenis van gestolen gegevens 67

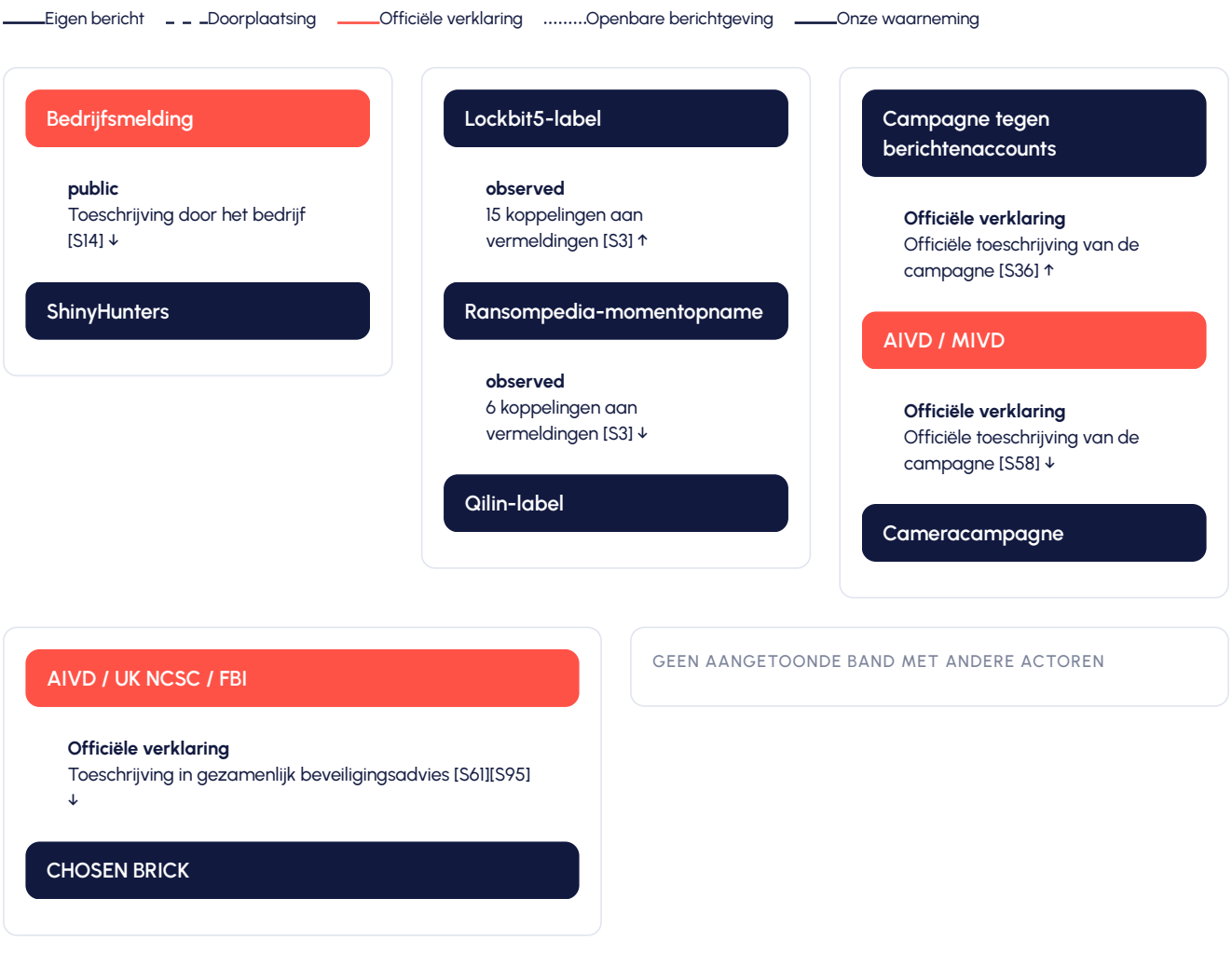
HOOFDSTUK 07

Actoren, campagnes en de grenzen van toeschrijving

IN HET KORT

Criminele vermeldingen, bedrijfstoeschrijvingen en beoordelingen van inlichtingendiensten beantwoorden verschillende vragen. Lockbit5 voert de bewaarde Nederlandse ransomwarevermeldingen aan; Odido noemt ShinyHunters. Officiële campagneberichten betreffen afzonderlijk berichtenaccounts, camera's en gerichte malware. Dit vormt geen gezamenlijk netwerk. Bewaar die grenzen met de kaart waarop elke relatie een bewijstype heeft en geef daarna prioriteit aan herstel, accountbescherming en de specifiek beschreven middelen.

7.1 Een relatiekaart met bewijs op iedere lijn

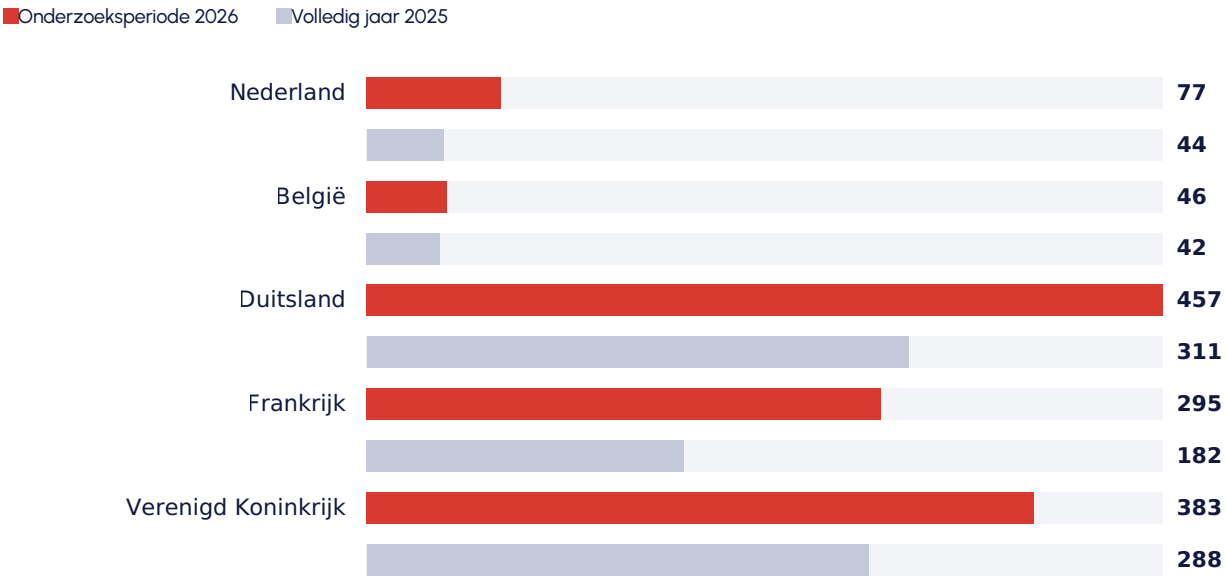


Een lijn toont een gedocumenteerde relatie van het aangegeven type. Een officiële campagnetoeschrijving, bedrijfsbeschrijving, actoradvertentie en gedeeld bericht zijn geen gelijkwaardig bewijs. Een verband toont geen gemeenschappelijke dader aan. Een losstaande knoop is beter dan een verzonnen verbinding.

Dit rapport voegt de ransomwaremerken, ondergrondse adverteerders en staatsgerelateerde campagnes niet samen tot één organisatie. Gedeelde landeninteresse of vergelijkbare termen bewijzen geen coördinatie. Als bij een incident geen actor vaststaat, blijft de verdedigende analyse ook zonder toeschrijving bruikbaar.

7.2 Ransomwarevermeldingen en regionale context

Nederlandse vermeldingen overtreffen het vorige jaartotaal, met ongelijke perioden en zonder nationale risicorangschikking



Bron: geaccepteerde Brandefense Ransompedia-vermeldingen. 2026: 1 januari–22 november; 2025: volledig jaar. Ongelijke perioden; geen nationale risicorangschikking [S3].

Land	Geaccepteerde vermeldingen in de onderzoeksperiode van 2026	Vermeldingen over heel 2025
Nederland	77	44
België	46	42
Duitsland	457	311
Frankrijk	295	182
Verenigd Koninkrijk	383	288

[S3]

De kolom voor 2026 betreft een deel van het jaar en eindigt bij de bewaarde momentopname op de peildatum. De kolom voor 2025 beslaat een volledig jaar. Het Nederlandse deeltotaal ligt al boven het vorige jaartotaal, maar dit is geen groeipercentage over gelijke perioden. De tabel corrigeert evenmin voor bevolkingsomvang en geeft geen inbraakkans.

België, Duitsland en Frankrijk bieden nabije EU-context; het Verenigd Koninkrijk biedt een nabije niet-EU-vergelijking. Economische omvang, openbaarmaking, sectorsamenstelling en crimineel publicatiegedrag kunnen aantallen beïnvloeden. Deze cijfers zijn daarom beschrijvende vergelijkingen, geen ranglijst van nationale beveiligingsprestaties.

Groepslabel zoals bewaard	Nederlandse vermeldingen	Interpretatie
Lockbit5	15	Meest voorkomende label in deze momentopname
Thegentlemen	9	Tweede naar bewaarde Nederlandse vermeldingen
Qilin	6	Zes vermeldingsclaims, geen zes onafhankelijk vastgestelde inbraken
INC Ransom	4	Alleen de vermeldingspopulatie
DragonForce	4	Alleen de vermeldingspopulatie
Overige labels	39	Het restant verdeeld over meerdere merken

[S3]

Lockbit5

Vermeldingslabel in de bewaarde momentopname

Alias bij ransomware- en afpersingsvermeldingen | Hier is geen toeschrijving aan een staat vastgesteld

IN NEDERLAND, 2026

Periode in 2026

15 vermeldingen met landlabel Nederland onder deze naam

GECLAIMDE DOELWITTEN

Organisaties gekoppeld aan vermeldingen met landlabel Nederland; identiteiten weggelaten

IN OPENBARE BERICHTGEVING

[S3] De Ransompedia-momentopname bevat 15 vermeldingen onder het label Lockbit5

ONZE BEOORDELING

Dit label komt het vaakst voor in deze Nederlandse momentopname. Het bewijst geen verwantschap tussen code, gedeelde affiliate, versleuteling, betaling of juistheid van elke landkoppeling. Bereid herstel en het veiligstellen van bewijs voor, ongeacht de gebruikte naam.

ZEKERHEID
Hoog voor het aantal bewaarde vermeldingen; afzonderlijke claims niet geverifieerd

Qilin

Vermeldingslabel in de bewaarde momentopname

Alias bij ransomware- en afpersingsvermeldingen | Hier is geen toeschrijving aan een staat vastgesteld

IN NEDERLAND, 2026

Periode in 2026

6 vermeldingen met landlabel Nederland onder deze naam

GECLAIMDE DOELWITTEN

Organisaties gekoppeld aan vermeldingen met landlabel Nederland; identiteiten weggelaten

IN OPENBARE BERICHTGEVING

[S3] De Ransompedia-momentopname bevat 6 vermeldingen met landlabel Nederland onder Qilin

ONZE BEOORDELING

Een vermelding vraagt om validatie en is geen geverifieerde vaststelling van een inbraak. Controleer incidentregistraties en leveranciersmeldingen voordat een organisatie aan een nieuwe gebeurtenis wordt gekoppeld. Het aantal vermeldingen wijst geen specifieke toegangsroute of zwakke plek in de verdediging aan.

ZEKERHEID
Hoog voor het aantal bewaarde vermeldingen; toegangsroute en gevolgen nog niet vastgesteld

7.3 ShinyHunters en bedrijfsspecifieke toeschrijving

ShinyHunters

Afpersing toegeschreven in bedrijfsberichtgeving | Toeschrijving door Odido; niet onafhankelijk vastgesteld in dit rapport

IN NEDERLAND, 2026

5–6 februari
Door Odido genoemde data van het incident in zijn klantsysteem

7 september
De politie beschreef hoe aanvallers zich voordeden als IT-collega's en later gegevens publiceerden

GECLAIMDE DOELWITTEN

Het openbaar bevestigde incident met klantcontactgegevens; er wordt geen bredere lijst van slachtoffers afgeleid

IN OPENBARE BERICHTGEVING

[S14] Odido schrijft zijn incident van februari toe aan ShinyHunters

[S15] De politie beschrijft het telefonische voorwendsel, de gegevensdiefstal en de afpersingseis

ONZE BEOORDELING

Controleer de beller en de gevraagde handeling afzonderlijk. Een vertrouwde stem of intern jargon geeft geen toestemming om in te loggen, een code te delen of klantgegevens te exporteren. Een bewaarde advertentie toont niet aan dat de poster de door het bedrijf genoemde dader is.

ZEKERHEID
Hoog voor de gepubliceerde toeschrijving door het bedrijf; identiteit van de dader niet onafhankelijk geverifieerd

Odido noemt ShinyHunters in zijn bijgewerkte beschrijving. De Ransompedia-momentopname bevat afzonderlijk twee Nederlandse vermeldingen onder het label Shinyhunters. Dit zijn verschillende records met verschillende betekenissen. Het rapport leidt niet af dat iedere gerelateerde klantgegevensmelding of leverancierszaak bij die groep hoort. [S14][S3]

7.4 Drie officiële campagnelijnen

Berichtenaccounts en herstelgeheimen

Het maartbericht van de AIVD en MIVD noemt Nederlandse overheidsmedewerkers als doelwitten en slachtoffers van een campagne die de diensten aan Russische staatshackers toeschrijven. Het betreft persoonlijke accounts, verificatie- of pincodes en gekoppelde apparaten. Het bericht sluit een platformbrede inbraak bij Signal of WhatsApp uit. [S36]

De juni-update beschrijft phishing naar herstelsleutels van Signal-back-ups als een ontwikkeling binnen die activiteit. Dit telt niet automatisch als een tweede afzonderlijke slachtoffergebeurtenis. De beschrijving van de diensten toont campagneontwikkeling; individuele totalen en inbraakdata zijn hier niet beschikbaar. [S57]

Campagne tegen berichtenaccounts

Campagne beschreven door de AIVD en MIVD

Campagne voor accounttoegang, toegeschreven aan een staat | Russische staatshackers, volgens de AIVD en MIVD

IN NEDERLAND, 2026

9 maart
De diensten meldden dat Nederlandse overheidsmedewerkers tot de doelwitten en slachtoffers behoorden

30 juni
De diensten waarschuwden voor phishing naar herstelsleutels van back-ups

GECLAIMDE DOELWITTEN

Accounts bij berichtendiensten; identiteiten van personen weggelaten

IN OPENBARE BERICHTGEVING

[S36] De AIVD en MIVD beschrijven misbruik van verificatiecodes en gekoppelde apparaten

[S57] De AIVD en MIVD beschrijven phishing naar herstelsleutels van back-ups

ONZE BEOORDELING

Controleer expliciet de routes voor accountherstel en het koppelen van apparaten. Deze waarschuwingen tonen geen kwetsbaarheid in de berichtenplatforms zelf aan. Beperk gevoelig werk tot goedgekeurde kanalen en onderzoek ongeautoriseerde apparaatkoppelingen samen met de accounteigenaar.

ZEKERHEID
Officiële toeschrijving zoals gepubliceerd; geen onafhankelijke toeschrijving aan een actor

Een reactie moet ook eerdere gesprekken en gekoppelde apparaten meenemen. Het wijzigen van één geheim bewijst niet dat de aanvaller nooit eerder materiaal las of dat iedere gekoppelde sessie is verwijderd. Gebruikers hebben een ondersteunde checklist en vertrouwelijke meldroute nodig, zeker wanneer openbaarmaking gevoelige relaties kan blootleggen.

Camera's en zicht op logistiek

De diensten schrijven in juli een Europese cameraspionagecampagne toe aan Russische staatsactoren. Ze bevestigen een klein aantal gehackte camera's langs Nederlandse militaire logistieke routes, zonder eigenaren of een exact aantal bekend te maken. Dit rapport identificeert de locaties niet. [S58]

Spionagecampagne met IP-camera's

Campagne beschreven door de AIVD en MIVD

Campagne voor cameratoegang, toegeschreven aan een staat | Russische staatsactoren, volgens de AIVD en MIVD

IN NEDERLAND, 2026

10 juli
De diensten meldden een klein aantal getroffen Nederlandse camera's

GECLAIMDE DOELWITTEN

Privaat beheerde camera's nabij militaire logistieke routes; eigenaren en locaties weggelaten

IN OPENBARE BERICHTGEVING

[S58] De AIVD en MIVD beschrijven gestructureerde cameraspionage in Europa en Nederlandse gevallen

ONZE BEOORDELING

Toegang tot camera's kan operationele patronen blootleggen zonder toegang tot een militair netwerk. Breng eigendom, beheer op afstand en afhankelijkheden van ondersteuning in kaart. Het bewaarde bewijs koppelt de afzonderlijke ondergrondse advertentie met een cameralijst niet aan deze campagne.

ZEKERHEID
Officiële toeschrijving en bevestiging van Nederlandse gevallen zoals gepubliceerd; geen exact binnenlands aantal

Een praktische inventaris moet beheer en gegevenstoegang omvatten, niet alleen gebouweigendom. Een facilitair aannemer kan de camera beheren terwijl een ander team beslist wat die opneemt. Maak die verantwoordelijkheden expliciet in het responsplan en behoud een lokale manier om te controleren of toegang bevoegd is.

Gerichte malware tegen personen

De AIVD beschrijft in september, na gezamenlijk onderzoek met Britse diensten, Iraanse cyberactoren die CHOSEN BRICK inzetten tegen critici in het Westen. De dienst bevestigt dat Nederlandse slachtoffers zijn geïnformeerd. Dit is de toeschrijving van de brondiensten, geen onafhankelijke toeschrijving door dit rapport of oordeel over de doelwitten. [S61]

CHOSEN BRICK-campagne

Naam uit het gezamenlijke beveiligingsadvies

Malwarecampagne, toegeschreven aan een staat | Iraanse cyberactoren, volgens de AIVD en partnerdiensten

IN NEDERLAND, 2026

15 september

Gezamenlijk beveiligingsadvies gepubliceerd; de beschreven doelwitselectie in Nederland gaat terug tot ten minste 2025

GECLAIMDE DOELWITTEN

Personen die de diensten omschrijven als dissidenten, activisten en journalisten; identiteiten weggelaten

IN OPENBARE BERICHTGEVING

[S61] De AIVD meldt dat Nederlandse slachtoffers zijn geïnformeerd

[S95] Het gezamenlijke beveiligingsadvies beschrijft de malware en campagnetechnieken

ONZE BEOORDELING

Bied mensen met een verhoogd risico een veilige meldroute en isoleer verdachte bestanden voor analyse door bevoegde onderzoekers. De matrix beschrijft gedrag en mogelijkheden van de campagne. Zij toont niet aan dat elke techniek tegen ieder Nederlands slachtoffer is gebruikt.

ZEKERHEID

Officiële toeschrijving zoals gepubliceerd; aantallen slachtoffers en individuele data weggelaten

TECHNIEKEN UIT HET GEZAMENLIJKE OVERHEIDSADVIES, PER TACTIEK

Eerste toegang	Uitvoering	Persistentie	Verzameling	Exfiltratie	Impact
T1566.003 Spearphishing via een dienst	T1204.002 Kwaadaardig bestand	T1547.001 Run-registersleutels / opstartmap	T1113 Schermopname	T1041 Exfiltratie via een C2-kanaal	T1485 Gegevensvernietiging

De techniek-ID's voor CHOSEN BRICK staan expliciet in het gezamenlijke beveiligingsadvies [S95]. De geselecteerde rijen beschrijven gedrag of mogelijkheden van de campagne en bewijzen niet dat elke techniek tegen Nederlandse slachtoffers is gebruikt. Aan de waarschuwingen over berichtenaccounts en camera's zijn geen niet-onderbouwde techniek-ID's toegekend. [S95]

Het gezamenlijke beveiligingsadvies levert de techniekindeling in de widget. Die beschrijft campagnegedrag en mogelijkheden. Ze bewijst niet dat iedere techniek tegen ieder Nederlands slachtoffer is gebruikt en stelt geen slachtofferidentiteiten vast. [S95]

China-gerelateerde beoordelingen en historische context

Een AIVD-bericht uit april onderschrijft advies over verborgen netwerken die Chinese hackgroepen tegen Nederlandse en geallieerde belangen gebruiken. Een MIVD/AIVD-bericht uit oktober behandelt spionage via randapparatuur en een meerjarig patroon, naast verwachte verdere activiteit. Geen van beide levert een nieuwe, volledige Nederlandse slachtofferlijst. [S48][S62]

De jaarverslagen over 2025, gepubliceerd in april 2026, bespreken ook eerdere berichtentoegang, inbraken bij Nederlandse hostingaanbieders en dreiging rond Noord-Koreaanse IT-werkers. De publicatie hoort bij de context van dit jaar; activiteit uit 2025 wordt daardoor geen nieuw incident in 2026. [S90][S91]

Een Zimbra-advies uit juli biedt een andere nuttige grens. De AIVD beschreef een campagne tegen westerse organisaties, maar meldde expliciet dat dit incident geen Nederlandse slachtoffers had. Het kan productvoorbereiding ondersteunen zonder als binnenlandse inbraak te tellen. [S59]

Softwarepakketten en de ontwikkelomgeving

Het NCSC-bericht uit april beschrijft kwaadaardige pakketversies na Trivy-toegang, verspreiding van Canister-Worm en een afzonderlijk axios-incident. Het noemt aanwijzingen voor exfiltratie zonder Nederlandse slachtoffers te tellen. Houd deze gebeurtenissen gescheiden bij controles van ontwikkelcredentials, pakketvertrouwen en diensten die ontwikkelaars kunnen bereiken. [S43]

7.5 Opsporing verandert infrastructuur, niet de geschiedenis van gestolen gegevens

Bekendgemaakt	Officiële actie	Wat de cijfers beschrijven
4 maart	Internationale actie haalde een gestolen-gegevensforum offline [S89]	Verstoring van een criminele markt, geen nieuw gemeten Nederlands datalektotaal
21 mei	Politie beschreef het offline halen van een crimineel gerichte VPN-dienst met Franse autoriteiten [S51]	33 gekoppelde servers ontmanteld en 83 informatiepakketten; internationale opsporing
28 mei	Botnetactie van politie/NCSC [S52]	Minstens 17 miljoen besmette apparaten wereldwijd en 200 infrastructuurservers in Nederland
18 juni	SocGholish-gerelateerde verstoring, door de politie gekoppeld aan EvilCorp [S55]	14.971 websites internationaal opgeschoond; infrastructuur- en credentialcijfers zijn geen Nederlandse slachtofferaantallen
24 juni	Infostealerinfrastructuur en teruggevonden inloggegevens [S56]	Meer dan 24 miljoen inloggegevens van minstens 384.000 systemen bij een internationale actie

Bekendgemaakt	Officiële actie	Wat de cijfers beschrijven
28 oktober	Actie tegen een hostingbedrijf dat volgens de politie criminele diensten ondersteunde [S65]	Infrastructuurhandhaving, zonder telling van getroffen Nederlandse klanten
12 november	Verdere Operation Endgame-actie [S71][S72]	Cijfers over locaties in Nederland en internationale cijfers vragen afzonderlijke behandeling

Bij de novemberactie meldde de politie verwijdering van 14 Gootloader-servers in Nederland en zes Nederlandse servers binnen een CastleRAT-actie met 120 servers. Het StealC-cijfer omvatte 80 door de Nederlandse politie verwijderde servers. Dat laatste stelt hun locatie niet vast. Teruggevonden persoonsgegevens waren internationaal. [S71][S72]

Tel de juni- en novembertotalen niet op als onafhankelijke unieke slachtoffers of records. Perioden en infrastructuurrelaties kunnen overlappen. Belangrijker: een server ontmantelen trekt niet alle gestolen inloggegevens in en verwijdert niet alle eerder geplaatste malware.

KERNPUNTEN

01

Houd criminele claims, bedrijfstoeschrijvingen en dienstbeoordelingen op iedere kaart gescheiden.

02

Ransomwarevergelijkingen beschrijven vermeldingen met expliciete perioden, geen nationaal risico.

03

Ook na infrastructuuracties moeten organisaties inloggegevens, toegang en eerdere inbraken valideren.

HOOFDSTUK 08

De fraude-economie en schade na openbaarmaking

DIT HOOFDSTUK BEANTWOORDT

Hoe kan geadverteerde identiteit of een gestolen record een fraude- of veiligheidsprobleem worden?

36

verschillende betaalkaarten zichtbaar als leesbare tekst in de bewaarde berichten, zonder toeschrijving aan uitgevers

8.1 Accounts en identiteit als aangeboden producten 70
8.2 Echte informatie kan een vals verzoek overtuigend maken 74
8.3 Persoonlijke veiligheid na gegevensdiefstal 75
8.4 Betaalkaarten als leesbare tekst: een beperkte waarneming 76
8.5 Politiepreventie toont een reactie, geen verliesbedrag 76

HOOFDSTUK 08

De fraude-economie en schade na openbaarmaking

IN HET KORT

De bewaarde berichten bieden financiële accounts, identiteitsmateriaal, contactlijsten en vermeende toegang aan. Ze tonen aanbiedingen, geen afgeronde transacties of gemeten fraudemarkt. Officiële berichtgeving voegt een ernstiger gevolg toe: gestolen bankklantinformatie gekoppeld aan een poging tot geweld. Verbind fraudemaatregelen, privacycommunicatie en escalatie bij persoonlijke onveiligheid. Valideer getroffen informatie, verifieer betaalinstructies onafhankelijk en geef mensen een duidelijke route voor verdachte benaderingen.

8.1 Accounts en identiteit als aangeboden producten

Binnen de 3.286 bewaarde berichten met landtag die op thema zijn beoordeeld, verschijnt handel in financiële accounts in 1.000 berichten. Identiteits- of verificatiemateriaal verschijnt in 432 en phishing of fraude in 443. Categorieën overlappen en landvermeldingen kunnen terloops zijn. Deze aantallen zijn niet te extrapoleren naar Nederlandse transacties of verliezen. [S1]

Een financieel merk in een advertentie kan het beoogde misbruikproduct beschrijven, niet de bron van een datalek. Een rekeningopeningsaanbod bewijst niet dat een rekening de controles van die instelling doorstond. Een per bank ingedeelde contactlijst bewijst niet dat de bank de lijst leverde.

Een bericht van 20 november biedt een phishingpaneel voor meerdere landen aan, noemt een Nederlandse uitgever en claimt interactieve inlogcodefuncties. Het bewijst geen inzet, effectiviteit of geslaagde omzeiling. Een afzonderlijk aanbod van 8 november beschrijft 265.000 Nederlandse cryptoleads; niet vastgesteld is dat dit het forex-bestand uit Case E betreft. [S1]

Een bericht van 22 november herhaalt de reclametaal voor de kit. De herhaling toont geen daadwerkelijk gebruik, effectiviteit, geslaagde omzeiling of gemeenschappelijke operator aan. [S1]

Bewijskaart B15 20 nov 2026

Verkoper van phishingkits (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

[phishing-panel brand] is a live panel phishing kits customized to target specific banks [...] Netherlands [card issuer] [...] Multi-Country Targeting [...] Mobile and desktop interfaces [...] Live Chat (with victim) [...] OTP/TAN/2FA support [...] [contact removed]

VERTALING

[merk van phishingpaneel] is een livepaneel met phishingkits op maat voor specifieke banken [...] Nederland [kaartuitgever] [...] Gericht op meerdere landen [...] Interfaces voor mobiel en desktop [...] Livechat met het slachtoffer [...] Ondersteuning voor OTP/TAN/2FA [...] [contactgegevens verwijderd]

Opmerking. Een bericht van 22 november herhaalt de reclametaal voor de kit. Herhaling toont verspreiding aan, geen daadwerkelijk gebruik, geslaagde omzeiling of gemeenschappelijke operator.

Vastgesteld
Op 20 november biedt een verkoper een phishingpaneel voor meerdere landen aan dat een Nederlandse kaartuitgever noemt en interactieve ondersteuning voor inlogcodes claimt.

Niet vastgesteld
Daadwerkelijk gebruik, effectiviteit, slachtoffers, het precieze mechanisme, geslaagde omzeiling of een inbraak bij een uitgever.

Bewijskaart B16 8 nov 2026

Verkoper van leadgegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Format: Country + Email + Name + Currency + Phone + Deposits Amount. [...] Premium Dataset [265K] NETHERLANDS CRYPTO LEADS [VIP DATA] [...] [contact removed]

VERTALING

Formaat: land + e-mail + naam + valuta + telefoon + stortingsbedrag. [...] Premiumgegevensverzameling [265.000] NEDERLANDSE CRYPTOLEADS [VIP-GEGEVENS] [...] [contactgegevens verwijderd]

Opmerking. Het is niet vastgesteld dat de geadverteerde cryptoleads hetzelfde bestand zijn als het forex-aanbod in B05.

Vastgesteld
Een bericht van 8 november biedt een gegevensverzameling met 265.000 Nederlandse cryptoleads aan en beschrijft de vermeende velden.

Niet vastgesteld
Herkomst, actualiteit, echtheid, aantal unieke personen of een verband met de forex-lijst van 230.000 rijen.

B17 biedt bankgelabelde leads aan naast andere landen. B18 promoot een vermeende verificatieomzeiling met virtuele camera's. B19 vraagt USD 200 voor een geadverteerde bankrekening, of USD 250 met een gekoppeld exchange-account. Geen daarvan bewijst geleverde rekeningen, rechtmatige identiteiten, bruikbare tegoeden of afgeronde verkopen. Behandel geadverteerde verificatieondersteuning niet als bewezen omzeiling. [S1]

Bewijskaart B17 18 jul 2026

Verkoper van leadgegevens (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

SMS & E-Mail leads DBs on sale. [bank] NL leads, [bank] DE Leads [...] Various countries Leads phone partial email [...] Banking customers leads Dbs - various countries [...]

VERTALING

Databases met sms- en e-mailleads te koop. [bank] NL-leads, [bank] DE-leads [...] Leads uit verschillende landen: telefoon, gedeeltelijk e-mailadres [...] Databases met leads van bankklanten: verschillende landen [...]

Vastgesteld
Een terugkerende verkooptekst biedt bankleads met het label Nederland aan naast andere financiële gegevensverzamelingen.

Niet vastgesteld
Herkomst bij een bank, verzamelingsdatum, aantal unieke personen, geldigheid van de gegevens, identiteit van de exploitant of een afzonderlijk datalek per doorplaatsing.

Bewijskaart B18 13 sep 2026

Promotor op een forum (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

Netherlands Bank kyc bypass | KYC Bypass with Virtual Camera on Android [...] For free and Paid KYC Bypass Methods [...] [bank] Netherlands Virtual Camera [...] [links removed]

VERTALING

KYC van Nederlandse bank omzeilen | KYC omzeilen met een virtuele camera op Android [...] Voor gratis en betaalde methoden om KYC te omzeilen [...] [bank] Nederland virtuele camera [...] [links verwijderd]

Vastgesteld
Een forumpromotie claimt methoden met virtuele camera's voor identiteitsverificatie bij Nederlandse banken.

Niet vastgesteld
Of een methode bestaat of werkt, een geslaagde rekeningopening, aantallen slachtoffers of een datalek bij een bank.

Bewijskaart B19 — 15 apr 2026

Verkoper van accounts (alias weggelaten) | Forumdiscussie | Forum | Engels

ORIGINEEL

[Dutch bank] [...] on your own phone. Price: 200$ (with exchange on same name = 250$) [...] account verified on your own phone [...] NL IBAN - Docs + Selfie [...] Ideal payments [...] [contact removed]

VERTALING

[Nederlandse bank] [...] op je eigen telefoon. Prijs: $200 (met exchange op dezelfde naam = $250) [...] account geverifieerd op je eigen telefoon [...] NL-IBAN - documenten + selfie [...] iDEAL-betalingen [...] [contactgegevens verwijderd]

Vastgesteld
Een verkoper biedt een geverifieerde Nederlandse bankrekening, documenten/selfie en betaalfuncties aan tegen genoemde vraagprijzen.

Niet vastgesteld
Of rekeningen geleverd kunnen worden, eigendom, rechtmatigheid van de identiteit, beschikbare saldi, afgeronde verkopen of misbruik bij de bank.

Twee recente berichten vragen een andere lezing. B20 presenteert een zakelijke bankrekening en zoekt werk; de tekst toont geen criminele bedoelingen aan. B21 vraagt om een database van een cryptodienst, zonder het bestaan ervan aan te tonen. Geen van beide telt als fraude- of slachtofferincident. [S1]

Bewijskaart B20 15 nov 2026

Forumlid (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

I have a small company in netherland named zzp. I have [bank] Business. i can create and more. I m opened for any ideea, any kind of work [...] [contact removed]

VERTALING

Ik heb een klein bedrijf in Nederland, zzp genaamd. Ik heb [bank] Business. Ik kan er meer aanmaken. Ik sta open voor elk idee, elk soort werk [...] [contactgegevens verwijderd]

Opmerking. Het bericht toont geen criminele bedoelingen aan. Het telt niet mee als fraude-incident.

Vastgesteld
Een poster presenteert op 15 november een Nederlandse zakelijke bankrekening en vraagt om werk of voorstellen.

Niet vastgesteld
Criminele bedoelingen, beschikbaarheid van de rekening, identiteit, overboekingen, fraude of een datalek bij een bank.

Bewijskaart B21 10 nov 2026

Koper van databases (alias weggelaten) Forumdiscussie Forum Engels

ORIGINEEL

im looking to buy the [cryptocurrency service] databse [...] [contact removed]

VERTALING

Ik wil de database van [cryptodienst] kopen [...] [contactgegevens verwijderd]

Opmerking. Een koopverzoek toont niet aan dat er een database bestaat.

Vastgesteld
Een forumgebruiker vraagt op 10 november om een database met de naam van een cryptodienst te kopen.

Niet vastgesteld
Of er een database bestaat, hoe oud die is, de herkomst, een verkoop of een inbraak.

Prijzen in afzonderlijke advertenties zijn vraagprijzen. Het bewaarde bewijs toont geen betaling, levering of nationale marktwaarde aan. Een hoge databaseprijs kan een reclameclaim zijn; een gratis bestand kan toch serieus onderzoek rechtvaardigen als het geverifieerde actuele informatie bevat.

8.2 Echte informatie kan een vals verzoek overtuigend maken

Een bericht met iemands echte lidmaatschap, boeking of klantrelatie kan betrouwbaar lijken. De bevestigde incidenten in hoofdstuk 5 tonen waarom geheimhouding van zulke details geen veilig verificatieprincipe is. Dit is een verdedigende interpretatie, geen bewijs dat elk openbaar geworden record voor fraude is gebruikt.

Bevestig betalingen daarom via een route die onafhankelijk van het inkomende verzoek is vastgesteld. Verifieer gewijzigde bankinstructies niet via het nummer in het verdachte bericht. Bedrijfsprocessen moeten aangeven welk bekend record of officieel kanaal de contactroute levert.

Maak de veilige route gemakkelijk vindbaar. Alleen waarschuwen om alert te zijn laat gebruikers improviseren. Vermeld waar betaalverzoeken kunnen worden gecontroleerd, welke informatie de organisatie niet via ongevraagd contact vraagt en hoe benaderingen zonder brede verspreiding van gevoelige gegevens gemeld kunnen worden.

8.3 Persoonlijke veiligheid na gegevensdiefstal

P

CASE P

Revolut-gegevensdiefstal en een poging tot geweld

Bankklanten

Door politie gemeld onderzoek

WAT IS BEVESTIGD	Een politiebericht van 19 november beschrijft diefstal in september van identificerende informatie over honderden Europese Revolut-klanten, waaronder Nederlanders. Het koppelt het onderzoek aan verijdeld geweld en aanhoudingen. Individuele slachtoffers en identificerende locaties worden hier niet overgenomen. [S75]
GEMELD DETAIL	NOS citeerde de bank over 36 getroffen Nederlandse klanten en beschreef imitatie van een Italiaanse instantie. Dit aantal is toegeschreven berichtgeving, geen Nederlands aantal uit het politiebericht. Combineer het niet met andere account- of recordtotalen. [S76]
BEPERKING	Een openbare meldingsdatum is niet de inbraakdatum. Dit rapport reconstrueert niet de volledige criminele keten en leidt niet af dat iedere getroffen persoon dezelfde dreiging ondervond.
REACTIE	Neem een route voor geloofwaardige veiligheidszorgen op in klantincidentafhandeling, met getrainde escalatie naar bevoegde instanties en beperkte toegang tot gevoelige meldingen.

Conclusie

Verbind fraude, privacy en hulp bij persoonlijke veiligheid zonder een sectorbreed percentage aan te nemen.

De operationele kernles is de overdracht. Een klantmelding over een benadering kan bij een fraudeloket, privacymailbox of gewone support binnenkomen. Deze teams moeten een geloofwaardige directe zorg herkennen en doorgeven aan de verantwoordelijke incidentleider. Details horen alleen bij mensen die ze nodig hebben.

Een bank moet de praktische behoeften van de getroffen persoon scheiden van openbare toeschrijving. De klant kan advies nodig hebben voordat de organisatie het gehele incident kan beschrijven. Stel een bekende contactroute vast, registreer de melding en vraag mensen niet zelf de bedreigende partij te onderzoeken.

8.4 Betaalkaarten als leesbare tekst: een beperkte waarneming

REIKWIJDTE VAN DE KAARTCIJFERS

Kaartcijfers betreffen uitsluitend betaalkaarten die als leesbare tekst zichtbaar zijn in de bewaarde berichten. Brandefense detecteert gestolen kaarten ook met andere methoden buiten dit rapport. Deze waarnemingen meten geen nationale kaartdiefstal, actieve kaarten, prevalentie per uitgever of fraude-verliezen.

Het bewaarde resultaat bevat 36 verschillende kaarten, 66 verschijningen en 43 berichten. De merklabels zijn 30 Visa, vijf Mastercard en één Amex. Er wordt geen uitgever toegeschreven. Herhaalde verschijningen zijn geen extra verschillende kaarten en een merklabel is geen genoemde bank. [S4]

De passende operationele actie hangt af van bevoegde validatie. Een betaal- of fraudeteam moet een vertrouwde meldroute voor gecompromitteerde kaarten gebruiken, relevante kaarten binnen zijn bevoegdheid vaststellen en uitgeversbeleid toepassen. Een klein openbaar totaal bewijst niet dat een instelling buiten dat resultaat geen blootstelling heeft.

8.5 Politiepreventie toont een reactie, geen verliesbedrag

Het politiebericht uit januari over ticketfraude beschrijft een gesimuleerde winkeloefening van eind 2025 tot begin 2026. De 3.432 aankooppogingen waren interacties met een preventieoefening, geen gemeten criminele diefstal. Een afzonderlijke januariwaarschuwing betrof frauduleuze e-mails die de politie imiteerden en om een reactie, geld of informatie vroegen. [S78][S79]

Op 21 november meldde de politie een gesimuleerde webshopcampagne voor verzamelkaarten, gestart in september. De 5.312 advertentieklikken beschrijven campagne-interactie. Het zijn geen 5.312 slachtoffers, afgeronde fraudebetalingen of verliesraming. [S77]

KERNPUNTEN

01

Geadverteerde accounts en identiteitsmateriaal zijn aanbiedingen, geen vastgestelde transacties of nationale verliezen.

02

Verbind frauderespons, privacy en geloofwaardige persoonlijke veiligheidszorgen in de klantafhandeling.

03

Leesbare-kaartcijfers en preventie-interacties vereisen elk hun eigen beperkte noemer.

HOOFDSTUK 09

Bankwezen en financiën: onderscheid instelling, klant en leverancier

DIT HOOFDSTUK BEANTWOORDT

Welke financiële conclusies volgen uit de waargenomen domeinen en klantincidenten?

21 van 25

geselecteerde financiële domeinen met gepubliceerd DMARC-quarantine- of rejectbeleid

9.1 De financiële populatie 78

9.2 Drie verschillende risicolocaties 79

9.3 Wat eerst valideren 80

9.4 Meldingen en klantrespons delen één chronologie 80

HOOFDSTUK 09

Bankwezen en financiën: onderscheid instelling, klant en leverancier

IN HET KORT

De financiële categorie omvat banken, betaalbedrijven en handelsbedrijven. Het is geen lijst van 25 vergunninghoudende uitgevers. Openbare technische waarnemingen tonen e-mail- en webinstellingen; de Revolut-zaak betreft een specifiek klantgegevensincident. Blootstellingsrelaties beslaan de financiële categorie; het beperkte kaartresultaat bevat geen uitgeverstoeschrijving. Valideer eerst de institutionele reikwijdte en test vervolgens herstel, betaalwijzigingen en leveranciersroutes die klantinformatie bewaren.

9.1 De financiële populatie

De geselecteerde financiële categorie bevat 25 kandidaatdomeinen, met passieve waarnemingen voor alle 25. Ze is breder dan een banken- of kaartuitgeversgroep. DNB's register onderscheidt vergunninghoudende instellingen en buitenlandse paspoorthouders; de selectie van dit rapport vervangt dat niet. Er wordt geen blootstellingsranglijst per bank gepubliceerd. [S2][S7]

21 van 25

geselecteerde financiële domeinen met waargenomen DMARC-quarantine- of rejectbeleid

25 van 25

geselecteerde financiële domeinen met geldige TLS-resultaten in deze momentopname

19 van 19

waargenomen financiële homepages met HSTS; 6 andere kandidaat-homepages vallen buiten die noemer

0

uitgeverstoeschrijvingen in het beperkte resultaat voor leesbare kaarten, geen nulblootstelling bij uitgevers

REIKWIJDTE VAN DE KAARTCIJFERS

Kaartcijfers betreffen uitsluitend betaalkaarten die als leesbare tekst zichtbaar zijn in de bewaarde berichten. Brandefense detecteert gestolen kaarten ook met andere methoden buiten dit rapport. Deze waarnemingen meten geen nationale kaartdiefstal, actieve kaarten, prevalentie per uitgever of fraudeverliezen.

[S2][S4]

Waarneming	Resultaat	Beperking
DMARC reject / quarantine	16 / 5	Gepubliceerd beleid, geen gemeten phishing-slaagpercentage
Monitoringbeleid / beleid niet waargenomen	3 / 1	Validatie door eigenaar nodig vóór wijziging van legitieme e-mailstromen
SPF / DKIM waargenomen	23 / 23	Een recordwaarneming toont niet het authenticatieresultaat van ieder bericht aan
DS-record waargenomen	18	Toont geen volledige DNSSEC-validatie aan
Geldig TLS-resultaat	25	Beschrijft het waargenomen eindpunt en de momentopname
Homepage / HSTS waargenomen	19 / 19	HSTS-interpretatie gebruikt 19 homepages, niet alle 25 kandidaten
Apparaatrelaties / werknemersdeel	38.085 / 395	Overlappende waarnemingen, geen bevestigde interne inbraken
Inloggegevensrecords / actuele advertenties	178.904 / 11	Records en geselecteerde vermeldingen zijn verschillende populaties
Toegeschreven kaartuitgevers	Geen in dit resultaat	Geen uitgeversvergelijking of koppeling aan de financiële domeincategorie

[S2][S4]

De financiële categorie beslaat 25 geselecteerde vermeldingen, waaronder negen vermeldingen binnen een deelgroep van uitgeversdomeinen. In dit beperkte resultaat komt geen kaart met uitgeverstoeschrijving voor. Deze afwezigheid toont geen nulblootstelling aan kaarten aan. De bredere financiële categorie heeft minstens 38.085 apparaatrelaties, waaronder 395 relaties met werknemersapparaten, en 178.904 inloggegevensrecords. [S2][S4]

9.2 Drie verschillende risicolocaties

Toegang tot de instelling. Het beveiligingsteam moet eigen bevoorrechte accounts, herstelprocedures en extern bereikbare systemen beoordelen. Een klantmerk in een fraudebericht bewijst op zichzelf geen toegang tot die systemen. Omgekeerd bewijst een goed ingesteld openbaar domein niet dat intern accountherstel veilig is.

Klantinformatie en accounts. Het fraudeteam moet beslissingen testen die de geldbestemming veranderen, vertrouwde toegang creëren of gevoelige informatie vrijgeven. Een klant kan overtuigend worden benaderd met echte details zonder dat de aanvaller het actuele instellingswachtwoord heeft. Onafhankelijke bevestiging moet de bevoegdheid voor de gevraagde handeling toetsen.

Leveranciers- en diensttoegang. Klantinformatie kan bij een aanbieder staan of vrijkomen via een proces dat externe verzoeken vertrouwt. De bank moet de relevante dienst, toegestane gebruikers en updateroute kennen. Een leveranciersverklaring vervangt niet de eigen beoordeling van gegevens, klantcommunicatie en toezichtsverplichtingen.

Case P toont waarom deze verantwoordelijkheden moeten samenkomen. Het gemelde incident en latere politieonderzoek vragen een reactie voor getroffen klanten, naast een technische verklaring over de openbare bankwebsite. Die reactie vereist nog steeds persoonsgebonden bewijs; één zaak toont geen sectorbreed percentage aan.

9.3 Wat eerst valideren

Test bij herstel een beller met juiste klant- of medewerkersdetails die de bestaande vertrouwde route niet kan gebruiken. De geautoriseerde oefening moet aantonen of het proces een ingrijpende wijziging toestaat en welk bewijs de beslissing ondersteunt. Neem ook een echte gebruiker met een verloren factor op, zodat de goedgekeurde uitzondering werkbaar blijft.

Test bij betalingen een gewijzigde begunstigde, leveranciersrekening of salarisinstructie via het relevante bedrijfsproces. Beveiliging kan technische waarborgen bepalen, maar financiën en klantoperatie moeten de aanvaardingsbeslissing dragen. Afrondingsbewijs moet een onderschepte test en een registratie van bevoegde uitzonderingen omvatten.

9.4 Meldingen en klantrespons delen één chronologie

Financiële meldingen, privacybeoordeling en klantcommunicatie moeten één feitelijke chronologie gebruiken en hun afzonderlijke juridische toetsen behouden. DORA en AVG hebben verschillende aanleidingen en meldvereisten, zoals hoofdstuk 10 uitlegt. Een vroeg dossier moet vastleggen wat bij iedere beslissing bekend was.

KERNPUNTEN

01

De geselecteerde financiële domeinen vormen geen telling van vergunninghoudende banken of uitgevers.

02

Instellings-, klant- en leveranciersrisico's vereisen verschillend bewijs en verantwoordelijke eigenaren.

03

Test herstel, betaalwijzigingen en meldingen samen, met afzonderlijke juridische beslissingen.

HOOFDSTUK 10

Regelgeving en de nationale respons

DIT HOOFDSTUK BEANTWOORDT

Welke meldtermijn geldt, wie ontvangt de melding en wat moet de incidentverantwoordelijke vastleggen?

15 augustus 2026

datum van inwerkingtreding bevestigd door het Cyberbeveiligingsbesluit

10.1 Wat geldt en wat een entiteitsspecifieke beslissing vraagt 82
10.2 De meldvolgorde voor significante incidenten onder de Cyberbeveiligingswet 82
10.3 Privacymelding is een afzonderlijke risicobeslissing 83
10.4 Financiële ICT-incidenten hebben een andere termijn 83
10.5 Onderzoek en openbare respons zijn geen afgeronde bevindingen 84
10.6 Vier zaken om nu vast te stellen 84

HOOFDSTUK 10

Regelgeving en de nationale respons

IN HET KORT

De Cyberbeveiligingswet geldt; privacy- en financiële plichten hebben eigen aanleidingen en termijnen. Een significant cyberincident, een persoonsgegevenslek en een ernstig financieel ICT-incident vereisen verschillende juridische beoordelingen. Eén gebeurtenis kan meerdere beslissingen vragen. Bepaal toepasselijkheid en ontvangers vóór het incident. Bewaar daarna bewustwording, classificatie, meldingen en updates in één chronologie met een verantwoordelijke en vervanger.

10.1 Wat geldt en wat een entiteitsspecifieke beslissing vraagt

Het nationale overzicht en inwerkingtredingsbesluit stellen 15 augustus 2026 vast als startdatum van het Cyberbeveiligingswetkader. Organisaties moeten de vastgestelde tekst en toepasselijke sectorcriteria gebruiken, niet een oudere invoeringsverwachting. Neem niet aan dat het verwante kader voor kritieke entiteiten dezelfde incidentmeldingstoetsen heeft. [S8][S10]

Kader	Vereiste beslissing	Ontvanger en aandachtspunt
Cyberbeveiligingswet	Bepaal of entiteit en dienst binnen de reikwijdte vallen; registratie-, zorg- en significante-incidentplichten gelden zoals bepaald	Aangewezen CSIRT en bevoegde toezichthouder; gebruik toepasselijke sectorregels [S8][S9][S84]
AVG-artikelen 33–34	Verwerkingsverantwoordelijke beoordeelt het lek en risico; verwerker informeert zijn verantwoordelijke	Relevante toezichthouder en waar vereist getroffen personen; termijnen en toetsen verschillen [S11]
DORA-incidentmelding	Financiële entiteit binnen de reikwijdte beoordeelt of het ICT-incident ernstig is	Relevante financiële autoriteit; de technische norm bepaalt meld- en updatetermijnen [S12]

De Cyberbeveiligingswet bepaalt plafonds van EUR 10 miljoen of 2% voor essentiële entiteiten en EUR 7 miljoen of 1,4% voor belangrijke entiteiten, afhankelijk van welk bedrag hoger is. De percentages betreffen de totale wereldwijde jaaromzet van de onderneming in het voorgaande boekjaar. Deze plafonds gelden voor bepaalde overtredingen, niet voor opgelegde boetes in de zaken hier. [S9]

10.2 De meldvolgorde voor significante incidenten onder de Cyberbeveiligingswet

NCTV beschrijft een significant incident als ernstige feitelijke of mogelijke dienstverstoring of financieel verlies, of aanzienlijke materiële of immateriële schade voor anderen. Sectorcriteria verschillen. De meldroute gebruikt MijnNCSC voor het aangewezen CSIRT en de bevoegde toezichthouder. Voor bepaalde entiteiten gelden andere termijnen. [S84]

Cbw-fase	Algemene termijn volgens NCTV
Vroegtijdige waarschuwing	Binnen 24 uur na kennisname van een significant incident
Incidentmelding	Binnen 72 uur na die kennisname
Eindverslag	Binnen één maand na de incidentmelding

[S84]

Vroege meldingen moeten feiten van schattingen onderscheiden. De melder moet de getroffen dienst, bekende gevolgen, onzekerheden en volgende updateroute kunnen noemen. Een melding kan tijdig zijn zonder te doen alsof de volledige oorzaak of definitieve gevolgen al bekend zijn.

10.3 Privacymelding is een afzonderlijke risicobeslissing

Onder de AVG melden verwerkingsverantwoordelijken zonder onnodige vertraging en waar mogelijk binnen 72 uur na kennisname aan de toezichthouder, tenzij risico voor personen onwaarschijnlijk is. Verwerkers informeren de verantwoordelijke zonder onnodige vertraging. Artikel 34 vereist onverwijlde communicatie aan betrokkenen wanneer waarschijnlijk een hoog risico bestaat, behoudens uitzonderingen. [S11]

De leveranciersmelding en de toezichthoudersmelding door de verantwoordelijke zijn dus verschillende gebeurtenissen. Contracten moeten bruikbare informatie opleveren, inclusief bevestigde feiten en open vragen. Wachten op het definitieve leveranciersonderzoek kan de verantwoordelijke beletten zelf tijdig te beoordelen.

Communicatie aan personen moet praktische opties uitleggen. Een getroffen klant moet weten welke informatie een verdachte benadering kan ondersteunen en hoe contact te verifiëren is. Presenteer een algemene wachtwoordwijziging niet als volledige reactie bij blootstelling van identiteitsdocumenten, boekingsdetails of andere informatie die niet eenvoudig kan worden gereset.

10.4 Financiële ICT-incidenten hebben een andere termijn

Artikel 5 geeft de financiële meldvolgorde:

Fase	Termijn
Initieel	Zo vroeg mogelijk, binnen vier uur na classificatie als ernstig en uiterlijk 24 uur na kennisname
Late classificatie	Als classificatie na het punt van 24 uur volgt, vier uur na classificatie als ernstig
Tussentijds	Binnen 72 uur na de eerste melding
Definitief	Binnen één maand na het tussentijdse verslag of de laatste update

Voor initiële meldingen en tussentijdse rapportages geldt geen weekend- of feestdaguitstel voor kredietinstellingen, centrale tegenpartijen, exploitanten van handelsplatforms en financiële entiteiten die als essentieel of belangrijk zijn aangemerkt. Artikel 5(5) sluit eindrapportages niet van dit uitstel uit. [S12]

Privacy- en financiële meldingen kunnen feiten delen zonder dezelfde juridische conclusie. Eén dossier moet beide ondersteunen; het beslislogboek toont welke toets iedere melder toepaste. Dit is betrouwbaarder dan losse tijdlijnen die later verschillen over wanneer de organisatie wat wist.

10.5 Onderzoek en openbare respons zijn geen afgeronde bevindingen

Het in maart aangekondigde RDI/AP-onderzoek betrof het Odido-incident. De juli-update en ACM-aankondiging onderscheiden beveiliging, zorgplicht en bewaartermijnen. Dit zijn onderzoeken en toezichtstaken, geen definitieve bevindingen die ieder vermeend gebrek of aanvallersaantal vaststellen. [S16][S17][S34]

Een bestuursoefening moet de route van technisch bewijs naar iedere beslissing testen. Vraag wie de melding goedkeurt, wie kan indienen, wie betrokkenen bijpraat en wie redenen vastlegt om niet te melden wanneer de wettelijke toets niet is gehaald. Afrondingsbewijs is het getimede beslisdossier, niet alleen deelname aan de oefening.

10.6 Vier zaken om nu vast te stellen

1. **Toepasselijkheid.** Bepaal relevante entiteiten en diensten, inclusief kritieke leveranciersrelaties, en los juridische onzekerheid vóór een incident op.
2. **Eigenaarschap.** Benoem melder en vervanger voor iedere relevante CSIRT-, toezichts-, privacy- en aangifteroute.
3. **Chronologie.** Bewaar detectie-, kennisname-, classificatie-, meldings- en updatetijden in één dossier met ondersteunende feiten.
4. **Bruikbare meldingen.** Maak sjablonen die bevestigde informatie, schattingen, gevolgen, actie en volgende update scheiden. Test ze met een leverancier en klantgericht team.

Dit hoofdstuk ondersteunt planning. De verantwoordelijke organisatie moet eigen toepasselijkheid, sectorcriteria en meldkanaal aan de actuele gezaghebbende tekst toetsen. Het 90-dagenplan bevat de oefening en het bewijs; een werkelijk materieel incident gaat direct het responsproces in.

KERNPUNTEN

01

Cyber-, privacy- en financiële meldingstoetsen vereisen afzonderlijke beslissingen.

02

Leg kennisname en classificatie expliciet vast, met de juiste melder en vervanger.

03

Leveranciersafspraken en oefeningen moeten tijdige, bruikbare meldingen ondersteunen zonder op definitieve zekerheid te wachten.

HOOFDSTUK 11

Vooruitblik: beslissingen veranderen met het bewijs

11

DIT HOOFDSTUK BEANTWOORDT

Waarop moeten organisaties zich voorbereiden en welke signalen rechtvaardigen een gewijzigd plan?

5

voorwaardelijke oordelen met een relevant signaal voor de eigenaar

11.1 Vijf oordelen 86

11.2 Bewijs dat de beoordeling zou veranderen 87

11.3 Voorwaardelijke oefenscenario's 87

HOOFDSTUK 11

Vooruitblik: beslissingen veranderen met het bewijs

IN HET KORT

Bereid u voor op herhaling van de vastgestelde mechanismen: accountimitatie, leveranciersgegevensverlies, blootgesteld beheer en dienstafhankelijkheid. Het bewijs ondersteunt geen voorspelling van ieder volgend doelwit of nationaal aanvalspercentage. Elk oordeel hieronder noemt basis, beperking en signaal. Wijs een eigenaar aan die deze signalen maandelijks beoordeelt en verander prioriteiten wanneer relevant bewijs verandert.

11.1 Vijf oordelen

Oordeel	Vertrouwen	Basis, beperking en signaal
Als klantrecords bruikbaar blijven voor identiteitscontroles, kunnen incidenten overtuigende vervolgbenaderingen ondersteunen	Gemiddeld, voorwaardelijk	Cases G, O en P tonen waarom gegevens en klantrespons bij elkaar horen. Er is geen vervolgmisbruikpercentage gemeten. Signaal: geverifieerde klantmeldingen met incidentspecifieke informatie
Gedeelde-dienstincidenten blijven een belangrijk scenario voor continuïteitsplanning	Hoog als planningsprioriteit	Cases K, L, M en O betreffen verschillende dienstafhankelijkheden, geen gemeenschappelijke route. Signaal: leveranciersmeldingen en benodigde tijd om de reikwijdte per klant vast te stellen
Actuele openbare technische tekortkomingen vragen validatie door een eigenaar, geen nationale risicoscore	Hoog voor deze selectie	Hoofdstuk 3 bevat afgebakende waarnemingen en groepsoverlap. Signaal: bevestigde correcties, goedgekeurde uitzonderingen en onduidelijk eigendom in het eigen kwestieregister
Voorbereiding op afpersing moet naast herstel ook gegevenspublicatie omvatten	Hoog als voorbereidingsoordeel	Ransomwarevermeldingen zijn claims; de zaken tonen niet voor iedere vermelding een toegangsroute aan. Signaal: geaccepteerde vermeldingsactiviteit plus bewijs specifiek voor de eigen gegevens [S3]
Verbonden middelen en persoonlijke accounts vereisen expliciete eigenaren bij gevoelig werk	Gemiddeld als planningsoordeel	Officieel campagnebewijs betreft specifieke berichten-, camera- en malwareactiviteit. Het voorspelt geen aanval op ieder middel. Signaal: officiële campagne-updates en gevalideerde blootstelling van eigen middelen

11.2 Bewijs dat de beoordeling zou veranderen

Huidige interpretatie	Bewijs dat deze zou veranderen	Betrokken beslissing
Een databaseaanbod is een ongeverifieerd signaal	Bevoegde validatie verbindt materiaal met een specifiek actueel systeem of officiële bevestiging stelt reikwijdte vast	Activeer het relevante incident- en klantbeschermingsproces
Een leveranciersincident heeft onzekere klantreikwijdte	De aanbieder identificeert met bewijs de getroffen klanttenant, records of koppeling	Pas meldings-, indammings- en heraansluitbeslissingen aan
Een domeinwaarneming vraagt eigenaarsvalidatie	De eigenaar bevestigt een productietekortkoming of een goedgekeurde architectuur verklaart het resultaat	Herstel het gebrek of registreer de uitzondering; behoud geen onverklaarde waarschuwing
Een claim over een verbonden systeem heeft onbekende fysieke gevolgen	Lokale registraties en operationeel personeel stellen een onbevoegde instellingwijziging of materiële dienstgevolgen vast	Schaal operationele indamming en continuïteitsrespons op
Een staatstoeschrijving behoort aan de geciteerde bron	De verantwoordelijke bron publiceert met bewijs een wezenlijk andere beoordeling	Werk de toeschrijving bij en behoud bewijsgerichte maatregelen
Een dienststoring heeft geen vastgestelde kwaadwillige oorzaak	Aanbieder of overheid stelt een aanval op de relevante dienst vast	Voeg incidentrespons- en meldbeoordelingen toe aan continuïteitswerk

11.3 Voorwaardelijke oefenscenario's

Een leverancier stuurt een onvolledige melding. Als de melding een dienst noemt maar geen klantgegevens, vraag dan naar de reikwijdte voor de eigen klantbeoordeling. Het signaal is ontbrekende tenant-, gegevens- of koppelingsinformatie. De beslissing betreft wie escaleert, wat voorlopig wordt geïsoleerd en wanneer de volgende update nodig is.

Een beller kent echte details en vraagt een herstelwijziging. Als de beller de bestaande vertrouwde route niet kan gebruiken, volg de goedgekeurde uitzonderingsprocedure. Bekendheid is geen bevoegdheid. Het signaal is de gevraagde vertrouwenswijziging. De beslissing betreft wie die mag autoriseren en welk bewijs in het dossier moet blijven.

Een afstandsbedieningsclaim valt samen met een dienstprobleem. Als lokale meetwaarden of logs een relevante wijziging tonen, betrek bedrijfsvoering direct en beoordeel veilige isolatie. Het signaal is geverifieerd apparaat- of dienstbewijs, niet alleen de advertentie. De beslissing betreft procesbescherming met behoud van een geautoriseerde herstelroute.

De normale communicatieaanbieder is onbeschikbaar. Als responders geen berichten ontvangen of de dienstverantwoordelijke niet bereiken, gebruik de geteste onafhankelijke route. Het signaal is verlies van de vereiste functie. De beslissing betreft wie de status publiceert en hoe het team zonder die dienst leveranciers- en juridische input krijgt.

Deze scenario's zijn planningsaannames, geen gemeten intervallen of claims dat een genoemde organisatie een maatregel miste. Hun waarde ligt in het beslisdossier van een realistische oefening: wat het team wist, deed en wat de volgende actie blokkeerde.

KERNPUNTEN

01

Voorspellingen moeten een voorwaarde, bewijsgrens en waarneembaar signaal noemen.

02

Verander de respons wanneer geverifieerde reikwijdte of operationele gevolgen veranderen.

03

Beoordeel het plan maandelijks en escaleer werkelijke materiële dreigingen onmiddellijk.

HOOFDSTUK 12

Een 90-dagenplan met afrondingsbewijs

12

DIT HOOFDSTUK BEANTWOORDT

Wat moet elk team doen en hoe ziet de leiding dat het werk een echte maatregel veranderde?

23

acties met verantwoordelijke eigenaren en afrondingsbewijs

12.1 Acties en afrondingsbewijs 90
12.2 Een scorekaart voor afgerond werk 93
12.3 Technische referentie: patchstatus en eerdere toegang 94
12.4 Eerste beslissingen per rol 94
12.5 Hoe Brandefense kan helpen 95

HOOFDSTUK 12

Een 90-dagenplan met afrondingsbewijs

IN HET KORT

Begin met een vertrouwde route voor incidentsignalen, accountherstel, leveranciersmeldingen en operationele escalatie. Verhelp daarna bevestigde technische en procestekorten, inclusief browserafhankelijkheden en beheer op afstand. Oefen herstel, fraudeafhandeling en meldtermijnen samen. De data hieronder ordenen verbeterwerk; ze vertragen geen actieve-dreigingsrespons. Rapporteer uiterlijk op dag 90 het afrondingsbewijs, resterende uitzonderingen en verantwoordelijke eigenaren aan de leiding.

12.1 Acties en afrondingsbewijs

Dit is een volgorde, geen wachttijd. Een geloofwaardig materieel signaal gaat direct het incidentproces in. Als vereiste waarschuwingen of leveranciersinformatie ontbreken, registreer de afhankelijke taak als geblokkeerd, benoem de eigenaar en de deblokkerende voorwaarde. Monitoring kan van een intern team of passende aanbieder komen.

Begin direct met patchen of mitigatie volgens gezaghebbende adviezen bij toepasselijke kritieke of actief misbruikte kwetsbaarheden in extern bereikbare diensten. Wacht niet op de onderstaande mijlpalen of signalen van misbruik. [S22]

1Dagen 1-30

Bevestig de route voor relevante account-, gegevensaanbod- en dienstsignalen; test één overdracht naar incidentrespons

EIGENAAR
CISO en dreigingsinformatie

AFRONDINGSBEWIJS
Bron en dienstverantwoordelijke benoemd; test ontvangen en bevestigd

Vereis onafhankelijke verificatie voor wachtwoord-, MFA- en ingrijpende herstelwijzigingen; test een nagebootste collega

EIGENAAR
Identiteitsbeheer en servicedesk

AFRONDINGSBEWIJS
Goedgekeurde procedure; geautoriseerde test onderschept; uitzondering voor echte gebruiker getest

Valideer bij geloofwaardige accounttoegangssignalen eigendom en actuele toegang; trek waar gerechtvaardigd relevante sessies of tokens in

EIGENAAR
Identiteitsbeheer en incidentrespons

AFRONDINGSBEWIJS
Gedateerde beoordeling per signaal; actieve toegangsbeslissingen vastgelegd

Inventariseer kritieke leveranciers met klant-, patiënt-, student-, leden- of zaakgegevens, met incidentcontact en vervanger

EIGENAAR

Inkoop en diensteigenaren

AFRONDINGSBEWIJS

Gedateerde diensten-/gegevenslijst; contacten met succes getest

Breng toepasselijke Cbw-, AVG- en DORA-plichten in kaart, inclusief kennisname, classificatie, ontvanger en melder

EIGENAAR

Juridische zaken, privacy en CISO

AFRONDINGSBEWIJS

Entiteitsspecifieke meldkaart goedgekeurd; vervangers benoemd

Identificeer koeling en andere operationele besturingen met beheer op afstand; valideer toegangseigenaar en veilige isolatiebeslissing

EIGENAAR

Bedrijfsvoering, facilitair beheer en OT

AFRONDINGSBEWIJS

Eigen middelen beoordeeld; onveilige routes aangepakt of urgente uitzonderingen geëscaleerd

Test incidentcommunicatie zonder normale cloudmail of samenwerkingsdienst

EIGENAAR

Incidentleider en communicatie

AFRONDINGSBEWIJS

Dienstcontacten bereikt; statusupdate goedgekeurd via onafhankelijke route

Bereid klantsupportescalatie voor op geloofwaardige veiligheidszorgen na gegevensdiefstal

EIGENAAR

Fraude, klantoperatie en beveiliging

AFRONDINGSBEWIJS

Vertrouwelijke route getest; medewerkers kennen het dienst-contact

2Dagen 31-60

Valideer bevoegde e-mailafzenders en voer waar passend gefaseerde DMARC-handhaving in

EIGENAAR

E-mailbeheer en zakelijke afzenders

AFRONDINGSBEWIJS

Inventaris van uitgelijnde afzenders; gecontroleerde test en terugdraaiprocedure

Rond de geplande patchachterstand voor extern bereikbare producten uit relevante gezaghebbende waarschuwingen af; verifieer herstel en beslis afzonderlijk of eerdere toegang onderzoek vereist

EIGENAAR

Infrastructuur en incidentrespons

AFRONDINGSBEWIJS

Bewijs van middel/versie en verificatie; afzonderlijke beslissing over toegangsonderzoek vastgelegd

Inventariseer browserscripts van derden en wijzigingsbevoegde accounts; test nooduitschakeling

EIGENAAR

Web, beveiliging en digitale marketing

AFRONDINGSBEWIJS

Afhankelijkheidseigenaar en wijzigingstoegang bekend; uitschakel-/terugdraaitest geslaagd

Spreek bewijs voor leveranciersheraansluiting af, inclusief bedrijfsgoedkeuring en terugdraaien

EIGENAAR

Diensteigenaren en leveranciersbeheer

AFRONDINGSBEWIJS

Heraansluitchecklist geoefend op één kritieke afhankelijkheid

Test gewijzigde betaal- of boekingsinstructies tegen een aanvaller met echte klantdetails

EIGENAAR

Financiën, fraude en klantoperatie

AFRONDINGSBEWIJS

Onafhankelijke verificatie onderschept een geautoriseerde simulatie

Stel meldings- en hersteladvies op voor werkgerelateerde persoonlijke berichtenaccounts

EIGENAAR

Beveiliging en relevante bedrijfseigenaren

AFRONDINGSBEWIJS

Beoordeling van apparaatkoppelingen/herstel beschikbaar; vertrouwelijke escalatie getest

Controleer camerabeheer en opnametoegang bij gevoelige activiteiten

EIGENAAR

Facilitair beheer en beveiliging

AFRONDINGSBEWIJS

Bevoegde toegangslijst; standaardtoegang of onnodige externe toegang verwijderd

Controleer exports en tijdelijke gegevenskopieën uit dienstomwegen

EIGENAAR

Privacy en gegevenseigenaren

AFRONDINGSBEWIJS

Kopielocaties en toegang afgestemd; bewaar-/verwijderbeslissingen vastgelegd

Werk klantmeldingen bij met onderscheid tussen getroffen informatie, dienststatus, veilige verificatie en volgende update

EIGENAAR

Privacy, communicatie en support

AFRONDINGSBEWIJS

Goedgekeurde sjablonen getest op twee wezenlijk verschillende zaken

3Dagen 61-90

Herstel één kritisch bedrijfsproces via de gedocumenteerde terugvaloptie en stem tijdelijk werk af

EIGENAAR

Infrastructuur en proceseigenaar

AFRONDINGSBEWIJS

Getimed resultaat tegen hersteldoel; afstemmingsbewijs

Oefen een onvolledige leveranciersmelding tegelijk met een onbeschikbare koppeling

EIGENAAR

Incidentrespons, leverancier en bedrijfseigenaar

AFRONDINGSBEWIJS

Reikwijdtevragen, beslissingen, updatetijden en blokkades vastgelegd

Oefen waar van toepassing Cbw-, privacy- en financiële meldingen met één chronologie

EIGENAAR

Juridische zaken, privacy en wettelijke melders

AFRONDINGSBEWIJS

Getimede kennisname-/classificatiebeslissingen en conceptmeldingen bewaard

Voer een geautoriseerde fraude-/herstelsimulatie uit met een uitzondering voor een echte gebruiker en klantescalatie

EIGENAAR

Fraude en identiteitsbeheer

AFRONDINGSBEWIJS

Fraudepoging gestopt; legitiem herstel voltooid via goedgekeurde route

Controleer bevestigde domein-, certificaat- en headertekorten opnieuw na herstel

EIGENAAR

Netwerk-, web- en e-mailbeheer

AFRONDINGSBEWIJS

Voor-/nabewijs; goedgekeurde uitzonderingen hebben eigenaren en data

Presenteer scorekaart, uitzonderingen en afrondingsbewijs per rij aan de leiding

EIGENAAR

CISO en verantwoordelijke diensteigenaren

AFRONDINGSBEWIJS

Bestuursstuk met restrisico's, beslissingen en einddata

12.2 Een scorekaart voor afgerond werk

De doelen hieronder zijn voorgestelde uitgangspunten voor het eigen beheersprogramma. Ze meten niet hoe Nederlandse organisaties al werken. Pas ze aan de bedrijfscontext aan en registreer wie een uitzondering goedkeurt.

Maatstaf	Voorgesteld doel
Kritieke diensten met incidentverantwoordelijke, vervanger en getest contact	100% uiterlijk op dag 30
Geloofwaardige toegangssignalen met gedateerde beoordeling door een eigenaar	Binnen vijf werkdagen, of directe incidentescalatie bij materieel belang
Kritieke gegevensleveranciers met geteste meldroute	100%, of een gedateerde uitzondering, uiterlijk op dag 60
Ingrijpende herstelwijzigingen via het goedgekeurde verificatieproces	100%; uitzonderingen onafhankelijk geautoriseerd en vastgelegd

Maatstaf	Voorgesteld doel
Beheer op afstand van operationele besturingen met verantwoordelijke eigenaar	100% uiterlijk op dag 30; urgente onveilige toegang direct behandelen
Browserafhankelijkheden van derden met eigenaar en uitschakelplan	100% van kritieke klantreizen, of een gedateerd plan, uiterlijk op dag 60
Toepasselijke meldroutes getest met benoemde vervangers	Voltooid uiterlijk op dag 90
Herstel van kritieke processen en afstemming van tijdelijk werk	Geslaagd tegen het eigen doel, of een gedateerde herstelactie, uiterlijk op dag 90

12.3 Technische referentie: patchstatus en eerdere toegang

Het PHP-advies van het NCSC uit oktober toont het onderscheid tussen preventie en een bevestigde aanval. Het bericht scheidde voorzorgssluiting van vastgestelde binnendringing. De PHP-adviezen noemen herstelde versietakken voor CVE-2026-109618 en CVE-2026-109619. Tijdelijke terugtrekking van een site bewijst niet dat een van beide fouten daar is misbruikt. [S22][S25][S26][S27][S28]

PHP-tak	Getroffen versies voor beide CVE's	Herstelde versie
8.2	8.2.x vóór 8.2.35	8.2.35
8.3	8.3.x vóór 8.3.36	8.3.36
8.4	8.4.x vóór 8.4.27	8.4.27
8.5	8.5.x vóór 8.5.12	8.5.12

De adviezen noemen geen herstelde versies voor oudere, niet meer ondersteunde takken. Migreer zulke installaties naar een ondersteunde tak. [S25][S26][S27][S28]

De eigenaar moet de gebruikte versietak aan het gezaghebbende advies koppelen, de wijziging vastleggen en de blootgestelde dienst verifiëren. Een afgeronde patchregistratie mag niet stilzwijgend een onderzoek naar eerdere toegang sluiten. De Ivanti-campagne in Case H geeft de afzonderlijke reden om te vragen wat vóór herstel gebeurde.

12.4 Eerste beslissingen per rol

Rol	Eerste beslissing
Bestuur en directie	Vraag welke kritieke dienst-, leveranciers- en herstelbeslissingen geteste eigenaren hebben en welke uitzonderingen middelen vereisen

Rol	Eerste beslissing
CISO	Verbind relevant bewijs met incidentverantwoordelijkheid, leveranciersreikwijdte en meldchronologie
SOC en incidentrespons	Definieer de onderzochte bewering, bewaar bewijs en maak van een waarschuwing geen onbewezen toeschrijving
Identiteitsbeheer en servicedesk	Stel bevoegdheid voor herstelwijzigingen onafhankelijk van de kennis van de beller vast
Infrastructuur, web en bedrijfsvoering	Bevestig het relevante middel, de externe beheerroute en veilige herstel- of isolatieroute
Fraude en klantoperatie	Verifieer ingrijpende instructies via bekende kanalen en escaleer geloofwaardige veiligheidszorgen snel
Privacy, juridische zaken en communicatie	Houd reikwijdte, juridische toetsen, openbare verklaringen en updates consistent zonder op volledige zekerheid te wachten

KERNPUNTEN

01

Bevestig signaalroutes, herstelbevoegdheid en operationeel eigendom in de eerste 30 dagen.

02

Verhelp uiterlijk op dag 60 gevalideerde leveranciers-, browser-, toegangs- en communicatietekorten.

03

Toon uiterlijk op dag 90 herstel, meldingen en frauderespons aan met bewijs en beheerde uitzonderingen.

12.5 Hoe Brandefense kan helpen

Brandefense combineert Cyber Threat Intelligence, Digital Risk Protection en External Attack Surface Management. Het rapport toont hoe externe berichten, openbare technische waarnemingen en ransomwareclaims afgebakende onderzoeksvragen ondersteunen. Een signaal is het bruikbaarst wanneer het verbonden is met middelen, gegevens en beslissingen die de organisatie kan valideren.

Een demonstratie kan die relatie tonen met de domeinen, merken en beveiligingsprioriteiten van de organisatie. Bespreek wat een dienst waarneemt, welke eigenaar een relevant signaal ontvangt en hoe de organisatie een beoordeling vastlegt. Historische informatie en criminele claims vereisen nog steeds validatie.

Vraag een demo aan

BIJLAGEN

Bijlagen

A–D

DIT HOOFDSTUK BEANTWOORDT

Bijlage A. Reikwijdte, bewijs en interpretatie · Bijlage B. Bewijsregister van berichten · Bijlage C. Bronnen · Bijlage D. Begrippenlijst

109
bronnen

Bijlage A. Reikwijdte, bewijs en interpretatie 97
Bijlage B. Bewijsregister van berichten 100
Bijlage C. Bronnen 102
Bijlage D. Begrippenlijst 107

Bijlage A. Reikwijdte, bewijs en interpretatie

A.1 Periode en bronppopulaties

De onderzoeksperiode loopt van 1 januari tot de bewaarde momentopname op 22 november 2026. De recente-activiteitsperiode begint op 8 november. De peildag beschrijft de gebruikte momentopname en garandeert geen dekking tot middernacht. Bericht-, incident-, meldings- en updatedata blijven gescheiden.

Brandefense Blackhole-berichten, openbare waarnemingen van geselecteerde domeinen, Ransompedia-vermeldingen en waarnemingen van leesbare betaalkaarten zijn afzonderlijke populaties. Bedrijfsverklaringen, overheden en technisch onderzoek leveren extern bewijs en context. Het rapport combineert ze niet tot een nationaal aanvalsaantal. [S1][S2][S3][S4]

A.2 Ondergrondse berichten

De bewaarde populatie omvat 5.160 berichten, waaronder 329 uit de recente periode. Landtagtotalen bedragen 127.762, met 3.286 bewaarde tagberichten. Thema- en taaltabellen betreffen die bewaarde tagdeelverzameling; de platformtabel betreft de gezamenlijke bewaarde verzameling. Landvermeldingen kunnen terloops zijn en talen kunnen overlappen. [S1]

Berichten tonen advertenties, verzoeken, beweringen of reacties aan. Ze bewijzen geen unieke incidenten, werkende toegang, echte gegevens, nationaliteit van de dader of afgeronde verkopen. Een doorplaatsing toont verspreiding aan; een oude gebeurtenis wordt niet actueel door een nieuwe advertentie.

A.3 Geselecteerde kandidaatdomeinen

De verzameling bevat 250 kandidaatdomeinen in twaalf sectorcategorieën, met blootstellingswaarnemingen voor alle vermeldingen en passieve waarnemingen voor 249. Vermeldingen kunnen instellingen, groepen of operationele merken vertegenwoordigen. Groepsoverlap en domein-/entiteitsonzekerheid beletten interpretatie als onafhankelijke nationale organisaties of representatieve populatie. De niet-beschikbare kandidaat telt niet als falende maatregel. [S2]

A.4 Grens van Atlas-blootstelling

De nationale Atlas-hoofdwaarde is 50 op 100 voor 250 geselecteerde vermeldingen. Alleen die nationale beoordeling wordt gepubliceerd. Apparaat-, inloggegevens-, advertentie- en documentrelaties beschrijven de bewaarde momentopname, kunnen overlappen en historisch materiaal bevatten. Zij tonen geen unieke personen, actuele werkende accounts of bevestigde inbraken aan. [S2]

A.5 Passieve instellingen

Openbare resultaten betreffen het waargenomen domein en de momentopname. DMARC-handhaving betekent gepubliceerd quarantine- of rejectbeleid. Niet-waargenomen DKIM bewijst geen afwezigheid van ondertekening. Een DS-record bewijst geen geldige DNSSEC-keten. Certificaat-, homepage- en HSTS-resultaten gebruiken hun werkelijke waarnemingsbasis. [S2][S85][S86][S88]

A.6 Reikwijdte van kaartcijfers

Alleen betaalkaarten die als leesbare tekst zichtbaar zijn in de bewaarde berichten tellen mee: 36 verschillende kaarten, 66 verschijningen en 43 berichten, zonder uitgeverstoeschrijving. Brandefense detecteert gestolen kaarten ook met andere methoden buiten dit rapport. Deze cijfers meten geen actieve kaarten, nationale diefstal, uitgeversprevalentie of verliezen. [S4]

A.7 Ransomwarevergelijking

Ransompedia bevat 77 geaccepteerde Nederlandse vermeldingen uit de onderzoeksperiode. Vergelijkingslanden gebruiken de overeenkomstige bewaarde periode; de vorigejaarskolom beslaat heel 2025. Aantallen beschrijven criminele claims en kunnen herhaalde slachtofferverwijzingen bevatten. Het zijn geen unieke bevestigde inbraken of voor bevolkingsomvang gecorrigeerde nationale risico's. [S3]

A.8 Incidentdatering en uitsluitingen

Campagnes, afzonderlijke voorbeelden, leveranciersmeldingen, latere updates, opsporing en preventie worden overal onderscheiden. Een collectieve melding stelt niet de volledige klant- of personenpopulatie vast. Een wereldwijd cijfer wordt niet Nederlands doordat Nederlandse autoriteiten aan de respons deelnamen.

De volgende grenzen voorkomen dat oudere of ongerelateerde berichtgeving in actuele Nederlandse incidentconclusies belandt:

Materiaal	Behandeling
Botnetbericht van september 2024 [S80]	Historische context, uitgesloten van incidentconclusies voor 2026
DDoS-berichten uit april en juni 2025 [S81][S82]	Historische context, gescheiden van geverifieerde DigiD-berichtgeving uit 2026
Ransomwarebericht van april 2024 [S83]	Historische context, geen nieuwe campagne in 2026
Opnieuw gepubliceerde maritieme berichtgeving over een gebeurtenis uit juni 2023 [S100]	Toont geen nieuw havenincident in 2026 aan

Materiaal	Behandeling
Treinpasmelding uit 2026 met bestandsoverdracht in december 2025	Opgenomen als meldingscontext in Case R, met expliciete gebeurtenisdatum
Onbevestigde beschuldigingen over een boekhouddienst of havenransomware	Geen openbare zaak of aanvaard incidentoordeel zonder ondersteunend bewijs
GPS-verstoring en cloudstoring	Continuïteitsbewijs, zonder vastgestelde kwaadwillige oorzaak in de aangehaalde officiële beschrijvingen
B22 en B23	Zichtbare uitsluitingsvoorbeelden; geen vastgesteld Nederlands incident

Afwezigheid uit dit rapport bewijst geen afwezigheid van een incident. Private transacties, niet-gemelde incidenten en onvolledige openbare informatie beperken het beeld. Het rapport claimt geen volledige telling van Nederlandse cybercriminaliteit.

A.9 Vertrouwen, naamgeving en openbare bescherming

Vertrouwen geldt voor een specifieke bewering. Een correct weergegeven criminele uitspraak kan hoog vertrouwen verdienen als berichtwaarneming terwijl de beweerde inbraak ongeverifieerd blijft. Alternatieven en beperkingen blijven zichtbaar waar ze de beslissing beïnvloeden.

Slachtoffernamen vereisen officiële bevestiging en brede berichtgeving; elders blijven algemene rollen passend. Actortoeschrijving blijft bij het bedrijf, de overheid of onderzoeker die haar doet. Openbare fragmenten laten persoonsgegevens, contactroutes en werkende indicatoren weg. Volledige gevoelige herkomstinformatie valt buiten dit openbare rapport.

Bijlage B. Bewijsregister van berichten

Iedere getoonde kaart vermeldt berichtdatum, algemene vindplaats, rollabel en grenzen aan de conclusies. Berichtdata zijn geen inbraakdata. Korte fragmenten behouden verwijderingen tussen blokhaken; B22 en B23 worden als uitsluitingen getoond, niet als Nederlands incidentbewijs. Volledige gevoelige herkomstinformatie valt buiten dit openbare rapport.

Kaart	Geplaatst	Vindplaats	Getoonde alias	Taal	Getoond in
B01	2026-02-19	Forumdiscussie	Verkoper van gegevens (alias weggelaten)	Engels	§4.4
B02	2026-11-08	Forumdiscussie	Verkoper van zorggegevens (alias weggelaten)	Engels	§4.4
B03	2026-10-18	Forumdiscussie	Verkoper van retailgegevens (alias weggelaten)	Engels	§4.4
B04	2026-04-03	Forumdiscussie	Verkoper van toegang (alias weggelaten)	Engels	§4.4
B05	2026-07-30	Forumdiscussie	Verkoper van leadgegevens (alias weggelaten)	Engels	§4.4
B06	2026-08-23	Forumdiscussie	Uploader op een forum (alias weggelaten)	Engels	§4.4
B07	2026-06-01	Forumdiscussie	Doorplaatser op een forum (alias weggelaten)	Engels	§4.5
B08	2026-01-31	Forumdiscussie	Uploader op een forum (alias weggelaten)	Engels	§4.5
B09	2026-02-01	Forumdiscussie	Verkoper van onderwijsgegevens (alias weggelaten)	Engels	§4.5
B10	2026-05-10	Forumdiscussie	Forumposter (alias weggelaten)	Engels	§4.5
B11	2026-05-03	Forumdiscussie	Verkoper van retailgegevens (alias weggelaten)	Engels	§4.5

Kaart	Geplaatst	Vindplaats	Getoonde alias	Taal	Getoond in
B12	2026-08-11	Forumdiscussie	Geautomatiseerde uploader (alias weggelaten)	Engels	§4.6
B13	2026-06-26	Forumdiscussie	Geautomatiseerde uploader (alias weggelaten)	Engels	§4.6
B14	2026-09-02	Forumdiscussie	Koper van logs (alias weggelaten)	Engels	§4.6
B15	2026-11-20	Forumdiscussie	Verkoper van phishingkits (alias weggelaten)	Engels	§8.1
B16	2026-11-08	Forumdiscussie	Verkoper van leadgegevens (alias weggelaten)	Engels	§8.1
B17	2026-07-18	Forumdiscussie	Verkoper van leadgegevens (alias weggelaten)	Engels	§8.1
B18	2026-09-13	Forumdiscussie	Promotor op een forum (alias weggelaten)	Engels	§8.1
B19	2026-04-15	Forumdiscussie	Verkoper van accounts (alias weggelaten)	Engels	§8.1
B20	2026-11-15	Forumdiscussie	Forumlid (alias weggelaten)	Engels	§8.1
B21	2026-11-10	Forumdiscussie	Koper van databases (alias weggelaten)	Engels	§8.1
B22	2026-05-02	Forumdiscussie	Forumposter (alias weggelaten)	Indonesisch origineel; bewaarde Engelse vertaling geciteerd	§4.7; uitgesloten
B23	2026-11-09	Forumdiscussie	Verkoper van toegang (alias weggelaten)	Engels	§4.7; uitgesloten
B24	2026-08-21	Forumdiscussie	Doorplaatser op een forum (alias weggelaten)	Engels	§4.5

Bijlage C. Bronnen

Verwijzingen behouden hun bron-ID's tussen edities. Eigen gegevens hebben geen openbare dataset-URL. Externe vermeldingen noemen bron en controledatum; als een artikelpad een weggelaten doelwit identificeert, blijft alleen de hoofd-URL van de uitgever staan.

S1: Odin by Brandefense, Bewaarde Nederland-gerelateerde ondergrondse berichten. Bewaarde onderzoeksmomentopname, 22 november 2026.

S2: Odin by Brandefense, Atlas- en Blackhole-blootstellingsrelaties voor 250 geselecteerde kandidaatdomeinen, gelezen op 21–22 november 2026, plus passieve waarnemingen. Bewaarde onderzoeksmomentopname, 22 november 2026.

S3: Ransompedia, Momentopname van Nederlandse en regionale ransomwarevermeldingen. Bewaarde onderzoeksmomentopname, 22 november 2026.

S4: Brandefense Blackhole, Betaalkaarttotalen in bewaarde berichten. Bewaarde onderzoeksmomentopname, 22 november 2026.

S5: NCSC, DTC en NCSC samengevoegd per 1 januari 2026 (2026-01-06). https://www.ncsc.nl/nieuws/versterkt-ncsc-alle-nederlandse-organisaties-krijgen-een-aanspreekpunt-voor-digitale-weerbaarheid. Gecontroleerd op 2026-11-22.

S6: CBS, ICT-gebruik bij bedrijven, Digitalisering en kenniseconomie 2025 (2026-02-10). https://www.cbs.nl/nl-nl/longread/rapportages/2026/digitalisering-en-kenniseconomie-2025/3-ict-gebruik-bij-bedrijven. Gecontroleerd op 2026-11-22.

S7: De Nederlandsche Bank, Register van banken. https://www.dnb.nl/openbaar-register/register-van-banken/. Gecontroleerd op 2026-11-22.

S8: NCTV, Cyberbeveiligingswet. https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet. Gecontroleerd op 2026-11-22.

S9: Staatsblad, Cyberbeveiligingswet, Staatsblad 2026,187 (2026-07-10). https://zoek.officielebekendmakingen.nl/stb-2026-187.html. Gecontroleerd op 2026-11-22.

S10: Staatsblad, Cyberbeveiligingsbesluit, Staatsblad 2026,189 (2026-07-10). https://zoek.officielebekendmakingen.nl/stb-2026-189.html. Gecontroleerd op 2026-11-22.

S11: EUR-Lex, Algemene verordening gegevensbescherming, artikelen33–34 (2016-04-27). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. Gecontroleerd op 2026-11-22.

S12: EUR-Lex, Technische norm voor DORA-incidentmeldingen, Verordening2025/301 (2025-02-20). https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng. Gecontroleerd op 2026-11-22.

S13: Odido, Eerste melding van cyberaanval (2026-02-12). https://newsroom.odido.nl/en-us/odido-informs-customers-of-cyber-attack/. Gecontroleerd op 2026-11-22.

S14: Odido, Bijgewerkte FAQ over cyberaanval. https://www.odido.nl/veiligheid-eng. Gecontroleerd op 2026-11-22.

S15: Politie, Stem van vermoedelijke beller bij diefstal uit klantsysteem (2026-09-07). https://www.politie.nl/nieuws/2026/september/7/11-stem-van-verdachte-odido-hack-te-horen-in-opsporing-verzocht.html. Gecontroleerd op 2026-11-22.

S16: RDI, Gezamenlijk onderzoek en juli-update over klantsysteemincident (2026-03-26). https://www.rdi.nl/actueel/nieuws/2026/03/26/rdi-en-ap-starten-onderzoek-naar-aanleiding-van-het-incident-bij-odido. Gecontroleerd op 2026-11-22.

S17: ACM, ACM sluit aan bij onderzoek naar telecomdatalek (2026-07-13). https://www.acm.nl/en/publications/acm-joins-investigations-data-breach-dutch-telecom-operator-odido. Gecontroleerd op 2026-11-22.

S18: ChipSoft, Tijdlijn van ransomware-incident bij leverancier (2026-04-28). https://informatie.chipsoft.com/chip-soft-informatiepagina-ransomware-incident/. Gecontroleerd op 2026-11-22.

S19: Ahold Delhaize, Update over cyberbeveiligingsincident (2026-10-19). https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident. Gecontroleerd op 2026-11-22.

S20: Ahold Delhaize, Tussentijds rapport derde kwartaal2026 (2026-11-04). https://media.aholddelhaize.com/media/voehurnq/ahold-delhaize-q3-2026-interim-report.pdf. Gecontroleerd op 2026-11-22.

S21: NCSC, Tijdlijn van misbruik van Ivanti EPMM (2026-02-27). https://www.ncsc.nl/alerts/casus-kwetsbaarheden-ivanti-epmm-systemen. Gecontroleerd op 2026-11-22.

S22: NCSC, Bijgewerkt advies over PHP-kwetsbaarheden (2026-10-23). https://www.ncsc.nl/alerts/update-php-kwetsbaarheden-nog-steeds-reden-om-direct-te-patchen. Gecontroleerd op 2026-11-22.

S25: NVD, Registratie van CVE-2026-109618 (2026-10-21). https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2026-109618. Gecontroleerd op 2026-11-22.

S26: NVD, Registratie van CVE-2026-109619 (2026-10-21). https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2026-109619. Gecontroleerd op 2026-11-22.

S27: PHP Security Team, Advies over PHP-geheugenuitputting (2026-10-21). https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w. Gecontroleerd op 2026-11-22.

S28: PHP Security Team, Advies over verouderde toestand in PHP (2026-10-21). https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp. Gecontroleerd op 2026-11-22.

S29: Report URI, Kwaadaardige scripts verspreid via experimentleverancier (2026-11-16). https://blog.report-uri.com/worlds-largest-brands-infected-with-malware-via-optimizely/. Gecontroleerd op 2026-11-22.

S30: Tweakers, Klantgegevensincident bij webshop (organisatie weggelaten) (2026-09-18). https://tweakers.net/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S31: ncsc.nl, Actieve misbruikcampagne (sectoroverstijgend). https://www.ncsc.nl/alerts/casus-kwetsbaarheden-ivanti-epmm-systemen. Gecontroleerd op 2026-11-22.

S32: open.overheid.nl, Misbruik van systeem voor mobiel beheer (openbaar bestuur / rechtspraak). https://open.overheid.nl/documenten/3ea80b7e-deca-41cc-82f6-3a1b9ab84120/file. Gecontroleerd op 2026-11-22.

S33: nos.nl, Misbruik van systeem voor mobiel beheer (openbaar bestuur / rechtspraak) (2026-02-06). https://nos.nl/artikel/2601216-datalek-bij-autoriteit-persoonsgegevens-en-raad-voor-de-rechtspraak. Gecontroleerd op 2026-11-22.

S34: autoriteitpersoonsgegevens.nl, Klantcontactgegevensdiefstal / afpersing (telecommunicatie) (2026-03-26). https://www.autoriteitpersoonsgegevens.nl/actueel/ap-en-rdi-starten-onderzoek-naar-odido. Gecontroleerd op 2026-11-22.

S35: nos.nl, Klantcontactgegevensdiefstal / afpersing (telecommunicatie) (2026-02-12). https://nos.nl/artikel/2602080-hack-bij-odido-gegevens-miljoenen-klanten-in-handen-van-criminelen. Gecontroleerd op 2026-11-22.

S36: aivd.nl, Phishingcampagne tegen berichtenaccounts (doelwitselectie overheid / defensiesector / media) (2026-03-09). https://www.aivd.nl/actueel/nieuws/2026/03/09/rusland-voert-cybercampagne-uit-tegen-signal--en-whatsapp-accounts. Gecontroleerd op 2026-11-22.

S37: rijksoverheid.nl, Onbevoegde systeemtoegang / verstoring door indamming (Rijksoverheid) (2026-03-23). https://www.rijksoverheid.nl/actueel/nieuws/2026/03/23/ministerie-van-financien-onderzoekt-ongeautoriseerde-toegang-tot-systemen. Gecontroleerd op 2026-11-22.

S38: nos.nl, Onbevoegde systeemtoegang / verstoring door indamming (Rijksoverheid) (2026-03-23). https://nos.nl/artikel/2607547-ministerie-van-financien-gehackt-systemen-geblokkeerd-door-ministerie. Gecontroleerd op 2026-11-22.

S39: politie.nl, Phishing / kortdurende onbevoegde toegang (opsporing). https://www.politie.nl/nieuws/2026/maart/25/00-politie-doelwit-van-phishing.html. Gecontroleerd op 2026-11-22.

S40: ad.nl, Phishing / kortdurende onbevoegde toegang (opsporing) (2026-03-25). https://www.ad.nl/binnenland/hacker-had-uur-lang-toegang-tot-politiedata-na-phishingactie-maar-schade-lijkt-beperkt~a39827e6/. Gecontroleerd op 2026-11-22.

S41: epe.nl, ClickFix-gerelateerde netwerkinbraak en bestandsdiefstal (gemeentebestuur). https://www.epe.nl/datalek-gemeente-epe. Gecontroleerd op 2026-11-22.

S42: nos.nl, ClickFix-gerelateerde netwerkinbraak en bestandsdiefstal (gemeentebestuur) (2026-04-23). https://nos.nl/artikel/2611660-persoonsgegevens-van-vrijwel-alle-inwoners-epe-gestolen-bij-cyberaanval. Gecontroleerd op 2026-11-22.

S43: ncsc.nl, Campagne via softwareleveringsketen (softwareontwikkeling). https://www.ncsc.nl/alerts/ontwikkelaars-opgelet-gecompromitteerde-npm-en-python-packages. Gecontroleerd op 2026-11-22.

S44: z-cert.nl, Ransomware en patiëntgegevensdiefstal (zorgsoftware / zorg) (2026-04-17). https://z-cert.nl/actueel/nieuws/ransomware-incident-chipsoft-nieuwe-informatie-17-april. Gecontroleerd op 2026-11-22.

S45: theregister.com, Ransomware en patiëntgegevensdiefstal (zorgsoftware / zorg) (2026-04-08). https://www.theregister.com/security/2026/04/08/ransomware-knocks-dutch-healthcare-software-vendor-offline/5220887. Gecontroleerd op 2026-11-22.

S46: s25.q4cdn.com, Onbevoegde toegang tot gastboekingsinformatie (reistechnologie). https://s25.q4cdn.com/383369491/files/content_files/BKNG-3Q26-10Q.pdf. Gecontroleerd op 2026-11-22.

S47: abc.net.au, Onbevoegde toegang tot gastboekingsinformatie (reistechnologie) (2026-04-13). https://www.abc.net.au/news/2026-04-13/booking-com-data-security-breach-personal-details/106557630. Gecontroleerd op 2026-11-22.

S48: Brits NCSC, AIVD en MIVD, Advies over verborgen netwerken met China-verband (sectoroverstijgend / nationale veiligheid) (2026-04-23). https://www.ncsc.gov.uk/news/international-cyber-agencies-fresh-advice-defend-against-china-linked-covert-networks. Gecontroleerd op 2026-11-22.

S49: uva.nl, Gegevensdiefstal bij leverancier en voorzorgssluiting (hoger onderwijs / onderwijstechnologie) (2026-05-07). https://www.uva.nl/content/nieuws/nieuwsberichten/2026/05/stand-van-zaken-datalek-bij-leverancier-canvas.html. Gecontroleerd op 2026-11-22.

S50: nos.nl, Gegevensdiefstal bij leverancier en voorzorgssluiting (hoger onderwijs / onderwijstechnologie) (2026-05-08). https://nos.nl/artikel/2613564-universiteiten-en-hogescholen-blokkeren-studie-app-canvas-na-hack. Gecontroleerd op 2026-11-22.

S51: politie.nl, Verstoring van VPN-dienst (criminele infrastructuur). https://www.politie.nl/nieuws/2026/mei/21/criminele-vpn-dienst-first-vpn-offline-gehaald.html. Gecontroleerd op 2026-11-22.

S52: politie.nl, Botnetverstoring (hosting / verbonden apparaten). https://www.politie.nl/nieuws/2026/mei/28/06-politie-en-ncsc-halen-groot-botnetwerk-offline.html. Gecontroleerd op 2026-11-22.

S53: hospecs.com, Onderzoek naar blootstelling van gastgegevens / gerichte betaalphishing (horeca). https://www.hospecs.com/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S54: nos.nl, Onderzoek naar blootstelling van gastgegevens / gerichte betaalphishing (horeca) (2026-06-02). https://nos.nl/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S55: politie.nl, Malwareverspreidingscampagne / internationale verstoring (sectoroverstijgend webecosysteem). https://www.politie.nl/nieuws/2026/juni/18/11-politie-en-om-openen-de-jacht-op-beruchte-malwaregroep-socgholish.html. Gecontroleerd op 2026-11-22.

S56: politie.nl, Infostealerverstoring / teruggevonden inloggegevens (sectoroverstijgend). https://www.politie.nl/nieuws/2026/juni/24/11-operatie-endgame-opnieuw-twee-infostealers-offline.html. Gecontroleerd op 2026-11-22.

S57: aivd.nl, Phishing naar herstelsleutels van berichtenback-ups (overheid / defensiesector / media) (2026-06-30). https://www.aivd.nl/actueel/nieuws/2026/06/30/russische-hackers-richten-zich-op-signal-backups-via-nieuwe-phishing-methode. Gecontroleerd op 2026-11-22.

S58: aivd.nl, Spionagecampagne met IP-camera's (logistiek / private verbonden infrastructuur) (2026-07-10). https://www.aivd.nl/actueel/nieuws/2026/07/10/nederland-doelwit-van-russische-spionageoperatie-via-ip-cameras. Gecontroleerd op 2026-11-22.

S59: aivd.nl, Zimbra-spionageadvies (buitenlandse defensiesector / ICT) (2026-07-23). https://www.aivd.nl/actueel/nieuws/2026/07/23/russische-hackersgroep-laundry-bear-hackt-zimbra-mailservers. Gecontroleerd op 2026-11-22.

S60: autoriteitpersoonsgegevens.nl, Actief misbruik en golf van persoonsgegevenslekken (sectoroverstijgende websites). https://autoriteitpersoonsgegevens.nl/actueel/advies-van-de-ap-aan-wordpress-gebruikers-die-getroffen-zijn-door-datalek. Gecontroleerd op 2026-11-22.

S61: aivd.nl, Gerichte CHOSEN BRICK-malwarecampagne (maatschappelijk middenveld / media / personen) (2026-09-15). https://www.aivd.nl/actueel/nieuws/2026/09/15/cyberactoren-uit-iran-zetten-malware-in-tegen-dissidenten-activisten-en-journalisten. Gecontroleerd op 2026-11-22.

S62: aivd.nl, Advies over spionage via randapparatuur met China-verband (sectoroverstijgend) (2026-10-07). https://www.aivd.nl/actueel/nieuws/2026/10/07/mivd-en-aivd-verwachten-toename-chinese-cyberaanvallen-via-edge-devices. Gecontroleerd op 2026-11-22.

S63: ncsc.nl, Meerdere cyberincidenten / beoordeling van samenhang (voedselvoorziening). https://www.ncsc.nl/nieuws/in-het-nieuws-cyberaanvallen-op-levensmiddelensector. Gecontroleerd op 2026-11-22.

S64: cityam.com, Gemelde onbevoegde toegang tot interne mappen / actorclaim (luchtvervoer) (2026-10-12). https://www.cityam.com/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S65: politie.nl, Internationale opsporingsactie (hosting / criminele infrastructuur). https://www.politie.nl/nieuws/2026/oktober/28/03-internationale-actie-tegen-bulletproof-hoster.html. Gecontroleerd op 2026-11-22.

S66: ncsc.nl, Cyberaanvallen op koelsystemen (retail / voedsel / operationele technologie). https://www.ncsc.nl/nieuws/in-het-nieuws-cyberaanvallen-op-koelinstallaties-in-europa. Gecontroleerd op 2026-11-22.

S67: aa.com.tr, Cyberaanvallen op koelsystemen (retail / voedsel / operationele technologie) (2026-11-02). https://www.aa.com.tr/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S68: allunited.nl, Databasegegevensdiefstal / koppelingsverstoring (SaaS voor sportlidmaatschappen / verenigingen). https://www.allunited.nl/artikelen/datalek/. Gecontroleerd op 2026-11-22.

S69: nu.nl, Databasegegevensdiefstal / koppelingsverstoring (SaaS voor sportlidmaatschappen / verenigingen) (2026-11-11). https://www.nu.nl/tech/6416219/meer-dan-350-sportclubs-melden-datalek-na-cyberaanval-op-allunited.html. Gecontroleerd op 2026-11-22.

S70: politie.nl, Waarschuwing tegen criminele onlinemarkten (publieke preventie). https://www.politie.nl/nieuws/2026/november/9/08-ben-jij-zichtbaar-op-een-verdacht-online-platform-november-2026.html. Gecontroleerd op 2026-11-22.

S71: politie.nl, Operation Endgame-verstoring (sectoroverstijgend / hosting). https://www.politie.nl/nieuws/2026/november/12/11-internationale-actie-maakt-netwerken-van-cybercriminelen-onschadelijk.html. Gecontroleerd op 2026-11-22.

S72: politie.nl, Operation Endgame-verstoring (sectoroverstijgend / hosting). https://www.politie.nl/en/news/2026/november/international-action-disables-cybercriminal-network.html. Gecontroleerd op 2026-11-22.

S73: ncsc.nl, Dienststoring (cloudproductiviteit / digitale leveringsketen). https://www.ncsc.nl/nieuws/in-het-nieuws-storing-microsoft-exchange-online. Gecontroleerd op 2026-11-22.

S74: support.optimizely.com, JavaScript-injectie via derden (SaaS voor webexperimenten / sectoroverstijgend). https://support.optimizely.com/hc/en-us/articles/50521849710605. Gecontroleerd op 2026-11-22.

S75: politie.nl, Klantgegevensdiefstal en latere poging tot geweld (bankwezen / persoonlijke veiligheid). https://www.politie.nl/nieuws/2026/november/19/06-onderzoek-naar-datadiefstal-bij-bank-revolut.html. Gecontroleerd op 2026-11-22.

S76: nos.nl, Klantgegevensdiefstal en latere poging tot geweld (bankwezen / persoonlijke veiligheid) (2026-11-19). https://nos.nl/artikel/2640151-verdachten-opgepakt-die-geweld-wilden-plegen-bij-klanten-van-revolut-na-datadiefstal. Gecontroleerd op 2026-11-22.

S77: politie.nl, Bewustwordingscampagne met nepwebshop (consumentene-commerce / preventie). https://www.politie.nl/nieuws/2026/november/21/00-oeps%E2%80%A6-je-trapte-er-bijna-in-nieuwe-nepwebsite-van-de-politie.html. Gecontroleerd op 2026-11-22.

S78: politie.nl, Bewustwordingscampagne over ticketfraude (preventie van consumentenfraude). https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html. Gecontroleerd op 2026-11-22.

S79: politie.nl, Waarschuwing voor phishing-/afpersingsmail (consumenten / imitatie van overheid). https://www.politie.nl/nieuws/2026/januari/23/pas-op-voor-phishingmail-over-kinderporno.html. Gecontroleerd op 2026-11-22.

S80: ncsc.nl, Historisch advies over Chinees botnet (verbonden apparaten). https://www.ncsc.nl/nieuws/nederlandse-apparaten-onderdeel-van-chinees-botnet. Gecontroleerd op 2026-11-22.

S81: ncsc.nl, Historisch advies over DDoS-campagne (sectoroverstijgend). https://www.ncsc.nl/nieuws/lopende-ddos-aanvallen-op-nederlandse-organisaties. Gecontroleerd op 2026-11-22.

S82: ncsc.nl, Historisch DDoS-advies (context openbaar bestuur / vervoer). https://www.ncsc.nl/nieuws/opnieuw-ddos-aanvallen-rondom-navo-top-vervoerssector-ook-doelwit. Gecontroleerd op 2026-11-22.

S83: ncsc.nl, Historisch ransomwareadvies (sectoroverstijgend). https://www.ncsc.nl/nieuws/ook-nederlandse-bedrijven-slachtoffer-van-ransomwaregroepering-cactus. Gecontroleerd op 2026-11-22.

S84: NCTV, Melding van significante incidenten onder de Cyberbeveiligingswet. https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/meldplicht. Gecontroleerd op 2026-11-22.

S85: RFC Editor, DMARC-protocolreferentie. https://www.rfc-editor.org/rfc/rfc7489.html. Gecontroleerd op 2026-11-22.

S86: RFC Editor, DKIM-handtekeningen. https://www.rfc-editor.org/rfc/rfc6376.html. Gecontroleerd op 2026-11-22.

S87: RFC Editor, Sender Policy Framework. https://www.rfc-editor.org/rfc/rfc7208.html. Gecontroleerd op 2026-11-22.

S88: RFC Editor, HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html. Gecontroleerd op 2026-11-22.

S89: politie.nl, Internationaal offline halen van forum (criminele marktinfrastructuur). https://www.politie.nl/nieuws/2026/maart/4/politie-ontmantelt-groot-cybercrimineel-forum-in-wereldwijde-actie.html. Gecontroleerd op 2026-11-22.

S90: Rijksoverheid, Terugblik in jaarverslag (sectoroverstijgend / nationale veiligheid). https://www.rijksoverheid.nl/documenten/2026/04/22/openbaarjaarverslagmivd2025. Gecontroleerd op 2026-11-22.

S91: aivd.nl, Terugblik in jaarverslag (sectoroverstijgend / nationale veiligheid) (2026-04-23). https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025. Gecontroleerd op 2026-11-22.

S94: nos.nl, Gemelde leveranciersgerelateerde blootstelling van persoonsgegevens (amusement / horecamarketing / onderzoekshosting) (2026-11-12). https://nos.nl/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S95: AIVD, Brits NCSC en FBI, Gezamenlijk campagneadvies over CHOSEN BRICK (2026-09-15). https://www.ncsc.gov.uk/sites/default/files/2026-09/Advisory-Iranian-Cyber-Targeting-of-Dissidents-Activists-and-journalists.pdf. Gecontroleerd op 2026-11-22.

S96: tweedekamer.nl, Terugkerende DDoS-beschikbaarheidsverstoring (digitale overheid / authenticatie) (2026-10-07). https://www.tweedekamer.nl/downloads/document?id=2026D49475. Gecontroleerd op 2026-11-22.

S97: ad.nl, Terugkerende DDoS-beschikbaarheidsverstoring (digitale overheid / authenticatie) (2026-10-30). https://www.ad.nl/binnenland/storing-na-ddos-aanval-bij-online-diensten-digid-weer-opgelost~a1a03520/. Gecontroleerd op 2026-11-22.

S98: rdi.nl, GPS-signaalverstoring in onderzoek (luchtvaart / radionavigatie) (2026-11-16). https://www.rdi.nl/actueel/nieuws/2026/11/16/rdi-start-onderzoek-naar-storing-gps-vliegtuigen. Gecontroleerd op 2026-11-22.

S100: gcaptain.com, Historisch DDoS-verhaal opnieuw gepubliceerd in 2026 (havens / zeevaart) (2023-06-14). https://gcaptain.com/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S101: dustingroup.com, Inbraak in intern leverancierssysteem; ongeverifieerde klantspecifieke claims (IT-wederverkoper / beheerdiensten / leveranciersketen). https://www.dustingroup.com/en/information. Gecontroleerd op 2026-11-22.

S102: dutchitleaders.nl, Inbraak in intern leverancierssysteem; ongeverifieerde klantspecifieke claims (IT-wederverkoper / beheerdiensten / leveranciersketen). https://www.dutchitleaders.nl/ (artikel-URL weggelaten). Gecontroleerd op 2026-11-22.

S103: interrail.com, Klantgegevenslek gemeld in 2026; exfiltratie in 2025 (reizen / treinpasdiensten) (2026-02-13). https://www.interrail.com/en-int/ni/data-security-incident. Gecontroleerd op 2026-11-22.

S104: bleepingcomputer.com, Klantgegevenslek gemeld in 2026; exfiltratie in 2025 (reizen / treinpasdiensten). https://www.bleepingcomputer.com/news/security/eurail-says-december-data-breach-impacts-300-000-individuals/. Gecontroleerd op 2026-11-22.

S105: interrail.com, Interrail News: aankondiging gegevensbeveiligingsincident (2026-01-10). https://www.interrail.com/en/about-us/press-room/interrail-news. Gecontroleerd op 2026-11-22.

Bijlage D. Begrippenlijst

- **AIVD / MIVD:** Algemene Inlichtingen- en Veiligheidsdienst en Militaire Inlichtingen- en Veiligheidsdienst. Toeschrijvingen in dit rapport blijven die van de diensten.
- **AP:** Autoriteit Persoonsgegevens, de Nederlandse privacytoezichthouder.
- **Rvdr:** Raad voor de rechtspraak.
- **NCSC:** het Nederlandse Nationaal Cyber Security Centrum; te onderscheiden van de Britse organisatie met dezelfde afkorting.
- **NCTV:** Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- **RDI / ACM:** Rijksinspectie Digitale Infrastructuur en Autoriteit Consument & Markt; hun onderzoeksbevoegdheden blijven gescheiden.
- **DNB:** De Nederlandsche Bank. Het bankenregister verschilt van de geselecteerde financiële domeincategorie in dit rapport.
- **Cbw:** Cyberbeveiligingswet, besproken in hoofdstuk 10.
- **CSIRT:** team voor de respons op computerbeveiligingsincidenten; bepaal welk team voor het toepasselijke meldregime is aangewezen.
- **AVG / verwerkingsverantwoordelijke / verwerker:** Europese persoonsgegevensregels; de verantwoordelijke bepaalt verwerkingsdoelen en -middelen, terwijl de verwerker namens de verantwoordelijke handelt.
- **DORA:** de Europese Digital Operational Resilience Act voor financiële entiteiten binnen de reikwijdte; de meldfasen verschillen van privacymeldingen.
- **Nationale Atlas-hoofdwaarde:** één blootstellingssamenvatting voor de geselecteerde portefeuille, geen nationale prevalentie of kans op binnendringing.
- **Blackhole / Ransompedia / Atlas:** gegevens- en productnamen van Brandefense. Berichten, ransomwarevermeldingen en blootstellingsbeoordelingen zijn verschillende begrippen; alleen de nationale Atlas-hoofdwaarde wordt in deze editie gepubliceerd.
- **Combinatie van inloggegevens / stealerlog:** respectievelijk een bestand aangeboden als inlogparen en informatie gekoppeld aan informatiediefstalmalware. Alleen bestandslabels bewijzen geen herkomst of geldigheid.
- **MFA / sessie / gekoppeld apparaat:** respectievelijk een extra inlogfactor, voortdurende geauthenticeerde toegang en een ander apparaat verbonden met een account. Herstel- en intrekkingsbeslissingen moeten de relevante toegang aanpakken.
- **KYC:** identiteitscontroles om de klant te kennen. Een geclaimde omzeiling bewijst geen geslaagde rekeningopening.
- **RDWEB / EPMM:** webtoegang tot extern bureaublad en Endpoint Manager Mobile; productbeschrijvingen tonen niet de werkelijke doelwitconfiguratie aan.
- **SaaS / tenant:** software geleverd als dienst en de afzonderlijke dienstomgeving van een klant.
- **DDoS:** gedistribueerde aanval op beschikbaarheid. Een beschikbaarheidsaanval toont op zichzelf geen gegevensdiefstal aan.

- **OT:** operationele technologie die een fysiek proces bestuurt. Camerabeelden bekijken en inloggegevens aanbieden betekenen niet automatisch toegang tot industriële besturingen.
- **DMARC / SPF / DKIM:** e-maildomeinbeleid, bevoegdheid van verzendende hosts en berichtondertekening. Gepubliceerde instellingen zijn geen gemeten bezorgings- of fraude-uitkomsten.
- **TLS / HSTS:** technologie voor versleutelde verbindingen en HTTPS-browserbeleid; iedere waarneming is beperkt tot het relevante eindpunt of de homepage.
- **DNSSEC / DS:** ondertekende DNS en een delegatierecord. Alleen DS-aanwezigheid toont geen volledige validatie aan.
- **CVE:** een kwetsbaarheidsidentificator, te onderscheiden van bewijs dat de kwetsbaarheid bij een bepaalde organisatie is misbruikt.
- **Berichtkaart / claim / bevestigd incident:** een geredigeerd bewijsfragment, een bewering en een door de relevante organisatie of overheid vastgestelde gebeurtenis. Hun bewijsrollen verschillen.
- **TLP:CLEAR:** deelbaar zonder TLP-beperking; privacy-, contractuele en andere toepasselijke verplichtingen blijven gelden.

Over dit rapport

Opgesteld door Odin by Brandefense. Versie 1.0 gebruikt een onderzoeksmomentopname op 22 november 2026 en een recente-activiteitsperiode vanaf 8 november. Openbare meldingen kunnen eerdere incidenten beschrijven; die data blijven expliciet. Het rapport stelt afgebakend bewijs voorop en onderscheidt criminele claims van door organisaties of overheden vastgestelde gebeurtenissen.

Dit is geen nationale telling, juridisch oordeel of garantie over de volledige beveiliging van een organisatie. Aanbevelingen beschrijven mogelijke lezersacties; ze bewijzen niet dat een genoemde organisatie die maatregelen miste. Deze Nederlandse editie begeleidt de Engelse hoofdtekst; bij verschillen is de Engelse editie leidend.

© 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