AUTORITEIT
PERSOONSGEGEVENS

Meldplicht datalekken: facts & figures
Overzicht feiten en cijfers eerste helft 2019

Aantal meldingen eerste helft 2019	Verwachte stijging op jaarbasis	Sector met meeste gemelde datalekken
11.906	↑ 14%	Zorg

Introductie

Sinds 2016 geldt in Nederland de meldplicht datalekken. Organisaties moeten een datalek melden aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de personen waarvan de gegevens zijn gelekt. Daarnaast moet een datalek gemeld worden aan de getroffen personen wanneer het lek waarschijnlijk een hoog risico voor hen oplevert. Deze rapportage geeft inzicht in het aantal datalekmeldingen dat de AP heeft ontvangen in de eerste helft van 2019, de sectoren waarin de meeste gemelde datalekken hebben plaatsgevonden, de aard van de datalekken en het maximum aantal betrokkenen bij de datalekken.

Thema: zorgsector

Sinds de meldplicht datalekken in 2016 van kracht is gegaan zijn de meeste datalekmeldingen afkomstig uit de zorgsector. In de eerste helft van 2019 is dat ook niet anders. Om hier meer inzicht in te krijgen en te geven zoomen we in deze rapportage in op datalekmeldingen uit deze sector met behulp van cijfers, analyses, voorbeelden en geven we praktische tips hoe deze datalekken mogelijk kunnen worden voorkomen.

Campagne met praktische informatie over datalekken

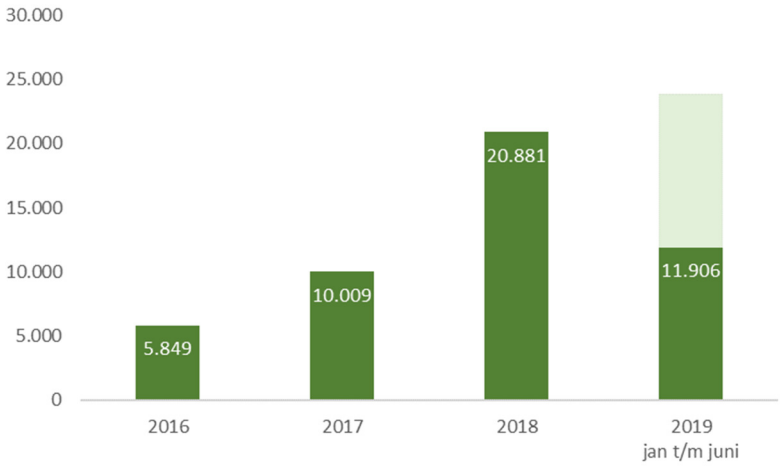
In het kader van de campagne 'Wat betekent de privacywet voor jou(w) bedrijf?' heeft de AP in juli 2019 de informatie over datalekken op haar websites uitgebreid. Bestaande QenA's zijn aangepast, er zijn nieuwe QenA's toegevoegd en de AP biedt praktische hulpmiddelen om de naleving makkelijker te maken.

AUTORITEIT
PERSOONSGEGEVENS

Cijfers eerste helft 2019

Aantal meldingen

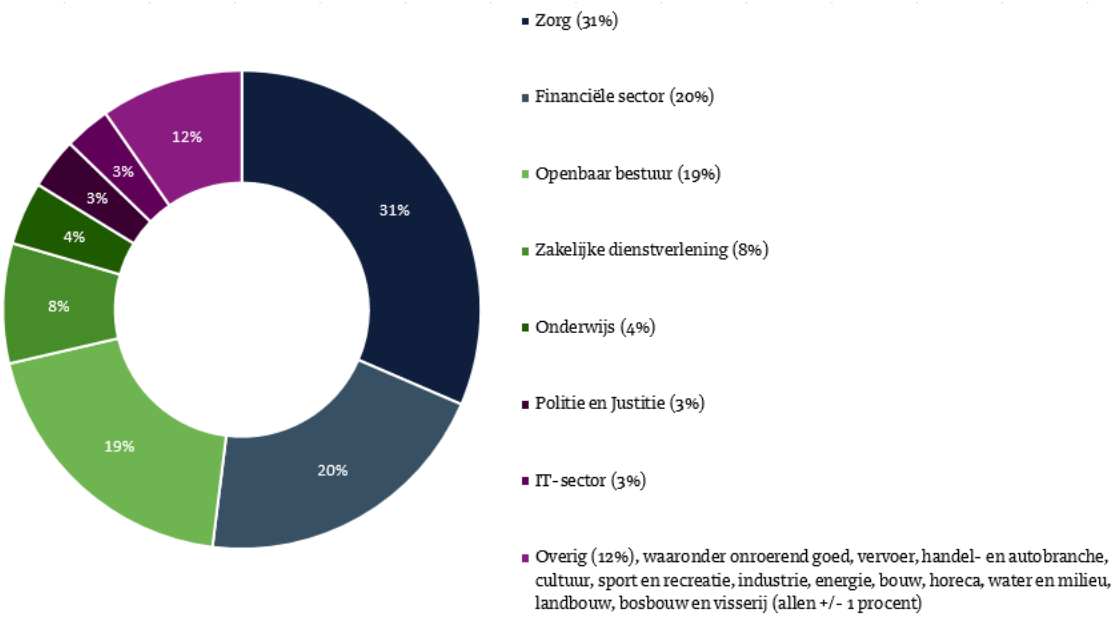
In de eerste helft (januari tot en met juni) van 2019 ontving de AP 11.906 meldingen van datalekken. Dat komt neer op ongeveer 2.000 meldingen per maand. Als deze trend voortzet, zal het aantal datalekmeldingen in 2019 wederom hoger zijn dan het voorgaande jaar (een stijging van rond de 14%). Het aantal datalekmeldingen over geheel 2019 zal dan uitkomen op ongeveer 24.000. De laatste maanden lijkt het aantal meldingen enigszins te stabiliseren. De onderstaande grafiek toont de toename van het aantal datalekmeldingen sinds 2016.



Grensoverschrijdende datalekken

De 11.906 meldingen zijn meldingen van datalekken die de AP in Nederland heeft ontvangen via het meldloket datalekken op de website van de AP. Daarnaast hebben andere Europese toezichthouders in 21 gevallen een grensoverschrijdend datalek gedeeld met de AP. Dat gebeurt bijvoorbeeld als een datalek bij een andere Europese toezichthouder is gemeld, maar het datalek gevolgen heeft voor betrokkenen in meerdere lidstaten waaronder personen in Nederland.

Meldingen datalekken per sector



De meeste datalekken zijn gemeld vanuit de sector zorg (31%), de financiële sector (20%) en de sector Openbaar bestuur (19%). Dit zijn ook de sectoren waarvan de AP in voorgaande jaren het grootste aantal datalekmeldingen ontving. Binnen deze top 3 is het aantal meldingen in de zorg ten opzichte van 2018 gestegen met 2 procent, het aantal meldingen in de financiële sector gedaald met 6 procent en het aantal meldingen in de sector Openbaar bestuur gestegen met 2 procent.

Zorg

Het grootste aantal datalekmeldingen binnen de zorgsector is afkomstig van ziekenhuizen (23%), apotheken (22%) en stichtingen die bevolkingsonderzoek uitvoeren (9%). Bij de meeste meldingen in de zorgsector (65%) ging het om een datalek met één betrokkene. Een uitgebreidere analyse van de datalekmeldingen door de zorgsector is opgenomen in het laatste deel van deze rapportage.

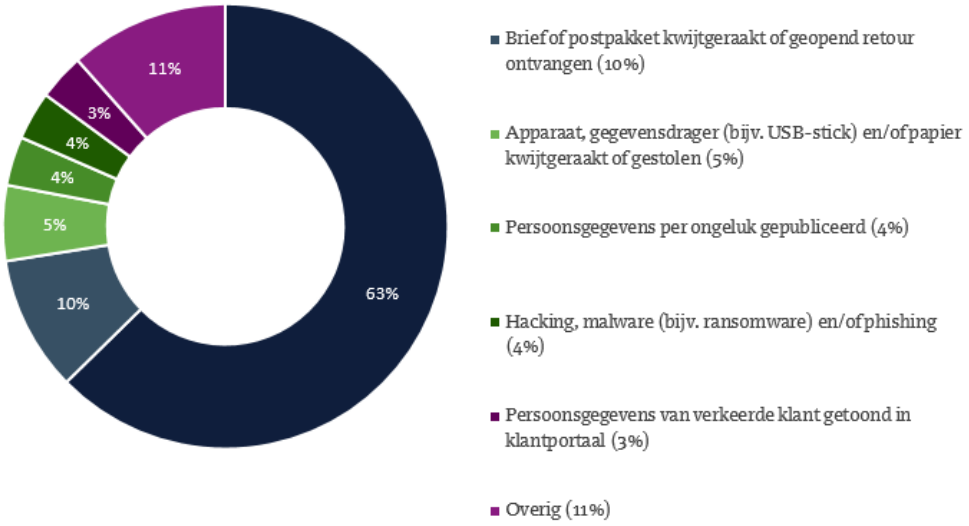
Financiële sector

Het grootste aantal datalekken binnen de financiële sector wordt gemeld door incassobureaus (54%). Daarbij gaat het meestal om een herinneringsbrief voor een openstaande factuur die geopend retour komt. 18% van de meldingen binnen de financiële sector is afkomstig van financiële instellingen zoals banken, en 18% van verzekeringsmaatschappijen en pensioenfondsen.

Openbaar Bestuur

Binnen de sector Openbaar bestuur worden de meeste datalekken gemeld door zelfstandige bestuursorganen (37%), gevolgd door gemeenten (34%) en de Rijksoverheid (26%).

Type datalekken



Versturen of afgeven van persoonsgegevens aan verkeerder ontvanger

In de meerderheid van de meldingen (63%) gaat het om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Dit was ook verreweg het meest gemelde type datalek in 2018 (eveneens 63%) en in 2017 (47%). Bij dit type datalek kan het gaan om een e-mail met daarin gevoelige persoonsgegevens die wordt verzonden naar de verkeerde ontvanger. Bijvoorbeeld door een typefout of omdat er in het e-mailprogramma een verkeerde geadresseerde wordt geselecteerd. Daarnaast komt het voor dat personen hun eigen gegevens opvragen bij organisaties, maar door een administratieve fout vervolgens ook persoonsgegevens van anderen ontvangen.

Voorbeeld datalek: Versturen persoonsgegevens aan verkeerder ontvanger

Een medewerker van een bedrijf stuurt per ongeluk een e-mailbericht intern naar de verkeerde collega. In de bijlage van deze e-mail zijn verslagen van functioneringsgesprekken van een aantal medewerkers van het bedrijf bijgevoegd. Daarin staan ook gegevens over de gezondheid van deze medewerkers, in het kader van een aantal lopende re-integratietrajecten. De medewerker die de e-mail ten onrechte ontving heeft de e-mail geopend en heeft inzage gekregen in de bovengenoemde gegevens van diens collega's. De verzender van de e-mail ontdekt zijn fout en verzoekt de verkeerde ontvanger om het e-mailbericht en gedownloade bijlage te verwijderen.

Het bedrijf meldt het incident aan de AP. In de melding geeft het bedrijf aan het datalek niet mede te delen aan de medewerkers wiens gegevens zijn gelekt. Als reden geeft het bedrijf dat alle medewerkers van het bedrijf een geheimhoudingsverklaring hebben ondertekend, waardoor het risico voor de betrokkenen te verwaarlozen is. De AP stuurt naar aanleiding van de melding een brief aan het bedrijf waarin het bedrijf verzocht wordt om de betrokkenen te informeren, aangezien het datalek waarschijnlijk een hoog risico op (o.a.) reputatieschade oplevert. Omdat het hier medische persoonsgegevens van directe collega's van de onjuiste ontvanger betrof, is het niet relevant dat een geheimhoudingsverklaring is getekend. Het bedrijf dient naar aanleiding van de brief van de AP een vervolgmelding in waarin zij aangeeft de betrokkenen te informeren via een persoonlijk bericht en een bericht op het Intranet.

Datalekken met post

In 10% van de gevallen gaat het om poststukken met gevoelige gegevens die bij de verkeerde persoon terechtkomen en geopend retour worden gestuurd. De onjuiste ontvanger heeft dan kennis kunnen nemen van de inhoud van de brief. Dit soort datalekken komt het meeste voor in de sector zorg (42%), zakelijke dienstverlening (19%) en openbaar bestuur (14%).

Datalekken met mobiele apparatuur

Het komt ook voor dat mobiele apparaten of gegevensdragers zoals laptops, tablets, smartphones en USB-sticks waarop persoonsgegevens zijn opgeslagen, kwijtraken of worden gestolen. Dit type datalek komt het meest voor in de zorgsector (27%), gevolgd door de sector openbaar bestuur (18%) en de sector onderwijs (13%).

Datalekken door hacking, malware en/of phishing

Vier procent van de meldingen die de AP ontving ging over datalekken met hacking, malwaren en/of phishingincidenten. Dit type datalek komt het meest voor in de sector zakelijke dienstverlening (16%) gevolgd door de zorgsector (13%), de sectoren ICT-dienstverlening en onderwijs (beiden 11%), en de sector Handel en autobranche (9%).

TIP: voorkomen van datalekken

In de bijlage bij deze rapportage, en op de campagnewebsite hulpbijprivacy.nl, vindt u enkele praktische tips over hoe u de bovengenoemde typen datalekken kunt voorkomen, en/of de eventuele schade als gevolg van deze datalekken kunt beperken.

Aard van de gegevens

De meeste datalekken in de eerste helft van 2019 hadden betrekking op naam (11.161), geslacht (7.373) en contactgegevens (6.739). In 2018 was dit ook het geval. De AP ontving daarnaast een behoorlijk aantal meldingen over datalekken met gegevens over de gezondheid (4.255). In 3.456 gevallen ging het om Burgerservicenummers (BSN). Datalekken met BSN vonden vooral plaats in de sectoren zorg (37%) en in de sector openbaar bestuur (36%). Tot slot vonden 409 datalekken plaatst met kopieën van paspoorten en/of legitimatiebewijzen.

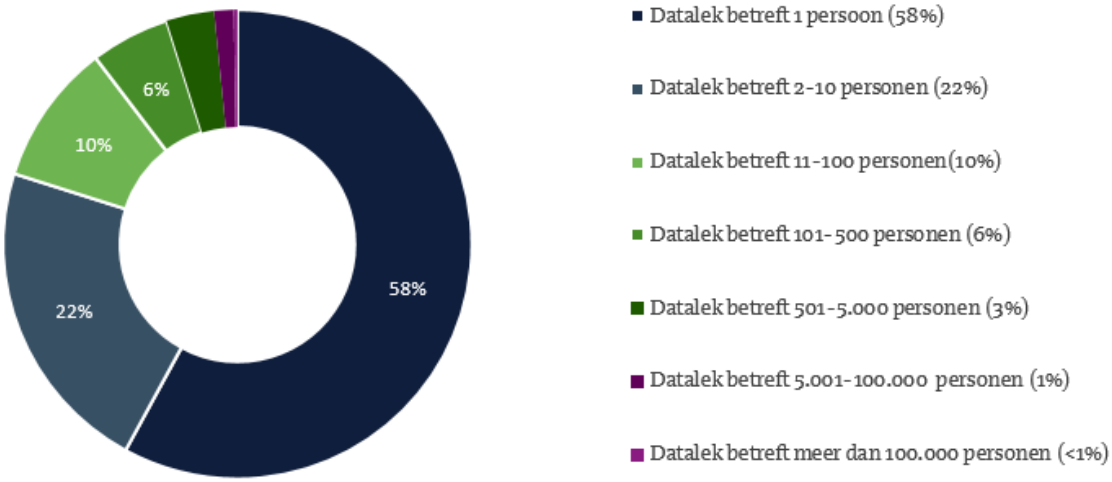
Gegevens over de gezondheid zijn over het algemeen zeer gevoelig. Wanneer dit soort gegevens getroffen worden door een datalek zal er over het algemeen sprake zijn van een hoog risico voor de betrokkenen.

Dit geldt ook voor datalekken waarbij het BSN getroffen is, met name wanneer daarnaast ook nog aanvullende persoonsgegevens zijn gelekt. Wanneer het BSN in combinatie met andere persoonsgegevens in handen komt van onbevoegden kunnen de betrokkenen een risico lopen op (identiteits-)fraude. Hetzelfde geldt voor datalekken met kopieën van paspoorten en legitimatiebewijzen. Houd er daarom rekening mee dat u het datalek moet melden aan de AP en aan de betrokkenen.

TIP: Gevoelige gegevens

Medische gegevens en Burgerservicenummer zijn gevoelig. Houd er rekening mee dat dit soort datalekken gemeld moeten worden aan de AP.

Maximum aantal betrokkenen



Meestal 1 persoon betrokken

In de ruime meerderheid van de gevallen, namelijk 58 procent, raakt het datalek 1 persoon. Het gaat in deze gevallen meestal om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger (78 procent). In 1,6 % van de gevallen treft het datalek een zeer groot aantal betrokkenen. Datalekken die 5.000 of meer personen raken, worden vaak (in 47% van de gevallen) veroorzaakt door hacking, malware en/of phishing.

Niet gemelde en te laat gemelde datalekken

De AP merkt dat, net zoals in 2018, niet alle meldplichtige datalekken door organisaties worden gemeld. Dat wordt bijvoorbeeld duidelijk als betrokkenen melding maken van een (meldplichtig) datalek, terwijl dat door de organisatie zelf niet is gemeld. In de eerste helft van 2019 zijn 17 onderzoeken in uitvoering bij organisaties die (mogelijk) een meldplichtig datalek niet hebben gemeld. Deze onderzoeken kunnen mogelijk leiden tot een sanctie.

Belang van de meldplicht aan de AP en aan betrokkenen

De meldplicht stelt de AP onder meer in staat om te controleren of er adequaat op de inbreuk is gereageerd, of de inbreuk is beëindigd, of de genomen of aangekondigde beveiligingsmaatregelen voldoende zijn om nieuwe inbreuken te voorkomen, en of de personen die zijn getroffen door het datalek moeten worden geïnformeerd, en zo ja, of de organisatie dat heeft gedaan of nog gaat doen. Met de meldplicht aan de betrokkene is beoogd de betrokkene op de hoogte te stellen van wat er met diens gegevens is gebeurd, en de consequenties die dat voor zijn belangen heeft. Hierdoor kan de getroffen persoon, voor zover dat mogelijk is, zich tegen de gevolgen wapenen door bijvoorbeeld extra voorzorgsmaatregelen te treffen.

Te laat gemelde datalekken

De AP merkt dat niet alle meldplichtige datalekken door organisaties op tijd worden gemeld. Dat wordt bijvoorbeeld duidelijk wanneer uit een melding blijkt dat de organisatie al langer dan 72 uur op de hoogte was van het datalek. Of wanneer uit een tip of klacht blijkt dat de organisatie al eerder op de hoogte was. De AP beschouwt dit als een ernstige zaak. In de eerste helft van 2019 zijn vier onderzoeken gestart naar aanleiding van een te laat gemeld datalek. In de tweede helft van 2019 zal de AP zich meer focussen op deze te laat gemelde datalekken. Onderzoeken die daaruit voortvloeien zullen mogelijk tot sancties leiden.

Belang van op tijd melden aan de AP

U dient een meldplichtig datalek, voor zover mogelijk, te melden binnen 72 uur nadat u het datalek ontdekt heeft. Het is belangrijk dat u een datalek op tijd meldt. Soms lopen betrokkenen als gevolg van een datalek direct risico op schade. Dan is het belangrijk dat betrokkenen zo snel mogelijk worden gewaarschuwd en dat er onmiddellijk maatregelen worden genomen om de gevolgen van het datalek te beperken. Door op tijd te melden stelt u de AP in de gelegenheid om snel in te grijpen, indien uit de melding blijkt dat het besluit om betrokkenen niet te informeren niet correct is, bijvoorbeeld, omdat de risico's van het datalek worden onderschat. Of wanneer uit de melding blijkt dat u onvoldoende maatregelen heeft genomen om de gevolgen van het datalek te beperken of om nieuwe datalekken te voorkomen. Door tijdig te melden kan de AP dus snel ingrijpen wanneer dat nodig is. Daardoor worden de betrokkenen beter beschermd.

Acties AP

Bij 502 datalekmeldingen is actie ondernomen richting organisaties die een datalek gemeld hebben. Daarbij ging het om verschillende soorten acties:

- In 84 procent van de gevallen is telefonisch contact opgenomen met de meldende organisatie om aanvullende vragen te stellen over het datalek,
- In 5 procent van de gevallen is schriftelijk contact opgenomen met de meldende organisatie om aanvullende informatie op te vragen over het datalek,
- In 10 procent van de gevallen is een normuitleggende brief gestuurd en
- In 1 procent van de gevallen is een gesprek gevoerd met de organisatie, waarbij op de privacyregels wordt gewezen en zo nodig op maatregelen wordt aangedrongen.
- Er zijn 17 onderzoeken in uitvoering bij organisaties die (mogelijk) een meldplichtig datalek niet hebben gemeld. Deze onderzoeken kunnen mogelijk leiden tot een sanctie.
- Er zijn 4 onderzoeken gestart naar aanleiding van een te laat gemeld datalek.

Wat doet de AP met een datalekmelding?

De AP kijkt zorgvuldig naar alle ontvangen meldingen van datalekken. Gelet op het grote aantal meldingen dat wij jaarlijks ontvangen, kunnen wij niet alle meldingen even uitgebreid onderzoeken.

Wanneer uit uw melding blijkt dat de meldplicht goed is nageleefd en voldoende maatregelen zijn genomen krijgt de meldende organisatie geen reactie. Als de AP inhoudelijke vragen heeft over de melding neemt de AP in de meeste gevallen binnen 2 weken contact met u op.

Acties naar aanleiding van een datalek

Afhankelijk van de situatie kan de AP het volgende te doen na melding van een datalek:

- u bellen voor meer informatie over het datalek;
- een inlichtingenverzoek doen. Bijvoorbeeld om het rapport van uw onderzoek naar het datalek op te vragen;
- u bellen om u extra uitleg en advies te geven;
- u een brief sturen met extra uitleg over de normen en hoe te handelen bij datalekken;
- u verplichten om de betrokken personen te informeren wanneer u dat onterecht niet heeft gedaan;
- een kortlopend onderzoek starten bij een mogelijke overtreding van de meldplicht. Bijvoorbeeld wanneer u een datalek niet heeft gemeld aan de AP. Of te laat heeft gemeld.
- een diepgaander onderzoek starten. Bijvoorbeeld naar het naleven van de verplichting om passende maatregelen te nemen om persoonsgegevens te beveiligen.
- de melding sluiten. Wanneer uit uw melding blijkt dat u de meldplicht goed heeft nageleefd en voldoende maatregelen zijn genomen om nieuwe inbreuken te voorkomen.

Toezichtbeleid AP

Het aantal datalekmeldingen is in 2019 opnieuw toegenomen ten opzicht van 2018. Het aantal meldingen lijkt sinds enkele maanden ongeveer gelijk te blijven (circa 2.000 meldingen per maand). Om het gestegen aantal datalekmeldingen, en signalen over niet gemelde datalekken, grondig te kunnen onderzoeken zal de capaciteit van de AP moeten groeien. In de tweede helft van 2019 zullen door de AP meer onderzoeken gestart worden naar niet gemelde datalekken en te laat gemelde datalekken. Ook zal in de tweede helft van 2019 gestart worden met een project om het huidige meldformulier te vernieuwen en gebruiksvriendelijker te maken.

Meldplicht datalekken facts & figures zorgsector

Aantal meldingen eerste helft 2019	Top 3 organisaties die het meest melden	Meest voorkomende inbreuk
3.747	1. Ziekenhuizen 2. Apotheken 3. Bevolkings-onderzoek	62% persoonsgegevens verstuurd aan verkeerde ontvanger

Aantal meldingen zorgsector

In de eerste helft van 2019 ontving de AP 3.747 meldingen van datalekken in de zorgsector. Dit aantal is licht gestegen (1,1%) ten opzichte van het aantal meldingen dat de AP in het laatste half jaar van 2018 uit de zorgsector ontving.

De zorgsector is sinds de invoering van de meldplicht datalekken in Nederland op 1 januari 2016 de sector die de meeste datalekmeldingen doet van alle sectoren. Daarbij speelt een rol dat zorginstellingen grote hoeveelheden gevoelige (medische) persoonsgegevens verwerken. Datalekken die plaatsvinden binnen de zorg zullen daardoor vaak een risico opleveren voor de betrokkenen, en dus gemeld moeten worden aan de AP.

Meldingen datalekken in de zorgsector

Zorg	Percentage
Ziekenhuizen	23%
Apotheken	22%
Bevolkingsonderzoek	9%
GGZ-instellingen en verslavingsklinieken	6%
Zorgverzekeraars	5%
Verpleeghuizen en verzorgingshuizen	5%
Jeugdzorg	4%
Maatschappelijke dienstverlening	3%
Huisartsen	3%
Psychiaters, psychologen en pedagogen	1%
Tandartsen	1%
Fysiotherapeuten	1%
Overig* waaronder laboratoria/diagnostische centra, gehandicaptenzorg, arbodiensten etc.	17%

Het grootste aantal datalekmeldingen binnen de zorgsector is afkomstig van ziekenhuizen (23%), apotheken (22%) en stichtingen die bevolkingsonderzoek uitvoeren (9%). Ook in 2018 waren dit de instellingen met de meeste meldingen in de zorg. Bij de meeste meldingen in de zorgsector (65%) ging het om een datalek met één betrokkene. In ongeveer 1% van de gevallen ging het om een datalek met 5.000 of meer betrokkenen.

Phishing bij ziekenhuizen

De AP heeft opnieuw meerdere datalekmeldingen ontvangen van ziekenhuizen die getroffen zijn door phishing. Vaak worden bij phishingaanvallen nep-e-mails verstuurd aan alle medewerkers van een organisatie. In de mail wordt dan gevraagd om inloggegevens in te voeren op een nep-website. Wanneer een nietsvermoedende medewerker zijn gegevens vervolgens invoert, krijgt de hacker toegang tot het account van die medewerker. Meestal wordt dat account dan gebruikt om nieuwe phishing mails te sturen, soms wordt ook de complete inhoud van de mailbox van de medewerker gekopieerd door de hacker. Omdat ziekenhuizen relatief grote organisaties zijn met veel medewerkers, is de kans op een geslaagde phishing aanval daardoor groter. Soms kan het voorkomen dat meerdere medewerkers binnen een ziekenhuis reageren op een phishingmail, waaronder verpleegsters en artsen. De hacker krijgt dan ook toegang tot de inhoud van de mailbox van deze medewerkers, die vaak medische persoonsgegevens bevatten van patiënten.

Voorbeeld datalek: Phishing bij ziekenhuis

Een ziekenhuis is getroffen door een phishingaanval. Diverse medewerkers van het ziekenhuis hebben op een phishingmail geklikt en vervolgens hun inlognaam en wachtwoord ingevoerd. Hierdoor hebben hackers toegang gekregen tot de e-mailaccounts van de betreffende medewerkers, en zijn via deze accounts vervolgens grote hoeveelheden vergelijkbare phishing e-mails verstuurd. Het ziekenhuis meldt het datalek aan de AP. In de melding wordt aangegeven dat het ziekenhuis een extern bureau heeft ingehuurd om onderzoek te doen naar het datalek.

De AP neemt naar aanleiding van de melding contact op en stelt aanvullende vragen. Onder andere of er (mogelijk) toegang is geweest tot de gegevens in de e-mailbox van de getroffen medewerkers en welke maatregelen de organisatie neemt om phishing in de toekomst te voorkomen. Ook vraagt de AP het onderzoeksrapport op van het externe bureau. Daaruit blijkt dat het mogelijk is dat de hackers door de verkregen toegang tot het e-mailaccount, ook inzage hebben gehad in de inhoud van de mailboxen. Daarin stonden gegevens van patiënten. De AP neemt naar aanleiding van de ontvangen informatie opnieuw contact op met het ziekenhuis. Naar aanleiding van dit contact informeert het ziekenhuis de betrokken patiënten, onder meer via een mededeling op de website, advertenties in de media en per e-mail. Ook neemt het ziekenhuis extra maatregelen om nieuwe phishingaanvallen te voorkomen, en de gevolgen van inbreuken te beperken, waaronder het toepassen van multi-factor authenticatie, het onderhouden van een incident response plan, het trainen van security awareness van medewerkers, en het continu monitoren op gelekte accounts met behulp van de Managed Intelligence Service.

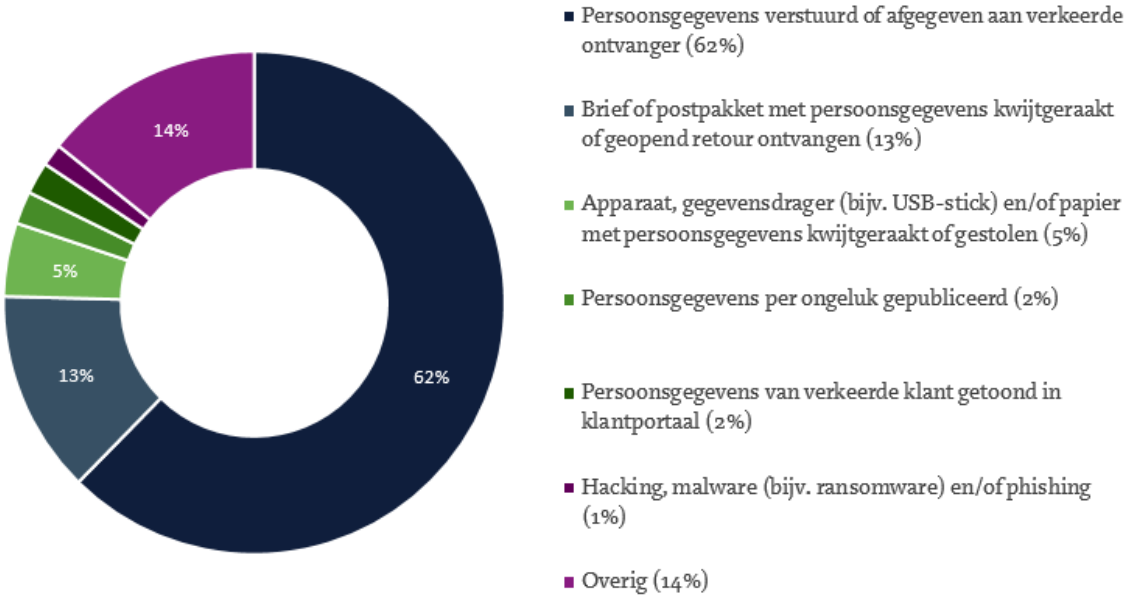
Autorisaties bij ziekenhuizen

Een ziekenhuis moet alle technische en organisatorische maatregelen treffen om ervoor te zorgen dat patiëntgegevens veilig zijn. Patiëntdossiers moeten daarom ook intern goed beveiligd worden. Wanneer dit niet goed is geregeld kan dat ertoe leiden dat ziekenhuismedewerkers in medische dossiers kunnen kijken van patiënten waarmee ze geen behandelrelatie hebben.

Haga beboet voor onvoldoende interne beveiliging patiëntendossiers

In juli 2019 rondde de AP een onderzoek af bij het HagaZiekenhuis. Uit dat onderzoek bleek dat het ziekenhuis de interne beveiliging van patiëntendossiers niet op orde had. De AP heeft het HagaZiekenhuis voor de onvoldoende beveiliging een boete opgelegd van 460.000 euro.

Type datalekken in de zorg



Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

Bij alle zorgorganisaties, met uitzondering van de stichtingen die bevolkingsonderzoek uitvoeren, komt het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger, verreweg het meeste voor. Dit type datalek komt met name voor bij apotheken (30%) en bij ziekenhuizen (26%). Bij apotheken komt het regelmatig voor dat recepten of pakketjes met medicijnen door menselijke fouten worden verwisseld, waardoor gegevens over medicijngebruik bij de verkeerder ontvanger terecht komen.

TIP : Beveiligd e-mailen

De AP merkt dat sommige zorginstellingen gevoelige persoonsgegevens, zoals gegevens over (jeugd)zorg of medische gegevens, onbeveiligd e-mailen naar externe partijen. Door menselijke fouten kunnen deze gegevens bij een verkeerde ontvanger terecht komen, bijvoorbeeld door een typefout in het e-mailadres, of door een verkeerde geadresseerde aan te klikken. Dit soort incidenten kan voorkomen worden door de gevoelige gegevens als bijlage op te nemen in het e-mailbericht en deze bijlage te versleutelen met een wachtwoord. Of door de communicatie via een beveiligd portaal te laten verlopen.

TIP: Betrouwbare ontvanger

In de zorg worden regelmatig door menselijke fouten, of door verouderde of onjuiste contactgegevens, medische gegevens van personen verstuurd aan een verkeerde zorginstelling, apotheek of huisarts. Dit zijn professionele partijen met een medisch beroepsgeheim. In de meeste gevallen kunt u er vanuit gaan dat dergelijke partijen zorgvuldig zullen omgaan met de onterecht ontvangen gegevens, waardoor de risico's van het datalek beperkt zijn. Is dit het geval, dan hoeft u het datalek niet te melden aan de AP of aan de betrokkenen. Wel moet u het incident altijd registreren in uw interne datalekkenregister. Meer informatie over deze uitzondering op de meldplicht vindt u onder de Q&A's op de website van de AP .

Datalekken met post

In 13 procent van de datalekmeldingen in de zorg gaat het om een brief of postpakket dat is kwijtgeraakt, of geopend retour ontvangen. Dit gebeurt in de meeste gevallen (86%) bij stichtingen die bevolkingsonderzoek uitvoeren. Het gaat dan om brieven met uitslagen van bevolkingsonderzoek.

Datalekken met mobiele apparatuur

Datalekken als gevolg van verloren of gestolen mobiele apparatuur met daarop persoonsgegevens komen binnen de zorgsector het meest voor bij diverse (kleinere) overige zorginstellingen (32%) en bij ziekenhuizen (21%). Daarbij speelt een rol dat kleinere zorginstellingen over het algemeen minder volwassen zijn op het gebeid van informatiebeveiliging dan grotere (professionelere) zorginstellingen, en zijn zich daardoor minder bewust van de risico's van het opslaan van persoonsgegevens van patiënten op mobiele apparatuur.

Voorbeeld datalek: Gestolen laptop

Een zorginstelling meldt een datalek bij de AP als gevolg van een inbraak in de privéauto van een medewerker. Daarbij zijn de tas en de laptop van de medewerker gestolen. In de tas zaten dossiers met functioneringsgesprekken en kopieën van paspoorten van enkele werknemers. Op de laptop stonden medische gegevens van patiënten. De laptop was beveiligd met een wachtwoord, de gegevens op de laptop waren versleuteld. Nadat de inbraak werd ontdekt is de laptop direct op afstand gewist. Het risico voor de patiënten is gering, de patiënten worden daarom niet geïnformeerd. In de melding wordt verder aangegeven dat de werknemers waarvan gegevens in de papieren dossiers stonden ook niet zullen worden geïnformeerd, omdat de dieven volgens de zorginstelling alleen uit waren op de laptops en niet op de dossiers.

De AP verstuurt naar aanleiding van de melding een brief aan de zorginstelling en wijst hierin onder meer op de gevoeligheid van de gesprekverslagen en het risico op identiteitsfraude als gevolg van het verlies van de paspoort kopieën. De zorginstelling besluit naar aanleiding van de brief de medewerkers alsnog te informeren en bevestigt dit aan de AP. Verder kondigt de zorginstelling aan om alle personeelsdossiers te digitaliseren, en wordt het beleid om geen dossiers met persoonsgegevens mee naar huis te nemen aangescherpt en opnieuw onder de aandacht van het personeel gebracht.

TIP: Versleutelen

Soms ontvangt de AP meldingen van organisaties die bijzondere persoonsgegevens, bijvoorbeeld medische gegevens, zonder versleuteling opslaan op werklaptops. Een datalek kan dan plaatsvinden omdat de laptop wordt gestolen. De laptop alleen beveiligen met een wachtwoord is niet genoeg. De dief kan de harde schijf namelijk verwijderen uit de laptop en op deze wijze alsnog toegang krijgen tot de gegevens.

Wanneer u draagbare apparatuur gebruikt, zoals tablets, telefoons, laptops of USB-sticks, zorg dan dat gevoelige en/of bijzondere persoonsgegevens, zoals medische gegevens, altijd versleuteld zijn opgeslagen. Zo beperkt u de risico's voor de betrokkenen, wanneer u een draagbaar apparaat verliest of wanneer deze wordt gestolen.

Datalekken door hacking, malware en/of phishing

In de zorgsector worden datalekken door hacking, malware en/of phishing relatief vaak gemeld door kleinere zorginstellingen, in vergelijking met andere (grotere) zorginstellingen. Dit type datalek wordt met name veel gemeld door (kleinere) gezondheids- en welzijnsorganisaties (24%), maatschappelijke dienstverlening (15%) en tandartsen (6%). Daarbij speelt een rol dat dat kleinere zorginstellingen vaak minder kennis hebben over informatiebeveiliging en ICT, en minder financiële middelen tot hun beschikking hebben om passende beveiligingsmaatregelen te nemen en de beveiliging up-to-date te houden. Malware, zoals ransomware, kan dan makkelijker binnenkomen op de systemen. Dit kan grote schade gevolg hebben, met name wanneer geen recente back-ups beschikbaar zijn van de getroffen gegevens.

Voorbeeld datalek: ransomware bij tandartsenpraktijk

Een organisatie doet een datalekmelding bij de AP waarin zij aangegeven dat ze zijn getroffen door een ransomware-aanval op de hoofdserver. Door de hackaanval zijn alle gegevens op de server versleuteld en daardoor niet meer benaderbaar. Op de computer stonden persoonsgegevens van alle patiënten en medewerkers van de praktijk opgeslagen, waaronder gegevens over de behandeling en Burgerservicenummers (BSN) van de patiënten. De tandarts beschikte nog over een back-up van de gegevens. De tandarts geeft aan dat de betrokkenen niet zullen worden geïnformeerd. Alle gegevens zijn immers nog beschikbaar.

De AP neemt naar aanleiding van de melding contact op en stelt aanvullende vragen. Bijvoorbeeld of er onderzoek is gedaan naar het type ransomware dat op de server stond. Ransomware kan naast versleutelen namelijk ook als functionaliteit hebben dat de gegevens worden gekopieerd en weggezonden.
De tandarts laat, naar aanleiding van de brief van de AP, een onderzoek uitvoeren door een extern bureau. Daarbij wordt vastgesteld dat er verhoogd uitgaand netwerkverkeer heeft plaatsgevonden ten tijde van de inbreuk. Er kan niet worden uitgesloten dat het virus de gegevens heeft gekopieerd en weggesluisd. De tandarts besluit daarom de patiënten alsnog te informeren over het datalek.

5 tips voor zorginstellingen om een datalek te voorkomen

Zorginstellingen kunnen bepaalde maatregelen nemen om de kans op een datalek te verkleinen, of de gevolgen ervan te beperken. Met deze maatregelen kunt u een aantal veel voorkomende typen datalekken voorkomen.

Door menselijke fouten kunnen medische gegevens bij een verkeerde ontvanger terecht komen, bijvoorbeeld door een typefout in het e-mailadres, of door een verkeerde geadresseerde aan te klikken.

- Dit kunt u voorkomen door ervoor te kiezen om de gevoelige gegevens als bijlage op te nemen in het e-mailbericht en deze bijlage te versleutelen met een wachtwoord.
- Dit wachtwoord kunt u vervolgens via een apart kanaal (bijvoorbeeld door te bellen of per SMS) doorgeven aan de ontvanger.
- U kunt zich ook afvragen of e-mail wel het juiste digitale communicatie middel is om dit soort gevoelige gegevens te versturen en bijvoorbeeld overwegen om communicatie via een portaal te organiseren.

Gevoelige dossiers zoals medische dossiers, (jeugd)hulpdossiers, en verslagen over behandeltrajecten worden weleens meegenomen naar huis, bijvoorbeeld in het kader van thuiswerken. Dossiers worden per abuis verloren, vergeten in de trein, of soms zelfs gestolen.

- Voorkom dit door nooit gevoelige papieren zorgdossiers mee naar huis te nemen.
- Scan de dossiers op kantoor en bewaar deze op een beveiligde (versleutelde) harde schijf, USB-stick of in een veilig documentmanagementsysteem binnen het IT-netwerk van uw organisatie. U kunt in het laatstgenoemde geval de dossiers dan thuis raadplegen wanneer u inlogt op de beveiligde netwerkomgeving.

Zorginstellingen slaan soms medische gegevens van patiënten lokaal op draagbare apparatuur, zoals tablets, smartphones, laptops of USB-sticks op. Medewerkers nemen deze gegevensdragers weleens mee naar huis. Met risico's op verlies en diefstal waardoor persoonsgegevens in verkeerde handen kunnen vallen.

- Voorkom dit door geen medische gegevens op te slaan op draagbare apparatuur.
- Maakt u wel gebruik van draagbare apparatuur? Zorg dan dat u deze persoonsgegevens altijd versleuteld opslaat. Zo beperkt u de risico's voor de betrokkenen, wanneer u een draagbaar apparaat verliest of wanneer deze wordt gestolen.

Zorginstellingen, met name ziekenhuizen, zijn vaak doelwit zijn van dit phishing-aanvallen. Daardoor kan een hacker toegang krijgen tot het account van de medewerker. Vaak misbruiken hackers het account vervolgens om nieuwe phishing- of spamberichten te versturen. Dat kan tot nieuwe inbreuken leiden, en/of tot (financiële) schade voor de betrokkenen.

- Verklein de kans op phishing-aanvallen door uw medewerkers bewust te maken van phishing.
- Zorg ervoor dat medewerkers phishing e-mails kunnen herkennen.
- Installer goede firewalls en update deze tijdig, zodat u ongewenste e-mailberichten, zoals spam- en phishing berichten, zoveel mogelijk kunt onderscheppen en blokkeren.

Met name kleinere zorginstellingen en zorgverleners zoals fysiotherapeuten en huisartsen worden regelmatig getroffen door ransomware. Vaak als gevolg van gebrekkige (kennis over) beveiliging. Als gevolg van ransomware kunnen de gegevens op uw systeem in handen komen van hackers, en kunt u permanent of tijdelijk de toegang tot uw gegevens verliezen.

Maatregelen waarmee u het risico op een datalek bijvoorbeeld door ransomware verkleint:

- Installeer software-updates op tijd
- Gebruik geen verouderde (netwerk)protocollen
- Zorg voor gesegmenteerde (gescheiden) computernetwerken en -systemen
- Maak regelmatig back-ups te zodat u altijd beschikking heeft tot de persoonsgegevens, ook wanneer u getroffen wordt door een ransomware-aanval.