Datalekkenrapportage 2024

Datadiefstal bijna verdubbeld

AP | bescherming in een digitale wereld

Juli 2025

Inhoudsopgave

Voorwoord

De Autoriteit Persoonsgegevens (AP) staat voor bescherming in een digitale wereld. Deze digitale wereld wordt steeds groter en is volop in ontwikkeling. De AP moedigt deze groei en ontwikkelingen aan, maar maakt zich ook zorgen. Want bij deze groei en ontwikkelingen horen ook gevaren. Gevaar ligt op de loer bij het creëren van een veerkrachtig digitaal landschap en het digitaal weerbaarder maken van organisaties en burgers.

In deze zevende editie van de datalekkenrapportage laat de AP je graag meer zien van de ontwikkelingen, zorgen en gevaren op het gebied van datalekken en cyberaanvallen.

Cyberaanvallen schaden het vertrouwen

Nederland heeft een grote digitale infrastructuur. Tegelijkertijd maakt dat ons land kwetsbaar. Nederland is een doelwit van cyberaanvallen, ziet de AP in de Datalekkenrapportage 2024. Deze conclusie ligt in lijn met het cybersecuritybeeld Nederland van 2024 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV stelt in dit stuk dat geopolitieke gebeurtenissen hun weerslag hebben op de digitale dreiging voor Nederland.

Burgers geven veel persoonsgegevens aan organisaties. Daarbij mogen zij erop vertrouwen dat organisaties zorgvuldig omgaan met deze persoonsgegevens en ze goed beveiligen. Een cyberaanval die een datalek veroorzaakt schaadt het vertrouwen in organisaties, de economie en de samenleving. Een belangrijke waarde bij het verwerken van persoonsgegevens is het waarborgen van de veiligheid van persoonsgegevens. De AP zet zich dagelijks in voor het weerbaarder maken van ons digitale landschap, van slachtoffers en van organisaties.

Grote impact op slachtoffers

Datalekken door cyberaanvallen hebben grote impact op de levens van slachtoffers. Hun wereld kan op zijn kop staan na een cyberaanval. Wanneer we het hebben over slachtoffers, praten we vaak over aantallen en soorten persoonsgegevens. Toch mogen we niet vergeten dat we het ook hebben over mensen. Mensen zoals jij en ik. Iedereen kan namelijk slachtoffer worden van een cyberaanval. De AP vindt het belangrijk om deze slachtoffers een gezicht te geven. Daarom bevat deze rapportage het verhaal van een slachtoffer van een datalek.

De AP verwacht meer van organisaties

Na een datalek door een cyberaanval komt er veel op een organisatie af. Het datalek moet worden verholpen. Misschien moet het lek gemeld worden aan de AP en aan slachtoffers. Ook moet de organisatie maatregelen nemen om een volgend datalek te voorkomen. Op dit gebied verwacht de AP écht meer van organisaties.

Net als het Nationaal Cyber Security Centrum (NCSC) ziet de AP dat cybercriminelen het vaakst toegang tot systemen krijgen door het overnemen van accounts, of het misbruiken van kwetsbaarheden in software. En dat terwijl organisaties relatief goedkope en eenvoudige maatregelen kunnen nemen om datalekken te voorkomen. We roepen organisaties die persoonsgegevens verwerken actief op om maatregelen te nemen, zodat cyberaanvallen voorkomen kunnen worden. De tijd van achteroverleunen is echt voorbij.

De AP treedt ook naar buiten als partner die meedenkt met organisaties en slachtoffers, en hen ondersteunt bij een datalek. Deze samenwerking is essentieel om een digitaal landschap te creëren dat tegen een stootje kan. Een veerkrachtig digitaal landschap bouwen we niet alleen met regels en technologie, maar vooral met samenwerking en verantwoordelijkheid.

ALEID WOLFSEN

VOORZITTER AP

Samenvatting

1. Toezicht op datalekken in 2024

De AP richt zich op de datalekken met de grootste risico's voor slachtoffers. Bij deze datalekken is het belangrijk dat slachtoffers weten wat er gebeurd is. Zo weten zij waar ze extra alert op moeten zijn en wat zij zelf kunnen doen om zo min mogelijk last te hebben van het datalek. Hiermee versterkt de digitale weerbaarheid van Nederland. In 2024 werden er 37.839 datalekken bij de AP gemeld. De AP deed nader onderzoek naar 28 datalekmeldingen met het hoogste risicoprofiel. Inspecteurs van de AP hielden verdiepend toezicht op 11.024 datalekmeldingen. In 2024 werden 26.815 datalekmeldingen gemonitord.

Lees meer de acties van inspecteurs bij datalekken in 2024 op pagina 5

2. Datadiefstal in 2024 bijna verdubbeld

De AP deed ook onderzoek naar cyberaanvallen die in 2024 zijn gemeld. Hieruit bleek dat het aantal ransomware-aanvallen waarbij data werden gestolen, bijna is verdubbeld ten opzichte van 2023. Ook zag de AP tijdens dit onderzoek organisaties die tonnen aan schade hadden na een cyberaanval. De AP roept organisaties op om actie te ondernemen op het gebied van beleid tegen cyberaanvallen.

Lees meer over dit onderzoek en de oproep van de AP op pagina 9

3. Door één cyberaanval de digitale veiligheid van 1,5 miljoen mensen in gevaar

In mei 2024 werd klantcommunicatiebedrijf AddComm getroffen door een ransomware-aanval. De aanval raakte ook ruim 5.000 klanten van AddComm uit de hele leverancierskeketen. Ruim 1,5 miljoen mensen werden slachtoffer van dit datalek. Door de grote aantallen (gevoelige) persoonsgegevens zag de AP grote risico's voor slachtoffers. De AP startte een onderzoek en sprak met de CEO van AddComm. Zij zei onder meer: "De hack is het beste wat ons is overkomen."

Lees meer over deze quote en de ingrijpende cyberaanval op pagina 15

4. Feiten & cijfers

De AP constateert dat het aantal cyberaanvallen in 2024 is toegenomen. In 2024 zijn er 1.430 datalekken na een cyberincident gemeld. In 2023 waren dit er nog 1.309. De sectoren Onderwijs en Gezondheid & welzijn meldden in 2024 de meeste cyberaanvallen. De sector Onderwijs deed veel datalekmeldingen na een cyberaanval bij een schoolboekenleverancier die veel onderwijsinstellingen raakte. De meeste datalekken werden gemeld door de sectoren Gezondheid & welzijn, Openbaar bestuur en Financiële dienstverlening.

Lees meer over feiten, cijfers en duiding hiervan op pagina 18

1. Toezicht op datalekken in 2024

In het kort

- De AP richt zich op datalekken met de grootste risico's voor slachtoffers.
- Bij deze datalekken is het belangrijk dat slachtoffers weten wat er gebeurd is, waar zij alert op moeten zijn en wat zij zelf kunnen doen om zo min mogelijk last te hebben van het datalek.
- Ook organisaties waar het datalek heeft plaatsgevonden, moeten in actie komen. Handelt een organisatie na een datalek niet goed? Dan grijpt de AP in.
- In 2024 deed de AP onderzoek naar **28** zeer ernstige datalekken. Bijvoorbeeld omdat de basisbeveiliging bij een organisatie niet op orde was en dit leidde tot een (groot) datalek.

Toezicht met het oog op digitale weerbaarheid

De AP focust zich op de datalekken met de grootste risico's voor slachtoffers. Bij een datalek gaat het om toegang tot persoonsgegevens zonder dat dit mag, of zonder dat dit de bedoeling is. Slachtoffers moeten worden geïnformeerd over een datalek als hierdoor hun rechten en vrijheden in gevaar komen. Bijvoorbeeld als slachtoffers van wie een kopie van een paspoort is gelekt, hier niet over worden gewaarschuwd. Het is belangrijk dat slachtoffers in dit geval worden gewezen op mogelijke identiteitsfraude en op wat zij daar zelf tegen kunnen doen. Door te vertellen over een datalek en slachtoffers te helpen bij het nemen van maatregelen, wordt de digitale weerbaarheid van burgers versterkt.

Waar nodig, grijpt de AP in. Bijvoorbeeld omdat een organisatie de meldplicht aan slachtoffers niet naleeft. Hierover voert de AP dan eerst een gesprek met de organisatie. Dit levert vrijwel altijd het gewenste resultaat op. Is dit niet het geval, dan kan de AP het toezicht op dit datalek intensiveren.

Ook de organisaties waar het datalek heeft plaatsgevonden zijn aan zet. Zij moeten maatregelen nemen om de kans te verkleinen dat het datalek kan uitgroeien tot een hoog risico voor slachtoffers. Als dat niet direct goed gaat, kan de AP ingrijpen. De AP kan bijvoorbeeld toetsen of de juiste maatregelen worden genomen om nieuwe datalekken te voorkomen. Zo helpt de AP ook organisaties bij het versterken van hun digitale weerbaarheid.

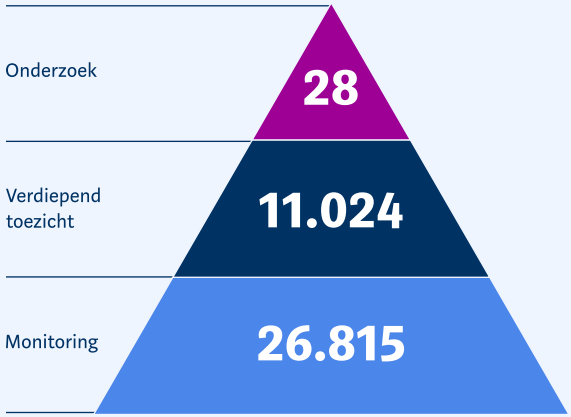
Datalekken in 2024

In 2024 zijn er **37.839** datalekken gemeld aan de AP. Het toezicht van de AP op datalekken is risicogestuurd. Dat betekent dat de AP zich voornamelijk richt op de datalekken die de grootste risico's met zich meebrengen voor slachtoffers. De AP rangschikt ontvangen meldingen naar ernst. Dit helpt inspecteurs van de AP om prioriteit te kunnen geven aan ernstige datalekken die met spoed moeten worden opgepakt.

Toezichtspiramide

Gemelde datalekmeldingen verdeelt de AP in drie categorieën van toezicht. Van de 37.839 datalekken werden er in 2024 **26.815** datalekken gemonitord. Op **11.024** hielden inspecteurs van de AP verdiepend toezicht. Naar **28** zeer ernstige datalekmeldingen is in 2024 onderzoek gedaan.

FIGUUR 1 TOEZICHTSPIRAMIDE



Monitoring

Inspecteurs gebruiken de datalekken uit de categorie 'monitoring' om schadelijke trends te ontdekken. Inspecteurs bundelen deze schadelijke trends om te kijken of er bepaalde patronen, soorten datalekken of thema's verder onderzocht moeten worden. Datalekken uit de categorie 'monitoring' worden daarom niet vaak per geval (uitgebreid) onderzocht, maar maken bijvoorbeeld deel uit van een onderzoek naar een patroon of thema.

Bij de meeste datalekken uit deze categorie ondernemen inspecteurs na de melding niet direct actie. Bijvoorbeeld omdat er voor betrokkenen geen grote risico's bestaan, of omdat de AP geen prioriteit kan geven aan de melding. Naar datalekken in deze categorie wordt door inspecteurs geen uitgebreid onderzoek gedaan.

Inspecteur aan het woord over monitoring

"In 2024 ontdekten we een terugkerend patroon in datalekken bij een financiële organisatie. Gevoelige, financiële persoonsgegevens werden niet altijd gekoppeld aan de juiste persoon. Zo werden er onterecht schulden geregistreerd bij personen die helemaal geen schulden hadden. Ook konden burgers gegevens van anderen onbedoeld inzien. Dit gebeurde vaak bij burgers die elkaar kennen. Hoe vervelend is het wel niet als een bekende jouw schulden kan inzien?

Dit type datalekken kan zorgen voor reputatieschade. We zijn daarom direct overgegaan tot actie.
We hebben met de organisatie gesproken om het probleem in kaart te brengen. Ook hebben we kritische vragen gesteld en met de organisatie meegedacht over het voorkomen van dit type datalekken. De organisatie heeft toegezegd maatregelen uit te werken en door te voeren, waardoor deze datalekken nu minder vaak voorkomen. Door trends te zien in gemelde datalekken en deze te doorgronden, kan de AP gericht bijsturen om datalekken te voorkomen."

Verdiepend toezicht

Datalekken die ernstiger zijn, worden ingedeeld in de categorie 'verdiepend toezicht'. Bij deze datalekken ziet de AP grote risico's voor slachtoffers. Bijvoorbeeld omdat het gaat om veel slachtoffers, of (veel) gevoelige persoonsgegevens. Zoals financiële gegevens over iemands inkomen of een burgerservicenummer (BSN).

Inspecteurs houden bij datalekken in de categorie 'verdiepend toezicht' een vinger aan de pols en stellen organisaties vragen over het datalek. Ook zorgen inspecteurs dat met voorlichting partijen die de regels nog niet snapten, deze alsnog begrepen en zich aan deze regels houden.

Alert bij cyberaanvallen in sector Specialistische zakelijke dienstverlening

De AP zag in 2024 dat 42% van de gemelde cyberaanvallen bestond uit een account-takeover. **Lees hierover meer op pagina 13.**

Ook constateerde de AP een groei van het aantal cyberaanvallen in de sector Specialistische zakelijke dienstverlening. Dit is de sector waar onder meer advocatenkantoren onder vallen. Voor inspecteurs reden genoeg om bij meldingen van cyberaanvallen in deze sector extra alert te zijn en hier verdiepend toezicht op te houden.

Verdiepend toezicht bij inbraak in de mailbox van een advocatenkantoor

In 2024 ontving de AP een datalekmelding van een advocatenkantoor. Een aanvaller had toegang gehad tot de mailbox van een advocaat. De aanvaller had grote aantallen phishingmails verstuurd naar willekeurige e-mailadressen. Uit de datalekmelding bleek dat de mailbox niet was onderzocht, waardoor niet duidelijk was welke persoonsgegevens ingezien waren. Bovendien kon niet uitgesloten worden dat persoonsgegevens uit de mailbox waren gestolen. Niemand van wie mogelijk gegevens in de mailbox voorkwamen, werd over het datalek geïnformeerd. Ook de ontvangers van de phishingmails niet, omdat het advocatenkantoor niet direct een hoog risico zag. Het kantoor dacht dat veel mailservers de phishingmails als "onbetrouwbaar" zouden bestempelen, waardoor ontvangers niet op de link zouden klikken. Ook was het volgens het kantoor onhaalbaar om alle ontvangers te informeren over het datalek.

Voor de inspecteur die de zaak behandelde, was het onbekend welke persoonsgegevens mogelijk in de mailbox stonden. Daarom kon zij de mogelijke risico's voor slachtoffers niet inschatten. Daarop besloot ze het advocatenkantoor te bellen, vragen te stellen en aan te dringen op een onderzoek naar de inbraak in de mailbox.

Inspecteur aan het woord over verdiepend toezicht bij het advocatenkantoor

"Telefonisch hebben we het advocatenkantoor verschillende vragen gesteld over het datalek. Daarna stuurden we het kantoor een brief waarin we vertelden dat het belangrijk was om onderzoek te doen naar de mailbox. Het was namelijk onbekend of er gevoelige persoonsgegevens van cliënten van de advocaten in de mailbox stonden. Ook gaven we informatie over het informeren van betrokken personen en het nemen van beveiligingsmaatregelen. Hierna is de mailbox alsnog onderzocht. Uit dit onderzoek bleek dat er van 32 personen een kopie van hun paspoort in de mailbox stond. Voor deze personen bestond een groot risico op identiteitsfraude, zonder dat zij hierover geïnformeerd waren. Na het onderzoek zijn deze personen alsnog geïnformeerd en gewezen op de risico's. Ook is er een nieuwe werkwijze voor paspoorten geïmplementeerd en heeft het kantoor meerfactorauthenticatie (MFA) ingesteld om inbraak in de mailbox in de toekomst te kunnen voorkomen. Bij een inbraak in de mailbox is vaak onbekend wat er gebeurd is, welke (gevoelige) persoonsgegevens ingezien en/of gestolen zijn, welke risico's voor betrokken personen er zijn en of het gemeld moet worden aan de AP en slachtoffers. Door goed onderzoek krijgt men antwoord op deze vragen en kunnen de juiste beveiligingsmaatregelen genomen worden."

Onderzoek

In 2024 waren er ook datalekken waarbij het noodzakelijk was om deze nader te onderzoeken. Vanwege de capaciteit van de AP onderzoeken inspecteurs datalekken die de grootste risico's voor slachtoffers met zich meebrengen. Bijvoorbeeld het risico op oplichting op grote schaal, door het grote aantal slachtoffers en het lekken van veel financiële- en NAW-gegevens, of de (grote) schade die slachtoffers lijden na een datalek.

Tijdens een onderzoek bekijken inspecteurs wat er gebeurd is en hoe de organisatie het lek probeert te dichten. De AP stuurt meestal bij of toetst de te nemen beveiligingsmaatregelen. Soms legt de AP bij overtreding van de wet een boete op. Bijvoorbeeld omdat basismaatregelen niet op orde waren.

Onderzoek na een impactvolle cyberaanval

Het is mogelijk dat door één cyberaanval een datalek wordt veroorzaakt waarbij een (grote) groep organisaties getroffen wordt. De AP signaleert over 2024 een groei in dit soort datalekken. Ook klantcommunicatiebedrijf AddComm werd getroffen door dit type cyberaanval. Hierdoor werden ook klanten van AddComm geraakt door het datalek. Vanwege de groei in het aantal cyberaanvallen en de grote risico's voor slachtoffers - door het grote aantal betrokkenen en gevoelige persoonsgegevens in de AddComm-zaak - startten inspecteurs van de AP een onderzoek. **Lees hierover meer op pagina 15.**

Datalektips

Iedereen kan bij de AP een datalektip indienen. Zo ontvangt de AP extra informatie over een datalek. Ook kan een burger bij de AP terecht als diegene denkt dat zijn of haar persoonsgegevens zijn gelekt. Datalektips geven de AP waardevolle informatie over datalekken die (wellicht) nog niet gemeld zijn. Als dat het geval is, en slachtoffers zijn bijvoorbeeld nog niet geïnformeerd, dan kunnen inspecteurs ervoor zorgen dat dat alsnog gebeurt. Ook kan een tip een reden zijn om een onderzoek naar het datalek te starten.

Schadevergoeding bij een datalek

Slachtoffers van een datalek hebben in sommige gevallen recht op een schadevergoeding. Dat kan het geval zijn als een organisatie in strijd met de AVG handelt en het slachtoffer daardoor schade lijdt. En als dit de organisatie kan worden verweten. Slachtoffers kunnen een rechtszaak beginnen bij de rechtbank.

Europese datalekken

Samen met andere Europese (privacy)toezichthouders houdt de AP namens alle Europeanen toezicht op onder meer datalekken. Hiervoor werkt de AP veel samen met andere Europese toezichthouders.

In 2024 ontving de AP geregeld datalekmeldingen en –signalen over datalekken waar platforms bij betrokken zijn. Zo namen cybercriminelen regelmatig platformaccounts van hotels over, om daarna hotelgasten op te lichten. Wanneer zo'n platform een hoofdvestiging heeft in Nederland, treedt de AP bij een datalek op namens alle Europese slachtoffers.

Slachtoffer aan het woord: Matthijs (44 jaar, werkzaam in de financiële sector)

"Voor mijn wintersportvakantie heb ik via internet een hotelkamer geboekt. Hierna ontving ik via WhatsApp een bericht met een link om mijn boeking te bevestigen. Ik klikte op de link en kwam terecht op een reserveringswebsite. Ik zag dat alle boekingsgegevens klopten, van mijn naam tot aan de periode en het bedrag. De website kwam me bekend voor en leek op een website die hier vaker voor wordt gebruikt. Omdat het er zo echt uit zag, en het niet ging om betaling maar om bevestiging van mijn boeking, klikte ik op de knop om dat te doen. Niets wees erop dat het om een betaling ging. Toch was er binnen een paar seconden 2.700 euro van mijn creditcard afgeschreven! Ik heb direct de bank gebeld en die vertelde mij dat ik was opgelicht. Ik voelde me hier heel stom over. Je wordt hier zo vaak voor gewaarschuwd en toch is het mij ook gebeurd. Het verbaasde me hoeveel van mijn gegevens de oplichters in handen hadden. Ook klopten deze gegevens allemaal. De website waarop ik moest bevestigen leek heel echt. Oplichters gaan dus heel slim en geavanceerd te werk. Als ik nu een hotel via internet boek, ben ik nog scherper en alerter. Mijn advies is dan ook: klik niet zomaar op een knop om een betaling te bevestigen, ook al lijkt het erop dat je niets hoeft te betalen. Dat scheelt je een hoop geld en gedoe."

2. Datadiefstal in 2024 bijna verdubbeld

In het kort

- De AP deed verdiepend onderzoek naar cyber-aanvallen die in 2024 zijn gemeld. Dit deed de AP door **253** datalekmeldingen te onderzoeken en de getroffen organisaties vragenlijsten te sturen.
- Het aantal ransomware-aanvallen waarbij data werden gestolen is **zo goed als verdubbeld** ten opzichte van 2023.
- Cyberaanvallen kunnen duur uitpakken. De AP zag tijdens het onderzoek organisaties die voor **tonnen** aan schade hadden na een aanval.
- In **40%** van de onderzochte gevallen was er wel beleid tegen cyberaanvallen, maar werd het niet juist uitgevoerd, of was er gebrekkige controle op (uitvoering van) dit beleid. In **33%** van de gevallen was er geen of onvoldoende beleid tegen cyber-aanvallen. Dat maakte deze getroffen organisaties zeer kwetsbaar voor cyberaanvallen.
- De AP ziet dat **42%** van de gemelde cyberaanvallen bestaat uit een account takeover, zoals een gehackte mailbox.
- De AP roept organisaties op effectief beleid te maken over bescherming tegen cyberaanvallen. En dit beleid daadwerkelijk uit te voeren.

Stijging in het aantal cyberaanvallen

Persoonsgegevens zijn voor criminelen goud waard. Om dit goud in handen te krijgen, voeren cybercriminelen steeds vaker cyberaanvallen uit. In 2024 ontving de AP **1.430** datalekmeldingen van cyberaanvallen. Ten opzichte van 2023 is het aantal gemelde cyberaanvallen met **9%** toegenomen. De AP schat dat in 2024 **5 miljoen** mensen slachtoffer werden van een cyberaanval.

Bijna verdubbeling van datadiefstal bij onderzochte ransomware-aanvallen

Waar in 2023 in **24%** van de ransomware-aanvallen gegevens werden gestolen, werden er in 2024 bij **minimaal 53%** aanvallen data gestolen ('data-extractie'). Bij de organisaties die deelnamen aan het onderzoek van de AP werd er zelfs in **89%** van de gevallen data gestolen. Ten opzichte van 2023 is dat **bijna een verdubbeling**. Criminelen gaan op zoek naar (financieel) gevoelige gegevens om deze te stelen en om daar organisaties, of zelfs hun klanten, mee af te persen. Voor deze diefstal gebruiken criminelen speciale programma's om de data uit de systemen van slachtofferorganisaties te halen. Zo was er in 2024 een organisatie die slachtoffer werd van een ransomware-aanval. Van honderden slachtoffers werden kopieën van paspoorten en adresgegevens gestolen. Na de aanval plaatsten cybercriminelen een deel van deze gegevens op het dark web.

Grote risico's voor slachtoffers

De AP ziet grote risico's voor slachtoffers wanneer hun data worden gestolen bij een cyberaanval. Bijvoorbeeld omdat een grote hoeveelheid (gevoelige) persoonsgegevens na de diefstal wordt doorverkocht op het dark web, maar ook op forums op het reguliere internet. Hiermee kunnen cybercriminelen bijvoorbeeld identiteitsfraude plegen. Volgens het Centraal Meldpunt Identiteitsfraude (CMI) deden ruim 7.000 burgers in 2024 melding van (mogelijke) identiteitsfraude.

Flinke financiële schade voor organisaties

Ook voor de getroffen organisatie kan een cyberaanval rampzalige financiële gevolgen hebben. De gevolgen van een datalek kunnen namelijk flinke kosten met zich mee brengen. Het afgelopen jaar zag de AP organisaties die voor **tonnen** aan schade hadden na een ransomware-aanval. Een cyberaanval kost een organisatie gemiddeld **103.976 euro**. De meeste organisaties die getroffen werden door een cyberaanval hadden voor **30.000 euro** aan schade. Dit schadebedrag bestaat bijvoorbeeld uit kosten voor het inhuren van externe specialisten die onderzoek doen naar de aanval, en de (eventuele) betaling van losgeld.

Het onderzoek

In 2024 ontving de AP 6.837 datalekmeldingen van een cyberaanval. Bij dit soort datalekken gaat het om hacking, ransomware, malware en/of phishing. Van de ransomware-aanval bij AddComm, die meerdere organisaties trof, ontving de AP 5.407 datalekmeldingen. Van de overige 1.430 datalek-meldingen over cyberaanvallen, heeft de AP 853 van deze meldingen onderzocht. Bij deze meldingen was in 600 gevallen sprake van een accountovername ('account-takeover'). Bij 112 gemelde cyberaanvallen vond een ransomware-aanval plaats. Bij 15 gevallen was er data-extractie met een losgeldeis. De andere 126 gemelde cyberaanvallen waren malware-incidenten.

De meldingen van account-takeovers zijn niet nader onderzocht. De AP onderzocht 253 organisaties die waren getroffen door ransomware, data-extractie met een losgeldeis, of een malware-incident. De AP analyseerde de 253 datalekmeldingen van deze cyberaanvallen. Verder ontving het grootste gedeelte van de organisaties een vragenlijst over de cyberaanval. Niet alle van de 253 onderzochte organisaties ontvingen een vragenlijst, bijvoorbeeld omdat de zaak nog niet afgerond was.

Organisaties werkten vrijwillig mee aan het onderzoek.

Soorten cyberaanvallen

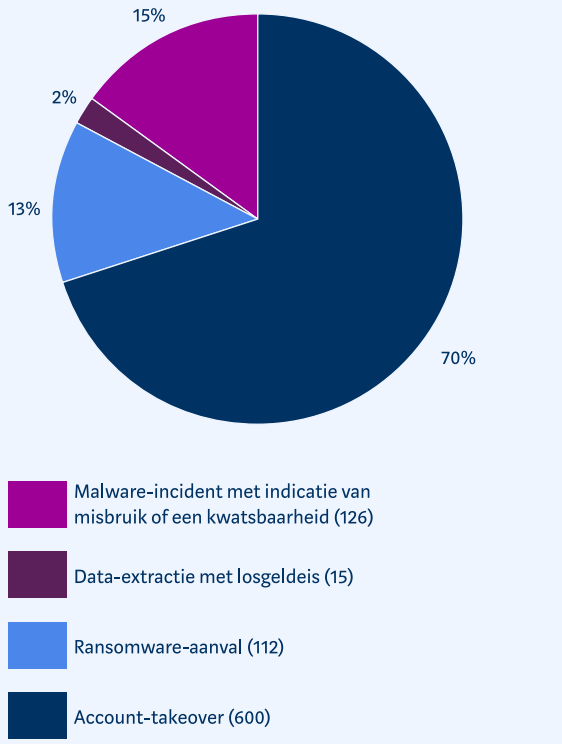
Van de 1.430 unieke datalekmeldingen over cyberaanvallen onderzocht de AP er 853. Uit deze aanvallen konden vier typen cyberaanvallen worden onderscheiden, zie figuur 2.

De overige 577 gemelde incidenten zijn niet verdiepend onderzocht, bijvoorbeeld omdat meerdere meldingen over hetzelfde incident gingen. Dit zijn bijvoorbeeld meldingen van een cyberaanval bij één organisatie, waar meerdere organisaties door geraakt werden.

Figuur 2 laat zien dat in **70%** van de onderzochte gevallen een cyberaanval bestond uit een account-takeover. Bij een account-takeover had een onbevoegde toegang tot een online-account. Bijvoorbeeld het inzien van een mailbox.

13% van de onderzochte cyberaanvallen was een ransomware-aanval. Bij een ransomware-aanval dringt een aanvaller systemen binnen, versleutelt deze en eist vervolgens losgeld om de systemen te ontgrendelen. Ook kan er naast de versleuteling data-extractie hebben plaatsgevonden.

FIGUUR 2 SOORT CYBERAANVAL



Bij data-extractie met een losgeldeis kreeg een kwaadwillende toegang tot de systemen, is er data gestolen, en is er losgeld geëist. Anders dan bij een klassieke ransomware-aanval, is er bij dit type aanval geen versleutelingssoftware uitgerold. **2%** van de onderzochte aanvallen bestond uit data-extractie met een losgeldeis.

Bij de overige **15%** van de onderzochte cyberaanvallen was sprake van een malware-incident met een indicatie van misbruik, of een kwetsbaarheid. Bijvoorbeeld schadelijke software die na toegang op systemen wordt geplaatst om gevoelige data te stelen, zoals inloggegevens ('infostealer').

Beleid tegen cyberaanvallen

De AP heeft de onderzochte organisaties vragen gesteld over hun beleid tegen cyberaanvallen. De antwoorden hierop zijn verwerkt in figuur 3.
Een voorbeeld van beleid tegen cyberaanvallen is een plan waarin staat hoe de systemen beveiligd worden en wanneer updates moeten worden uitgevoerd, en door wie. Ook kan dit plan afspraken bevatten over welke accounts toegang hebben tot welke systemen. De AP vroeg de onderzochte organisaties ook naar uitvoering van dit beleid.

Goede bedoelingen op papier, toch onvoldoende bescherming

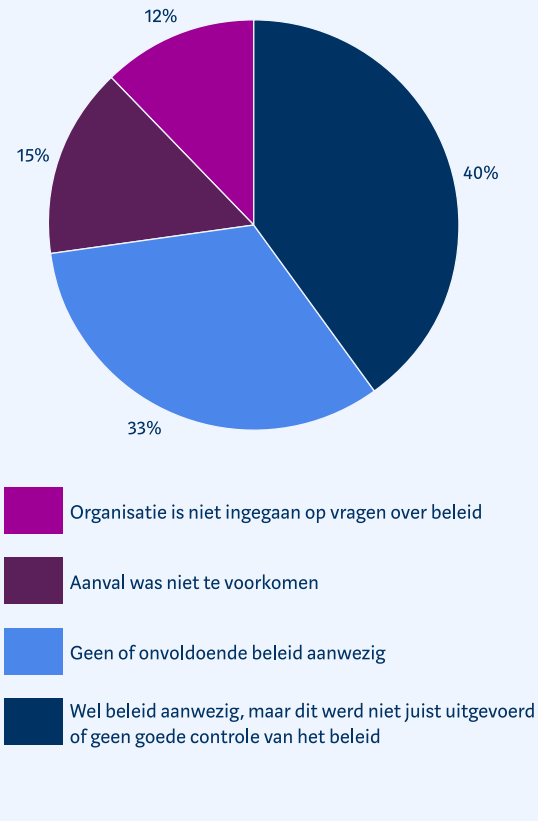
Uit het onderzoek van de AP blijkt dat **40%** van de onderzochte organisaties wel beleid tegen cyberaanvallen had, maar dat dit niet juist werd uitgevoerd, of dat er geen goede controle van dit beleid was. Ondanks dat het grootste gedeelte van de onderzochte organisaties wel beleid over bescherming tegen cyberaanvallen had, werd dat beleid vaak niet juist uitgevoerd of gecontroleerd. Hierdoor zijn veel organisaties onvoldoende beschermd tegen digitale dreigingen, ondanks de goede bedoelingen op papier. De AP roept daarom op om beleid tegen cyberaanvallen te maken, en dit ook juist uit te voeren.

Een derde (**33%**) van de onderzochte organisaties gaf aan dat er helemaal geen beleid tegen cyberaanvallen was, of dat het beleid onvoldoende was. Zo vertelde een organisatie bijvoorbeeld dat er beleid was om alle accounts te voorzien van meerfactorauthenticatie (MFA), maar dat er een uitzondering was voor admin-accounts. Dit zijn bijvoorbeeld accounts die systemen kunnen bewerken. Een kwaadwillende had via deze accounts toegang gekregen tot de organisatiesystemen.

Daarnaast gaf slechts **15%** van de onderzochte organisaties aan dat de aanval niet te voorkomen was. Bij deze organisaties was er beleid en werd dit beleid correct uitgevoerd, maar vond er alsnog een succesvolle cyberaanval plaats. Bijvoorbeeld omdat er een aanval plaatsvond die niemand aan zag komen. Zoals misbruik van een kwetsbaarheid in software, terwijl deze kwetsbaarheid bij de softwareontwikkelaars nog niet bekend was.

12% van de organisaties die deelnamen aan het onderzoek hebben deze vraag niet ingevuld.

FIGUUR 3 BELEID BIJ CYBERAANVALLEN



Eerste toegangspunt tot systemen (‘initial access’)

De AP heeft bij 253 organisaties gekeken hoe cybercriminelen bij een cyberaanval toegang kregen tot de systemen, zie figuur 4. Dit eerste toegangspunt wordt ook wel ‘initial access’ genoemd.

Toegang vaak door misbruik kwetsbaarheid

Van de 253 onderzochte cyberaanvallen was in **48%** van de gevallen onbekend hoe cybercriminelen voor het eerst toegang kregen tot systemen. In veel gevallen weet de getroffen organisatie dit wel, maar kwam het bijvoorbeeld niet expliciet naar voren in de melding aan de AP.

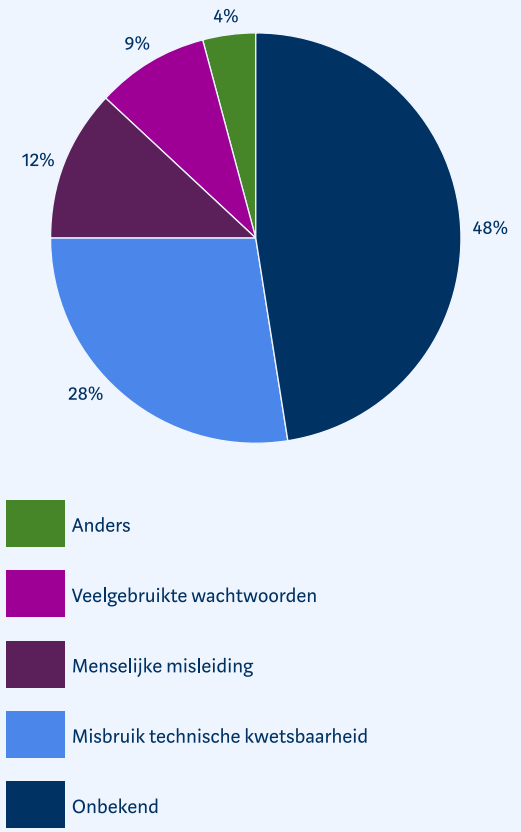
Als het eerste toegangspunt wel bekend was, ging het vaak om misbruik van een technische kwetsbaarheid (**28%**). Een technische kwetsbaarheid is bijvoorbeeld een systeem dat niet op tijd geüpdatet is.

In **12%** van de onderzochte gevallen kregen de cyberaanvallers toegang door menselijke misleiding. Bijvoorbeeld een medewerker die op een phishinglink in een e-mail klikt en inloggegevens invoert. Zo krijgt de aanvaller toegang tot het account van de medewerker. Vanaf dit account kan dan een verdere aanval worden opgestart.

Daarnaast gebruikten cybercriminelen regelmatig veelgebruikte of eerder gelekte wachtwoorden om toegang tot systemen te krijgen. Het uitproberen van veelgebruikte of eerder gelekte wachtwoorden staat ook wel bekend als ‘credential stuffing’. Of het kan een ‘brute force-aanval’ zijn geweest. Hiervan was sprake bij **9%** van de onderzochte cyberaanvallen.

In **4%** van de gevallen werd op een andere manier toegang verkregen. Bijvoorbeeld door moedwillig handelen van een medewerker.

FIGUUR 4 EERSTE TOEGANGSPUNT TOT SYSTEMEN



Onderhandelingen en losgeld na ransomware

Het onderzoek van de AP laat zien dat **60%** van de onderzochte organisaties na een ransomware-aanval contact opneemt met de criminelen. Waar de AP dit kon vaststellen, betaalde **24%** losgeld na de aanval. Omdat niet alle organisaties deze vraag beantwoordden, ligt het daadwerkelijke aantal organisaties dat losgeld betaalde waarschijnlijk tussen de **30 en 35%**.

Inspecteur aan het woord over het betalen van losgeld na een cyberaanval

"We zien regelmatig dat een organisatie losgeld betaalt en hiermee denkt het datalek in te kunnen perken, of gestolen data terug te kunnen krijgen. Toch houd je hiermee een illegaal systeem in stand. Ook is er geen garantie dat cybercriminelen zich na betaling aan hun woord houden. Tijdens dit onderzoek viel ons oog op een ransomware-aanval bij een IT-leverancier. Na de aanval nam deze organisatie contact op met de cybercriminelen en betaalde losgeld. In ruil daarvoor zouden de criminelen de gestolen data verwijderen en niet verder verspreiden. De IT-leverancier stond vervolgens raar te kijken toen de cybercriminelen snel na betaling van het losgeld alsnog de data op het dark web publiceerden. De criminelen hadden zich dus niet gehouden aan de afspraak. Al lijkt een hackersgroep nog zo 'professioneel'; het blijven criminelen en er is geen enkele garantie dat zij zich aan de afspraak houden."

Gevolgen account-takeovers onderschat

42% van alle cyberaanvallen uit 2024 waren account-takeovers. Dit type cyberaanval lijkt op het eerste oog onschuldiger, maar schijn bedriegt. Een account-takeover is een op zichzelf staand datalek en kan daarna ook nog leiden tot grotere incidenten. Zo wordt een account-takeover vaak gebruikt als springplank voor andere criminele activiteiten, bijvoorbeeld het uitrollen van ransomware. Ook worden accounts die zijn overgenomen vaak doorverkocht op het dark web.

Tijdens het onderzoek zag de AP enkele account-takeovers bij hotels, met grote risico's voor slachtoffers. Vaak beschikken cybercriminelen na geslaagde cyberaanvallen over grote hoeveelheden gevoelige persoonsgegevens van een groot aantal slachtoffers. Ook komen bij account-takeovers van hotels vaak creditcardgegevens in handen van cybercriminelen. Hiermee worden hotelgasten gericht opgelicht, met financiële schade tot gevolg.

Wapenen tegen account-takeovers

Om een minder makkelijk doelwit te zijn voor account-takeovers, is het cruciaal dat organisaties zich wapenen tegen dit soort cyberaanvallen. Dat kan relatief eenvoudig en goedkoop. Bijvoorbeeld door het controleren van verdachte inlogpogingen en het implementeren van MFA. Zie hierbij de aanbeveling hieronder en die op de volgende pagina.

Kritisch over verwerken en bewaren data

De AP ontving in 2024 475 datalekmeldingen waarbij meerdere organisaties slachtoffer werden van dezelfde cyberaanval. Zo zorgde het datalek bij klantcommunicatie-bedrijf AddComm ervoor dat er met één cyberaanval data van 5.407 organisaties gelekt werden. Dit laat de kwetsbaarheid van de keten zien, en de noodzaak dat organisaties zich hiervan bewust zijn en tegen wapenen.

Wil een organisatie zich goed wapenen tegen een cyberaanval, dan is het allereerst belangrijk dat een organisatie weet welke data zij verzamelen. En welke data eventueel aan andere organisaties worden doorgegeven. Als eigenaar van de data is en blijft de organisatie namelijk verantwoordelijk voor de beveiliging ervan. Ook als de organisatie deze data delen met andere organisaties.

Het is daarom essentieel dat een organisatie als eigenaar of gebruiker van de data grip houdt op de data en de beveiliging ervan. Niet alleen bij zichzelf, maar ook bij de organisaties waarmee wordt samengewerkt.

Lees op pagina 8 hoe een 44-jarige man, die werkzaam is in de financiële sector, voor 2.700 euro werd opgelicht nadat hij een hotelkamer boekte en zijn creditcardgegevens in handen kwamen van cybercriminelen.

Aanbeveling: controleer verdachte inlogpogingen

Controleer op verdachte inlogpogingen om account-takeovers tegen te gaan. Het is bijvoorbeeld aan te raden om inlogactiviteiten op accounts te monitoren, bijvoorbeeld door IP-adrescontrole. Detecteer inlogpogingen van verdachte of onbekende IP-adressen, vooral als deze IP-adressen uit landen komen waar een gebruiker normaal geen toegang heeft. Ook is het bijvoorbeeld raadzaam om login-alerts in te stellen. Vaak bieden systemen de mogelijkheid om een melding aan een gebruiker te sturen wanneer een inlogpoging wordt gedaan vanaf een nieuwe locatie, een nieuw apparaat of ander IP-adres.

Aanbeveling: implementeer MFA

Een andere manier om een account-takeover tegen te gaan, is het instellen van MFA. MFA betekent dat er altijd twee of meer 'factoren' nodig zijn om mee in te loggen: iets dat je weet (bijvoorbeeld een wachtwoord) en iets dat je hebt (bijvoorbeeld een tijdelijke code via een app). MFA implementeren op een mailbox is relatief goedkoop en gemakkelijk.

Aanbeveling: denk kritisch na over verwerken en bewaren

"Wat je niet (meer) hebt, kan ook niet lekken" is een bekende spreuk en een aanrader om kritisch over na te denken. Door minder data te verwerken en deze korter te bewaren, kan een cyberaanval minder impact hebben op een organisatie. Denk daarom kritisch na over welke data je verwerkt, en hoe lang je deze bewaart. Gooi weg wat je niet langer nodig hebt.

Denk ook kritisch na over welke data je aan partijen geeft waarmee je samenwerkt. Geef deze partij niet meer data dan nodig is voor het uitvoeren van hun diensten. En vraag de andere organisatie regelmatig of oude data, of data die niet langer nodig zijn, worden verwijderd.

Aanbeveling: pak verantwoordelijkheid en controle

Neem verantwoordelijkheid over de data die je zelf opslaat en gebruikt. Controleer regelmatig de beveiliging van data. Check bijvoorbeeld of het geldende beveiligingsbeleid nog juist is, maar ook of het daadwerkelijk goed wordt uitgevoerd. Loop geregeld systemen na: staat er niet per ongeluk nog ergens een toegangspoort open die eigenlijk dicht hoort te staan? Of moet er nog iets geüpdatet worden? En ook: controleer de gemaakte afspraken met andere organisaties aan wie je data geeft. Toets of zij gemaakte afspraken nakomen, en of ze de door jou geleverde data goed beveiligen. Dit kun je doen door hierover in gesprek te gaan met de organisaties waarmee je samenwerkt.

Pak de beveiliging van data binnen de gehele organisatie op; het gaat namelijk niet alleen de ICT-afdeling aan. Zet het onderwerp regelmatig op de (directie-)agenda en maak het organisatiebreed bespreekbaar.

3. Hoe één cyberaanval de digitale veiligheid van 1,5 miljoen mensen in gevaar bracht

In het kort

- De AP ziet geregeld dat één cyberaanval een hele keten van dienstverlening van verschillende organisaties raakt.
- Zo zag de AP dat in 2024, door één ransomware-aanval bij een bedrijf dat klantcommunicatie voor andere bedrijven verzorgt, een hele keten van dienstverlening werd geraakt.
- Hierdoor waren **5.407** klantorganisaties uit de hele leveranciersketen ook de dupe van het datalek.
- **Ruim 1,5 miljoen** mensen werden slachtoffer van de cyberaanval.
- Door interventies van de AP hebben vrijwel alle klanten van het communicatiebedrijf het datalek bij de AP gemeld en zijn slachtoffers gewezen op de risico's die bij de aanval kwamen kijken.
- Door een interventie van de AP zijn **82.893** slachtoffers alsnog geïnformeerd over het datalek en de risico's.
- Leonie van der Veen, CEO van AddComm: "De hack is het beste wat ons is overkomen."

Cyberaanvallen treffen de hele keten

Veel organisaties maken gebruik van elkaars diensten. Zo kan een supermarkt een ander bedrijf inschakelen om salarissen aan het personeel uit te betalen. Om dit te kunnen doen, ontvangt het salarisadministratiebedrijf (gevoelige) persoonsgegevens van de supermarkt en slaat deze persoonsgegevens op.

Doordat organisaties gebruikmaken van elkaars diensten, is deze manier van werken vatbaar voor cyberaanvallen. De AP ziet geregeld dat een hele keten van dienstverlening door één cyberaanval wordt platgelegd. Dit kan tot gevolg hebben dat bedrijven hun werkzaamheden niet kunnen voortzetten, of dat persoonsgegevens (tijdelijk) niet gebruikt kunnen worden.

Ransomware bij een dienstverlener

Ook in 2024 was er een grote cyberaanval waardoor een keten van dienstverlening werd geraakt. In mei van dit jaar werden de systemen van AddComm, een dienstverlener die voor andere bedrijven klantcommunicatie verzorgt, getroffen door een ransomware-aanval. Op deze systemen waren data opgeslagen die persoonsgegevens bevatten. Cyberaanvallers hebben deze systemen versleuteld en een grote hoeveelheid aan persoonsgegevens ingezien en mogelijk gestolen. Hierdoor werden ruim **1,5 miljoen** mensen slachtoffer van één cyberaanval.

Grote hoeveelheden gevoelige persoonsgegevens

Vrij snel na de aanval stroomden de datalekmeldingen van de klanten van het communicatiebedrijf binnen. Zo ontving de AP onder andere datalekmeldingen van een groot bedrijf uit de energiesector, een bank, een drinkwaterbedrijf en een bedrijf dat facturen van huisartsen en tandartspraktijken verstuurt.

Al gauw werd duidelijk dat op grote schaal gevoelige persoonsgegevens getroffen waren door de cyberaanval. Zoals BSN's, medische gegevens en factuurgegevens.

Grote risico's voor betrokkenen

Door de gevoeligheid van de getroffen persoonsgegevens en de hoeveelheden aan data, zag de AP direct grote risico's voor de slachtoffers van de ransomware-aanval. Met deze persoonsgegevens kunnen cybercriminelen namelijk slachtoffers gericht oplichten. Hoe makkelijk is het wel niet om een factuur voor een tandartsbehandeling na te maken, daarin het juiste factuurbedrag te noemen en deze te versturen naar het e-mailadres van het slachtoffer?

Vanwege de grote risico's voor slachtoffers, waren klanten van AddComm verplicht om het datalek te melden aan de AP en aan de slachtoffers. Om de context van het datalek in kaart te brengen en waar nodig bij te sturen, intensiveerden inspecteurs van de AP het toezicht.

Op toezichtsbezoek bij AddComm

Bij de start van het onderzoek gingen inspecteurs langs bij AddComm. Zij spraken met AddComm over de aanval en de gevolgen. Ook hebben ze de organisatie gewezen op wat voor de AP het belangrijkste was: het informeren van betrokken partijen en slachtoffers en een zorgvuldig onderzoek doen naar het datalek.

AddComm aan het woord: Leonie van der Veen (CEO)

"De eerste drie weken na de aanval stonden we echt in overlevingsmodus. Onderling merkte ik een enorme inzet en verbroedering: iedereen werkte enorm hard om het datalek te verhelpen. Toen de AP op toezichtsbezoek kwam, vonden we dat best spannend. We zaten namelijk middenin een crisis en hadden nooit eerder contact gehad met de AP. Aan het begin van het gesprek wisten we niet goed wat we konden verwachten. We vertelden de AP zoveel mogelijk over het datalek, zodat zij het datalek beter in kaart konden brengen. Gaandeweg werd duidelijk dat de AP niet kwam om te bestraffen, maar om informatie te krijgen en bij te sturen. Achteraf gezien was het contact met de AP niet zo spannend als dat we dachten.

'De hack is het beste wat ons is overkomen.'
Dat klinkt misschien raar, maar wij en onze klanten hebben hier veel van geleerd. Een belangrijke les voor ons en onze klanten is: weet welke data je verzamelt of deelt met een andere organisatie. Door minder data te verwerken en deze korter te bewaren, is de impact van een hack kleiner. Kijk ook kritisch naar de beveiliging van je leverancier. Je kunt zelf alles op orde hebben, maar jouw data is in de hele keten kwetsbaar. De tweede les is dat beveiliging en privacy verantwoordelijkheden zijn van het gehele bedrijf, en niet alleen van de ICT-afdeling. Zet het regelmatig op de directieagenda en ga er samen mee aan de slag."

Onderzoek naar een cyberaanval

Bij een grote cyberaanval is het belangrijk dat er zorgvuldig onderzoek naar het datalek wordt gedaan. Zo kan een organisatie klanten goed informeren over het datalek en de gevolgen, en hen wijzen op de grootste risico's. Hierdoor kunnen slachtoffers zich hiertegen wapenen door zelf ook maatregelen te nemen.

Omdat bij de cyberaanval bij AddComm financiële-, medische gegevens en e-mailadressen waren gelekt, wezen de klanten van AddComm slachtoffers op het risico van gerichte oplichting. Daardoor konden slachtoffers extra alert zijn op ongebruikelijke berichten en vreemde betaalverzoeken van onbekende afzenders.

Inspecteur aan het woord

"Bij grote cyberaanvallen komt er veel over een organisatie heen, en dat allemaal op hetzelfde moment. De getroffen organisatie moet bijvoorbeeld onderzoek doen naar het datalek, maar ook nadenken over het informeren van hun klanten en eventuele slachtoffers. Grote datalekken komen helaas vaker voor. De ervaring leert dat de AP bij deze datalekken achteraf veel moest bijsturen. Om dit te voorkomen, en om onze verwachtingen aan een getroffen organisatie duidelijk te maken, kan een toezichtsbezoek heel nuttig zijn. De meeste organisaties vinden het spannend als we langskomen. Dat is begrijpelijk. Daar zijn we ons bewust van en daar proberen we zo goed mogelijk op in te spelen. Daarom vertellen we bij een toezichtsbezoek direct waarvoor we komen. Zo kunnen we hopelijk bij veel organisaties een stukje spanning wegnemen. Door kennis en verwachtingen te delen, maken we getroffen organisaties weerbaarder tegen datalekken."

Gesprekken over informeren betrokkenen

Na het toezichtsbezoek van de AP onderzocht AddComm het datalek verder en informeerde hun klanten. Omdat er voor slachtoffers hoge risico's bestonden, zoals de mogelijkheid tot gerichte oplichting, moesten de klanten van AddComm daarna de slachtoffers van het datalek informeren.

5.407 klanten van AddComm deden na de cyberaanval een datalekmelding bij de AP. De AP analyseerde deze gemelde datalekken en ontdekte dat 16 organisaties hun slachtoffers niet hadden geïnformeerd over de aanval. Deze organisaties vonden bijvoorbeeld dat er geen sprake was van een hoog risico voor betrokkenen, omdat het ging om "normale" persoonsgegevens, zoals een telefoonnummer en een e-mailadres. De AP zag wel degelijk hoge risico's bij het datalek, omdat het lek bij één organisatie al zorgde voor **24.000** slachtoffers. Door het lekken van onder meer een e-mailadres konden deze duizenden slachtoffers bijvoorbeeld per e-mail op grote schaal worden gephisht.

Na een gesprek met een inspecteur informeerden deze 16 organisaties alsnog **82.893** slachtoffers. Daarna rondde de AP het onderzoek af en sloot het dossier.

4. Feiten & cijfers

Stijging in het aantal cyberaanvallen

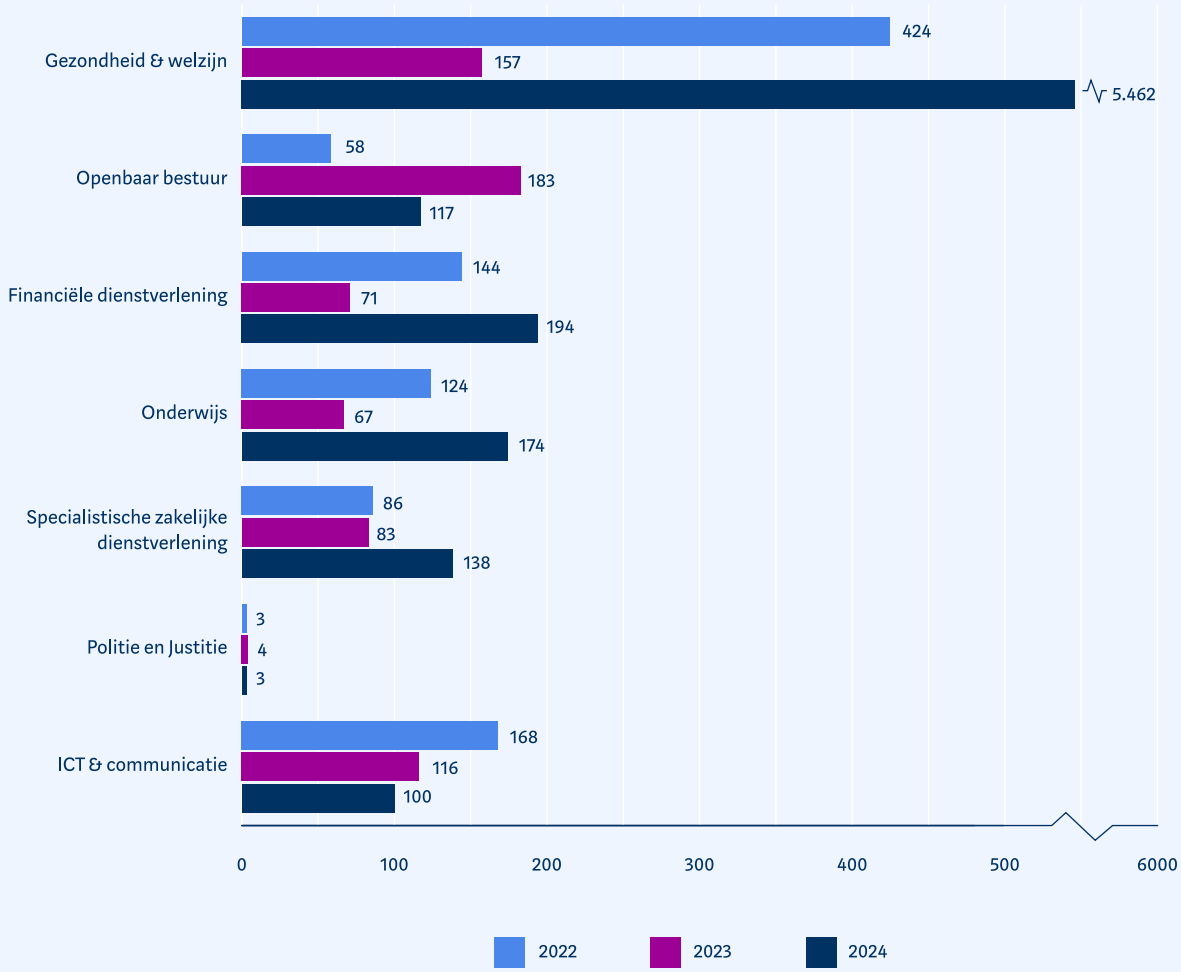
Het totale aantal datalekmeldingen naar aanleiding van een cyberaanval steeg in 2024 van 1.309 naar **6.837**.

Door één datalek bij AddComm werden in één keer ruim 5.000 organisaties getroffen. Deze 5.407 organisaties vielen onder de meldplicht datalekken en deden een datalekmelding bij de AP. Los daarvan steeg het aantal meldingen van cyberaanvallen alsnog met **9%**, van 1.309 naar **1.430**. Deze stijging kan onder andere worden verklaard door het feit dat het voor cybercriminelen steeds eenvoudiger is om cyberaanvallen uit te voeren. Ook als zij minder technisch onderlegd zijn. Zo kunnen criminelen phishingmails met artificiële intelligentie (AI) opstellen die moeilijker zijn te onderscheiden van echte e-mails. Omdat AI-tools steeds beter worden, kan dit ervoor zorgen dat mensen eerder in phishingmails 'trappen', waardoor na het klikken op de phishinglink persoonsgegevens worden buitgemaakt.

Aantal cyberaanvallen in Onderwijs en Specialistische zakelijke dienstverlening steeg

De AP zag in 2024 een stijging van het aantal cyberaanvallen in de sectoren Onderwijs en Specialistische zakelijke dienstverlening. Onder deze laatste sector vallen onder meer advocaten-, notaris- en deurwaarderskantoren en accountants. De stijging in de onderwijssector is deels te

FIGUUR 5 TOTAAL AANTAL CYBERAANVALLEN PER SECTOR



verklaren door een ransomware-aanval bij een schoolboeken-leverancier. Een groot aantal onderwijsinstellingen was betrokken bij dit datalek.

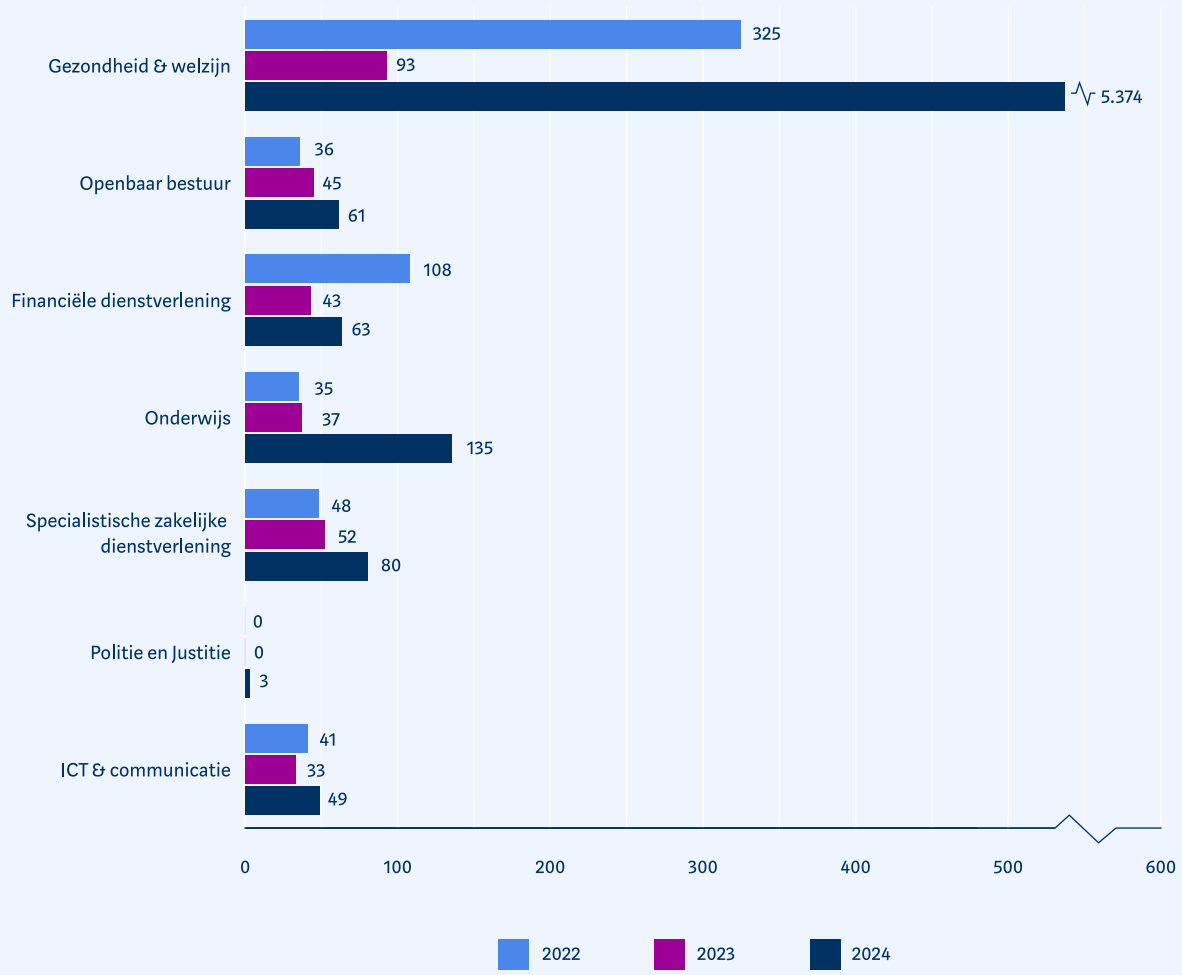
In 2024 meldden de sectoren Onderwijs en Gezondheid & welzijn de meeste cyberaanvallen bij de AP. De onderwijs-sector deed het afgelopen jaar **174** meldingen en de gezondheidssector **5.462**.

Eén cyberaanval, meerdere organisaties betrokken

De AP ziet geregeld dat een cyberaanval plaatsvindt bij één organisatie die diensten levert aan veel andere organisaties. Zo kan één cyberaanval een hele keten aan dienstverlening treffen. Deze cyberaanvallen hebben veel impact op een vaak grote keten van dienstverlening.

Figuur 6 laat zien bij hoeveel datalekmeldingen in een bepaalde sector meerdere organisaties geraakt werden door één cyberaanval. In figuur 5 op de vorige pagina is te zien dat de sector ICT & communicatie het afgelopen jaar 100 datalekken door een cyberaanval meldde. In aansluiting hierop laat figuur 6 zien dat bij 49 van de 100 gemelde cyberaanvallen door de sector ICT & communicatie, meerdere organisaties door deze cyberaanval geraakt zijn.

FIGUUR 6 CYBERAANVALLEN DIE MEERDERE ORGANISATIES TREFFEN (PER SECTOR)



Onderwijs en Specialistische zakelijke dienstverlening vaak getroffen door één cyberaanval

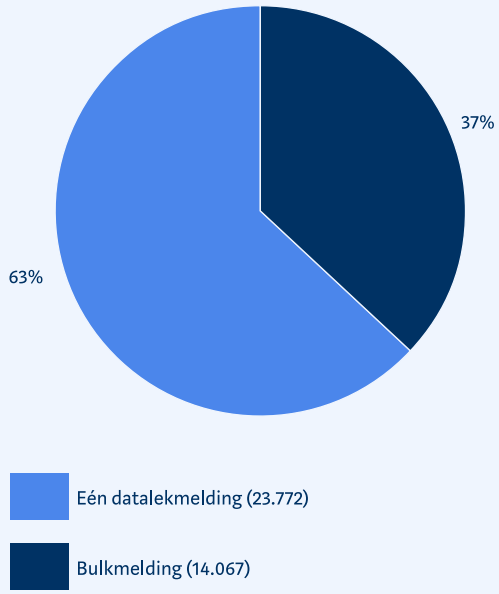
In de sector Onderwijs waren bij 135 van de 174 meldingen over cyberaanvallen andere organisaties betrokken, oftewel **78%**. Veel van deze meldingen zijn gedaan na een ransomware-aanval bij een schoolboekenleverancier.

In de sector Specialistische zakelijke dienstverlening ging **58%** van de meldingen over cyberaanvallen waarbij andere organisaties betrokken waren. Een mogelijke verklaring voor deze stijging is dat organisaties in deze sector de afgelopen jaren steeds afhankelijker werden van cloud-diensten en online dossierbeheer. Als dan de beveiliging van systemen of de kennis hierover onvoldoende op orde is, levert dit beveiligingsrisico's op.

In 2024 37.839 datalekken gemeld bij de AP

In 2024 zijn in totaal **37.839** datalekken gemeld aan de AP. Daarvan zijn **14.067** datalekken gemeld via een zogenoemde bulkmelding. In een bulkmelding meldt een organisatie meerdere van dezelfde datalekken in één melding. Daarnaast zijn er het afgelopen jaar **23.772** enkele datalekmeldingen gedaan bij de AP.

FIGUUR 7 AANTAL GEMELDE DATALEKKEN BIJ DE AP



Stijging van het aantal bulkmeldingen

Het melden van datalekken in een bulkmelding kan de administratieve last voor organisaties verlichten. Naast verkeerd verzonden brieven kunnen sinds 2024 ook digitale datalekken, zoals verkeerd verzonden e-mails, in bulk worden gemeld. Ook heeft de AP het aantal organisaties dat datalekken in bulk kan melden, verruimd. Dit verklaart de stijging van het aantal in bulk gemelde datalekken van 5.480 in 2023, naar 14.067 in 2024.

Lees meer over een cyberaanval bij AddComm die een gehele keten aan dienstverlening raakte op **pagina 15**.
Door één cyberaanval werden ruim 1,5 miljoen mensen slachtoffer en werden 5.407 andere organisaties geraakt.

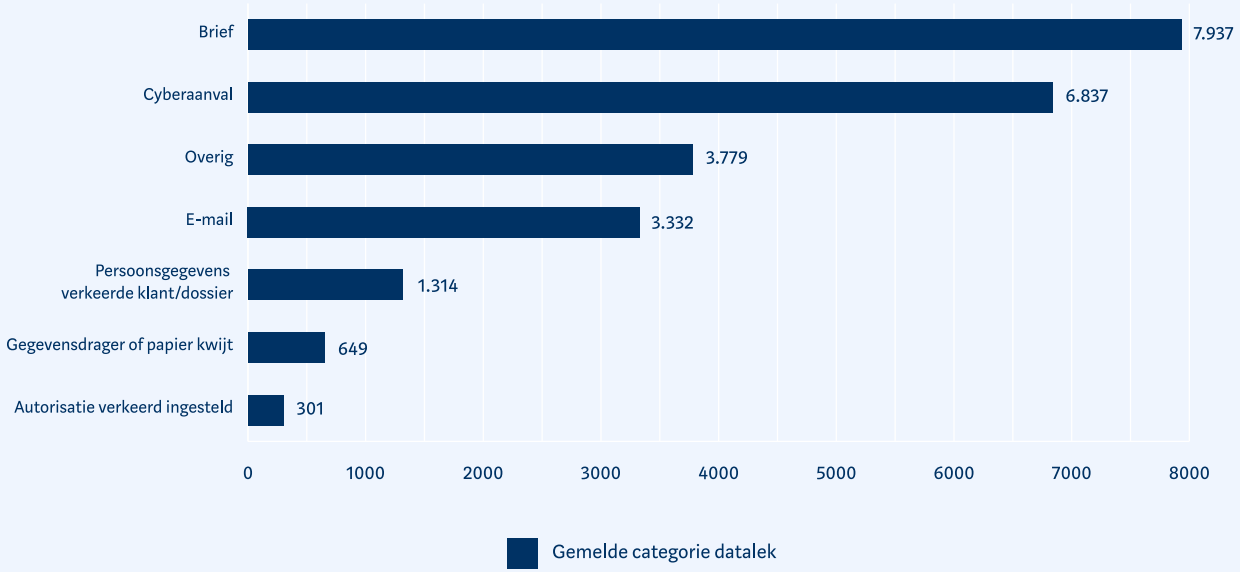
Verkeerd verzonden brieven en e-mails het meest gemeld

Net als voorgaande jaren ontving de AP in 2024 de meeste datalekmeldingen over verkeerd verzonden brieven met daarin persoonsgegevens (7.937 meldingen, **42%** van het totale aantal). Dit aantal is iets gedaald ten opzichte van 2023, toen dit type datalekken 9.899 keer werd gemeld (**49%** van het totale aantal). De AP ziet bijvoorbeeld geregeld dat brieven met financiële gegevens over (problematische) schulden naar de verkeerde ontvanger worden gestuurd. Dit is een voorbeeld van een datalek dat moet worden gemeld aan de AP.

Door het melden van datalekken en het registeren van datalekken in het interne datalekkenregister, krijgen organisaties meer inzicht in de mogelijke risico's van de werkwijzen binnen de organisatie. Zo kunnen organisaties leren van hun datalekken en hun processen aanpassen, waardoor minder (van dezelfde) datalekken plaatsvinden.

Het hoge aantal datalekmeldingen in de categorie cyberaanval is te verklaren door de 5.407 datalekmeldingen na de cyberaanval bij AddComm.

FIGUUR 8 MEEST GEMELDE CATEGORIEËN VAN DATALEKKEN



Datalekmeldingen in de categorie 'overig'

In de categorie 'overig' zijn 3.779 datalekken gemeld. Deze bestonden uit de volgende typen datalekken:

- overig (**76%**): bijvoorbeeld inzage door een geautoriseerd persoon maar zonder geldige reden, of meer persoonsgegevens doorgestuurd dan nodig;
- per ongeluk gepubliceerde persoonsgegevens (**14%**);
- verkeerd ingestelde toegangsrechten (autorisaties) op een netwerkmap of locatie (**8%**);
- persoonsgegevens waren (tijdelijk) niet beschikbaar door een storing (**2%**);
- documenten met daarin persoonsgegevens waren bij het oud papier gezet (**1%**).

Meeste datalekmeldingen uit de gezondheidssector

Net als voorgaande jaren ontving de AP in 2024 de meeste datalekmeldingen van organisaties in de sectoren Gezondheid & welzijn (6.873), gevolgd door Openbaar bestuur (4.874) en Financiële dienstverlening (1.985). Dit is te verklaren omdat deze sectoren relatief veel en gevoelige persoonsgegevens verwerken. Daardoor moeten kleine incidenten al snel aan de AP gemeld worden, bijvoorbeeld een verkeerd geadresseerde brief of onrechtmatige inzage in persoonsgegevens.

Zo ontving de AP in de zomer van 2024 diverse datalekmeldingen doordat medewerkers persoonsgegevens van bijvoorbeeld patiënten of klanten deelden met een chatbot die gebruikmaakt van AI. Door het invoeren van persoonsgegevens in AI-chatbots, kunnen de bedrijven achter de chatbots ongeoorloofd toegang krijgen tot die persoonsgegevens. Vaak gebruiken medewerkers de chatbots op eigen initiatief en tegen afspraken met de werkgever in. Als de medewerker hierbij persoonsgegevens invoert, is sprake van een (meldplichtig) datalek.

Daarnaast versturen organisaties in de sectoren Gezondheid & welzijn, Openbaar bestuur en Financiële dienstverlening veel poststukken en e-mails met gevoelige persoonsgegevens. Bijvoorbeeld medische gegevens in de sector Gezondheid & welzijn en het BSN en financiële gegevens in de sectoren Openbaar bestuur en Financiële dienstverlening. In deze sectoren ging het in ongeveer 50% van de meldingen om een brief aan een onjuiste ontvanger en in ongeveer 15% van de gevallen om een verkeerd verzonden e-mail.

Dat de sector Gezondheid & welzijn de meeste meldingen doet is daarnaast te verklaren omdat zorginstellingen gebonden zijn aan strenge eisen op basis van sectorale wetgeving. Hierdoor hebben zij vaak al beleid en procedures om datalekken snel en systematisch aan de AP te melden, ook bij kleine incidenten. Bovendien is dit aantal meldingen te verklaren omdat zorginstellingen vaak grote hoeveelheden gevoelige persoonsgegevens verwerken.

FIGUUR 9 TOTAAL AANTAL DATALEKMELDINGEN PER SECTOR