Rapportage Datalekken 2023

Rapportage april 2024

AUTORITEIT
PERSOONSGEGEVENS

Voorwoord

De digitale samenleving is volop in ontwikkeling. Data spelen een steeds grotere rol in het leven van mensen. Het toenemende gebruik van data biedt mogelijkheden, maar brengt ook risico's met zich mee. Zoals het risico op datalekken.

In 2023 kreeg de Autoriteit Persoonsgegevens (AP) ruim 25.000 meldingen van bedrijven, overheden en andere organisaties over een datalek. Persoonlijke informatie van mensen werd onbedoeld gedeeld met anderen, kwam op straat te liggen of werd gestolen. Dat laatste gebeurt vaak door hackersbendes en andere cybercriminelen, voor wie persoonlijke gegevens van mensen geld waard zijn. Deze cyberaanvallen hebben grote impact op slachtoffers van wie persoonsgegevens zijn gelekt én op de getroffen organisatie.

Cyberaanvallers richten zich vaak op ICT-leveranciers. Die beheren in opdracht van bijvoorbeeld bedrijven of overheidsinstanties steeds meer gegevens. Deze organisaties blijven verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens van hun klanten en burgers.

De AP ziet dat organisaties die getroffen worden door een cyberaanval, het risico voor de slachtoffers vaak te laag inschatten. Dat zorgt ervoor dat zij de slachtoffers niet altijd informeren. Terwijl dat vaak wel noodzakelijk – en verplicht – is. Een zogenoemde slachtoffernotificatie kan mensen namelijk helpen om alerter te zijn op phishingberichten.

De AP houdt hier toezicht op. En treedt actief op. Na een grote cyberaanval op IT-leverancier Nebu intervenieerde de AP vorig jaar bijvoorbeeld bij 34 klantorganisaties van Nebu die de risico's van dit datalek te laag inschatten en mensen er ten onrechte niet over informeerden. Na de interventie van de AP deden zij dit alsnog.

Mensen moeten erop kunnen vertrouwen dat organisaties veilig met hun persoonsgegevens omgaan. Dit vertrouwen is bovendien een fundament voor de uitwisseling van gegevens die nodig is voor de dienstverlening en bedrijfsvoering in Nederland. Datalekken schaden dit vertrouwen. Dit alles maakt dat de bescherming van persoonsgegevens een voortdurende uitdaging vormt voor ons allemaal.

De AP staat voor een maatschappij waarin mensen controle hebben over hun persoonsgegevens en waarin organisaties intrinsiek gemotiveerd zijn om de persoonsgegevens die zij verwerken goed te beschermen. Een maatschappij waarin de digitale weerbaarheid van mensen en organisaties groeit. Met het besef dat dit alleen goed gaat als we dat samen doen.

Aleid Wolfsen
Voorzitter AP

Inhoudsopgave

1. Samenvatting

Veel slachtoffers door cyberaanvallen

In 2023 zijn 25.694 datalekken gemeld bij de AP. Op basis van de meldingen van deze datalekken kan de AP een inschatting maken van het aantal personen dat het afgelopen jaar is getroffen door een cyberaanval: ongeveer 20 miljoen personen. Het gaat zowel om personen in Nederland als in andere landen (binnen en buiten Europa).

Lees verder op pagina 11 →

Cyberaanval bij Nebu

In maart 2023 vond een cyberaanval plaats bij Nebu, een ICT-leverancier van software voor markt- en klanttevredenheidsonderzoek. De AP schat dat dit datalek 2,5 miljoen mensen heeft getroffen. De AP heeft na het datalek streng toezicht gehouden op de naleving van de meldplicht aan slachtoffers, om zo hun digitale weerbaarheid te versterken.

Lees verder op pagina 7 →

Slachtoffers cyberaanvallen vaak niet geïnformeerd door lage risico-inschatting

Datalekken door cyberaanvallen leveren over het algemeen hoge risico's op voor slachtoffers, zoals financiële schade of identiteitsfraude. In 2023 deden ruim 7000 mensen melding van identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude (CMI). Het toezicht van de AP is er mede op gericht om getroffen organisaties de juiste risico-afweging te laten maken.

Lees verder op pagina 5 →

Samenwerking cruciaal

Het maken van een juiste risico-inschatting door getroffen organisaties is een eerste stap naar een digitaal weerbare maatschappij. Inzicht in feiten en cijfers over datalekmeldingen kan daarbij helpen. Daarom stelt de AP informatie uit datalekmeldingen beschikbaar aan het CBS voor wetenschappelijk onderzoek. Verder maakt de AP zich klaar om straks bij de NIS2-richtlijn intensiever samen te werken met andere toezichthouders op cybersecurity. De NIS2-richtlijn stelt strenge eisen aan de cybersecurity van de Nederlandse vitale infrastructuur, zoals de overheid en ziekenhuizen.

Lees verder op pagina 10 →

2. Risico cyberaanvallen te laag ingeschat

In het kort

- Gemiddeld 69% van de organisaties die getroffen worden door een cyberaanval, schat het risico voor de slachtoffers te laag in. Gemiddeld 46% van de organisaties informeert de slachtoffers. Dat blijkt uit een analyse van de AP.
- Mensen die niet weten dat ze slachtoffer zijn van een datalek, kunnen verrast worden door een phishingaanval of het slachtoffer worden van oplichting of identiteitsfraude.
- Organisaties moeten datalekken door cyberaanvallen vrijwel altijd melden aan de AP en aan de slachtoffers.

Slachtoffers cyberaanvallen vaak niet geïnformeerd

De AP heeft een analyse gemaakt van de risico-inschatting van organisaties die een cyberaanval hebben gemeld. Daarbij heeft de AP gekeken naar cyberaanvallen waarbij een dataset met gevoelige persoonsgegevens is getroffen. De resultaten van de analyse staan rechts in de tabel.

Het gaat om datalekken waarbij bijvoorbeeld medische persoonsgegevens, creditcardgegevens of kopieën van paspoorten betrokken zijn. Maar het gaat ook om datalekken waarbij ogenschijnlijk minder gevoelige persoonsgegevens getroffen zijn, zoals e-mailadressen en NAW-gegevens. Toch kunnen criminelen ook deze gegevens gebruiken voor phishingberichten.

Wat is een cyberaanval?

Bij een cyberaanval proberen criminelen in te breken in digitale systemen. Zo kunnen criminelen bijvoorbeeld inbreken in mailboxen en naar de contacten phishing-mails versturen. Een ander voorbeeld is een ransomware-aanval waarbij de criminelen data versleutelen, waardoor de getroffen organisatie niet meer bij de data kan. In ruil voor losgeld beloven criminelen de 'sleutel' te geven zodat de organisatie weer bij de data kan.

RISICO-INSCHATTING DOOR ORGANISATIES BIJ CYBERAANVALLEN

Cyberaanval met:	% risico-inschatting: laag	% risico-inschatting: hoog	% betrokkenen geïnformeerd	Aantal datalek-meldingen in deze categorie
bijzondere persoonsgegevens	66%	34%	38%	198
kopieën van paspoorten	67%	33%	60%	135
creditcardgegevens	70%	30%	59%	37
gegevens van kwetsbare personen	68%	32%	53%	146
groot aantal e-mailadressen of telefoonnummers	81%	19%	60%	96
Gemiddeld:	**69%**	**31%**	**46%**	

Cyberaanvallen vrijwel altijd melden aan AP en slachtoffers

Datalekken door cyberaanvallen leveren over het algemeen hoge risico's op voor de slachtoffers, zoals identiteitsfraude, phishing of oplichting.

- Met een gelekt identiteitsbewijs kunnen criminelen identiteitsfraude plegen. Zij maken dan misbruik van het identiteitsbewijs door bijvoorbeeld een lening af te sluiten op naam van het slachtoffer.
- Met NAW- en contactgegevens hebben criminelen voldoende informatie om een geloofwaardig phishing-bericht op te stellen. Met een e-mail of SMS proberen criminelen – ogenschijnlijk uit naam van de getroffen organisatie – geld of informatie afhandig te maken, zoals inloggegevens.
- Met creditcardgegevens kunnen criminelen aankopen doen.
- Met gebruikersnamen en wachtwoorden kunnen criminelen inbreken in gebruikersaccounts van consumenten.
- De gestolen persoonsgegevens kunnen worden toegevoegd aan bestaande datasets, die bijvoorbeeld te koop zijn op het darkweb. Deze gegevens worden uiteindelijk gebruikt bij grootschalige hacks met als doel toegang te krijgen tot gebruikersaccounts.

Daarom moet dit soort datalekken vrijwel altijd gemeld worden aan de AP en aan de slachtoffers.

Lage risico-inschatting is zorgelijk

De AP concludeert dat mensen te vaak ten onrechte niet worden geïnformeerd bij een datalek door een cyberaanval. Cyberaanvallen waarbij gevoelige persoonsgegevens of gegevens van kwetsbare personen zijn getroffen, leveren in veel gevallen een hoog risico op voor de slachtoffers. Organisaties die in 2023 melding deden van een dergelijke cyberaanval, schatten het risico voor de slachtoffers echter slechts in 30 tot 34% van de gevallen als hoog in. Dit lage percentage baart de AP zorgen. Een te lage risico-inschatting kan tot gevolg hebben dat organisaties besluiten om de slachtoffers niet of niet volledig te informeren, en/of onvoldoende maatregelen te nemen om nieuwe datalekken te voorkomen. De AP ziet er op toe dat organisaties de risico's voor slachtoffers juist inschatten en de vereiste vervolgstappen nemen om met deze risico's om te gaan.

VOORBEELDEN WAAROM ORGANISATIES SLACHTOFFERS NIET INFORMEREN

Welke verkeerde afweging maakten veel organisaties in het Nebu-datalek?	Wat is de juiste afweging na een cyberaanval?
"We gaan de slachtoffers van het datalek niet informeren omdat het onduidelijk is welke data er gestolen zijn." "Wij willen geen onnodige onrust bij slachtoffers veroorzaken."	Kunt u met onderzoek niet uitsluiten dat de persoonsgegevens waartoe de hacker toegang had (ook) gekopieerd zijn door de hacker? Dan moet u uitgaan van het ernstigste scenario.
"Er zijn alleen contactgegevens getroffen door de ransomware-aanval, het risico is laag. Dus wij gaan de slachtoffers niet informeren."	Zijn grote aantallen contactgegevens van klanten buitgemaakt door een hacker, zoals e-mailadressen of telefoonnummers, met aanvullende persoonsgegevens, zoals NAW-gegevens? Of is dit niet uit te sluiten? Dan moet u de slachtoffers informeren.

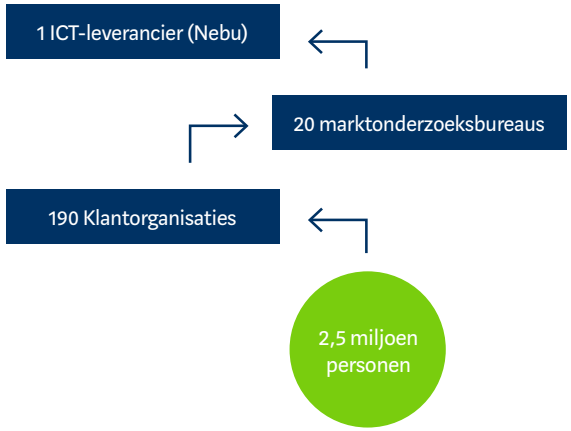
3. Cyberaanval Nebu

In het kort

- In maart 2023 werden de servers van het Canadese Nebu, een ICT-leverancier, getroffen door een cyberaanval. Dit trof ook organisaties die klant waren van Nebu.
- Ongeveer 2,5 miljoen Nederlanders waren slachtoffer van de cyberaanval.
- Organisaties waren verplicht om slachtoffers te informeren, omdat hun e-mailadres, telefoonnummer en NAW-gegevens waren getroffen. Niet alle organisaties deden dat, omdat ze het risico voor de slachtoffers te laag inschatten.
- De AP heeft richting 34 klantorganisaties interventies gepleegd, omdat die niet voldeden aan hun wettelijke meldplicht aan de AP en/of de slachtoffers.
- 50.000 slachtoffers zijn na interventie van de AP alsnog geïnformeerd over de cyberaanval.

Getroffen Nederlandse organisaties

Nebu levert in Nederland software voor markt- en klanttevredenheidsonderzoek aan 20 marktonderzoeksbureaus. Diverse Nederlandse klantorganisaties, waaronder VodafoneZiggo, maken gebruik van de diensten van deze marktonderzoeksbureaus. Deze Nederlandse klantorganisaties hadden de verplichting om het datalek te melden aan de AP en aan de slachtoffers. Zij verwerkten persoonsgegevens van mensen die meewerkten aan een markt- of klanttevredenheidsonderzoek. In de meeste gevallen waren dit e-mailadressen, telefoonnummers, namen en woonadressen.



Functionaris gegevensbescherming (FG) van VodafoneZiggo: “Oefen hoe je omgaat met een datalek”

”Omdat de hack in de systemen van Nebu plaatsvond, was niet meteen duidelijk of er klantdata waren geraakt en zo ja, welke. Voor dit soort incidenten stellen we direct een team samen. Het team loopt een vooraf opgesteld proces door. We hebben op tijd een datalekmelding bij de AP ingediend, omdat het ging om een hack. We vonden het ook belangrijk om onze klanten snel te informeren. Ondanks dat nog niet alle details van de hack bekend waren. Er zijn klanten geweest die nog contact met ons opnamen hierover. Onze klantenservice heeft een belangrijke rol gespeeld bij het wegnemen van de zorgen van onze klanten. Het helpt om een ‘datalek-oefening’ te doen. Voor een klein bedrijf is dat handig, omdat je misschien nog nooit met een groot lek te maken hebt gehad. Voor een groot bedrijf is het ook handig, zodat je kunt oefenen hoe de verschillende afdelingen samenwerken.”

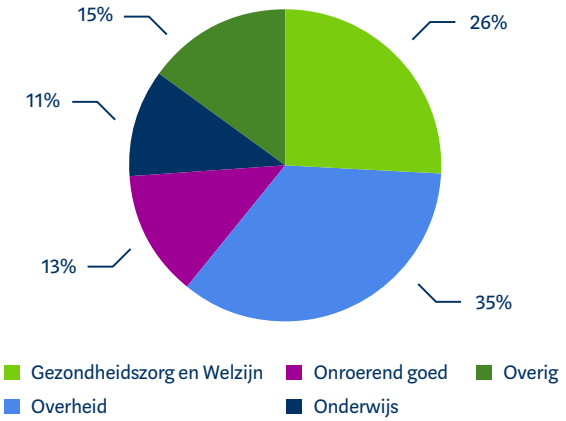
Toezicht door de AP

Direct na het datalek heeft de AP een persbericht gepubliceerd en getroffen organisaties opgeroepen om aan hun meldplicht te voldoen, om te zorgen dat klantorganisaties het datalek onverwijld zouden melden aan de AP en aan de slachtoffers. Een grote meerderheid (82%) voldeed aan de meldplicht. De overige 34 klantorganisaties voldeden pas aan hun meldplicht na interventies van de AP.

Door deze interventies van de AP zijn ongeveer 50.000 personen alsnog geïnformeerd dat zij het slachtoffer zijn van de cyberaanval. Hierdoor zijn zij extra alert op mogelijke phishingberichten. Alle 190 klantorganisaties hebben uiteindelijk aan hun meldplicht voldaan. Op dit moment doet de AP ook onderzoek naar ICT-leverancier Nebu.

Klantorganisaties blijven altijd verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens, ook als de verwerking wordt uitbesteedt aan een andere organisatie, zoals een ICT-leverancier.

SECTOREN WAAR INTERVENTIES VAN DE AP PLAATSVONDEN OM ORGANISATIES TE WIJZEN OP DE MELDPLICHT



Amsta informeerde cliënten met een sms

Stichting Amsta is een van de organisaties die geraakt is door de cyberaanval bij Nebu. Amsta is een zorginstelling voor Amsterdammers die complexe, zware zorg nodig hebben. Er waren bij het datalek namen en telefoonnummers van enkele cliënten en voornamelijk van contactpersonen van cliënten betrokken. Amsta heeft dit datalek gemeld bij de AP en de betrokkenen geïnformeerd via een nieuwsbericht op hun website. De AP heeft Amsta vervolgens verzocht de betrokkenen persoonlijk te informeren via een persoonlijke brief. Amsta vond deze aanpak buitenproportioneel. Amsta en de AP hebben gezamenlijk nagedacht over een haalbare aanpak, die voor Amsta uitvoerbaar was en voor de AP acceptabel. Amsta heeft toen voorgesteld om de betrokkenen met een bulk SMS te wijzen op het nieuwsbericht op de website en zo nodig de betrokkenen daarna ook te woord te staan. Zo kon Amsta met een relatief kleine inspanning en met de contactgegevens waar zij over beschikten alle betrokkenen persoonlijk informeren.

FG van La Providence: “Ouderen zijn extra kwetsbaar bij een datalek”

La Providence is een kleinschalige verpleeg- en zorginstelling in Limburg. ”Bij het datalek waren namen en telefoonnummers van onze bewoners betrokken. Een telefoonnummer lijkt niet gevoelig. Maar na contact met de AP beseften wij dat informeren van de bewoners toch goed is, omdat zij extra kwetsbaar zijn voor telefonische oplichting door criminelen. Wij maakten ons zorgen dat we onrust zouden veroorzaken als wij de bewoners zouden informeren. We hebben daarom de bewoordingen van de melding op de doelgroep aangepast. We hebben bijvoorbeeld uitgelegd wat een hack is. En we hebben in de melding uitgelegd hoe onze bewoners oplichting via de telefoon of WhatsApp kunnen voorkomen. Een volgende keer zouden we onze bewoners graag nog sneller informeren. Dat gaan we doen met een vooraf opgesteld proces en een sjabloonmelding aan slachtoffers.”

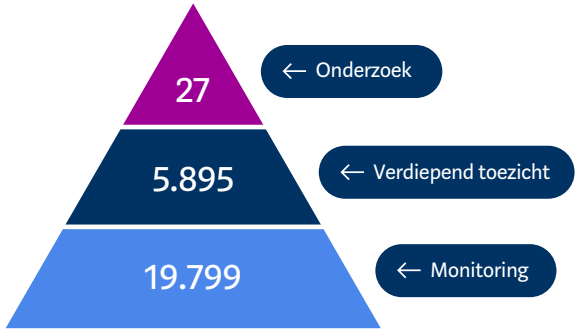
4. Risicogestuurd toezicht AP

In het kort

- Met toezicht versterkt de AP de digitale weerbaarheid van mensen, bedrijven en overheden.
- De AP heeft in 2023 bij bijna 6.000 datalekmeldingen actie ondernomen.

Digitale weerbaarheid versterken
Het toezicht op de meldplicht datalekken is risicogestuurd en heeft tot doel de digitale weerbaarheid van mensen, bedrijven en organisaties te versterken. De AP richt zich op datalekken die de grootste risico's opleveren voor de getroffen personen en de bescherming van hun persoonsgegevens. Voorbeelden hiervan zijn datalekken als gevolg van cyberaanvallen, datalekken die veel mensen treffen en datalekken met bijzondere of gevoelige persoonsgegevens.

RISICOGESTUURD TOEZICHT

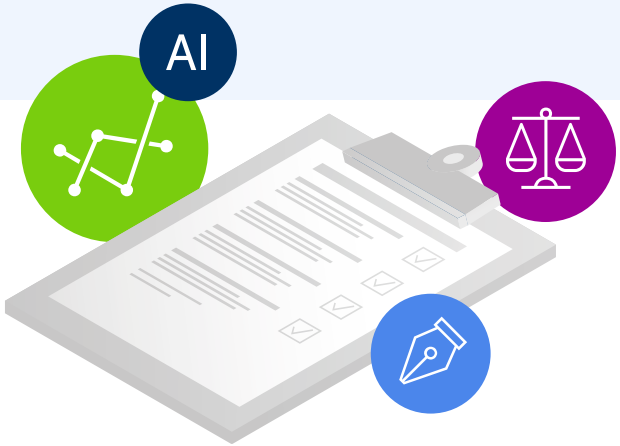


Monitoring
In 2023 zijn er 25.694 datalekken gemeld aan de AP. Bij een groot deel van de datalekmeldingen onderneemt de AP na een eerste beoordeling geen verdere actie. Van zulke datalekken ontving de AP er bijna 20.000 in 2023. Het gaat hier bijvoorbeeld om datalekken door verkeerd verzonden post of e-mails.

Verdiepend toezicht
Het afgelopen jaar heeft de AP bij 5.895 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.

Onderzoeken
In 2023 is de AP naar aanleiding van 27 datalekken een onderzoek gestart. Deze 27 datalekken brachten volgens de AP de grootste risico's voor de slachtoffers met zich mee. 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. Bij het onderzoek naar de cyberaanval bij Nebu moest de AP zich bijvoorbeeld richten op meerdere (klant)organisaties.



5. Beleid en regelgeving

In het kort

- De AP werkt onder de NIS2 richtlijn intensiever samen met andere toezichthouders.
- De AP stelt via het CBS informatie ter beschikking uit datalekmeldingen.

Samenwerking NIS2-richtlijn
Om de digitale weerbaarheid te versterken, werkt de AP samen met andere toezichthouders. Onder de NIS2-richtlijn zal deze samenwerking verder worden geïntensiveerd. Zo zullen NIS2-toezichthouders de AP op de hoogte stellen van (potentiële) datalekken die organisaties verplicht zijn te melden aan de AP. Denk aan cyberincidenten die de bedrijfscontinuïteit in gevaar brengen, en die een organisatie had kunnen voorkomen met passende technische, operationele en organisatorische maatregelen.

De AP zal met NIS2-toezichthouders samenwerken om de digitale weerbaarheid in de vitale sectoren te versterken. Daarbij heeft de EU bepaald dat de boetebevoegdheid van de AP voorrang heeft op de boetebevoegdheid van de andere toezichthouders als het gaat om een datalek waarbij persoonsgegevens zijn betrokken.

Informatie uit datalekken beschikbaar via het CBS
De AP is in 2023 samen met het Centraal Bureau voor de Statistiek (CBS) een project gestart om informatie uit datalekken die bij de AP gemeld zijn beschikbaar te stellen voor wetenschappelijk en statistisch onderzoek in de beveiligde microdata-omgeving van het CBS. Onderzoeksinstellingen kunnen deze informatie gebruiken voor wetenschappelijk onderzoek. De uitkomsten kunnen bijdragen aan de weerbaarheid van organisaties tegen cyberincidenten. Het is de eerste keer dat de AP informatie over datalekmeldingen op deze manier beschikbaar stelt. De informatie is niet herleidbaar tot individuele organisaties die een datalekmelding hebben gedaan.

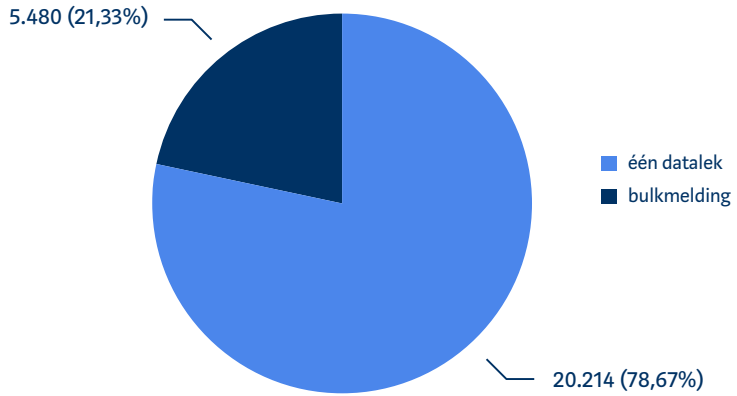
Met dit project geeft de AP invulling aan het advies van de Cyber Security Raad (CSR): 'Beschikbaar stellen datalekmeldingen voor onderzoeksdoeleinden'.

Omstreeks juni 2024 komt het eerste onderzoeksbestand met meldingsdata in de CBS-catalogus te staan. Gemachtigde onderzoeksinstellingen kunnen vanaf dat moment een projectaanvraag indienen bij het CBS.

6. Feiten en cijfers

25.694 datalekken gemeld in 2023

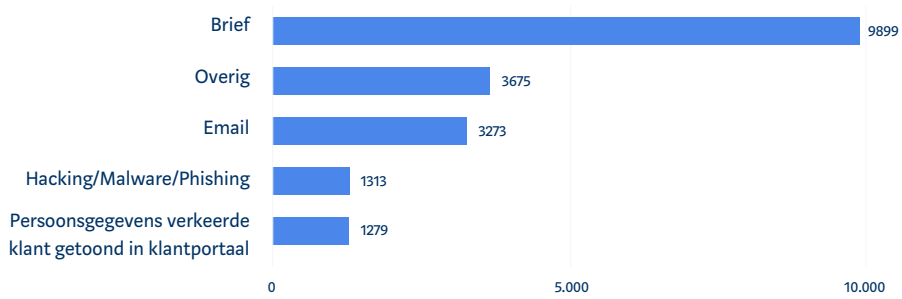
AANTAL GEMELDE DATALEKKEN IN 2023



In 2023 zijn er 25.694 datalekken gemeld aan de AP. Daarvan zijn 5.480 datalekken via een zogenoemde bulkmelding gemeld. In een bulkmelding meldt een organisatie meerdere datalekken die worden veroorzaakt door verkeerde postverzending. Het in bulk melden van gelijksoortige datalekken kan de administratieve last voor organisaties verlichten.

Verkeerd verzonden brieven het meest gemeld

MEEST GEMELDE CATEGORIEËN VAN DATALEKKEN - TOP 5



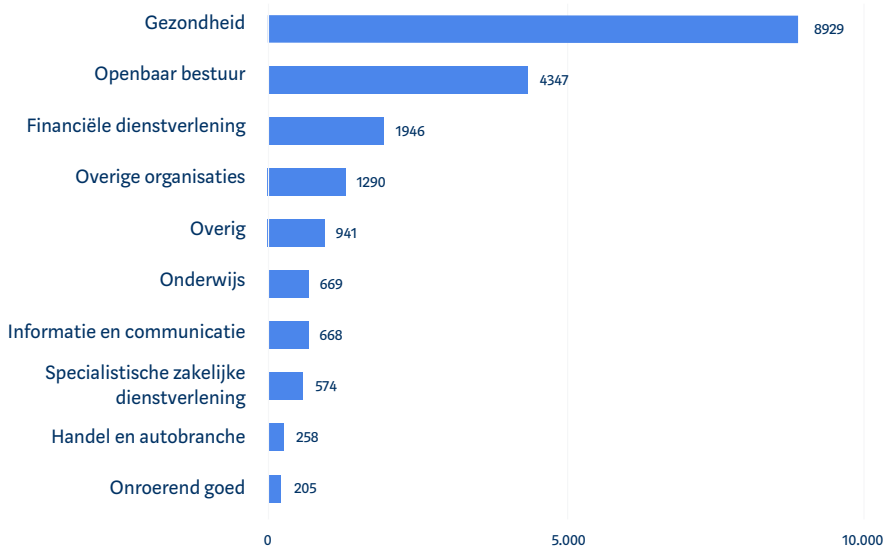
Net als voorgaande jaren ontving de AP in 2023 de meeste meldingen over een verkeerd verzonden brief met daarin persoonsgegevens (9.899 meldingen). Alleen als sprake is van een ernstig privacy inbreuk moet dit type datalek gemeld worden aan de AP.

Meldingen in de categorie 'overig' bestonden uit de volgende typen datalekken:

- overig (79,6%), bijvoorbeeld: inzage door geautoriseerd persoon maar zonder geldige reden, of: meer persoonsgegevens doorgestuurd dan nodig;
- persoonsgegevens per ongeluk gepubliceerd (11,6%);
- netwerkmap of locatie verkeerd ingesteld (7,2%);
- persoongegevens tijdelijk niet beschikbaar door storing (0,9%);
- documenten met persoonsgegevens bij oud papier gezet (0,6%).

Sector gezondheid meldde in 2023 de meeste datalekken

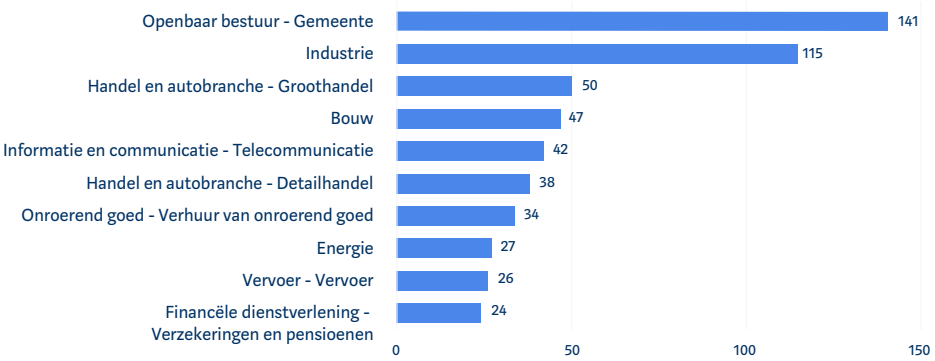
AANTAL MELDINGEN PER HOOFDSECTOR - TOP 10



In 2023 ontving de AP de meeste datalekmeldingen van organisaties in de sectoren gezondheid (8.929), openbaar bestuur (4.347) en financiële dienstverlening (1.946). De meldingen uit de sector gezondheid betroffen in 5.779 gevallen een verkeerd verzonden brief (65% van het totaal aantal meldingen in de sector). Bij de sector openbaar bestuur was dit aantal 2.218 (51% van het totaal aantal meldingen in de sector), in de sector financiële dienstverlening 881 (45% van het totaal aantal meldingen in de sector).

Gemeenten meldde meeste cyberaanvallen

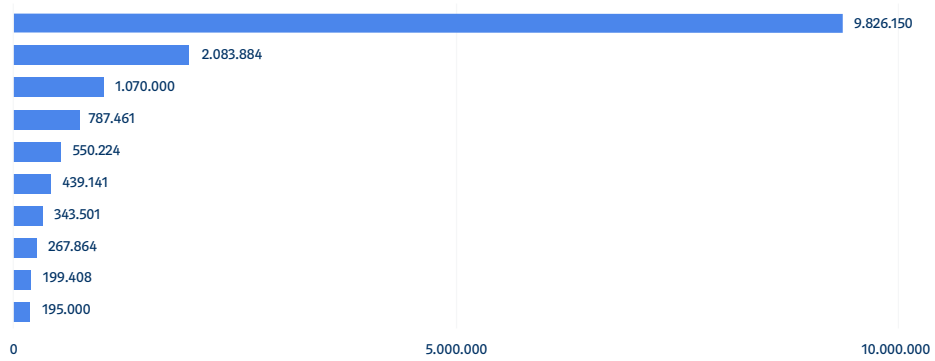
AANTAL MELDINGEN VAN CYBERAANVALLEN PER SUBSECTOR - TOP 10



De subsectoren die de meeste cyberaanvallen hebben gemeld in 2023 zijn gemeenten (141 meldingen), gevolgd door organisaties uit de industriesector (115 meldingen) en organisaties uit de sector handel en autobranche – groothandel (50 meldingen).

Door grootste cyberaanval bijna 10 miljoen slachtoffers

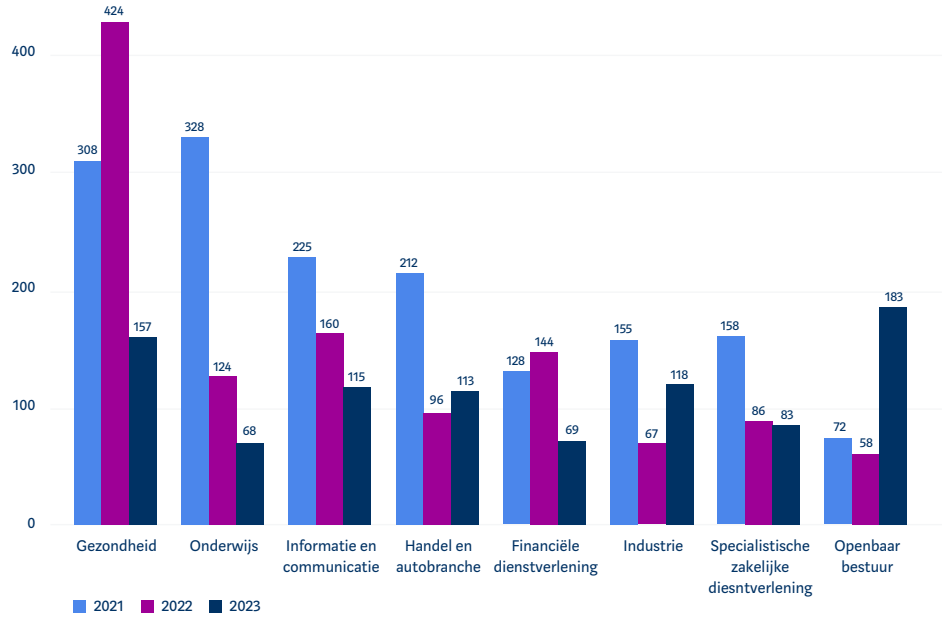
GROOTSTE CYBERAANVALLEN (IN AANTAL SLACHTOFFERS) - TOP 10



In 2023 heeft AP 1.309 datalekmeldingen ontvangen over cyberaanvallen, waarbij in totaal ongeveer 20 miljoen slachtoffers zijn getroffen. Bij de 10 grootste cyberaanvallen zijn in totaal bijna 16 miljoen slachtoffers getroffen (82% van het totale aantal slachtoffers).

Sector Openbaar bestuur meldde in 2023 de meeste cyberaanvallen

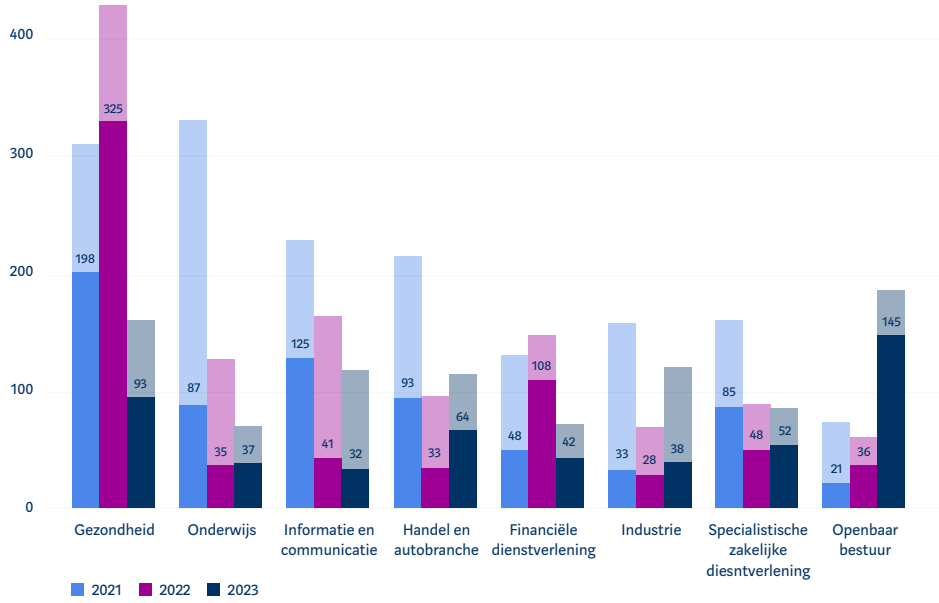
AANTAL MELDINGEN VAN CYBERAANVALLEN PER SECTOR IN 2021, 2022 EN 2023 - TOP 8



Het aantal meldingen naar aanleiding van cyberaanvallen (hacking, phishing of malware-incidenten) daalde in 2023 naar 1.309 meldingen, ten opzichte van 1.825 in 2022. In 2023 werden meldingen over cyberaanvallen het meest gedaan door organisaties uit de sectoren openbaar bestuur (183 meldingen), gezondheid (175 meldingen) en industrie (118 meldingen). Dit is een verschuiving ten opzichte van 2021 en 2022, toen de meeste meldingen over cyberaanvallen afkomstig waren uit de sectoren onderwijs (2021) en gezondheid (2022).

Sector Openbaar bestuur meldde in 2023 de meeste cyberaanvallen waar meerdere organisaties bij betrokken waren

AANTAL MELDINGEN VAN CYBERAANVALLEN PER SECTOR IN 2021, 2022 EN 2023 - TOP 8 - UITSPLITSING NAAR BETROKKENHEID MEERDERE ORGANISATIES



In bovenstaande tabel is het aantal meldingen over cyberaanvallen vermeld waarbij meerdere organisaties betrokken waren. Vooral in de sectoren openbaar bestuur en gezondheid waren vaak meerdere organisaties betrokken bij een cyberaanval. In veel gevallen ging het om cyberaanvallen die plaatsvonden bij ingehuurde bedrijven (verwerkers) zoals ICT-leveranciers, waardoor meerdere organisaties worden getroffen door hetzelfde datalek. In de sector openbaar bestuur waren bij 145 van de 183 meldingen over cyberaanvallen ingehuurde bedrijven betrokken, oftewel 79%. In de sector gezondheid ging het om 93 van de 157 meldingen over cyberaanvallen, oftewel 59%.

AUTORITEIT
PERSOONSGEGEVENS