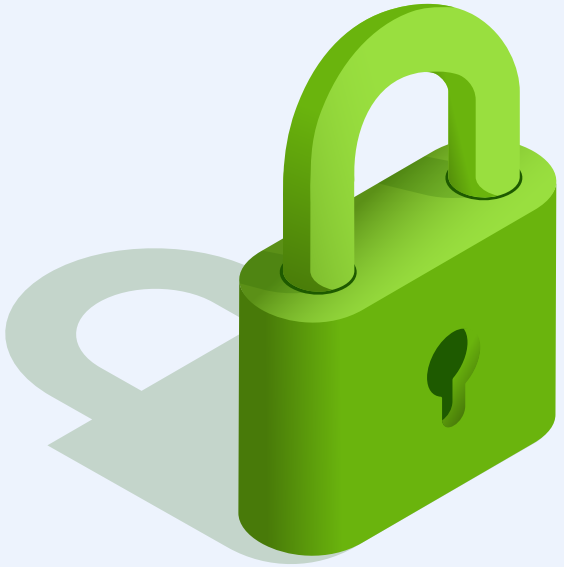
Datalekkenrapportage 2025

AI vergroot risico's rond phishing en datalekken

AP | bescherming in een digitale wereld

Juli 2026

Inhoud



Voorwoord

We leven in een online wereld die snel groeit. Dit landschap verandert elk moment. Er komen steeds meer nieuwe technieken bij die kansen, maar ook gevaren met zich meebrengen voor de maatschappij. De Autoriteit Persoonsgegevens (AP) helpt de veiligheid van mensen, organisaties en overheden in de online wereld te beschermen, zodat het vertrouwen in de digitale dienstverlening en maatschappelijke voorzieningen overeind blijft.

Datalekken hebben grote invloed op de veiligheid in de online wereld
Datalekken kunnen een enorme invloed hebben op de maatschappij. Dat werd in 2025 weer duidelijk, toen het laboratorium achter het Nederlandse Bevolkingsonderzoek en het Openbaar Ministerie (OM) werden gehackt. Hierbij werden maatschappelijke voorzieningen in de zorg en het strafrecht geraakt. En ook begin 2026 zagen we grote datalekken, zoals bij telecomprovider Odido en softwareleverancier voor gezondheidsdata ChipSoft.
Deze cyberaanvallen zorgden voor veel onrust bij slachtoffers en in de bredere maatschappij. En die onrust is terecht: met jouw gegevens kunnen hackers frauderen of je oplichten.

AI verhoogt risico op datalekken en op schade voor mensen
De bescherming van persoonsgegevens dreigt verder onder druk te komen door technologische ontwikkelingen. Zo verandert ook artificiële intelligentie (AI) snel.
De mogelijkheden en kansen voor de maatschappij nemen daardoor toe, maar de gevaren ook. Dit komt omdat cybercriminelen ook profiteren van nieuwe technologieën voor hun aanvals- en oplichtingspraktijken.

Zo vergroot AI het risico op phishing en dat heeft grote gevolgen voor mensen. Cybercriminelen kunnen met AI phishingberichten maken waarmee ze organisaties proberen te hacken, en oplichtingsberichten voor slachtoffers van datalekken. Met AI kan dit sneller, op grotere schaal en de berichten zijn moeilijker te ontdekken. In dit rapport waarschuwt de AP voor deze gevaren.

Organisaties moeten nú in actie komen en zorgen voor een hoog niveau van (cyber)beveiliging. Door in te zetten op dataminimalisatie en het naleven van bewaartermijnen, kunnen organisaties de gevolgen van een datalek beperken als zij toch worden getroffen.

De AP volgt de technologische veranderingen nauw en waarschuwt en adviseert organisaties, overheden en mensen. Zo helpt de AP de online wereld veiliger te maken.

Aleid Wolfsen
Voorzitter AP

Samenvatting

1. Toezicht op datalekken

In 2025 was te zien hoe groot de invloed is van datalekken op mensen en maatschappelijke voorzieningen. Grote datalekken bij het laboratorium achter het Nederlandse Bevolkingsonderzoek en bij het OM zorgden voor veel onrust in de maatschappij. De AP ziet erop toe dat organisaties goede beveiligingsmaatregelen nemen en dat ze slachtoffers informeren als dat nodig is. Wanneer dit niet gebeurt, kan de AP ingrijpen. En in ernstige gevallen kan de AP een boete opleggen. De AP signaleert ook trends en risico's, en adviseert organisaties en mensen.

Lees meer over het toezicht van de AP op pagina 5

2. AI vergroot risico's rond phishing en datalekken

Cybercriminelen maken ook gebruik van nieuwe technieken. Phishing- en oplichtingsberichten kunnen met AI sneller en op grotere schaal gemaakt worden. Ook kunnen deze berichten dan steeds echter lijken. In 2025 was er een aanzienlijke toename van datalekken door phishing. De AP waarschuwt dat dit door het gebruik van AI nog verder kan toenemen. Organisaties moeten hierop inspelen met hun beveiligingsmaatregelen. Ook de gevolgen van datalekken voor slachtoffers kunnen groter worden.

Lees meer over hoe cybercriminelen AI kunnen gebruiken voor oplichting op pagina 11

3. Feiten en cijfers

In 2025 zijn 39.407 datalekken gemeld aan de AP. In 2024 waren dat er 37.839. Van alle datalekken in 2025 kwamen er 2.428 door een cyberaanval. In 2025 zag de AP ook andere soorten datalekken, zoals datalekken waarbij persoonsgegevens per ongeluk online werden gezet.

Lees meer over deze feiten, cijfers en de duiding ervan op pagina 15

1. Toezicht op datalekken

In het kort

- De hacks bij het laboratorium achter het Nederlandse Bevolkingsonderzoek en bij het OM laten zien hoeveel effect datalekken hebben op levens van mensen en op organisaties.
- De AP zorgt dat organisaties na een datalek maatregelen nemen en slachtoffers informeren. Ook signaleert de AP trends en risico's. Daarnaast adviseert de AP hoe organisaties en mensen zichzelf veiliger kunnen houden. Daarbij deelt de AP bijvoorbeeld *best practices* van organisaties.

Het effect van datalekken op mensen en voorzieningen

Het jaar 2025 maakte de enorme gevolgen van datalekken duidelijk.

In de zomer hackten cyberaanvallers het laboratorium achter het bevolkingsonderzoek naar baarmoederhals-kanker en stalen gevoelige gegevens van honderdduizenden vrouwen. In diezelfde zomer moest het OM uit voorzorg belangrijke systemen offline halen na een hack.

Deze gebeurtenissen zorgen voor onrust en concrete problemen in de maatschappij. Deelnemers aan het bevolkingsonderzoek maken zich serieuze zorgen over misbruik van hun persoonsgegevens. Ze twijfelen om in de toekomst nog deel te nemen aan een bevolkings-onderzoek. Bij het OM waren rechtszaken vertraagd en konden medewerkers een tijdlang zelfs niet e-mailen.

Door dit soort datalekken verliezen mensen het vertrouwen in de digitale dienstverlening van bedrijven en overheden.

Toezicht van de AP zorgt voor veilige en betrouwbare online diensten

Organisaties moeten er met beveiligingsmaatregelen zo veel mogelijk voor zorgen dat datalekken niet kunnen gebeuren. En wanneer het toch fout gaat, en er een schadelijk datalek plaatsvindt, dan moeten zij maatregelen nemen om dit zo snel mogelijk te dichten, en slachtoffers snel en goed informeren.

De AP zorgt dat organisaties zich aan de regels houden. Ook geeft de AP een kijk op de veranderingen en risico's van datalekken. En de AP legt zo veel mogelijk uit hoe het moet en wat organisaties van elkaar kunnen leren. Zo houdt de AP toezicht om de veiligheid van mensen in de online wereld te beschermen.

Gelekte gegevens over bevolkingsonderzoeken naar baarmoederhalskanker

Een datalek met ingrijpende maatschappelijke gevolgen is de cyberaanval bij Clinical Diagnostics. Dit laboratorium hield zich bezig met testmateriaal van bevolkingsonderzoeken naar baarmoederhalskanker. Ook doet het laboratorium andere medische onderzoeken voor huisartsen en zorginstellingen. Cybercriminelen stalen namen, contactgegevens en uiterst gevoelige medische gegevens en plaatsten deze voor een deel op het darkweb. Meer dan één miljoen mensen kreeg bericht dat zij waakzaam moeten zijn voor de gevolgen van dit datalek.

Gevolgen van een datalek

Een slachtoffer aan het woord:

"Een paar jaar geleden heb ik meegedaan aan het bevolkingsonderzoek naar baarmoederhalskanker. In augustus en september 2025 kreeg ik het bericht dat er veel persoonlijke gegevens van mij zijn gelekt.

Het ging niet alleen om mijn adres en geboortedatum, maar ook om gevoelige gegevens, zoals mijn burgerservicenummer, het soort onderzoek en testuitslagen. Ik ben hier heel erg van geschrokken. Dat zelfs medische gegevens over mij zijn gelekt, voelt alsof mijn lichamelijke integriteit is aangetast.

In de media las ik daarna dat er ook gegevens van mensen op het darkweb stonden. Ik heb daarna erg lang in onzekerheid geleefd of mijn gegevens hiertussen zaten.

Uiteindelijk kreeg ik het bericht dat een deel van mijn gegevens ook op het darkweb is gezet. Je voelt je op dat moment echt machteloos. Wat gaat er met mijn gegevens gebeuren? Wat kan ik doen om mezelf te beschermen?

Je geeft je gegevens in de hoop dat er veilig met je informatie wordt omgegaan. Nu heb ik geen controle meer en kunnen criminelen mijn gegevens misbruiken. Ik krijg de laatste maanden meer ongewenste e-mails, dus ik let extra op phishing en misbruik van mijn gegevens."

Wat doet de AP?

Veel mensen lieten de AP weten dat ze bezorgd zijn en klachten hebben over het datalek. In het derde kwartaal van 2025 heeft de AP ongeveer 600 klachten, tips en telefoontjes van bezorgde mensen ontvangen. De AP heeft deze mensen gesproken en verteld wat zij kunnen doen.

Direct na het datalek heeft de AP intensief contact gehad met Clinical Diagnostics en Bevolkingsonderzoek Nederland, onder meer over het goed informeren van alle slachtoffers. In dit verband is de AP ook langs geweest bij het laboratorium om de regels uit te leggen, en heeft de AP het laboratorium ook daarna nog bijgestuurd waar dat nodig was.

Daarnaast zijn de AP en de Inspectie Gezondheidszorg en Jeugd (IGJ) onderzoeken gestart naar Clinical Diagnostics. Over de inhoud daarvan kan de AP nu nog geen uitspraken doen. Dat heeft goede redenen: de AP kan pas een onafhankelijk oordeel vellen als alle informatie vaststaat en is beoordeeld. Daarnaast kunnen vroegtijdige uitspraken het onderzoek schaden.

Achtergrond: wat doet een inspecteur van de AP?

De AP ontvangt elke dag meldingen van organisaties die een datalek hebben gehad. De inspecteurs van de AP houden op 3 manieren toezicht:

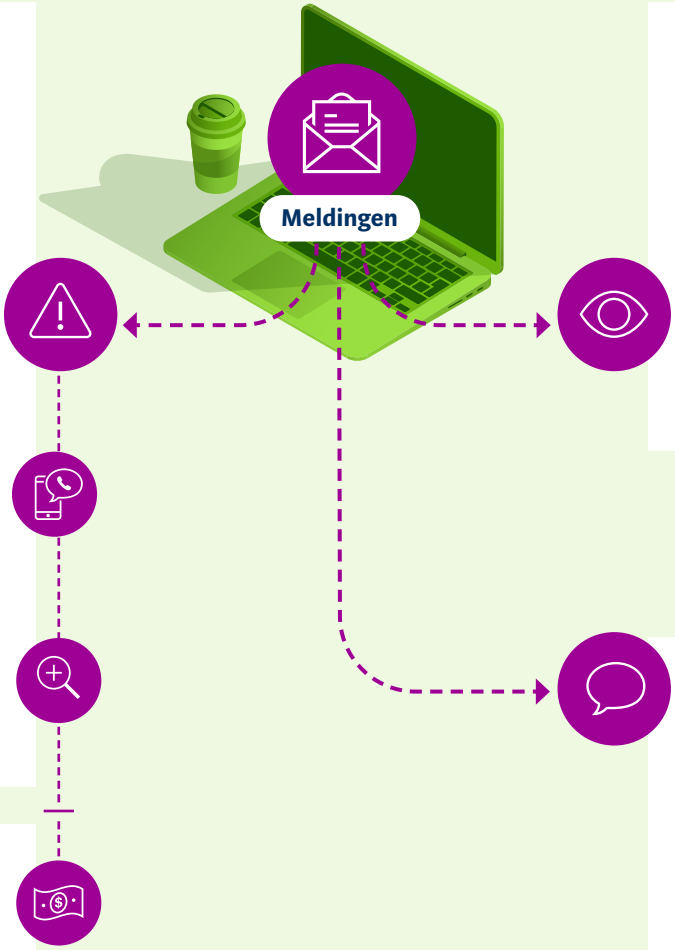
1. Onderzoek naar datalekken

Beoordelen op gevaar
Een inspecteur beoordeelt de melding: heeft een organisatie vooraf goed nagedacht over de beveiliging? En gaat deze organisatie goed om met het datalek? Denk aan: de risico's duidelijk in kaart brengen, direct maatregelen nemen om de schade te beperken en bij een hoog risico de slachtoffers informeren?

Contact via de telefoon
De inspecteur kan de organisatie bellen om vragen te stellen over het datalek en bindend advies te geven.

Verder onderzoek
De inspecteur kan besluiten het datalek verder te onderzoeken. Soms controleert de AP systemen ter plekke. Of eist de AP dat de organisatie extra maatregelen neemt. De AP kan hierbij samenwerken met andere toezichthouders.

Boete
Onderzoek kan in ernstige gevallen leiden tot een boete voor de organisatie. Bijvoorbeeld als blijkt dat de beveiliging niet op orde was. In 2025 heeft een onderzoek geleid tot een boete voor de Hogeschool van Arnhem en Nijmegen (HAN).



2. Trends en problemen signaleren

Met zicht op alle datalekmeldingen, ontdekt de inspecteur trends en nieuwe problemen. De inspecteur kan besluiten dit onder de aandacht te brengen bij organisaties die door deze trends en risico's worden geraakt of bij andere invloedrijke organisaties, zoals brancheverenigingen. Dat deed de AP in een verkennend onderzoek naar misbruik van persoonsgegevens door gemeenteambtenaren.

3. Adviseren

Inspecteurs hebben ook een adviserende rol. In de meldingen ziet een inspecteur met welke problemen organisaties te maken krijgen. Daarna kan een inspecteur gerichte voorlichting geven. Soms onderzoeken de inspecteurs thema's die leiden tot publicatie van aanbevelingen. Zoals het stappenplan leren van datalekken, en aanbevelingen voor verwerkersovereenkomsten.

Onderzoek naar datalekken: de AP zorgde bij een cyberaanval dat de ICT-leverancier klanten duidelijk informeerde

Inspecteur aan het woord:

"Ik ontving een datalekmelding van een ICT-dienstverlener die was geraakt door een ransomware-aanval. Een cyberaanvaller had de IT-omgeving van de dienstverlener en een aantal klantorganisaties versleuteld.

Ik heb de dienstverlener gebeld en een brief gestuurd over de vervolgstappen die wij verwachten na een ransomware-aanval. Daarbij gaf ik advies, zodat de dienstverlener de risico's van het datalek goed kon inschatten en de geraakte klanten goede informatie kon geven over de gevolgen van de ransomware-aanval.

Om te controleren of de dienstverlener juist handelde, vroeg ik om de resultaten van het forensisch onderzoek naar de cyberaanval en een kopie van het bericht aan hun klanten. Uit onze controle bleek dat de dienstverlener de grootte van het datalek niet goed had ingeschat.

Uit het forensisch onderzoek bleek dat de cyber-aanvaller veel gegevens had gestolen. Maar het was niet duidelijk om welke gegevens het precies ging, omdat er te weinig loggegevens waren. De dienstverlener had daarom de grootte van het datalek beoordeeld op wat de cyberaanvaller zei gestolen te hebben. Maar de bewijzen of stukken van een cyberaanvaller zijn niet te vertrouwen. Cyberaanvallers vallen een systeem aan om geld te verdienen. Zij zijn dus niet te vertrouwen voor een uitleg over wat ze van je gestolen hebben.

Hierdoor had de dienstverlener een verkeerd beeld aan de klantorganisaties geschetst van de risico's van de cyberaanval. Zo gingen sommige klanten er onterecht vanuit dat er geen persoonsgegevens van hun werknemers of klanten waren gestolen. We hebben de dienstverlener uitgelegd dat zij de klanten nieuwe informatie moest geven. Dit zorgde ervoor dat de klanten de risico's beter konden inschatten, en daarmee beter konden bepalen of zij de AP en de slachtoffers moesten informeren over het datalek. Mede dankzij onze acties zijn meer organisaties en slachtoffers goed geïnformeerd over het datalek. Zij weten hierdoor dat hun persoonsgegevens in handen van cybercriminelen kunnen zijn, en dat zij bijvoorbeeld moeten letten op oplichtingsberichten."

Cyberaanvallen leiden vaak tot grote risico's voor de slachtoffers. Organisaties moeten deze datalekken dus bijna altijd melden aan slachtoffers en aan de AP. Is er twijfel over het soort aanval en de grootte ervan? Dan moet de organisatie uitgaan van het slechtste.

Trends en problemen: cyberaanvallen in de toerismesector

De toerismesector was in 2025 een populair doelwit voor cyberaanvallen. De AP ontving veel datalek-meldingen, tips en klachten over cyberaanvallen bij hotels, accommodatieplatformen, reisorganisaties en vliegtuigmaatschappijen. Vakantiegangers uit heel Europa werden het slachtoffer van deze cyberaanvallen. Bij het toezicht op deze datalekken werkt de AP daarom samen met andere Europese privacytoezichthouders.

In 2025 stal een cyberaanvaller veel klantgegevens van een grote reisorganisatie. Deze gegevens werden al snel gebruikt voor oplichting. Klanten ontvingen persoonlijke phishingmails met de vraag om nog een deel van hun reis te betalen.

Bij datalekken in de toerismesector worden vaak contactgegevens gestolen in combinatie met informatie over de vakantiereservering. Mensen maken zich dan bijvoorbeeld zorgen dat dieven bij hen thuis inbreken als ze op vakantie zijn.

In 2025 heeft de AP een aantal adviezen gegeven aan organisaties in de toerismesector die geraakt zijn door een cyberaanval. Bijvoorbeeld:

- Sla gegevens niet allemaal op één plek op. Zo zorg je ervoor dat niet veel gegevens in één keer gestolen kunnen worden.
- Zorg dat je een goed monitoringssysteem hebt om aanvallen of pogingen tot aanvallen te detecteren.

In 2025 waarschuwde de AP ook voor dreigingen door phishing en de AP gaf tips om deze dreigingen te herkennen en schade tegen te gaan.

De AP verwacht dat dit probleem in 2026 blijft bestaan. Daarom zal de AP samen met Europese toezichthouders, scherp toezicht houden op datalekken in de toerismesector.

Datalektips

Als mensen een datalek ontdekken of hier slachtoffer van worden, kunnen zij de AP een tip geven. In 2025 ontving de AP 1.376 datalektips. Ook haalt de AP signalen over datalekken uit de media. Inspecteurs bij de AP gebruiken deze informatie om te controleren of datalekken bij de AP zijn gemeld en of slachtoffers goede informatie hebben gekregen over een datalek. Ook krijgt de AP regelmatig tips over een datalek dat nog niet gedicht is door de organisatie. Denk aan een webpagina met een lijst aan klantbestellingen waar iedereen bij kan. De inspecteur neemt dan direct contact op met de organisatie om het lek te laten dichten.

De inspecteurs gebruiken de informatie ook om te peilen wat er in de maatschappij speelt en waar mensen zich zorgen om maken. Slachtoffers van een datalek laten bijvoorbeeld weten dat zij door de organisatie zijn gewaarschuwd om te letten op oplichting, maar dat zij het onduidelijk vinden wat zij verder kunnen doen. Met deze informatie kan de inspecteur de organisatie bijsturen, zodat slachtoffers informatie krijgen waarmee zij maatregelen kunnen nemen tegen grotere schade.

Hoe gegevens werden misbruikt voor verjaardagsoplichting uit naam van Rituals

In 2025 ontving de AP signalen over phishingmails, zogenaamd verzonden door cosmeticabedrijf Rituals.

Jenny de Vries aan het woord, CFO van Rituals:

”Meerdere mensen maakten bij ons melding van een oplichtingsmail die zij op hun verjaardag ontvingen. Deze e-mail leek te komen van Rituals en was voor veel mensen erg overtuigend, omdat het echt hun verjaardag was en ze Rituals kennen. Ze moesten met creditcard €2 aan verzendkosten betalen om een verjaardagscadeau te ontvangen. Mensen die hun betaalgegevens hiervoor achterlieten, bleken vervolgens een doorlopend abonnement bij een oplichter te hebben geactiveerd.

Wij hebben onze klanten meermaals gewaarschuwd voor de oplichting die uit onze naam rondging. Wanneer zij het doelwit worden van oplichting waarbij onze naam en uitstraling worden misbruikt, raakt ons dat persoonlijk. Het gaat niet alleen om ”een incident”, maar om mensen die vertrouwen in ons hebben en daardoor ongerust kunnen worden, of zelfs schade kunnen oplopen.

Tegelijkertijd lag de oorzaak buiten onze invloed: de phishing kwam niet doordat data uit onze systemen waren gelekt. Dat is gebleken uit uitgebreid onderzoek waarbij wij ons lieten bijstaan door gespecialiseerde bedrijven. De oplichters gebruiken e-mailadressen en geboortedata die afkomstig zijn uit andere bronnen, zoals een datalek elders of gecombineerde sets uit datalekken. Juist daarom voelden we extra verantwoordelijkheid om te doen wat wél in onze macht ligt. We hebben er bewust voor gekozen om snel en duidelijk te communiceren, zodat klanten wisten wat er aan de hand was, hoe ze phishing kunnen herkennen en welke stappen ze kunnen nemen als ze toch op de phishingmail hadden geklikt of gegevens hadden gedeeld.

In deze kwestie konden wij met de AP bespreken wat we al wisten, wat nog onzeker was en waar onze dilemma's lagen. We kregen goed, praktisch toepasbaar advies dat hielp om onze klanten op een zo goed mogelijke manier te informeren en op die manier weerbaarder te maken voor deze internetcriminelen."

AP: Als er phishingmails rondgaan uit naam van een organisatie, moet die organisatie goed onderzoeken of er een datalek is geweest in de systemen, of in die van de dienstverlener(s). De cybercrimineel kan gegevens uit een datalek gebruikt hebben om persoonlijke phishingmails naar de klanten van de organisatie te sturen. Ook als blijkt dat er geen datalek bij de organisatie zelf heeft plaatsgevonden, is het goed om klanten te waarschuwen over rondgaande phishingmails. Dat schept duidelijkheid, beschermt de klanten en laat betrokkenheid met hen zien.

**In april 2026 heeft er een datalek bij Rituals plaatsgevonden, waarbij Rituals de getroffen personen heeft geïnformeerd. Dat staat los van dit verhaal wat zich in 2025 afspeelde.*

2. AI vergroot risico's rond phishing en datalekken

In het kort

- De AP waarschuwt dat phishing- en oplichtingsberichten sneller, grootschaliger en moeilijker te ontdekken kunnen zijn, als cybercriminelen AI gebruiken. Recente datalekken waarbij hackers persoonsgegevens in handen kregen, kunnen tot gevolg hebben dat nog meer mensen slachtoffer worden van oplichting.
- Phishing is niet alleen een gevolg van een datalek, maar ook steeds vaker de oorzaak. Een phishingaanval op een werknemer kan ertoe leiden dat het account van de werknemer wordt overgenomen en het beginpunt zijn voor een grotere cyberaanval. In 2025 zag de AP een aanzienlijke stijging van dit soort account takeovers. Van 607 aanvallen in 2024 naar 1.742 in 2025. Door AI kan dit aantal verder stijgen.
- AI biedt ook mogelijkheden om kwetsbaarheden te ontdekken en cyberaanvallen tegen te gaan. Maar als cybercriminelen deze technologie gebruiken, kunnen ook zij kwetsbaarheden sneller opsporen en misbruiken.

AI en datalekken

Ontwikkelingen op het gebied van AI gaan in een sneltreinvaart. AI lijkt voor bijna alles te worden gebruikt. Het is voor iedereen binnen handbereik, ook voor cybercriminelen.

Cyberaanvallen met behulp van AI vinden in de praktijk al plaats. Door de inzet van AI kunnen cyberaanvallen sneller, op grotere schaal en moeilijker te ontdekken zijn.

In 2025 zag de AP een aanzienlijke stijging van het aantal datalekken door phishing. Dit aantal kan verder stijgen als cybercriminelen AI gebruiken voor phishing. Met AI kunnen cybercriminelen beter en sneller:

1. Informatie verzamelen over doelwitten.
2. Geloofwaardige phishingberichten maken.
3. Phishingberichten op grotere schaal versturen.

Hierdoor is het risico op datalekken als gevolg van phishing groter. Ook de gevolgen van datalekken voor mensen worden groter, omdat zij met gebruik van die AI kunnen worden opgelicht.

In 2025 zag de AP een aanzienlijke stijging van het aantal aanvallen waarbij cybercriminelen accounts overnemen (account takeovers). Van 607 naar 1.742. Deze cyberaanvallen zijn bijna altijd het gevolg van phishing.

Lees hierover meer op pagina 17.

Phishing
Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Die informatie kan bijvoorbeeld worden misbruikt voor toegang tot accounts en systemen. Phishing gebeurt via e-mail, maar ook via telefoon, sms of app-berichten.

Artificiële intelligentie (AI)
AI gaat over alle technologieën en algoritmes die menselijke vaardigheden nadoen. AI-toepassingen kunnen veelsoortige informatie verwerken, redeneren, en tekst, plaatjes of spraak produceren. Generatieve AI-toepassingen, zoals taalmodellen, kunnen dit soort nieuwe content creëren of genereren. Vaak is deze content moeilijk te onderscheiden van door mensen gemaakte content. Wanneer AI-systemen worden gekoppeld aan andere computersystemen kunnen

zij automatisch handelingen uitvoeren. Er wordt dan gesproken van AI-agents.

In dit hoofdstuk wordt het begrip 'AI' ruim opgevat. Hieronder vallen bijvoorbeeld AI-toepassingen en AI-systemen.

Beveiligingsmaatregelen tegen phishing
Organisaties moeten technische maatregelen nemen tegen phishing en de gevolgen daarvan. Mensen maken nu eenmaal fouten en er blijft een risico dat een werknemer in een phishingbericht trapt. En juist door AI kunnen mensen phishing minder goed herkennen.

Denk bijvoorbeeld aan de volgende beveiligingsmaatregelen:

- Schakel multifactorauthenticatie (MFA) in voor de (mail)accounts van je werknemers.
- Zorg voor een algemeen beleid voor het filteren van mail- en netwerkverkeer, zoals het blokkeren van domeinnamen en IP-adressen (blocklisting) of het exclusief toestaan van bepaalde domeinnamen en IP-adressen (allowlisting).
- Maak het makkelijk voor werknemers om phishing te melden. Bijvoorbeeld met een meldknop in het mailsysteem.
- Zorg dat niet alle data op dezelfde plek staat (netwerksegmentatie) en dat werknemers alleen toegang hebben tot dat wat zij nodig hebben voor hun werk. Zo zorg je dat een cybercrimineel niet gelijk toegang heeft tot alle data van een organisatie.

Tegelijkertijd kun je werknemers wijzen op het volgende:

- Wees voorzichtig met mails waarin je iets met spoed moet doen of waarin je gevoelige informatie moet achterlaten, zoals creditcardgegevens of inloggegevens.
- Beweeg met de muis over een link in een mail om het webadres te controleren. Komt het webadres overeen met de officiële website van de organisatie?
- Onderzoek wie de afzender is. Controleer of het e-mailadres van de afzender overeenkomt met de naam van de organisatie en let goed op wat er achter het @- teken staat.

1. Met AI kunnen cybercriminelen waardevolle informatie verzamelen over doelwitten en slachtoffers

Cybercriminelen kunnen AI gebruiken om sneller en makkelijker waardevolle informatie over mensen te verzamelen en samen te voegen. Met AI kun je bijvoorbeeld makkelijker gelekte data aanvullen met informatie uit sociale media.

Vervolgens kunnen cybercriminelen mensen met persoonlijke informatie oplichten. Ook werknemers van organisaties kunnen worden opgelicht. Dat is het beginpunt voor nieuwe datalekken. Laat de werknemer inloggegevens achter? Of slaat de werknemer per ongeluk malware op? Dan krijgt de cybercrimineel toegang tot bijvoorbeeld het mail- of werkaccount van de werknemer. Deze datalekken zorgen voor veel schade. Denk aan ransomware-aanvallen, waarbij cybercriminelen systemen versleutelen en vaak persoonsgegevens stelen en online zetten.

Phishing in het tijdperk van AI

Een technoloog van de AP aan het woord:

"De term phishing bestaat al sinds de jaren 90 en verwijst sinds die tijd naar het online 'hengelen' naar waardevolle of gevoelige informatie. Online oplichters gebruiken vaak informatie die ze al hebben, zoals een e-mailadres of andere persoonsgegevens, om andere informatie te krijgen of de slachtoffers iets verkeerds te laten doen.

Oplichters misbruiken wat mensen met elkaar verbindt: vertrouwen en behulpzaamheid. Of ze maken gebruik van onze slechte eigenschappen: jaloezie of hebberigheid. Onder tijdsdruk letten we niet altijd goed op en dat maakt ons kwetsbaarder voor oplichting.

Ook cybercriminelen volgen, net als iedereen, de technologische trends. Toen we allemaal gingen e-mailen, kwam ook de ongewenste e-mail (spam), waarmee veel werd opgelicht. Na de eerste webwinkels verschenen al snel nep-webwinkels. Vanaf het moment dat we smartphones gingen gebruiken, ontvingen we ook oplichtings-sms'jes (smishing). De oplichters gebruiken veel social media en criminelen hebben natuurlijk ook toegang tot AI.

Met AI kunnen criminelen hun oplichtingstrucs veel persoonlijker maken. In Engelstalige landen zijn al de eerste voorbeelden van oplichting met voice-cloning gezien. Een oplichter gebruikt dan AI-technologie om de stem na te doen van iemand die jij vertrouwt.

Taalmodellen maken het vaak eenvoudiger om gelekte informatie samen te voegen en de oplichtingstruc persoonlijker te maken. Vroeger was dat nogal zeldzaam, maar met AI kunnen phishingberichten beter worden aangepast op de ontvangers, waardoor de kans groter is dat iemand erin trapt. Technologische veranderingen zijn dus niet altijd alleen maar goed."

Organisaties moeten de persoonsgegevens die ze zijn toevertrouwd goed beveiligen. Als er dan toch persoonsgegevens lekken, dan is nu het nog belangrijker om dat snel te laten weten aan de slachtoffers. Zij krijgen door AI sneller en vaker te maken met geloofwaardige en gepersonaliseerde berichten die moeilijk te herkennen zijn als oplichting.

2. Phishingberichten lijken net echt met AI

Cybercriminelen kunnen met AI sneller, makkelijker en meer persoonlijke informatie in een phishingbericht zetten. Denk bijvoorbeeld aan een geboortedatum, adres of burgerservicenummer (BSN). Hoe meer de cybercrimineel over de ontvanger weet, hoe overtuigender het phishing-bericht zal zijn.

Daarnaast is AI goed in het kopiëren van schrijfstijlen. Met bijvoorbeeld een taalmodel kan een cybercrimineel de tekst in een phishingbericht makkelijker aanpassen op de situatie. Daardoor lijkt het sneller alsof het bericht van een organisatie of persoon komt die de ontvanger vertrouwt.

AI zorgt ook voor een betere taal in phishingberichten. Met AI kunnen cybercriminelen hun phishingberichten zo goed als foutloos schrijven en makkelijk vertalen.

3. AI maakt phishing op grote schaal makkelijker

AI maakt de technische drempel om te phishen lager. Een crimineel heeft zelf minder technische kennis en ervaring nodig om te phishen. Er zijn zelfs AI-phishing kits, met hulpmiddelen om te phishen.

Ook zorgt AI ervoor dat cybercriminelen in heel korte tijd phishingberichten op grote schaal kunnen maken en versturen. AI-agents kunnen ook direct analyseren welke phishingberichten het best werken en de phishingberichten daarop automatisch aanpassen.

AI-phishingkits

Een AI-expert van de AP aan het woord:

"Het is steeds makkelijker om te phishen. Cybercriminelen kunnen daar phishingkits voor gebruiken, die soms worden verkocht als een dienst ('phishing-as-a-service'). Dit soort kant-en-klare pakketten bestaan al jaren en worden steeds beter gemaakt. En steeds meer mensen gebruiken de pakketten. Dat komt mede doordat AI het werk automatisch doet en de drempel voor gebruikers verlaagt.

Phishingkits bieden een omgeving om phishingaanvallen op te zetten en bij te houden. Ze bestaan bijvoorbeeld uit nepwebsites (zoals inlogpagina's van banken of e-maildiensten), tools om ingevulde gegevens te stelen en dashboards om campagnes te maken, volgen en bijsturen. Phishingkits bevatten vaak een beheerderspanel, waarin eenvoudig instellingen kunnen worden aangepast. Denk aan de vormgeving van berichten, de nepwebsite en de manier waarop gegevens worden verzameld.

Nieuwe phishingkits zijn steeds beter.
Ze combineren automatisering en AI om persoon-lijke berichten te maken die net echt lijken.
Vaak bestaan de berichten in meer talen en lijken ze erg op de huisstijl van vertrouwde organisaties.
Ook kunnen phishingkits proberen beveiligings-maatregelen, zoals extra inlogcontroles (MFA),

te omzeilen en detectie te vermijden. Dit gebeurt op een aantal manieren.

Soms misbruiken cybercriminelen inlogprocessen die net echt lijken. Via een phishingmail wordt de gebruiker gevraagd een code, bijvoorbeeld een 'device code', in te vullen op een echte inlogpagina. Het lijkt alsof de gebruiker normaal inlogt, maar in werkelijkheid geeft de gebruiker de cybercrimineel toegang tot zijn account.

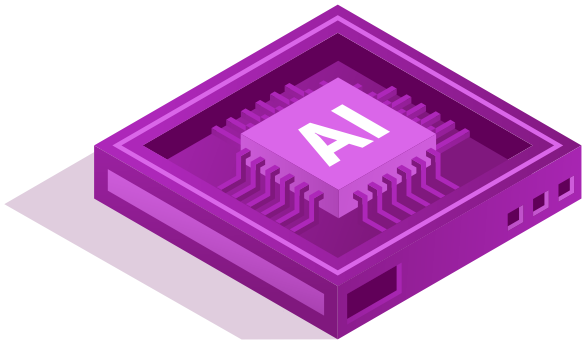
In andere situaties gebruiken phishingkits technieken om tussen de gebruiker en een bedrijf of organisatie in te zitten. De gebruiker logt in via een nepomgeving, die lijkt op de echte website. De inloggegevens en bevestiging komen eerst terecht in deze omgeving en worden vervolgens doorgestuurd naar het bedrijf of de organisatie waar is ingelogd. Na het inloggen ontvangt de aanvaller tokens om toegang te krijgen tot het account van de gebruiker zonder opnieuw in te loggen.

De verdere ontwikkeling van AI-agents kan deze kits nog krachtiger maken. AI-agents zouden phishingaanvallen straks misschien helemaal zelf kunnen uitvoeren en tussentijds kunnen aanpassen aan het gedrag van een doelwit. Dit kan leiden tot meer gerichte en snellere aanvallen op grotere schaal, die moeilijker te ontdekken zijn."

AI als wapen tegen cyberaanvallen

AI kan ook gebruikt worden om cyberaanvallen tegen te gaan. Daarom raadt de Cybersecurityraad de Nederlandse regering aan om te investeren in ontwikkeling van innovatieve producten voor betere detectie van aanvallen met behulp van AI. De AP staat hierachter.

De veranderingen van AI als wapen tegen cyberaanvallen gaan ook snel. In 2026 maakte AI-bedrijf Anthropic het model Mythos bekend. Met dit model kunnen kwetsbaarheden worden opgespoord en daarna worden opgelost. Maar als cybercriminelen deze technologie gebruiken, kunnen zij deze kwetsbaarheden sneller misbruiken. Daarom is het nog belangrijker voor organisaties om te zorgen voor een hoog beveiligingsniveau. Het NCSC adviseert om AI-ontwikkelingen mee te nemen in het bepalen van beveiligingsmaatregelen. Organisaties moeten beveiligingskwetsbaarheden in de software nog sneller oplossen (patchmanagement). Daarnaast is een goed monitoringssysteem essentieel om aanvallen op tijd te kunnen ontdekken en de gevolgen zoveel mogelijk te kunnen beperken.



3. Feiten en cijfers

In het kort

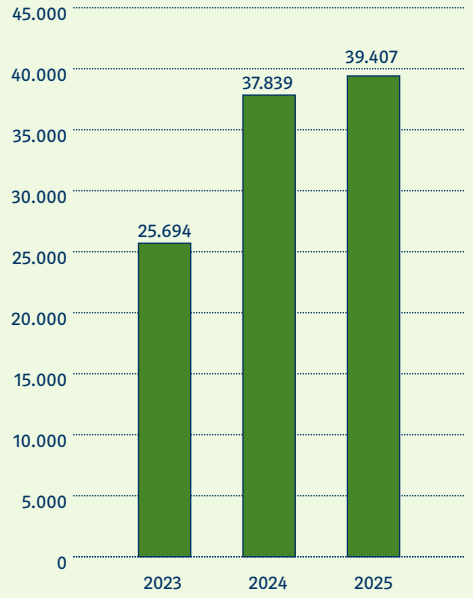
- In 2025 zijn 39.407 datalekken gemeld aan de AP.
- Het aantal datalekken door cyberaanvallen is gestegen sinds 2024.
- Opvallend is de stijging in cyberaanvallen waarbij accounts worden overgenomen. Deze aanvallen zijn bijna altijd het gevolg van phishing.
- In 2025 waren er ook opvallende datalekken waarbij persoonsgegevens per ongeluk werden gepubliceerd, en waarbij USB-sticks of documenten werden kwijtgeraakt.

AP ziet toename in datalekken door cyberaanvallen

In 2025 zijn alles bij elkaar 39.407 datalekken gemeld aan de AP.* Dat waren er in 2024 37.839. Opvallend was de toename van het aantal datalekken door cyberaanvallen. Dat wordt in dit hoofdstuk verder uitgelicht.

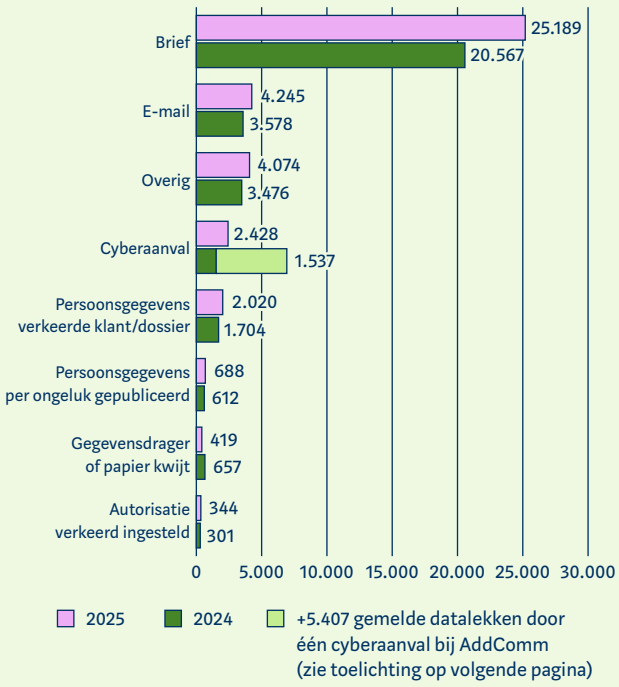
Organisaties uit de sectoren financiële dienstverlening, openbaar bestuur, en gezondheid en welzijn meldden de meeste datalekken. Deze organisaties werken met veel en gevoelige persoonsgegevens.

FIGUUR 1 | Gemelde datalekken in 2023, 2024 en 2025



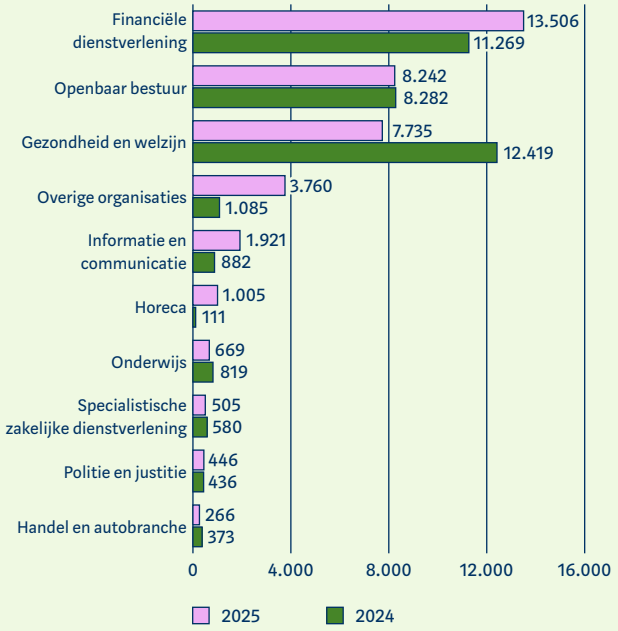
Sinds 2024 mogen meer organisaties meerdere datalekken in één keer melden. Dat doen ze met een zogeheten bulkmelding. Dit vermindert de administratieve druk voor organisaties. Bulkmeldingen gaan meestal over verkeerd verstuurde brieven. Sindsdien worden er meer datalekken gemeld.

FIGUUR 2 | Soorten datalekken in 2024 en 2025



* In het AP-jaarverslag 2025 staat dat 44.374 datalekken zijn gemeld. Na correctie van de datalekken komt de AP in deze datalekkenrapportage tot een totaal van 39.407 datalekken.

FIGUUR 3 | Sectoren met de meest gemelde datalekken in 2024 en 2025



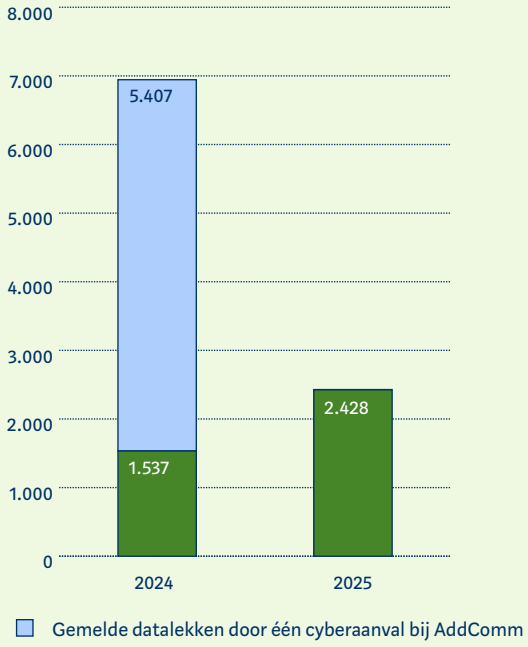
Datalekken door cyberaanvallen

In 2025 werden 2.428 datalekken door cyberaanvallen gemeld. Dat zijn er meer dan in 2024, toen waren dat er 1.537. In totaal ontving de AP in 2024 6.944 datalekken door cyberaanvallen, waarvan er echter 5.407 ontstonden door één aanval bij klantcommunicatiebedrijf AddComm. Door deze ene aanval moesten uitzonderlijk veel organisaties een datalek melden.

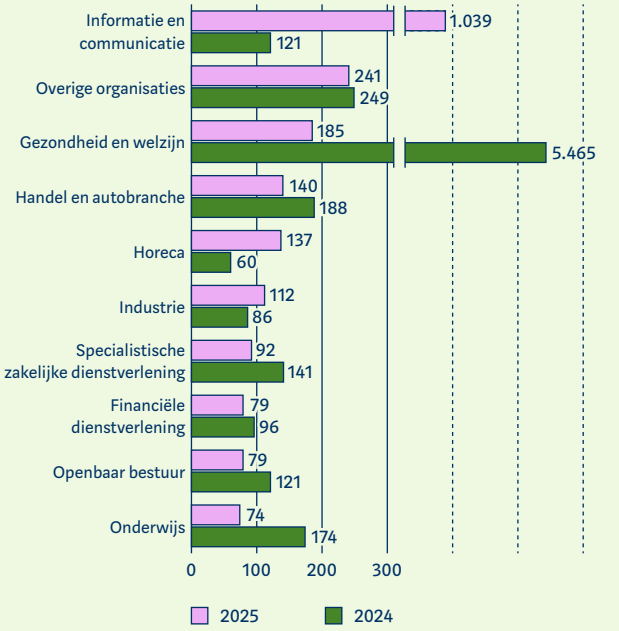
Er zijn verschillende soorten cyberaanvallen. In dit hoofdstuk gaat de AP specifiek in op account takeovers en ransomware-aanvallen. In 2025 zag de AP 1.742 account takeovers. Dit leidde tot zeker 1.780 datalekken die aan de AP werden gemeld. Daarnaast zag de AP in 2025 136 ransomware-aanvallen. Dit leidde tot zeker 283 gemelde datalekken.

Het aantal datalekken door account takeovers of ransomware-aanvallen ligt hoger dan het aantal aanvallen. Dat komt omdat één cyberaanval er soms voor zorgt dat meerdere organisaties een datalek melden. Bijvoorbeeld als dezelfde IT-leverancier van een aantal organisaties is aangevallen. Figuren 7 en 8 gaan in op het aantal aanvallen.

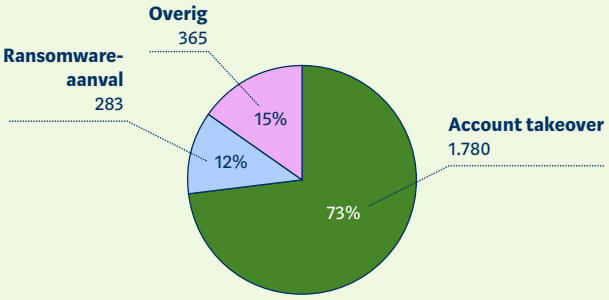
FIGUUR 4 | Datalekken door cyberaanvallen in 2024 en 2025



FIGUUR 5 | Cyberaanvallen: sectoren met de meest gemelde datalekken in 2024 en 2025



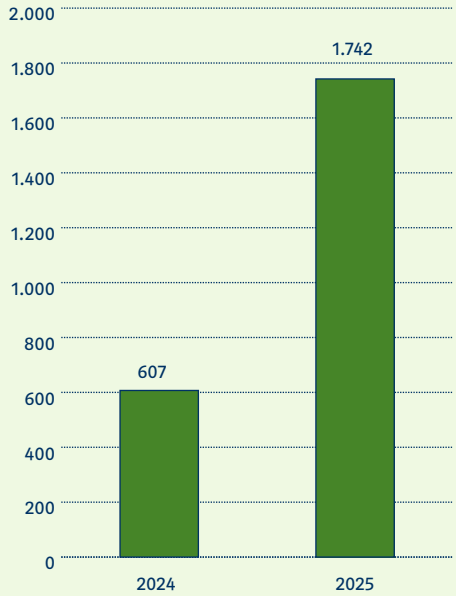
FIGUUR 6 | Datalekken door account takeovers en ransomware-aanvallen in 2025



Zorgelijke stijging van account takeovers

Het aantal cyberaanvallen waarbij accounts worden overgenomen (account takeovers) is aanzienlijk gestegen. Bij een account takeover krijgt een cybercrimineel toegang tot een account, bijvoorbeeld een mailbox. Zo'n takeover komt bijna altijd door phishing. In 2025 zag de AP 1.742 geslaagde aanvallen waarbij één of meerdere accounts werden overgenomen. Dat is flink gestegen sinds 2024, toen gebeurde dit 607 keer. De AP ziet dat dit een populaire manier is voor cybercriminelen om gegevens buit te maken en als opstart voor grotere aanvallen. De AP maakt zich zorgen over een verdere stijging door AI.

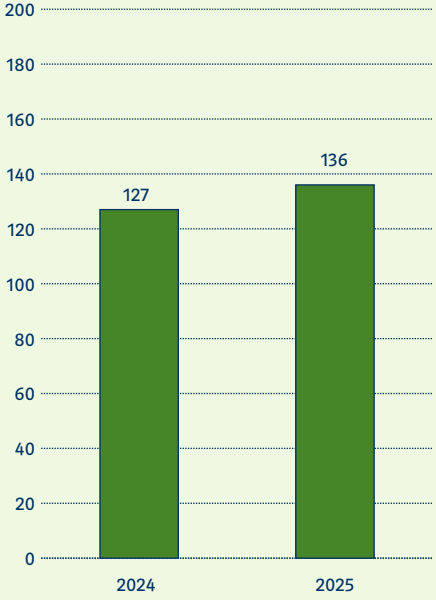
FIGUUR 7 | Account takeovers in 2024 en 2025



Ransomware-aanvallen licht gestegen

Ransomware is een heel schadelijke vorm van cyberaanvallen. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. Cybercriminelen kunnen bij deze aanvallen gegevens versleutelen en stelen en daarna dreigen die te publiceren. Tegenwoordig zien we vaak dat de cybercriminelen gegevens meteen stelen, zonder deze ook te versleutelen. Het stelen van gegevens is een zorgelijke ontwikkeling omdat dit verder misbruik mogelijk maakt. Sinds 2025 rekent de AP die aanvallen ook als ransomware-aanvallen. In 2025 zag de AP 136 ransomware-aanvallen. In 2024 waren dat er 127.

FIGUUR 8 | Ransomware-aanvallen in 2024 en 2025



Datalekken doordat persoonsgegevens per ongeluk door de organisatie zelf zijn gepubliceerd

Cyberaanvallers kunnen gegevens online zetten, maar ook organisaties doen dat regelmatig per ongeluk. In 2025 werden 688 van dit soort datalekken gemeld. Dit gebeurde vooral vaak in de sector openbaar bestuur. Overheidsinstanties zetten veel documenten online, bijvoorbeeld na een Woo(openbaarmakings)-aanvraag. De instanties vergeten dan persoonsgegevens weg te halen. Maar persoonsgegevens worden ook regelmatig verkeerd weggehaald of gelakt.

Persoonsgegevens van ambtenaren niet goed weggehaald in overheidsdocumenten

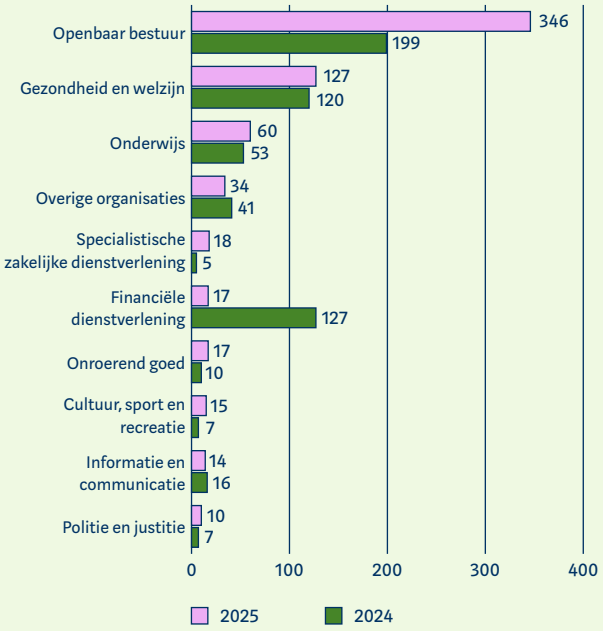
De AP ontving veel meldingen van datalekken bij ministeries, provinciehuizen en gemeentes. Zij hadden documenten online gezet, waar nog metadata als namen van ambtenaren of soms telefoonnummers in stonden. Ook werden documenten verkeerd gelakt, waardoor persoonsgegevens toch nog vindbaar waren.

Naar aanleiding van deze datalekken gaf de AP adviezen om dit soort datalekken tegen te gaan. Veel organisaties maken de fout om met een digitale zwarte markeerstift gegevens onleesbaar te maken. De gegevens zijn dan niet meteen te zien, maar staan nog wel in het document. Een ontvanger kan de gegevens dan alsnog terughalen.

Gemeente maakt namen en adressen van bezwaarmakers tegen een AZC per ongeluk bekend

De gemeente Midden-Delfland zette per ongeluk een document online met de namen en adressen van 133 inwoners, die het niet eens zijn met de komst van een asielzoekerscentrum. Dit leidde tot veel zorgen over de gevolgen en angst voor de mening van andere inwoners in de gemeente.

FIGUUR 9 | Persoonsgegevens per ongeluk door de organisatie gepubliceerd: sectoren met de meest gemelde datalekken in 2024 en 2025



Verloren USB-stick, apparaat of documenten met persoonsgegevens

Ook in de fysieke wereld worden nog regelmatig datalekken veroorzaakt. Met telefoons, laptops, USB-sticks en geprinte documenten kunnen medewerkers overal hun belangrijke informatie bij zich hebben. Ook gevoelige persoonsgegevens. Maar mensen kunnen de apparaten en papieren ook kwijtraken. De AP ontvangt dan ook regelmatig meldingen van een datalek omdat medewerkers een laptop of telefoon in de trein hebben laten liggen, of omdat zo'n gegevensdrager is gestolen, bijvoorbeeld uit een geparkeerde auto. In 2025 werd 419 keer zo'n datalek gemeld. De meeste meldingen hierover kwamen uit de sector gezondheid en welzijn.

Zorginstelling Pluryn raakt USB-stick kwijt met gegevens van cliënten en medewerkers

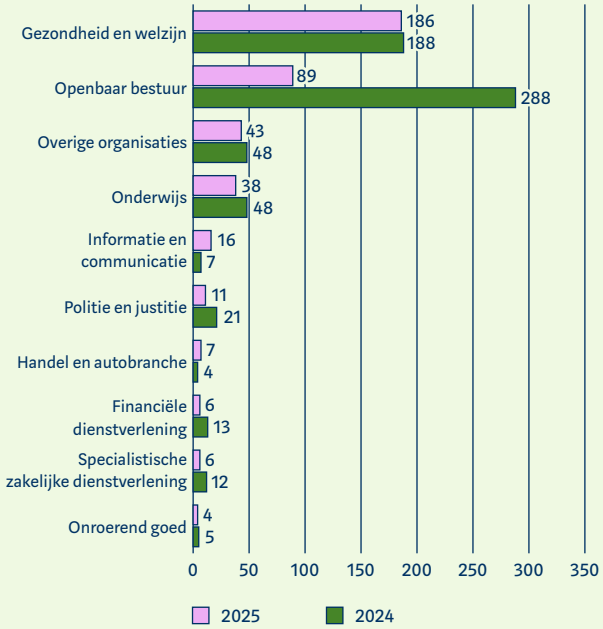
In 2025 verloor zorginstelling Pluryn een USB-stick die niet beveiligd was. Op de USB-stick stonden persoonsgegevens van alle cliënten die zorg kregen in de afgelopen 25 jaar. En persoonsgegevens van werknemers. Het ging om gegevens als contactinformatie, adressen en BSN's. Maar op de USB-stick stond bijvoorbeeld ook wat voor zorg een cliënt kreeg. En van medewerkers stond informatie over ziekmeldingen en het salaris opgeslagen.

Wanneer een USB-stick met zoveel gevoelige persoonsgegevens in verkeerde handen belandt, kan dat grote gevolgen hebben voor de mensen om wie het gaat.

Organisaties die het gebruik van USB-sticks toestaan, moeten ervoor zorgen dat ze goed beveiligd zijn zodat niet iedereen toegang kan krijgen tot wat erop staat. Als zo'n USB-stick dan kwijtraakt, is de kans op misbruik kleiner.

Organisaties die USB-sticks verbieden, moeten werknemers bewust maken van de risico's en veilige alternatieven aanbieden.

FIGUUR 10 | Gegevensdrager of papier kwijt: sectoren met de meest gemelde datalekken in 2024 en 2025



Bronnenlijst

Anthropic's frontiermodel Mythos vraagt om directe actie | NCSC

CSR Signaalbrief AI | Cyber Security Raad

Cybersecuritybeeld Nederland 2025 | Nationaal Coördinator Terrorismebestrijding en Veiligheid

Generatieve AI. Een transformatieve impact op cybersecurity | AIVD

Woordenboek - Cyberveilig Nederland

De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder op persoonsgegevens die mensen beschermt in een digitale wereld.

Autoriteit Persoonsgegevens
Postbus 93374
2509 AJ Den Haag

autoriteitpersoonsgegevens.nl