AUTORITEIT
PERSOONSGEGEVENS

Datalekkenrapportage 2022

Aantal datalekmeldingen 2022	Aantal meldingen van cyberaanvallen 2022	Aantal datalekmeldingen afgelopen 5 jaar
21.151	1.826	114.258

5 jaar datalekken: iedereen kan slachtoffer worden

Ga ervan uit dat je persoonlijke gegevens al eens gelekt zijn, of dat dit nog gaat gebeuren. Maar je kunt jezelf beschermen: maak daar werk van. Deze boodschap geeft de Autoriteit Persoonsgegevens (AP) Nederlanders mee, 5 jaar nadat de privacywet Algemene verordening gegevensbescherming (AVG) in werking is getreden.

In 5 jaar tijd heeft de AP meer dan 114.000 meldingen van datalekken ontvangen. Dat zijn er gemiddeld meer dan 20.000 per jaar. Van alle meldingen ging het in meer dan 6.500 gevallen om cyberaanvallen, die bijzonder schadelijk kunnen zijn voor mensen en organisaties. Omdat er inmiddels zo'n grote hoeveelheid data gestolen is, moeten mensen er van uitgaan dat hun persoonsgegevens zijn gelekt, of dat dit in de toekomst zal gebeuren.

Om mensen te helpen zichzelf te beschermen, zet de AP in deze datalekkenrapportage een aantal praktische tips op een rij. Ook komen slachtoffers van datalekken aan het woord. Daarnaast geeft de rapportage een overzicht van feiten en cijfers over datalekken.

Het afgelopen jaar zijn door de drie grootste cyberaanvallen in de zorg naar schatting 900.000 patiënten getroffen. Van hen zijn medische gegevens op straat komen te liggen. Bij na een kwart van de gemelde datalekken over cyberaanvallen was in 2022 afkomstig uit de zorgsector.

Ernstige gevolgen datalekken

Datalekken kunnen ernstige gevolgen hebben voor slachtoffers. Mensen kunnen financieel getroffen worden, bijvoorbeeld door identiteitsfraude en oplichting. Het Centraal Meldpunt Identiteitsfraude (CMI) ontving in 2022 ruim 6.000 meldingen van identiteitsfraude. Een ander gevolg van datalekken is dat

slachtoffers reputatieschade kunnen lijden als gegevens uit hun privéleven zijn gelekt. Denk aan privéfoto's, gevoelige informatie over (mentale) gezondheid of problemen in een thuissituatie.

Wat is een cyberaanval?
Bij een cyberaanval weten criminelen (hackers) in te breken in mailboxen of computersystemen. Ze proberen daarbij toegang te krijgen tot zoveel mogelijk gegevens. Criminelen proberen de gegevens te stelen of met een speciaal programma te gijzelen. Bij zo'n ransomware-aanval heeft de getroffen organisatie zelf geen toegang meer tot de data en moet eerst losgeld betalen om weer toegang tot de data te krijgen.

De AP ziet daarnaast steeds vaker dubbele afpersing: hackers gijzelen data, en dreigen ook om deze data te publiceren op het internet of door te verkopen. Het betalen van losgeld is geen oplossing of beveiligingsmaatregel. Het geeft namelijk geen zekerheid dat gelekte persoonsgegevens niet worden doorverkocht of gepubliceerd.

1. Slachtoffers van cyberaanvallen aan het woord

Het toezicht op de meldplicht datalekken helpt de digitale weerbaarheid van slachtoffers en organisaties te vergroten. En dat is heel belangrijk, want de AP ziet regelmatig hoe groot de impact van een datalek kan zijn op mensen.

Misdaadverslaggever John van den Heuvel weet als geen ander wat voor schadelijke gevolgen een datalek kan hebben. In 2021 werd informatie over zijn woonadres online te koop gezet. Er bleek een datalek te zijn geweest bij de GGD. Gevoelige gegevens zoals namen, adressen, telefoonnummers en Burgerservicenummers van mensen kwamen in verkeerde handen terecht.

'Het gaf me een buitengewoon vervelend, onbehaaglijk gevoel', zo blikt Van den Heuvel terug in een gesprek met de AP. Extra wrang voor Van den Heuvel was dat hij op het moment van het datalek al jarenlang werd beveiligd vanwege dreigementen. Dat zijn woonadres openbaar werd, vormde dus een veiligheidsrisico.

Ook los van zijn persoonlijke situatie maakt hij zich zorgen over datalekken. Als verslaggever ziet Van den Heuvel hoe oplichters proberen mensen om de tuin te leiden. Oplichters krijgen e-mailadressen bijvoorbeeld in handen na een datalek. Zij kunnen dan gerichte nepmails sturen met het verzoek om op een betaallink te klikken. 'Mensen kunnen vervolgens bang worden om online nog iets te kopen', aldus Van den Heuvel. 'Ze gaan vrezen voor hun gegevens.'

Wat Van den Heuvel ook ziet: hoe de misdaadwereld zich steeds meer toelegt op cyberdiefstal en de handel in persoonlijke gegevens van mensen. 'Daar wordt een nieuwe, jonge generatie van criminelen voor ingezet', zo schetst hij een trend.

Daarom waarschuwt hij: let goed op als je mailtjes of appjes krijgt met bijvoorbeeld een betaalverzoek, ook als de afzender er betrouwbaar uitziet. Controleer bij twijfel of de afzender echt is, bijvoorbeeld door het mailadres van de afzender goed te bekijken. Of door de organisatie waar het bericht vandaan zou komen, te bellen.

Belangrijk is ook dat bedrijven en organisaties mensen goed informeren als hun persoonlijke gegevens zijn getroffen door een datalek. Alleen dan kunnen mensen er rekening mee houden en zelf actie ondernemen. Bedrijven en organisaties zijn verplicht om mensen te informeren, bijvoorbeeld via een brief of een e-mail. In de praktijk zijn zulke berichten niet altijd even duidelijk, merkt de AP. Van den Heuvel sluit zich hierbij aan. 'Ik heb ook weleens zo'n mail gehad: "Uw gegevens zijn betrokken bij een datalek". Daar kan ik niet veel mee. Zulke berichten moeten duidelijker. Om welke gegevens gaat het?'

Hacking van mailbox

Dit jaar ontving de AP 1.826 meldingen van cyberaanvallen. Het slachtoffer van een van deze datalekken vertelt over de schadelijke gevolgen die de hack op hem had.

Edward had nooit gedacht dat hij slachtoffer zou worden van cyberdiefstal - hij heeft nota bene een achtergrond in de IT. Toch is dat wat er gebeurde. Edward, die anoniem blijft, werd voor tienduizenden euro's opgelicht toen hij dacht via online onderhandelingen een auto te kopen.

'Ik voelde me verpletterd toen het me overkwam, ik was erg emotioneel en boos'. 'Boos dat dit mij was overkomen. Dat ik een slachtoffer was geworden.'

Wat was er gebeurd? Edward had op de website van een erkende autodealer een auto gezien die hij mooi vond. Per telefoon en e-mail had hij meerdere keren contact met de dealer. Toen ze het eens waren over de verkoop en Edward de wagen ging ophalen, vroeg de autodealer aan hem of hij kon betalen. 'Maar ik heb toch al betaald?', zei Edward, die vlak daarvoor geld had overgemaakt naar de rekening van de autodealer. Tenminste: dat dacht hij.

In werkelijkheid bleek het e-mailaccount van de autodealer te zijn gehackt. Criminelen deden zich naar Edward voor als de autodealer. Ze stuurden Edward hun eigen rekeningnummer met het verzoek om daar het geld op te storten. Dat deed hij. Edward en de autodealer wisten op dat moment van niks.

'Toen we erachter kwamen, dachten we allebei: wat is hier in hemelsnaam aan de hand?'. Edward probeerde zijn geld terug te krijgen. Maar de negatieve gevolgen gaan voor hem verder dan het geld dat hij kwijt is. 'Deze hele kwestie kost me tijd en levert me stress op. Ik merk dat het me afleidt, bijvoorbeeld tijdens mijn werk.'

Hij heeft zich voorgenomen om beter op te letten als hij nog eens via internet een aankoop doet. 'Als ik online iets koop, is het meestal via een platform waarbij er een betrouwbare derde partij tussenin zit. Maar volgende keer dat ik rechtstreeks iets van iemand koop, is het waarschijnlijk goed om meer persoonlijk contact te hebben. Tegenwoordig doen we met z'n allen eigenlijk zo vaak zaken zonder dat we met een persoon praten.'

2. Slachtoffer van een datalek? Dit kunt u doen

Krijgt u bericht van een organisatie dat uw persoonsgegevens onderdeel zijn van een datalek? Dat betekent dat u de controle over uw persoonsgegevens bent kwijtgeraakt en dat kan vervelende gevolgen voor u hebben. Toch kunt u vaak nog iets doen om uzelf te beschermen tegen de gevolgen van het datalek. En zo de schade beperken.

Wat u precies kunt doen hangt af van welke gegevens van u zijn gelekt, en wie toegang tot deze gegevens heeft (gehad). U kunt hierover informatie vragen bij de organisatie. Wat kunt u verder doen? Hieronder enkele tips.

E-mailadres en wachtwoord gelekt? Wijzig uw wachtwoorden

Gebruikt u hetzelfde wachtwoord op andere websites? Verander dan ook op deze websites uw wachtwoord. Gebruik bij elke website een ander wachtwoord. Zorg voor een sterk wachtwoord.

E-mailadres of telefoonnummer gelekt? Wees alert op phishing

Phishing is een vorm van fraude waarbij criminelen proberen uw gegevens te achterhalen. Zoals inloggegevens, creditcardinformatie, pincodes of informatie op uw identiteitsbewijs. U ontvangt bijvoorbeeld een nepmail met het verzoek om uw gegevens achter te laten op een andere website. Wees dus extra alert op berichten op uw e-mailadres of telefoonnummer waarin u gevraagd wordt om iets te doen.

Identiteitsbewijs gelekt? Meld dit bij uw gemeente en vraag een nieuw identiteitsbewijs aan

Met een gelekt identiteitsbewijs kunnen criminelen identiteitsfraude plegen. Zij maken dan misbruik van uw gegevens, bijvoorbeeld door op uw naam:

- spullen te kopen zonder te betalen;
- een lening af te sluiten;
- een telefoonabonnement af te sluiten.

Om de kans op identiteitsfraude te verkleinen, meldt u bij uw gemeente dat uw identiteitsbewijs is gestolen. U kunt bij uw gemeente een nieuw identiteitsbewijs aanvragen.

Tip: Houd na een datalek in de gaten of u vreemde dingen ziet gebeuren op uw bankrekening. En of u e-mails of post krijgt over aankopen die u niet heeft gedaan.

Schadevergoeding voor datalek

Zijn uw gegevens gelekt? En heeft u hierdoor schade geleden? Dan heeft u misschien recht op een schadevergoeding. U heeft volgens de AVG recht op een schadevergoeding als een organisatie in strijd met de AVG handelt en u daardoor schade lijdt. En als dit deze organisatie kan worden verweten.

Voor een schadevordering tot een bedrag van €25.000 kunt u naar de kantonrechter. U heeft daarvoor geen advocaat nodig. Is uw schadevordering hoger dan € 25.000? Dan kunt u bij de civiele rechter een rechtszaak beginnen. U moet dan wel een advocaat inschakelen.

Zie voor meer informatie de website van de Rechtspraak.

3. Wat kunt u *vooraf* doen om schade te voorkomen?

De AP heeft de afgelopen 5 jaar ruim 114.000 datalekmeldingen ontvangen. De kans is zeer groot dat uw persoonsgegevens daar één of meerdere keren onderdeel van zijn geweest. U kunt nu maatregelen nemen om zoveel mogelijk te voorkomen dat u schade oploopt door toekomstige datalekken.

Dit kunt u doen:

- Gebruik overal een **ander wachtwoord**. En zorg voor een sterk wachtwoord. Verander uw wachtwoord als dat nodig is, bijvoorbeeld als het is gelekt.
- Biedt een organisatie een **extra beveiligde inlogmethode** aan? Maak daar dan gebruik van. U moet dan bijvoorbeeld ook een code invoeren die u via uw telefoon krijgt, naast uw gebruikersnaam en wachtwoord.
- Verstrek indien mogelijk een veilige kopie van uw identiteitsbewijs door bijvoorbeeld gebruik te maken van de **KopieID-app** van de Rijksoverheid. Met deze app kunt u gegevens doorstrepen die organisaties niet nodig hebben. Zo zorgt u ervoor dat u het risico op identiteitsfraude verkleint als de organisatie wordt getroffen door een cyberaanval.
- Let goed op wie om uw gegevens vraagt en op welke manier. Wees zelf de **baas over uw gegevens**. Vraagt een bedrijf om gegevens die het helemaal niet nodig heeft om u een dienst te verlenen? Geef die gegevens dan niet.

- Maak gebruik van uw privacyrechten. Vraag organisaties om bepaalde gegevens van u te verwijderen, door middel van een **verzoek om verwijdering**. Bijvoorbeeld als u een account voor een webshop niet meer gebruikt. Hoe minder gegevens organisaties van u hebben, hoe minder risico u loopt.

4. Welke informatie moeten organisaties verstrekken na een datalek?

Organisaties zijn meestal verplicht om slachtoffers te informeren over een datalek. Slachtoffers kunnen zich dan wapenen tegen de gevolgen.

De AVG stelt eisen aan die informatieverplichting aan de slachtoffers. De informatie moet in ieder geval antwoord geven op deze vragen:

1. Wat is er gebeurd?
2. Wat zijn (waarschijnlijk) de gevolgen?
3. Welke maatregelen treft de organisatie?
4. Wat kan het slachtoffer zelf doen?
5. Waar kan het slachtoffer terecht met vragen?

De AP merkt dat organisaties slachtoffers niet altijd even duidelijk informeren. De AP kan organisaties verplichten om die informatie aan te passen als dat nodig is. Informeert een organisatie slachtoffers niet, terwijl dat wel moet? Dan kan de AP handhavend optreden.

Tip voor organisaties: Vermijd in de melding aan de slachtoffers juridisch taalgebruik en gebruik korte zinnen. Zorg voor een duidelijke kop, introductie en onderwerp. Waarschuw voor concrete gevolgen, en geef praktische tips.

5. Overzicht feiten en cijfers 2022

Aantal datalekmeldingen

Nederland ontvangt relatief gezien de meeste datalekmeldingen binnen Europa.[1] Doordat Nederland sterk gedigitaliseerd is, is het risico op (grote of ernstige) datalekken hier relatief hoog. Extra aandacht voor de bescherming van persoonsgegevens en cybersecurity is daarom nodig.

Aantal grensoverschrijdende datalekmeldingen

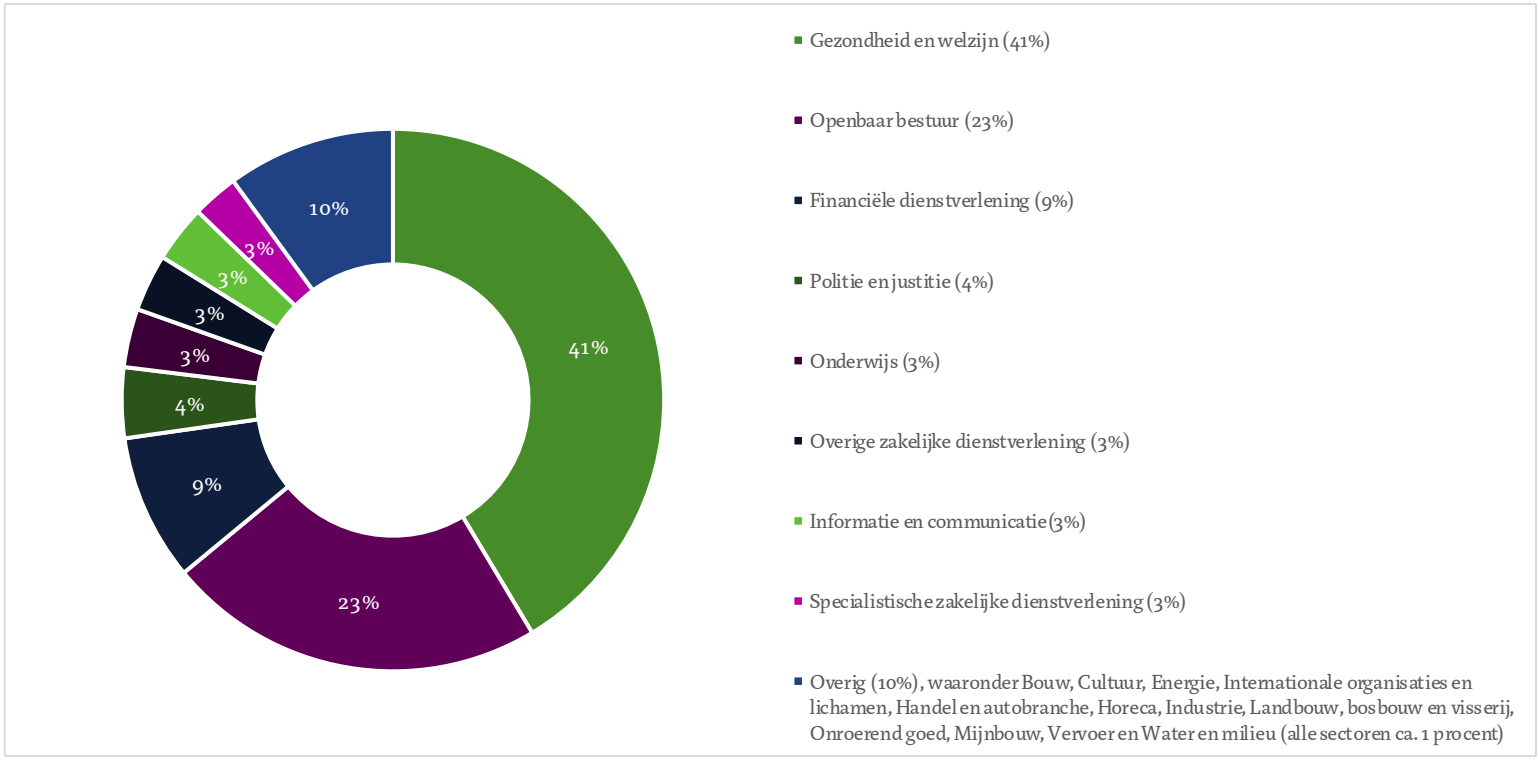
De 21.151 meldingen zijn meldingen van datalekken in Nederland die de AP in 2022 heeft ontvangen via het meldloket datalekken op de website van de AP. Daarnaast hebben andere Europese privacytoezichthouders in 47 gevallen een grensoverschrijdend datalek gedeeld met de AP. Dat gebeurt bijvoorbeeld als een datalek bij een andere Europese toezichthouder is gemeld, maar het mogelijk ook

[1] Aantal ontvangen datalekmeldingen per 100.000 inwoners tussen 28 januari 2021 en 27 januari 2022: (1) Nederland 150,71; (2) Liechtenstein 136,02; (3) Denemarken 130,60. Bron: DLA Piper GDPR fines and data breach survey: January 2022, p. 17.

significante gevolgen heeft voor slachtoffers in Nederland. De AP deelt in sommige gevallen ook meldingen over grensoverschrijdende datalekken met andere privacytoezichthouders. Dit deed de AP in 2022 7 keer.

Aantal datalekmeldingen per sector

In 2022 is het aantal meldingen uit de sector financiële dienstverlening gedaald met 29% ten opzichte van 2021. Het aantal meldingen uit de sector openbaar bestuur is gedaald met 16% en het aantal meldingen uit de sector gezondheid en welzijn is gedaald met 6%.

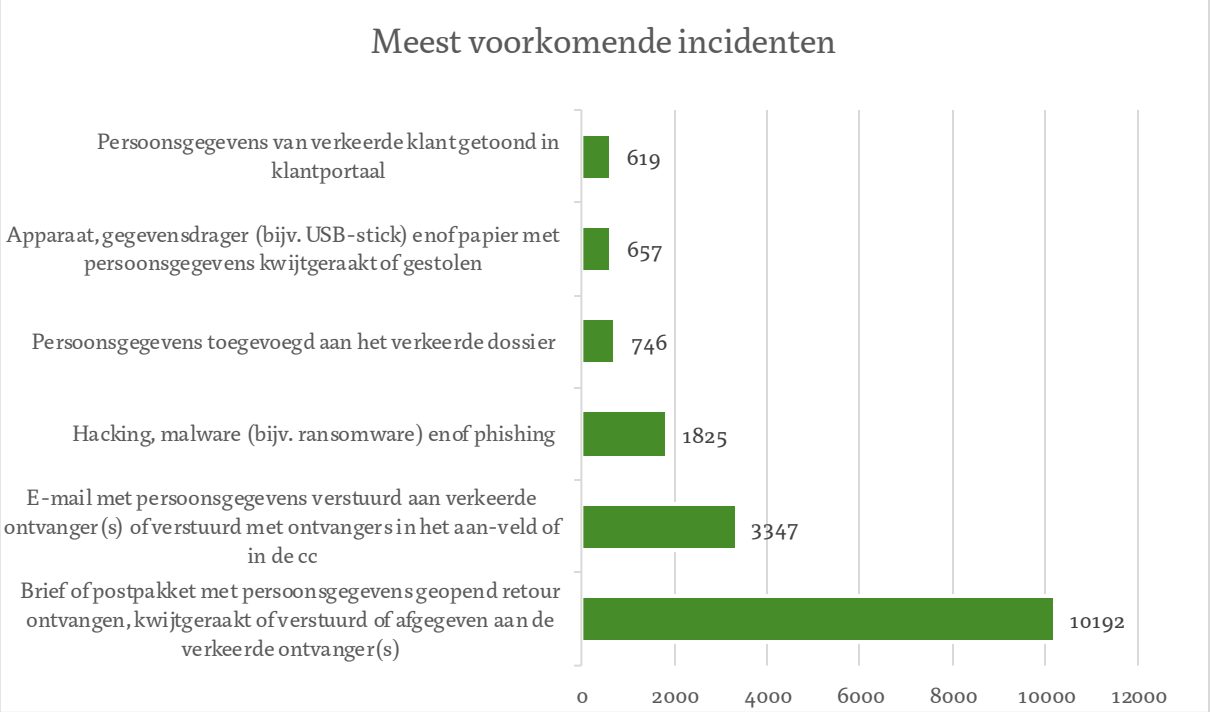


Binnen de sector Politie en justitie is het aantal meldingen juist gestegen, namelijk met 11%. Datalekmeldingen vanuit deze sector worden niet vanuit de AVG gedaan, maar vanuit de Richtlijn gegevensbescherming bij rechtshandhaving, die in Nederland is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Hier houdt de AP ook toezicht op.

Type datalekken

In 2022 ziet de AP een grote stijging in het aantal meldingen waarbij persoonsgegevens zijn toegevoegd aan een verkeerd dossier (+98%). Bijvoorbeeld wanneer een psychologisch rapport door een zorgverlener per ongeluk wordt toegevoegd aan het dossier van de verkeerde cliënt.

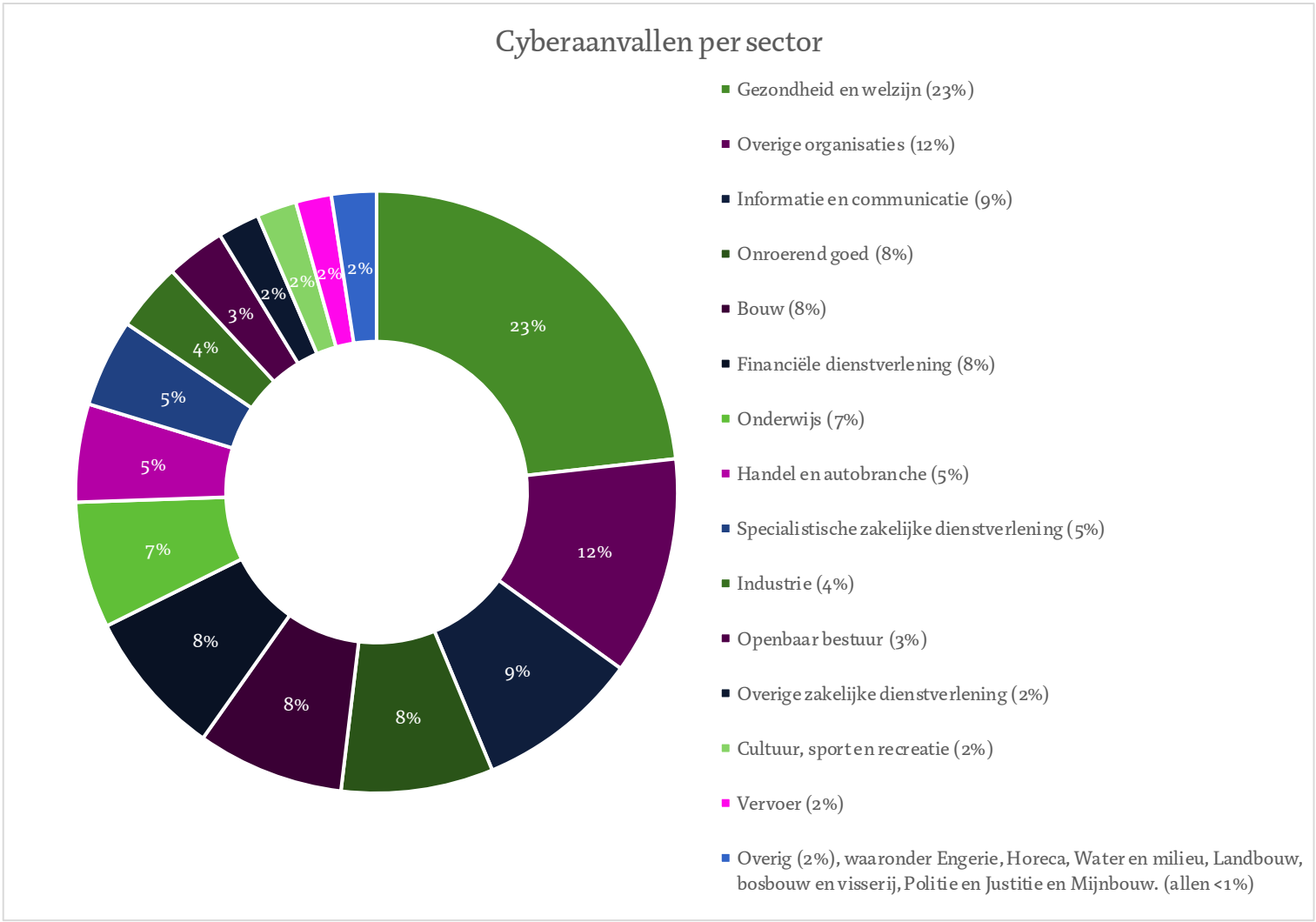
Verder ziet de AP een grote stijging van 65% van het aantal meldingen waarbij autorisaties van medewerkers te breed waren ingesteld. Als gevolg van dit type datalek kunnen medewerkers van organisaties persoonsgegevens inzien die ze voor hun werkzaamheden niet nodig hebben.



Aantal cyberaanvallen per sector

De meeste meldingen van cyberaanvallen heeft de AP in 2022 ontvangen uit de sector Gezondheid en welzijn (424 meldingen). Een groot deel van deze datalekmeldingen heeft de AP ontvangen naar aanleiding van cyberaanvallen bij ICT-leveranciers in de zorg. Alleen al door de grootste drie cyberaanvallen bij ICT-leveranciers zijn van ongeveer 900.000 patiënten of cliënten medische persoonsgegevens gelekt.

Daarnaast heeft de AP veel meldingen van cyberaanvallen ontvangen uit de sector Informatie en communicatie (160 meldingen), Onroerend goed (149 meldingen), Bouw (144 meldingen) en Financiële dienstverlening (144 meldingen). Onder de sector 'Informatie en communicatie' valt ook ICT-dienstverlening.



6. Toezicht AP op de meldplicht datalekken

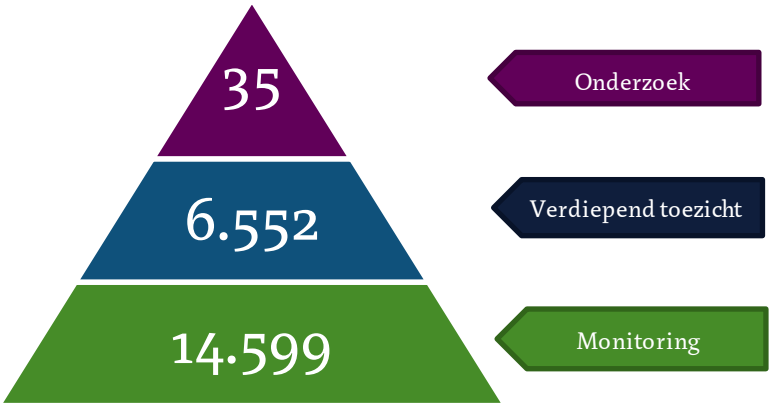
Het toezicht van de AP op de meldplicht datalekken bestaat uit twee onderdelen: het toezicht op gemelde datalekken (paragraaf 6.1) en het toezicht op niet gemelde datalekken (paragraaf 6.2). Om scherpe keuzes te maken is het toezicht van de AP op de meldplicht datalekken risicogestuurd. Dat betekent dat de AP zich voornamelijk richt op die datalekken die de grootste risico's opleveren voor slachtoffers. De AP identificeert risico's aan de hand van datalekmeldingen en dataleksignalen. Een signaal kan bijvoorbeeld een bericht uit de media of een tip van een burger zijn. De grootste risico's voor slachtoffers ziet de AP o.a. bij datalekken:

- als gevolg van een cyberaanval;
- waarbij slachtoffers ten onrechte niet worden geïnformeerd over het datalek;
- bij leveranciers, met name van ICT-diensten;
- met grote aantallen slachtoffers;
- met bijzondere en/of gevoelige persoonsgegevens;
- die ten onrechte niet aan de AP worden gemeld.

Het toezicht op de meldplicht datalekken heeft tot doel de digitale weerbaarheid van slachtoffers en organisaties te vergroten. De AP zorgt ervoor dat organisaties de slachtoffers van datalekken waarschuwen.

6.1 Toezicht op gemelde datalekken

Het is belangrijk dat organisaties datalekken melden aan de AP. Zonder datalekmelding kan de AP geen toezicht houden op de informatieverplichting naar de slachtoffers. Verder kan de AP dan ook niet controleren of de getroffen organisatie wel voldoende beveiligingsmaatregelen neemt om nieuwe datalekken te voorkomen. Daarnaast stellen datalekmeldingen de AP in staat om risicoanalyses te maken en nieuwe trends te signaleren.



Hoe groter de risico's die de AP identificeert, hoe intensiever het toezicht. Dat betekent dat de AP niet elke datalekmelding even uitgebreid onderzoekt. De AP kan datalekmeldingen monitoren, verdiepend toezicht toepassen of een onderzoek starten. De ruim 21.000 datalekmeldingen in 2022 hebben geleid tot 35 onderzoeken.

Verdiepend toezicht in de praktijk

De functionaris gegevensbescherming (FG) van een transportbedrijf doet een datalekmelding aan de AP. In de melding geeft de FG aan dat de mailbox van een HR-medewerker is gehackt. Een crimineel heeft toegang gehad tot de mailbox en phishingmails verstuurd naar alle contactpersonen van de medewerker. De FG geeft aan dat alle contactpersonen zijn gewaarschuwd voor de phishingmail.

De AP neem naar aanleiding van deze datalekmelding telefonisch contact op met het transportbedrijf. Naast het versturen van phishingmails, kan de hacker de inhoud van de mailbox gestolen hebben. In mailboxen kunnen waardevolle gegevens zitten, zoals kopieën van paspoorten die per mail verstuurd zijn aan de HR-medewerker. Veel organisaties zijn zich hier niet van bewust.

De AP draagt het transportbedrijf op om de inhoud van gehackte mailboxen te onderzoeken op gevoelige en/of bijzondere persoonsgegevens. Na onderzoek van de mailbox bleken er tientallen kopieën van identiteitsbewijzen in de mailbox te zitten, terwijl dat volgens de beveiligingsrichtlijnen van het transportbedrijf niet mag. Het transportbedrijf moet de mensen van wie de identiteitsbewijzen zijn informeren over het datalek en waarschuwen voor de kans op identiteitsfraude. Dat heeft de AP het transportbedrijf opgedragen.

Monitoring: bijna 15.000 meldingen

Bij een groot deel van de datalekmeldingen neemt de AP na een eerste beoordeling geen verdere actie. Van zulke meldingen ontving de AP er bijna 15.000 in 2022. Het gaat hier bijvoorbeeld vaak om meldingen van verkeerd verzonden post of e-mails.

Verdiepend toezicht: 6.552 meldingen

Het afgelopen jaar heeft de AP bij 6.552 datalekmeldingen extra toezichtshandelingen verricht. Dat was nodig omdat de AP in deze datalekmeldingen grote risico's identificeerde. Bijvoorbeeld omdat het ging om veel slachtoffers of (veel) gevoelige persoonsgegevens. Bij zulke meldingen doet de AP een diepgaandere controle.

Tijdens een verdiepende controle kan de AP contact opnemen met de organisatie om vragen te stellen over het datalek. Bijvoorbeeld omdat de datalekmelding onduidelijk is, onregelmatigheden bevat of inconsistent is. Daarnaast kan de AP na zo'n controle een zogenoemde normoverdragende brief sturen of een normoverdragend gesprek voeren. In zo'n brief of gesprek wijst de AP de organisatie op de regels. Zoals de verplichting om slachtoffers over het datalek te informeren. Een normoverdragend gesprek kan

ook op het kantoor van de AP plaatsvinden. Soms bezoekt de AP de organisatie na een datalekmelding ter plaatse, als dat nodig is voor het toezicht.

De AP neemt niet bij elke melding contact op met de organisatie. Bijvoorbeeld omdat uit de melding blijkt dat er al voldoende nieuwe beveiligingsmaatregelen zijn getroffen en alle betrokkenen op de juiste manier zijn geïnformeerd.

Onderzoeken naar aanleiding van datalekmeldingen

In 2022 is de AP naar aanleiding van 35 datalekmeldingen een onderzoek gestart. Deze 35 datalekmeldingen brachten de grootste risico's voor de slachtoffers met zich mee, oordeelde de AP. Het ging voornamelijk om situaties waarbij een organisatie de slachtoffers van een cyberaanval niet informeerde, terwijl dat wel moest. En om situaties waarbij een organisatie onvoldoende nieuwe beveiligingsmaatregelen had genomen om nieuwe datalekken te voorkomen.

Een onderzoek kan zich richten op een enkele organisatie maar ook op een groep organisaties. Bijvoorbeeld naar aanleiding van een cyberaanval bij een ICT-leverancier. Deze onderzoeken kunnen leiden tot een boete, maar dat hoeft niet. De AP weegt per situatie af wat het meest effectief is.

6.2 Toezicht op niet gemelde datalekken

De AP zorgt dat de meldplicht datalekken wordt nageleefd door organisaties. En richt zich daarmee dus ook op datalekken die niet worden gemeld. Hoe de AP handhaaft, verschilt per situatie. Soms is dat formeel, bijvoorbeeld via een onderzoek. In andere gevallen is dat informeel, bijvoorbeeld met een gesprek.

Toezicht op ICT-leveranciers

Cyberaanvallen zijn ontzettend schadelijk voor organisaties en personen. Organisaties kunnen zelf getroffen worden door een cyberaanval, maar het kan ook gebeuren bij een leverancier die zij inhuren. De AP merkt op dat getroffen ICT-leveranciers vaak te maken kregen met een cyberaanval omdat ze hun beveiliging niet op orde hadden.

Organisaties blijven eindverantwoordelijk als een leverancier getroffen wordt door een cyberaanval. Daarom is het belangrijk dat zij goede afspraken met leveranciers maken en ervoor zorgen dat deze leveranciers de beveiliging van persoonsgegevens op orde hebben en houden. Die afspraken moeten zij vastleggen in contracten. Alleen zo kunnen consumenten en burgers erop vertrouwen dat ze veilig gebruik kunnen maken van online diensten, zoals webshops.

Een belangrijk onderdeel van het toezicht op niet gemelde datalekken is het toezicht van de AP bij grootschalige cyberaanvallen bij ICT-leveranciers. Organisaties besteden diensten, waaronder ICT-diensten, vaker uit aan gespecialiseerde bedrijven. Bij een ICT-leverancier kunnen organisaties software op maat en opslagruimte voor hun data afnemen. Dit heeft tot gevolg dat een ICT-leverancier veel data beheert. Deze data zijn goud waard voor criminelen. Via de ICT-leverancier ziet de AP welke organisaties gebruikmaken van de diensten, en dus mogelijk ook betrokken zijn bij het datalek. De AP kan dan controleren of deze organisaties het datalek ook hebben gemeld aan de AP en slachtoffers op de juiste manier hebben geïnformeerd.

Toezicht na tips van burgers

De AP heeft in 2022 bijna 2.000 tips ontvangen over datalekken. Burgers melden dan dat er naar hun mening een datalek heeft plaatsgevonden bij een organisatie. Bij 35 signalen zag de AP voldoende reden om via een informele interventie contact op te nemen met organisaties die zich niet aan de meldplicht hielden. Daarna meldden al deze organisaties het datalek alsnog bij de AP. De AP kan ook een onderzoek starten naar het ten onrechte niet melden van een datalek. Bij het overtreden van de meldplicht kan de AP handhavende maatregelen opleggen, zoals een boete.

Preventief toezicht op niet gemelde datalekken

Bij een cyberaanval op een ICT-leverancier kijkt de AP naar de informatievoorziening van de ICT-leverancier aan zakelijke klanten (de organisaties). De ICT-leverancier is verplicht de organisaties van goede informatie te voorzien.

De informatievoorziening moet ervoor zorgen dat organisaties die samenwerken met de getroffen ICT-leverancier een melding kunnen doen aan de AP. Verder moeten deze organisaties de slachtoffers van de cyberaanval kunnen waarschuwen voor de gevolgen van het datalek. Organisaties die samenwerken met een ICT-leverancier blijven bij een datalek namelijk verantwoordelijk voor een melding aan de AP en aan de slachtoffers. Is de informatievoorziening vanuit de ICT-leverancier niet in orde, dan kan de AP daar actie op ondernemen. Het toezicht voorkomt onduidelijkheid bij organisaties en stimuleert om te voldoen aan de meldplicht.