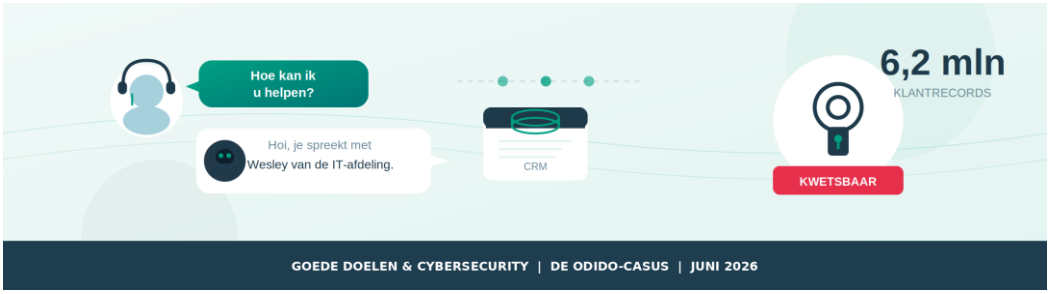

CASUS

De Odido-hack:

wat elke organisatie hiervan kan leren

Februari 2026. Een phishingmail, een telefoontje, een medewerker die zijn inloggegevens deelt. De persoonsgegevens van 6,2 miljoen Nederlanders belanden op straat. Geen geavanceerde hack, maar een aaneenschakeling van gevolgen van bestuurlijke keuzes die te lang niet zijn heroverwogen.

Dit document is een casus voor goede doelen en hun leveranciers, die werken met donateursdata en vrijwilligers- en partnernetwerken. De hack bij Odido laat zien wat er kan gebeuren als governance op toegangsbeheer, leveranciersrisico en detectie niet bestuurlijk wordt geagendeerd.

VOORWOORD

Wat mij bij de Odido-hack het meest trof, is niet de aanval zelf. Het is de combinatie van drie dingen die tegelijk fout gingen. Een leverancier die waarschuwde, maar niet werd gehoord. Een rechtenstructuur die waarschijnlijk nooit bestuurlijk is geagendeerd. En een detectiesysteem dat niet afging toen miljoenen records in korte tijd werden gedownload. Elk van die drie tekortkomingen had op zichzelf al voldoende moeten zijn om in actie te komen. Samen maakten ze dit tot een van de grootste datalekken in de Nederlandse geschiedenis.

Ik deel deze casus niet om Odido de maat te nemen. Als organisatie met een aanmerkelijke klantendatabase ben je voortdurend een target. Dat is ongelooflijk lastig. Ik ben er echter van overtuigd dat de lessen universeel zijn. Ook in de goede doelensector werken mensen dagelijks met grote hoeveelheden gevoelige donateursdata in CRM-systemen, via meerdere leveranciers en fondsenwervingsbureaus, met medewerkers en vrijwilligers die het doelwit zijn van steeds geraffineerder wordende social engineering. De druk om snel te handelen, de verwachting van behulpzaamheid, de gewoonte om collega's te vertrouwen: dat zijn de eigenschappen die aanvallers systematisch uitbuiten.

De vraag is niet of dit bij uw organisatie kan gebeuren. De vraag is hoe groot de schade zou zijn als het morgen zou gebeuren. Hoeveel donateursrecords zijn bereikbaar via een enkel gecompromitteerd account? Heeft u concrete afspraken met uw fondsenwervingspartners en dataverwerkende dienstverleners over toegangsrechten en bewustzijnstraining? En wat doet u als een leverancier een beveiligingswaarschuwing stuurt?

Dit zijn bestuurlijke vragen. Geen IT-vragen.

Patrick Jordens
Oprichter The Trusted Third Party (TT3P)

6,2 miljoen KLANTRECORDS GESTOLEN | **~500.000** SCHADECLAIMS INGEDIEND | **3** FORMELE ONDERZOEKEN

RECONSTRUCTIE

Wat er is gebeurd

5 febr.	Aanvallers bellen als IT-collega. Medewerker deelt inloggegevens via phishinglink. Toegang tot Salesforce CRM. 6,2 mln records worden gedownload.
7-8 febr.	Hack ontdekt. Account geblokkeerd na een uur, maar de data was al buitgemaakt. Zowel intern als via een extern securitybedrijf wordt aanvankelijk geconcludeerd dat er geen klantdata is gestolen.
7 febr. later	ShinyHunters meldt zich zelf. Pas dan wordt de omvang duidelijk. Extern securitybedrijf had aanvankelijk niets geconstateerd.
26 febr.	Na weigering losgeld: publicatie darkweb. OM, AP en RDI starten formele onderzoeken. Bijna 500.000 schadeclaims.

DE RESPONS

Cruciale fouten en gevolgen

ShinyHunters meldde zich eerst zelf voordat Odido de werkelijke omvang begreep. Zowel intern als via een extern cybersecuritybedrijf werd aanvankelijk geconcludeerd dat er geen klantdata was gestolen.

Boardlid Van Lammeren bood in mei 2026 voor het eerst formeel excuses aan en noemde crisiscommunicatie als voornaamste verbeterpunt: je moet ook communiceren over dingen die je nog niet weet.

Welke gegevens zijn buitgemaakt?

Namen, adressen en IBAN-nummers van 6,2 miljoen accounts. In een latere batch bleken ook BSN-nummers voor te komen van zzp'ers, via historische bedrijfsgegevens uit de periode dat het BSN onderdeel uitmaakte van het btw-nummer van zzp'ers.

DE KETENVRAAG | EIGEN MEDEWERKERS OF EXTERNE PARTNER?

Het is nooit officieel bevestigd of de getroffen medewerkers in dienst waren bij Odido zelf, of werkzaam bij een van de externe servicepartners die Odido inzet. De NOS berichtte dat de hack mogelijk plaatsvond via medewerkers van buitenlandse contact centers. Meerdere bronnen spraken dit later deels tegen. Odido hield het consequent bij "klantcontactmedewerkers" zonder verdere duiding.

Wat dit bestuurlijk relevant maakt: het maakt voor de aansprakelijkheid geen verschil. Als de toegang via een externe partij is verlopen, had die partij toegang tot de Salesforce-omgeving met dezelfde rechten als een eigen medewerker. De verwerkingsverantwoordelijkheid en daarmee de zorgplicht liggen onverkort bij Odido.

DE SALESFORCE-DIMENSIE

Wat er structureel fout zat

Salesforce zelf was niet het probleem. Het platform bevatte geen technische kwetsbaarheid. De aanvallers hadden geldige inloggegevens en daarmee precies dezelfde toegang als een legitieme medewerker.

Wat Salesforce wel had gedaan: het bedrijf waarschuwde zijn gebruikers eind januari 2026 specifiek voor de aanvalsmethode die ShinyHunters hanteerde. Dezelfde groep had in de maanden daarvoor al onder meer KLM-Air France, Palo Alto en Google via hun Salesforce-omgeving getroffen.

Of Odido die waarschuwing heeft ontvangen en opgevolgd, is nooit bevestigd. Dat is, zowel voor het OM, de AP als voor de massaclaim, een van de centrale vragen in de lopende onderzoeken.

Dataminimalisatie: wat er niet is, kan niet uitlekken

Naast de vraag wie toegang had, stelt de Odido-casus een tweede vraag: welke gegevens stonden er eigenlijk nog in het systeem? Van klanten die al jaren geleden waren vertrokken, lagen BSN-nummers en adresgegevens nog volledig toegankelijk in het CRM. Niet omdat iemand dat bewust had besloten, maar omdat niemand ooit had besloten ze te verwijderen. De Autoriteit Persoonsgegevens onderzoekt Odido expliciet op dit punt. Het bewaren van gegevens van ex-klanten na het einde van de relatie is een overtreding van het AVG-beginsel van dataminimalisatie (art. 5 lid 1 sub c). Voor goede doelen geldt hetzelfde: oud-donateurs, beëindigde campagnerelaties, vrijwilligers die al jaren geleden zijn vertrokken. Staan die gegevens er nog? Wat er niet is, kan niet uitlekken.

DE BLAST RADIUS

De kern van het probleem

Een medewerker die donaties verwerkt of contact heeft met donateurs, moet de gegevens van dat ene contact kunnen inzien. Hij heeft geen toegang nodig tot de namen, adressen en IBAN-nummers van honderdduizenden andere donateurs tegelijk.

Het principe van *'least privilege'* dicteert dat iemand alleen toegang heeft tot wat strikt noodzakelijk is voor zijn functie. Dat dit bij Odido niet het geval was, is geen technisch ongeluk. Het is het resultaat van een beheerskeuze die nooit bestuurlijk is getoetst.

Tot slot ontbrak gedragsmonitoring. Het downloaden van miljoenen records in korte tijd is een afwijkend patroon. Dat er geen alarm afging, wijst op een structureel gat in de detectiecapaciteit, een basismaatregel die de Cyberbeveiligingswet expliciet vereist.

Verwijdering bij leveranciers: de vergeten schakel

De derde laag is de minst zichtbare. Fondsenwervingsbureaus, mailingpartners en campagnebureaus hebben op enig moment toegang gehad tot donateursdata. Als de samenwerking eindigt, verplicht de AVG hen die gegevens te verwijderen of terug te geven. De verwerkersovereenkomst moet dit regelen. In de praktijk gebeurt verwijdering zelden proactief en wordt er vrijwel nooit op gecontroleerd. Organisaties weten daardoor niet wat er nog bij voormalige partners ligt, en of die partijen zelf afdoende beveiligd zijn. Dit is geen technisch vraagstuk. Het is een bestuurlijk vraagstuk: wie houdt bij welke verwerkers onze data hebben gehad, wanneer de relatie is beëindigd, en of verwijdering is bevestigd?

WETTELIJK KADER | CYBERBEVEILIGINGSWET (Cbw)

Drie artikelen uit de Cyberwet die direct raken aan wat bij Odido mis ging

Art. 21 lid 2 sub d Toeleveringsketen

Vastgesteld beleid over afhankelijkheden van leveranciers, aantoonbaar toegepast. Geldt ook voor fondsenwervingsbureaus, campagnepartners en andere externe partijen met toegang tot uw systemen.

Art. 21 lid 3 sub i Toegangsbeleid

Inzicht in wie op functieniveau toegang heeft tot welke data. Niet als technische instelling, maar als bestuurlijk vastgesteld en aantoonbaar beleid.

Art. 24 Bestuurlijke verantwoordelijkheid

Het bestuur keurt de maatregelen goed. Ontbreken van maatregelen is daarmee een bestuurlijk verzuim, geen technisch ongeluk.

BESTUURLIJKE LESSEN

Wat elke organisatie hiervan kan leren

Les 1

Ketenverantwoordelijkheid is niet uitbesteedbaar

Wie externe partijen toegang geeft tot zijn systemen, blijft verantwoordelijk voor de beveiliging van die toegang. Samenwerking met een fondsenwervingsbureau, campagnepartner of dataverwerkende dienstverlener verandert niets aan de zorgplicht voor rechten, bewustzijnstraining en incident response van die externe medewerkers.

Les 2

Waarschuwingen van leveranciers zijn bestuurlijk materiaal

Een beveiligingswaarschuwing van Salesforce is geen helpdesk-ticket voor IT. Het is informatie die de risicoafweging van het bestuur raakt. De vraag of een waarschuwing is ontvangen, beoordeeld en opgevolgd, is een governancevraag.

Les 3

De blast radius is een bestuurlijk gegeven

Hoe groot is de schade die een enkel gecompromitteerd account in uw organisatie kan aanrichten? Dit is geen vraag voor de CISO. Dit is een vraag voor het bestuur, en het antwoord moet aantoonbaar zijn vastgelegd.

VIER VRAGEN VOOR UW DIRECTIE, NU

01

Hebben wij vastgelegd wie toegang heeft tot welke donateursdata, op functieniveau, ook voor externe partijen en campagnepartners? En is dat recent getoetst?

02

Hoe gaan wij om met beveiligingswaarschuwingen van leveranciers? Wie is verantwoordelijk voor opvolging, en hoe maken wij dat aantoonbaar?

03

Wat is bij ons de blast radius? Welke schade kan een enkel gecompromitteerd account aanrichten, en is dat bestuurlijk besproken en vastgelegd?

04

Welke persoonsgegevens bewaren wij nog van donateurs en partners waarmee de relatie is beëindigd? En hebben wij bevestigd dat externe verwerkers die data na afloop hebben verwijderd?

OVER TT3P

The Trusted Third Party

TT3P ondersteunt organisaties en hun directies, besturen en raden van toezicht bij het opbouwen van cyberweerbaarheid als onderdeel van goed bestuur. Wij benaderen informatiebeveiliging niet als een IT-project, maar als een governance-, continuïteits- en risicomanagementvraagstuk.

Wij helpen organisaties met:

- Governance en risicomanagement: van beleid naar aantoonbare werking
- Leveranciersmanagement, audits en pentesting
- ISO 27001-certificeringsbegeleiding en auditvoorbereiding
- Gap-analyses en volwassenheidsbeoordelingen
- Bestuurderstrainingen, tabletop-oefeningen en crisissimulaties
- Remote Security Officer (RSO): vaste expertise zonder vaste overhead

Wilt u weten hoe weerbaar uw organisatie is?

Neem contact met ons op voor een vrijblijvende kennismaking. Wij denken graag met u mee over governance, risicomanagement en cyberweerbaarheid.

www.tt3p.nl
patrick.jordens@tt3p.nl
06 - 15 05 87 97