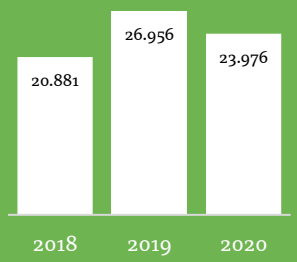
AUTORITEIT
PERSOONSGEGEVENS

# Meldplicht datalekken: facts & figures
# Overzicht feiten en cijfers 2020

| Aantal meldingen | Meerjarentrend | Stijging meldingen hacking & malware |
|---|---|---|
| 23.976 |  | ↑ 30% |



## Introductie

### Minder meldingen, maar meer hacking, malware & phishing

In 2020 ontving de Autoriteit Persoonsgegevens (AP) 23.976 datalekmeldingen. Dat is een daling van 11% ten opzichte van 2019. Deze daling komt vooral omdat incassobureaus minder datalekken hebben gemeld. Doordat zij hun werkwijze hebben aangepast, zijn er namelijk veel minder betalingsherinneringen bij verkeerde ontvangers terechtgekomen.

Het aantal meldingen naar aanleiding van hacking, malware of phishing-incidenten is daarentegen gestegen met 30% vergeleken met 2019. Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken hier doelwit van te zijn. In 2019 was er ook een stijging, toen van 25% ten opzichte van 2018.

### Thema: meerfactorauthenticatie

De AP maakt zich zorgen over de blijvende stijging van het aantal meldingen naar aanleiding van hacking, malware of phishing-incidenten. Daarom heeft de AP ervoor gekozen om in deze rapportage extra aandacht te besteden aan meerfactorauthenticatie (MFA). MFA is een techniek waarbij de persoon of het systeem een combinatie van minimaal twee verschillende typen authenticatiefactoren moet gebruiken om toegang te krijgen. Bijvoorbeeld een wachtwoord én een eenmalige code (token) per sms.

De AP merkt op dat vooral bij dit type datalek MFA de impact van het datalek had kunnen beperken of zelfs had kunnen voorkomen. Naar schatting van de AP waren in 2020 minimaal 600.000 en maximaal 2.000.000

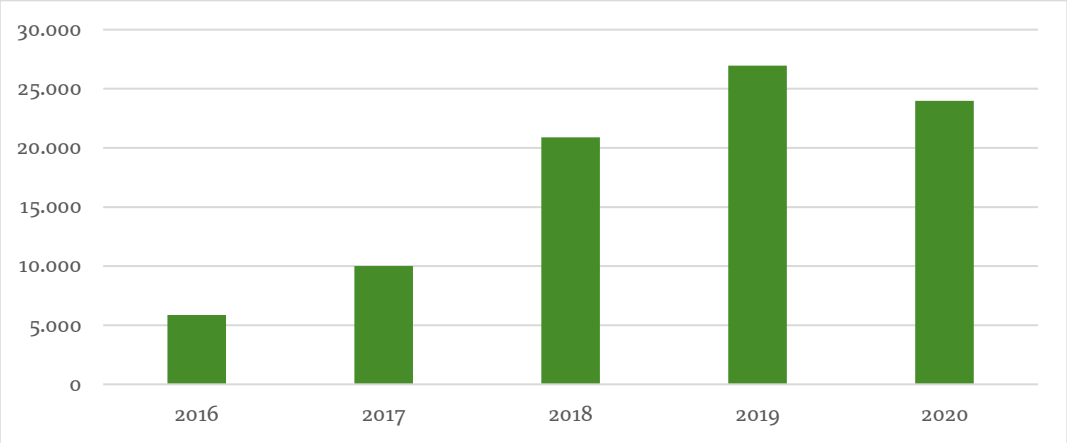
personen (mogelijk) betrokken bij een (gemeld) datalek dat voorkomen had kunnen worden met MFA. Meer over MFA treft u aan in het themablad op pagina 7.

# Cijfers 2020

## Aantal datalekmeldingen

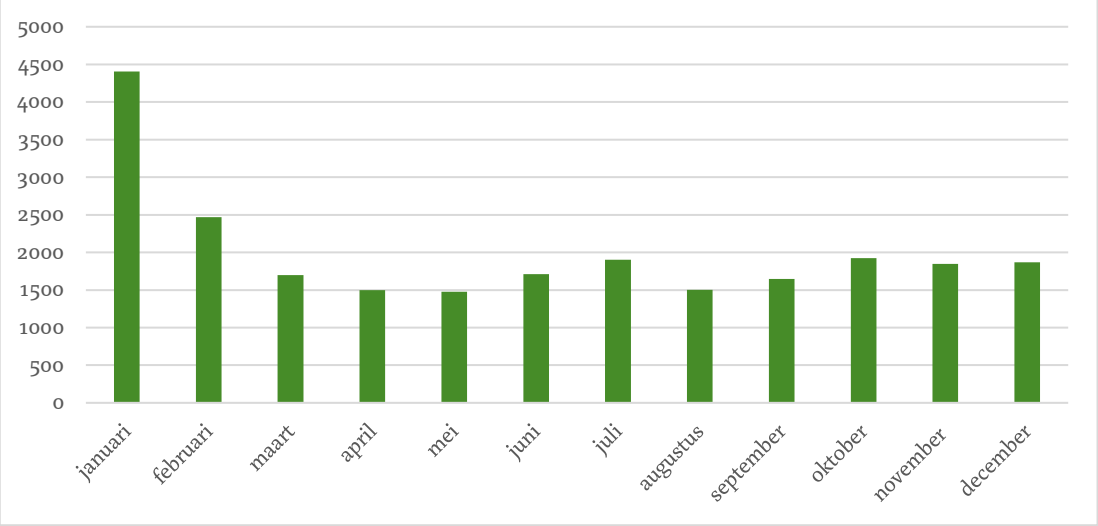
Nederland staat in de top 3 van Europese landen waar de meeste datalekken worden gemeld. Nederland is dan ook sterk gedigitaliseerd, waardoor het risico op (grote/ernstige) datalekken hier relatief hoog is. Dit betekent ook dat we in Nederland extra aandacht moeten hebben voor fundamentele vraagstukken als privacy, bescherming van persoonsgegevens en cybersecurity.

Onderstaande grafiek laat het verloop van het aantal datalekmeldingen sinds 2016 zien:




*Totaal aantal datalekmeldingen ontvangen door de AP 2016-2020*

Deze grafiek toont het aantal ontvangen datalekmeldingen per maand in 2020:

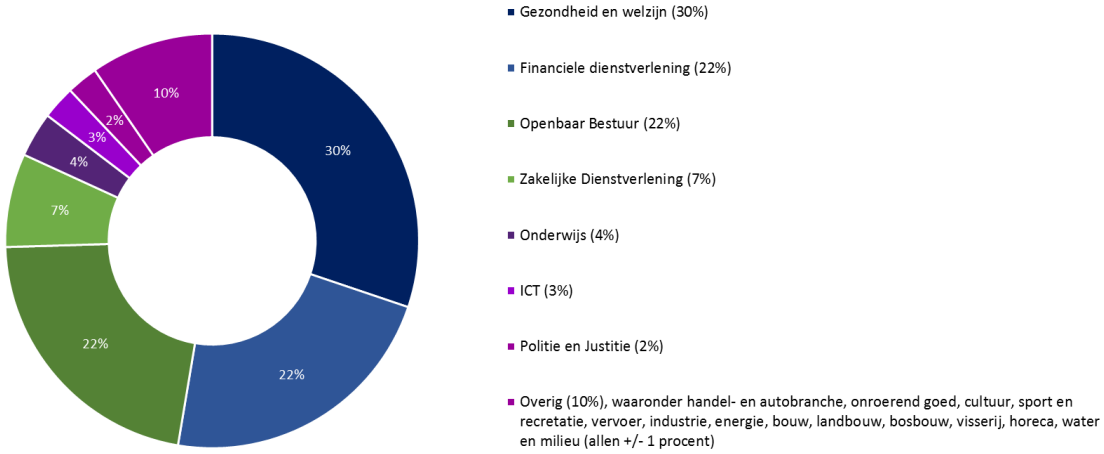



*Totaal aantal datalekmeldingen per maand ontvangen door de AP in 2020*

## Aantal grensoverschrijdende datalekmeldingen

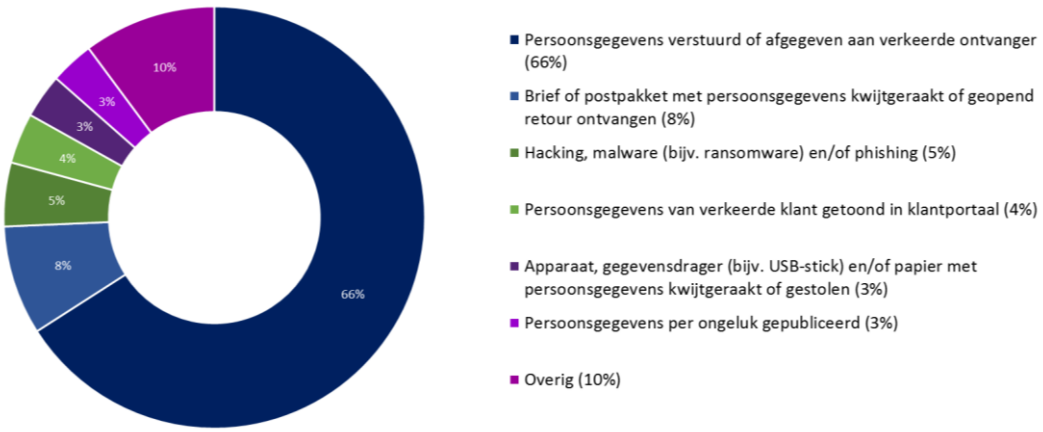
Naast de 23.976 Nederlandse datelekmeldingen die de AP heeft ontvangen, hebben andere Europese privacytoezichthouders in 79 gevallen een grensoverschrijdend datalek gedeeld met de AP. Dat gebeurt bijvoorbeeld als een datalek bij een andere Europese privacytoezichthouder is gemeld maar het datalek (mogelijk) ook gevolgen heeft voor betrokkenen in meerdere lidstaten, waaronder personen in Nederland. De AP deelt ook meldingen over grensoverschrijdende datalekken met andere toezichthouders. Dit gebeurde in 2020 11 keer.

## Aantal datalekmeldingen per sector




De meeste datalekmeldingen kwamen in 2020 uit de sector gezondheid en welzijn (30%), gevolgd door financiële dienstverlening en openbaar bestuur (beide 22%). Vergeleken met 2019 is het aantal meldingen vanuit de zorg gedaald met 4%, vanuit de financiële sector gedaald met 34% en vanuit de overheid gestegen met 13%. De stijging bij de overheid komt vooral doordat er meer persoonsgegevens zijn afgegeven of verstuurd aan een verkeerde ontvanger.

## Type datalekken



Net als in de afgelopen jaren worden de meeste datalekken veroorzaakt doordat persoonsgegevens naar een verkeerde ontvanger gaan. De stijging van het aantal meldingen vanuit de overheid komt hoofdzakelijk door dit type datalek.

## Uitgelicht: datalekken door hacking, malware of phishing

In 2020 ontving de AP 1.173 meldingen over hacking, malware[1] of phishing[2]-incidenten. Dit is een stijging van 30% ten opzichte van 2019. Bij 41,5% van de meldingen werden meer dan 500 personen getroffen. Dit type datalek komt het meest voor in de sector gezondheid en welzijn (13%) gevolgd door onderwijs (11%), ICT-dienstverlening (9%) en handel en autobranche (8%). Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken doelwit van hacking, malware of phishing.

**Voorbeeld phishing bij onderwijsinstelling**

Een onderwijsinstelling kreeg van een softwareleverancier (verwerker) te horen dat deze slachtoffer was geworden van phishing. Daardoor hadden onbevoegde personen toegang gekregen tot de mailbox van een medewerker van deze leverancier. Vanuit die mailbox waren weer nieuwe phishingmails gestuurd, onder meer naar deze onderwijsinstelling. Zo was toegang verkregen tot de inbox van de onderwijsinstelling. Onbevoegden hadden hierdoor toegang tot NAW-gegevens, contactgegevens en toegangs- of identificatiegegevens van duizenden betrokkenen bij de onderwijsinstelling. In deze mailbox stonden ook enkele kopieën van paspoorten en andere legitimatiebewijzen van docenten.

**Aangekondigde technische en organisatorische maatregelen**

De onderwijsinstelling heeft de wachtwoorden gewijzigd en op virussen en malware gescand. Daarnaast is MFA doorgevoerd, om dit soort incidenten in de toekomt te voorkomen. Na het invoeren van MFA hebben medewerkers nu ook een aparte token/code nodig om te kunnen inloggen.

## Risico's bij hacking, malware of phishing

Uit het rapport *Cybersecuritybeeld Nederland (CBSN) 2020*, opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC), blijkt dat het aantal ransomware-aanvallen in het afgelopen jaar waarneembaar is toegenomen.[3] De Nederlandse politie ziet dat ransomware het sluitstuk van een cyberaanval kan zijn.

Ook de AP ziet bij steeds meer meldingen dat hackers al langere tijd in een netwerk aanwezig zijn. Zij gebruiken deze tijd om het netwerk van de organisatie te verkennen en de bedrijfskritieke onderdelen te

[1] Malware is kwaadaardige software. Een bekend voorbeeld van malware is ransomware. Dit is 'gijzelsoftware' die de databestanden van gebruikers versleutelt. Meestal wordt daarna betaling geëist, bijvoorbeeld via prepaidkaarten of Bitcoin, in ruil voor het ontsleutelen van de databestanden. Besmetting verloopt vaak via besmette bestanden, zoals een e-mailbijlage, of via advertenties op internet die een lek in niet-geüpdatete software misbruiken.

[2] Phishing is een verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Een bekend voorbeeld van phishing is mensen oplichten door hen naar een valse website te lokken, die een kopie is van de echte website, om hen daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer te laten invullen. Hierdoor onderschept de fraudeur/hacker de gegevens.

[3] Nationaal Coördinator Terrorismebestrijding en Veiligheid, Cybersecuritybeeld Nederland (CSBN 2020), p. 16.

lokaliseren. Daarnaast proberen de hackers meer bevoegdheden te krijgen in het netwerk door administratorrechten te verkrijgen, waarna zij de ransomware-aanval uitvoeren.

Omdat hackers steeds vaker langer in netwerken en systemen zitten voordat zij toeslaan of worden opgemerkt, kunnen organisaties bij een ransomware-incident er niet van uitgaan dat alleen ransomware is geïnstalleerd op hun systemen. Hackers kunnen tijdens hun aanwezigheid in het netwerk ook gegevens hebben gekopieerd, vernietigd of gewijzigd. Ook kunnen hackers malware hebben geïnstalleerd, waardoor ze op een later moment eenvoudig weer toegang kunnen krijgen tot het netwerk of systeem.

Hierdoor kan vaak alleen na digitaal forensisch onderzoek vastgesteld worden welke persoonsgegevens zijn getroffen door het datalek en wat er met deze gegevens is gebeurd. Pas na een dergelijk aanvullend onderzoek is het mogelijk om de gevolgen voor de betrokkenen goed in te schatten. Bovendien kan met aanvullend onderzoek bepaald worden of alle malware van de hackers is verwijderd uit het netwerk of de systemen, zodat zij niet later nogmaals kunnen toeslaan. Malware kan bijvoorbeeld (nog steeds) in een back-upbestand zitten of nog in het systeem aanwezig zijn, vermomd als legitieme software.

**Datalekken door hacking, malware of phishing altijd melden**
Datalekken door hacking, malware of phishing kunnen grote risico's opleveren voor de betrokkenen. Ook wanneer alleen namen en e-mailadressen zijn getroffen. Deze gegevens kan de hacker namelijk misbruiken om nieuwe spam- en phishingaanvallen uit te voeren. Houd er rekening mee dat u dit soort datalekken over het algemeen moet melden aan de AP en aan de betrokkenen. Meld dit soort incidenten altijd op tijd (binnen 72 uur na ontdekking). Wanneer u het incident direct meldt, kan de AP controleren of u de risico's van het incident goed heeft ingeschat. En kan de AP, indien nodig, direct contact met u opnemen over het datalek.

# Acties AP

## Interventies bij niet gemelde datalekken

De AP merkt dat organisaties, net als in 2018 en 2019, nog steeds niet alle datalekken melden die zij zouden moeten melden. Dat wordt bijvoorbeeld duidelijk als betrokkenen bij de AP een klacht of tip achterlaten over een (meldplichtig) datalek, dat door de organisatie zelf niet gemeld blijkt te zijn.

In 2020 heeft de AP 10 onderzoeken afgerond in zaken waarbij (mogelijk) een meldplichtig datalek niet is gemeld. Deze onderzoeken hebben geleid tot een ofwel een waarschuwende brief, ofwel een normoverdragend gesprek. Onderzoeken kunnen ook leiden tot sancties. Op dit moment lopen er nog 9 onderzoeken.

## Interventies bij te laat gemelde datalekken

De AP merkt ook dat organisaties niet alle meldplichtige datalekken op tijd melden. 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 klacht of tip blijkt dat de organisatie al eerder op de hoogte was. De AP beschouwt dit als een ernstige zaak.

De meldplicht is onder meer bedoeld als stimulans voor organisaties om direct actie te ondernemen om (de oorzaak van) het datalek aan te pakken, de gevolgen ervan te beperken, de getroffen persoonsgegevens te herstellen als dat kan en de AP om advies te vragen, onder andere over de vraag of het besluit de betrokkenen wel of niet te informeren correct was.[4] Daarnaast stelt de meldplicht de AP in staat snel in te grijpen wanneer betrokkenen ten onrechte niet worden geïnformeerd of onvoldoende onderzoek is gedaan naar de omvang van het datalek.

In 2020 heeft de AP 3 onderzoeken afgerond naar aanleiding van een te laat gemeld datalek. De AP heeft in alle 3 de gevallen een waarschuwende brief gestuurd. Ook te laat melden kan leiden tot een sanctie.

## Overige acties

In 1.736 gevallen heeft de AP actie ondernomen. Dit kan naar aanleiding van datalekmeldingen zijn, maar ook als de AP een datatlek vermoedt door klachten, tips of andere datalekmeldingen.

Het ging hierbij om verschillende soorten acties:

- In 72% heeft de AP telefonisch contact opgenomen met de meldende organisatie om aanvullende vragen te stellen over het datalek, bijvoorbeeld omdat de datalekmelding onduidelijk was.
- In 10% heeft de AP een normoverdragende brief gestuurd. In zo'n brief legt de AP uit aan welke regels een organisatie zich moet houden en waarschuwt de AP dat bij nieuwe klachten een onderzoek kan volgen.
- In 15% heeft de AP een gesprek gevoerd met de organisatie. Daarbij heeft de AP op de privacyregels gewezen en, indien nodig, de organisatie verplicht om maatregelen te nemen, zoals het informeren van betrokkenen.
- In 1% heeft de AP schriftelijk contact opgenomen met een organisatie om aanvullende informatie op te vragen over een datalek.
- In 3 gevallen heeft de AP een normoverdragend gesprek op bestuursniveau gevoerd.

In 2020 heeft de AP bijna 2.500 klachten en tips van burgers ontvangen en beoordeeld over mogelijke datalekken. Niet elke klacht of tip leidt tot een interventie of een nader onderzoek door de AP. Bijvoorbeeld omdat het datalek al is gemeld of omdat er bij nader inzien geen sprake is van een datalek.

[4] EDPB, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, WP250rev.01, p. 18.

# Thema: meerfactorauthenticatie (MFA)

| Meldingen hacking & malware zonder MFA | Minimaal aantal betrokken personen | Maximaal aantal betrokken personen |
|---|---|---|
| 249 | 607.846 | 2.092.946 |

## Datalekken en MFA

De AP ontvangt veel datalekmeldingen in de categorie hacking, malware of phishing waarbij *geen* MFA als beveiligingsmaatregel is doorgevoerd. MFA had waarschijnlijk de impact van deze datalekken kunnen beperken en veel datalekken zelfs kunnen voorkomen.

In 2020 heeft de AP minstens 249 meldingen ontvangen waarbij MFA had kunnen voorkomen dat het datalek was ontstaan. Naar schatting werden minimaal 607.846 en maximaal 2.092.946 personen getroffen door een datalek wegens het ontbreken van MFA.

Van belang is dat MFA in veel gevallen een essentiële en daarmee verplichte maatregel is om aan de eisen te voldoen uit artikel 5, eerste lid, onder f, artikel 24 en artikel 32 AVG[5]. Het niet toepassen van MFA kan leiden tot een overtreding van de AVG. De AP zal de komende periode ook strenger toezien op het gebruik van MFA.

Vanzelfsprekend moet het gebruik van MFA niet op zichzelf worden gezien, maar als een *onderdeel* van de te nemen passende technische en organisatorische maatregelen, om een op het risico afgestemd beveiligingsniveau te kunnen waarborgen. Daarnaast kan nauwkeurig een data protection impact assessment (DPIA) uitvoeren en hieraan gevolg geven een positieve bijdrage leveren aan het voorkomen van datalekken.

[5] Algemene verordening gegevensbescherming. Te raadplegen op: VERORDENING (EU) 2016/ 679 VAN HET EUROPEES PARLEMENT EN DE RAAD - van 27 april 2016 - betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/ 46/ EG (algemene verordening gegevensbescherming) (autoriteitpersoonsgegevens.nl)

## MFA in het kort

Authenticatie is het beveiligingsmechanisme dat toegangscontrole regelt en vereist dat de (digitale) identiteit van een gebruiker of systeem wordt geverifieerd met een authenticatiemiddel. MFA is een techniek waarbij een persoon of systeem een combinatie van minimaal twee verschillende typen authenticatiefactoren moet gebruiken om toegang te krijgen.

Voorbeelden van MFA zijn:

- de combinatie van een wachtwoord én een eenmalige code (token) die per sms verstrekt wordt;
- de combinatie van een wachtwoord én een smartcard;
- het gebruik van een app of hardwaretoken die wisselende wachtwoorden genereert in combinatie met een wachtwoord of pincode.

### Authenticatiefactoren

Een authenticatiemiddel is gebaseerd op een van de authenticatiefactoren. De drie meest gebruikte authenticatiefactoren zijn:

- Iets wat je weet: deze authenticatiefactor is gebaseerd op een gegeven dat de persoon of het systeem weet, zoals een wachtwoord, pincode of andere unieke authenticatiecode, en die alleen bekend is aan de persoon of het systeem.
- Iets wat je hebt: deze authenticatiefactor is gebaseerd op een fysiek item dat de persoon heeft en kan gebruiken voor de authenticatie, zoals een smartcard, een token of een sleutel. Een (mobiele) telefoon behoort ook tot deze categorie en wordt vaak ingezet voor sms-tokens.
- Iets wat je bent: deze authenticatiefactor is gebaseerd op individuele karakteristieken. Dit kunnen biometrische eigenschappen zijn, zoals een vingerafdruk. Maar onder deze categorie vallen ook onderscheidende producten van handelingen, zoals een handtekening of kinetische metingen van een toetsenbord.

Andere authenticatiefactoren zijn:

- Waar je bent: deze authenticatiefactor is gebaseerd op een geografische bepaling, bijvoorbeeld door gebruik te maken van het IP-adres.
- Hoe je je gedraagt: deze authenticatiefactor is gebaseerd op het herkennen van gedrag van een persoon of systeem, bijvoorbeeld door een inlogtijd te hanteren. Deze factor is nauw gelieerd met Intrusion Detection/Prevention Systems (IDS/IPS), die op het ontdekken van ongeregeldheden gebaseerd zijn.

## Noodzaak inzet MFA

Ieder authenticatiemiddel gebruikt een authenticatiefactor met voor- en nadelen die direct of indirect invloed hebben op de effectiviteit van de toegangscontrole en daarmee op de bescherming van persoonsgegevens.

De effectiviteit van de toegangscontrole is alleen afdoende als nauwkeurig de identiteit van een persoon of systeem kan worden vastgesteld. Als anderen, op wat voor manier dan ook, in bezit kunnen komen van de authenticatiemiddelen van de persoon of het systeem, dan kan de identiteit worden overgenomen. In dat geval zijn meerdere kwaliteitskenmerken van systemen en gegevens in gevaar, zoals de vertrouwelijkheid, integriteit, beschikbaarheid, authenticiteit en onweerlegbaarheid.

Op basis van de gemelde datalekken concludeert de AP dat er steeds meer aanvallen gericht zijn op ongeoorloofd toegang krijgen tot een authenticatiemiddel. Dit gebeurt op diverse manieren, waaronder:

### I. Social engineering, waaronder phishing

Hierbij overtuigt een aanvaller, door sociale vaardigheden te gebruiken, mensen om hun inloggegevens of andere waardevolle informatie te delen.

**Voorbeeld social engineering**
Een ziekenhuis heeft een melding gedaan dat kwaadwillenden het voorzien hadden op de WhatsApp-accounts van zorgmedewerkers, om zo toegang te krijgen tot WhatsApp-groepen met collega's. Diverse aanvallen zijn succesvol geweest, omdat de aanvaller(s) met een smoes de zorgmedewerkers zo ver kregen dat zij de code te verstuurden die nodig is om het account over te nemen. Overigens kunnen derden ook via een slecht beveiligde voicemail aan dit nummer komen. Bij het datalek in kwestie zijn geen gevoelige/bijzondere gegevens betrokken.

**Aangekondigde technische en organisatorische maatregelen**
Het ziekenhuis heeft aangekondigd tweestapsverificatie op WhatsApp in te voeren én instructie te geven om geen persoonsgegevens te delen via WhatsApp.

De AP ontving het laatste jaar steeds vaker vergelijkbare meldingen die met WhatsApp te maken hebben.

### II. Password spraying

Hierbij wordt op een geautomatiseerde wijze geprobeerd om op een lijst van accounts in te loggen door achtereenvolgens veelgebruikte wachtwoorden te gebruiken. Per wachtwoord worden alle accounts geprobeerd en dan pas het volgende wachtwoord. Bekende voorbeelden van veelgebruikte wachtwoorden zijn 'password1' of '1234567890'.

### III. Credential stuffing

Hierbij worden op een geautomatiseerde en grootschalige manier eerder buitgemaakte inloggegevens (bijvoorbeeld afkomstig uit een ander datalek) gebruikt om ongeoorloofde toegang te krijgen tot accounts.

**Voorbeeld credential stuffing**

Een organisatie in de detailhandel heeft een melding gedaan nadat een 'medewerker' aan een collega vroeg om geld over te maken. De e-mail leek afkomstig van de betreffende 'medewerker' en daarom is het bedrag overgemaakt. Later bleek dat een kwaadwillende toegang had verkregen tot het account van de medewerker en op zijn naam deze e-mail stuurde. In dit geval is het geld naar een verkeerde rekening overgemaakt. Vermoedelijk zijn het wachtwoord en de gebruikersnaam bekend geraakt door een datalek bij een organisatie waar de medewerker een privé-account had. Het hergebruiken van wachtwoorden zorgt ervoor dat mensen kwetsbaar zijn als dit wachtwoord ergens wordt gelekt.

In totaal is deze organisatie voor ruim 50.000 euro opgelicht. Omdat de hacker toegang had tot de mailbox van de betreffende medewerker, had deze ook toegang tot e-mailadressen, NAW-gegevens en financiële gegevens van minimaal 500 personen.

**Aangekondigde technische en organisatorische maatregelen**

Na de hack zijn alle wachtwoorden veranderd en zijn er nieuwe procedures ingesteld. Deze verwerkingsverantwoordelijke gaf aan dat uit technisch onderzoek is gebleken dat MFA in dit geval niet was ingeschakeld en het gebruik hiervan het incident had kunnen voorkomen.

Mede gelet op de toename van dit soort aanvallen, de stand van de techniek en de uitvoeringskosten, moet MFA in principe als een essentiële (basis)maatregel worden beschouwd. Door het gebruik van meerdere factoren is de toegangscontrole niet langer afhankelijk van het geheimhouden van een authenticatiemiddel (zoals een wachtwoord), wat het aannemen van een valse identiteit bemoeilijkt.
Ook zorgt de toepassing van MFA op interne systemen en processen ervoor dat de schade eenvoudiger

**MFA-implementaties**

Om MFA effectief te laten zijn, moeten bij de implementatie de juiste keuzes worden gemaakt. Multi-step-authenticatie is bijvoorbeeld af te raden. Hierbij worden de verschillende authenticatiefactoren in verschillende stappen geverifieerd. Dit kan waardevolle informatie opleveren voor een aanvaller, doordat er al feedback komt of een combinatie van gebruikersnaam en wachtwoord correct is voordat de sms-token wordt verzonden. NB: een app-gebaseerde oplossing verdient de voorkeur boven MFA via sms.
Out-of-band-authenticatie is aan te raden. Hierbij worden de authenticatiefactoren over verschillende kanalen verstrekt. Dit bemoeilijkt man-in-the-middle-aanvallen (aanvallen waarbij informatie tussen twee of meer partijen wordt onderschept). De meeste MFA-implementaties zijn out-of-band.

beperkt blijft als een derde onverhoopt systeemtoegang heeft, omdat de aanvaller dan zonder toegang tot deze authenticatiemiddelen niet in deze systemen kan komen. Dit voorkomt of beperkt dat onbevoegden zich vrij kunnen bewegen binnen het netwerk tussen de verschillende servers (laterale beweging). Deze problematiek ziet de AP ook veel terug in gemelde datalekken.

**Voorbeeld phishing**
Een organisatie in de autobranche heeft melding gedaan dat een kwaadwillende zich toegang verschafte tot de mailbox van een medewerker. Kort hiervoor had de medewerker op een link geklikt uit een mail van een vermoedelijke klant. Het mailtje bleek achteraf gezien echter niet afkomstig van een klant maar van de oplichter. Deze heeft de gehele mailbox gedownload en via een ander e-mailadres een klant benaderd. Hiernaast is geprobeerd om het bankrekeningnummer van het bedrijf te wijzigen en is de klant gevraagd om een aangepaste factuur te betalen. Door dit incident zijn NAW-gegevens, contactgegevens en de financiële gegevens van minimaal 400 personen getroffen.

**Aangekondigde technische en organisatorische maatregelen**
De organisatie heeft aangegeven op zeer korte termijn op alle accounts van de medewerkers MFA te activeren, zodat niemand meer kan inloggen met alleen een combinatie van inlognaam en wachtwoord.

# Vijf aanbevelingen van de AP

MFA is een relatief eenvoudige maatregel die veel leed kan voorkomen. Bovendien is het gebruik van MFA in veel gevallen een essentieel onderdeel van een adequaat beveiligingsbeleid. Daarmee is deze maatregel vaak ook een juridische verplichting op grond van de AVG.

De AP adviseert:

1. MFA in te stellen voor alle systemen waar toegangscontrole op ingesteld is. Vooral bij externe toegangscontrole en systemen die veel (gevoelige of bijzondere) persoonsgegevens bevatten.
2. MFA in te stellen op (zakelijke) instantmessagingdiensten (zoals Signal, Telegram en WhatsApp) en mailapplicaties.
3. De effectiviteit van de toegangscontrole te blijven verifiëren.
4. Vanuit het intern toezicht in de organisatie na te gaan welke verwerkingen in aanmerking komen voor MFA.
5. Voor meer informatie over MFA en een gedegen wachtwoordmanagementbeleid de Factsheet Gebruik tweefactorauthenticatie van het NCSC te raadplegen.