AUTORITEIT
PERSOONSGEGEVENS

Persoonsgegevens zijn de 'witte vlek' in aanpak van cybersecurity

AP position paper juni 2023

Online fraude met persoonsgegevens is een steeds aantrekkelijker verdienmodel. Criminelen maken actief jacht op persoonsgegevens, onder andere door cyberaanvallen uit te voeren. De online beveiliging van grote en kleine databestanden is vaak niet op orde. Dit heeft grote gevolgen: voor onze digitale veiligheid, voor bedrijven en organisaties, maar ook voor de individuele burgers wiens persoonsgegevens ten prooi vallen aan criminelen.

De AP is verantwoordelijk voor het toezicht op de bescherming van persoonsgegevens. Juist ook in het cyberdomein. De kans dat er bij een cyberhack namelijk geen persoonsgegevens worden ontvreemd is klein. Immers, ook inloggegevens zijn vaak al persoonsgegevens. Kortom, goede bescherming van persoonsgegevens is de basis van digitale veiligheid van Nederland. Toch wordt die verbinding in het maatschappelijk debat en kabinetsstukken weinig gemaakt. Kortgezegd: persoonsgegevens zijn de 'witte vlek' in de aanpak van cybersecurity. Daarom stelt de AP: Cybersecurity, informatiebeveiliging en privacy zijn noodzakelijk voor digitale veiligheid.

Op donderdag 29 juni gaat de vaste Kamercommissie Digitale Zaken in debat over 'Online veiligheid en cybersecurity'. De bescherming van persoonsgegevens speelt ten onrechte een geringe rol in het debat over online veiligheid en cybersecurity. Daarom roept de AP op tot de volgende acties:

1. Goede beveiliging van persoonsgegevens is essentieel voor digitale veiligheid en privacy; Als het gaat over cybersecurity en informatiebeveiliging, spreek dan ook expliciet over persoonsgegevens.
2. Ook in de Netwerk- en Informatiebeveiligingsrichtlijn (NIB2) speelt de bescherming van persoonsgegevens een belangrijke rol; alertheid is gewenst.
3. Zorg ervoor dat de AP budgettair voldoende is toegerust in haar rol als aanjager van cybersecurity en online veiligheid, door een deel van de 111 miljoen structureel aan de AP toe te bedelen.

1. Goede beveiliging van gegevens essentieel voor digitale veiligheid en privacy

De digitale veiligheid van Nederland en haar burgers is onlosmakelijk verbonden met de bescherming van persoonsgegevens. Immers, als een bedrijf of organisatie zijn beveiliging niet op orde heeft, dan is de kans groot dat bij een cyberaanval niet alleen bedrijfsgevoelige informatie, maar ook persoonsgegevens buit gemaakt worden. De AP spreekt dan van een 'datalek': toegang tot persoonsgegevens zonder dat dit mag of zonder dat dit de bedoeling is. In Nederland geldt een meldplicht voor datalekken. Dit houdt in dat organisaties, zowel bedrijven als overheden, direct een melding moeten doen bij de AP zodra zij een datalek hebben. De bestaande wetgeving is hier expliciet in: in artikel 32 van de Algemene Verordening Gegevensbescherming (AVG) en in artikel 29 van de Richtlijn Gegevensbescherming bij Rechtshandhaving (RDR) staat nauwgezet beschreven dat organisaties die persoonsgegevens beheren ook verantwoordelijk zijn voor de beveiliging van deze gegevens. De AP spreekt organisaties daarom aan op

het op orde hebben van de beveiliging van de persoonsgegevens die zij onder hun hoede hebben, zodat datalekken worden voorkomen. Als datalekken onverhoopt toch optreden adviseert de AP organisaties zodat de juiste follow up wordt gegeven, om de opgetreden schade zoveel mogelijk te beperken.

De betrokkenheid van de AP bij cybersecurity en informatiebeveiliging is daarom dus groot. Onlangs publiceerde de AP haar jaarlijkse datalekkenrapportage. Die laat een zorgelijk beeld zien: iedereen moet er rekening mee houden dat je gegevens al een keer gelekt zijn, of dat dit nog gaat gebeuren. Slachtoffers lopen het risico op identiteitsfraude: het Centraal Meldpunt Identiteitsfraude (CMI) kreeg bijvoorbeeld in 2022 ruim 6.000 meldingen binnen. Zo worden er bijvoorbeeld leningen en dure telefoonabonnementen afgesloten met gelekte persoonsgegevens.

De schaal waarop persoonsgegevens worden buitgemaakt is enorm: bij de drie grootste gemelde cyberaanvallen van 2022 – allemaal bij ICT-leveranciers voor de zorgsector – zijn bij elkaar de medische gegevens van naar schatting 900.000 patiënten op straat beland. Het gaat hier om uiterst gevoelige gegevens, waarmee de slachtoffers veel schade kan worden berokkend. Denk bijvoorbeeld aan chantage met gevoelige medische informatie, zoals informatie over iemands mentale gezondheid of erfelijke aandoeningen.

Cyberaanvallen zijn ontzettend schadelijk voor organisaties en personen, maar het is ook vaak complex. Organisaties kunnen zelf getroffen worden door een cyberaanval, maar het kan ook gebeuren bij een leverancier die zij inhuren. Organisaties besteden diensten, waaronder ICT-diensten, vaker uit aan gespecialiseerde bedrijven. Bij een ICT-leverancier kunnen organisaties software op maat en opslagruimte voor hun data afnemen. Dit heeft tot gevolg dat een ICT-leverancier veel data beheert. Deze data zijn goud waard voor criminelen. De AP merkt op dat getroffen ICT-leveranciers vaak te maken kregen met een cyberaanval omdat ze hun beveiliging niet op orde hadden. Via de ICT-leverancier ziet de AP welke organisaties gebruikmaken van de diensten, en dus mogelijk ook betrokken zijn bij het datalek. De AP kan dan controleren of deze organisaties het datalek ook hebben gemeld aan de AP en slachtoffers op de juiste manier hebben geïnformeerd.

Ook signaleert de AP een nieuwe trend op het gebied van cyberaanvallen met ransomware: steeds vaker wordt het mogelijk lekken van persoonsgegevens op het dark web ingezet als chantagemiddel. Hackers maken met een cyberaanval grote hoeveelheden persoonsgegevens buit, om vervolgens organisaties te chanteren: betaal een losgeldsom, anders verspreiden wij deze gegevens op het dark web – waar fraudeurs staan te springen om jouw klantgegevens.

Kortom, de bescherming van persoonsgegevens en de beveiligingsplicht uit de AVG hebben een sterke link met cybersecurity en informatiebeveiliging; wanneer er sprake is van cyberaanval worden er in verreweg de meeste gevallen persoonsgegevens gelekt, waardoor grondrechten van burgers worden geschonden. Toch wordt deze verbinding in het gesprek over digitale veiligheid niet of nauwelijks gemaakt. Zo ontbreekt het werk van de AP in *Nederlandse Cybersecuritystrategie 2022-2028* en in het *Cybersecurity Beeld Nederland 2022*, en is ook in het debat over 'Cybersecurity en online veiligheid' van 14 september 2022 nauwelijks gesproken over rol van persoonsgegevens. De boodschap van de AP is dan ook: Als het gaat over cybersecurity en informatiebeveiliging, spreek dan ook expliciet over persoonsgegevens.

2. Netwerk- en Informatiebeveiligingsrichtlijn (NIB2) van groot belang voor persoonsgegevens; alertheid is gewenst

Online veiligheid en digitale weerbaarheid van sectoren zoals de financiële sector, energie, transport, ruimtevaart, drinkwater en de overheid zijn essentieel voor de veiligheid van onze samenleving en de continuïteit van ons dagelijks leven. Deze alsmaar toenemende afhankelijkheid van digitalisering maakt ons ook kwetsbaar. Ook het *CSBN 2022* erkent dit en stelt: 'Wanneer digitale processen niet naar behoren werken, heeft dat effect op het functioneren van organisaties. Keteneffecten kunnen sectoren of zelfs de gehele maatschappij raken.' Cybercriminelen kunnen met ransomware aanvallen hele sectoren 'gijzelen' en daar ook veel geld mee verdienen.

Het is een understatement om te zeggen dat het belangrijk is dat de digitale weerbaarheid tegen cyberaanvallen moet worden versterkt. De AP is daarom verheugd dat in het afgelopen jaar de NIB2-richtlijn is aangenomen. De NIB2-richtijn komt bovenop de al bestaande Netwerk- en Informatiebeveiligingsrichtlijn (NIB1). NIB2 zal naar verwachting worden verwerkt in Nederlandse wetgeving door een aanpassing van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Als gevolg van NIB2 krijgen meer vitale sectoren, van de voedings- en farmaceutische industrie tot ruimtevaart en datacenters, te maken met wettelijke verplichtingen voor de beveiliging van hun (informatie)systemen.

Gevolgen NIB 2 voor de AP

De komst van de NIB2 heeft een aantal grote gevolgen voor sectoren en toezichthouders, ook voor de AP. Zo komt er een uitbreiding van de 'meldplicht datalekken'. Praktisch betekent dit dat als een sectorale toezichthouder een melding krijgt van een bedrijf of onderneming uit hun sector, zij een 'doorzendplicht' heeft naar de AP. Daarnaast verwacht de AP dat door de uitbreiding van het aantal sectoren dat onder de NIB2 valt, er meer datalekmeldingen komen.

Op dit moment krijgt de AP jaarlijks 21.000 datalekmeldingen. Op basis hiervan heeft de AP een goed en actueel beeld van cyberaanvallen bij organisaties. Gezien de grote omvang is het toezicht 'risicogestuurd'. Dat betekent dat de AP zich voornamelijk richt op die datalekken die de grootste risico's opleveren voor slachtoffers. Er zijn een aantal toezichtsacties die vervolgens worden ondernomen. Allereerst zorgt de AP ervoor dat organisaties goede beveiligingsmaatregelen nemen om nieuwe cyberaanvallen en datalekken te voorkomen. Daarnaast wijst de AP erop dat de slachtoffers van datalekken worden geïnformeerd door bedrijven en organisaties. Zo kunnen slachtoffers bijvoorbeeld tijdig hun gelekte wachtwoord wijzigen, voordat die wordt verkocht op het dark web. Met deze 'slachtoffernotificatie' draagt de AP ook bij aan de ambitie om burgers digitaal veilig en weerbaar te maken, zoals verwoord in de *Nederlandse Cybersecurity Strategie 2022-2028*.

3. Zorg ervoor dat de AP budgettair voldoende is toegerust in haar rol als aanjager van cybersecurity en online veiligheid, door een deel van de 111 miljoen structureel aan de AP toe te bedelen.

Nederland staat voor grote uitdagingen op het gebied van cybersecurity, informatiebeveiliging en privacy. Dat toont ook een debat zoals 'Online veiligheid en cybersecurity' op 29 juni. De AP ziet de steeds

prominentere plek die digitalisering inneemt in de agenda van de Tweede Kamer en in het kabinetsbeleid als een zeer positieve ontwikkeling.

In de *Nederlandse Cybersecuritystrategie 2022-2028* staat dat dit kabinet een extra 111 miljoen euro structureel investeert in cybersecurity. De AP steunt deze investeringen uiteraard, maar komt hier zelf niet in voor. De AP speelt als Nederlandse privacytoezichthouder een aanzienlijke rol in de bevordering van de digitale veiligheid in Nederland. Daarnaast krijgt zij er door NIB2 extra werkzaamheden bij, terwijl ze al budgettaire krapte ervaart. Daarom doet de AP de oproep voor flinke versterking; dan kan de AP haar rol als aanjager van cybersecurity en online veiligheid echt vervullen.