Sancties van de Autoriteit Persoonsgegevens op NIS2-overtredingen

De valkuilen van toegang en authenticatie

Beveiliging van persoonsgegevens is een cruciale verplichting onder de AVG, de eis om maatregelen te nemen zijn beschreven in artikel 32. Sinds februari 2023 heeft de Autoriteit Persoonsgegevens (AP) meerdere sanctiebesluiten genomen, waaronder één boete wegens onvoldoende beveiliging. In dit artikel bespreekt Natascha van Duuren de sanctiebesluiten die de AP daarna heeft genomen, en de belangrijkste lessen die organisaties hieruit kunnen trekken.

IN FEBRUARI 2023 VERSCHEEN HET ARTIKEL 'ZO ZORG JE VOOR PASSENDE INFORMATIEBEVEILIGING. 10 lessen uit uitspraken van de Autoriteit Persoonsgegevens'. Jeroen van Helden en Michelle Wijnant formuleerden in dat artikel tien belangrijke aandachtspunten voor het realiseren van een passende informatiebeveiliging, gebaseerd op sanctiebesluiten van de Autoriteit Persoonsgegevens (AP):

1. **Risicoanalyse:** een organisatie moet beveiligingsmaatregelen treffen op basis van een risicoanalyse;
2. **Beveiligingsplan:** iedere organisatie moet een beveiligingsbeleid hebben opgesteld, waaronder een beveiligingsplan waarin is vastgelegd welke beveiligingsmaatregelen zijn geïmplementeerd op basis van risicoanalyses;
3. **Opleiding personeel:** personeel moet passende trainingen krijgen op het gebied van informatiebeveiliging;
4. **Autorisatiematrix:** een organisatie moet beschikken over formeel vastgestelde procedures voor het activeren en afmelden van toegangsrechten tot systemen;
5. **Sterke wachtwoorden:** sterke wachtwoorden moeten worden afgedwongen op zowel individuele als generieke accounts;
6. **Multi Factor Authentication**
7. **Netwerksegmentatie**
8. **Cryptografie:** waar passend moet een organisatie gebruik maken van versleuteling van persoonsgegevens;
9. **Logging en controle logbestanden:** handelingen die gebruikers uitvoeren met persoonsgegevens, zoals raadplegen en mutaties, moeten worden gelogd. Daarnaast moeten de logbestanden periodiek worden gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van gegevens. Deze controles moeten proactief, systematisch en consequent plaatsvinden;
10. **Procedure datalekken:** een organisatie moet beschikken over een procedure voor het melden en opvolgen van beveiligingsincidenten en datalekken.


Beeld: Shutterstock

Wettelijke beveiligings-verplichting

Iedere organisatie die persoonsgegevens verwerkt is op grond van artikel 32 van de Algemene verordening gegevensbescherming (AVG) verplicht om 'passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen'. Daarbij moet volgens overweging 83 van de AVG rekening worden gehouden met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.

Inmiddels zijn we twee jaar verder. Jeroen van Helden en Michelle Wijnant constateerden in februari 2023 dat voor geen enkele andere AVG-verplichting door de AP zoveel sancties werden opgelegd. Dit is in de daaropvolgende periode tot en met heden anders. De AP heeft sinds februari 2023 negen sanctiebesluiten genomen, waarbij één boete is opgelegd, omdat volgens de AP onvoldoende passende technische en organisatorische maatregelen waren genomen. Het desbetreffende boetebesluit zal hieronder kort worden besproken evenals de (aanvullende) lessen die hieruit kunnen worden getrokken.

Autorisatie, authenticatie en bewustwording

Op 19 januari 2023 heeft de AP besloten aan de Sociale verzekeringsbank (SVB) een bestuurlijke boete van €150.000 op te leggen wegens het nemen van onvoldoende passende maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het verwerken van persoonsgegevens in het kader van telefonisch klantcontact met AOW-verzekerden. Wat was er aan de hand (zonder diep op de casus in te gaan)? Op 1 november 2019 heeft de AP een klacht ontvangen. Klaagster gaf te kennen dat

een familielid persoonlijke informatie over haar zou hebben ontvangen van een medewerker van de SVB. Dit terwijl zij de SVB hiervoor geen toestemming had gegeven.

Deze zaak raakt aan drie belangrijke onderwerpen: autorisatie, authenticatie en bewustwording. Autorisatie is het proces waarin een persoon bepaalde rechten krijgt binnen een systeem. Denk hierbij aan toegangsrechten, leesrechten en mutatierechten. Een systeem waar veel personen bepaalde toegangsrechten hebben tot veel gegevens brengt dus, aldus de AP, (veel) beveiligingsrisico's met zich mee.
Het niet beschikken over formeel vastgestelde procedures voor het activeren en afmelden van toegangsrechten tot systemen en werkinstructies die niet formeel zijn vastgesteld, heeft eerder (op 24 februari 2022) geleid tot sancties richting het Ministerie van Buitenlandse Zaken.

Een ander onderwerp is authenticatie. Authenticatie is het proces waarbij de vermeende identiteit van een persoon wordt geverifieerd.
Een goede authenticatieprocedure kan bijdragen aan een passend beveiligingsbeleid omdat het helpt ongeoorloofde toegang en -verstrekking van gegevens te voorkomen.

Niet duidelijk

Zonder uitvoerig op de zaak in te gaan, wordt opgemerkt dat het authenticatiebeleid binnen de SVB in twee afzonderlijke werkinstructies beschikbaar was, die bovendien elk verschillende werkwijzen beschreven. Het was voor de servicemedewerkers dan ook niet duidelijk welke van de twee instructies gevolgd moest worden. Daarnaast had meer dan de helft van de controlevragen om de identiteit van de klanten aan de telefoon te controleren, betrekking op eenvoudig te achterhalen gegevens, zoals een combinatie van adres en geboortedatum. NAW-gegevens zijn echter gegevens die voor een groot aantal mensen beschikbaar zijn. Denk bijvoorbeeld aan vrienden, familie en collega's. Bovendien zijn zij eenvoudig te achterhalen via openbare bronnen, waaronder sociale media. Een dergelijk authenticatiebeleid acht de AP ontoereikend.

In het besluit van de AP wordt ook nogmaals het belang van bewustwording benadrukt. De organisatorische maatregelen die de SVB had getroffen op het vlak van bewustwording was volgens de AP ontoereikend. Zo was de frequentie van de verplichte opleidingen waar de regels en risico's van het werken met persoonsgegevens bij telefonisch klantcontact laag en waren medewerkers niet altijd op de hoogte van de meest recente instructies. Al eerder (6 februari 2017) zagen we dat de Nationale Politie tekort schoot in het verzorgen van passende trainingen voor medewerkers op het gebied van informatiebeveiliging, als gevolg waarvan de AP een sanctie oplegde.

NIS2

De organisaties die door de AP gesanctioneerd zijn wegens het gebrekkige beveiligingsmaatregelen, vallen onder het toepassingsbereik van de NIS2. Als we

SVB-medewerkers wisten niet welke van twee werkinstructies ze moesten volgen

kijken naar de aandachtspunten uit sanctiebesluiten AP tot februari 2023, zien we dat deze aandachtspunten nagenoeg allemaal expliciet terugkomen in de NIS2. Een uitzondering vormt het hebben van een procedure voor datalekken (dit hoort immers thuis in privacywet- en regelgeving), maar daarvoor in de plaats is een procedure voor het melden van significante (beveiligings) incidenten gekomen. Ook personeel, toegangsbeleid (autorisatie) en authenticatie zijn in de NIS2 (en het wetsontwerp Cyberbeveiligingswet) onderwerpen die uitdrukkelijk worden erkend en ten aanzien waarvan maatregelen worden verlangd.

Het personeel van een organisatie kan worden gezien als de eerste verdedigingslinie tegen cyberaanvallen. Het Digital Trust Center verwoordt het aldus: "Personeel speelt dus een cruciale rol bij het op pijl houden van de beveiliging van systemen en gegevens. Centraal staat dat een organisatie er voor zorgt (door middel van passende opleidingen of trainingen) dat medewerkers hun verantwoordelijkheden voor digitale beveiliging begrijpen en dit kunnen toepassen in hun werk". In de ontwerp Cyberbeveiligingswet worden 'beveiligingsaspecten ten aanzien van personeel' en 'toegangsbeleid' in artikel 21 lid 2 als minimumbeveiligingsmaatregel genoemd. Hetzelfde geldt voor een multifactorauthenticatie-regeling.

Toegangsrechten administreren

Alhoewel het formuleren en naleven van een passend toegangsbeleid in

NIS2/ontwerp Cyberbeveiligingswet als minimum beveiligingsmaatregel wordt gezien, blijkt het administreren van toegangsrechten in de praktijk regelmatig een uitdaging. Het blijkt niet zozeer de uitdaging om bij indiensttreding de toegangsrechten te administreren, maar wel bij functiewisselingen. Welke zaken moeten nu in een toegangsbeleid geborgd worden? De NIS2 geeft hier geen concrete handvatten voor. Het Digital Trust Center van het ministerie van Economische Zaken geeft aan dat een toegangsbeleid de volgende zaken moet bevatten:

- alleen geautoriseerde medewerkers kunnen toegangsrechten verstrekken;
- toegangsrechten moeten alleen worden verstrekt aan gebruikers voor wie toegang tot die systemen of gegevens relevant is;
- toegang wordt alleen gegeven voor de periode waarvoor toegang nodig is;
- (specifieke) rechten moeten worden uitgegeven volgens het principe van least privilege;

Het personeel van een organisatie is de eerste verdedigingslinie tegen cyberaanvallen

- bij het toekennen van toegang aan externen (zoals leveranciers of IT-dienstverleners), moeten duidelijke afspraken worden gemaakt over de toegang en welke veiligingseisen aan de toegang worden gesteld;
- er moet een procedure zijn voor het moment van aanpassen van de toegangsrechten (bij functiewisseling of vertrek);
- toegangsrechten moeten in een register worden bijgehouden;
- er dient logging te zijn op het beheer van toegangsrechten, zodat je weet wie wanneer welke rechten heeft verstrekt en ontvangen.

Het Digital Trust Center geeft daarbij Zero Trust als tip mee. Zero Trust neemt als uitgangspunt om niets en niemand te vertrouwen en telkens alles opnieuw te verifiëren. In de huidige wereld met steeds toenemende cyberdreigingen lijkt dit een zeer bruikbare tip.

Het beeld dat voor geen enkele AVG-verplichting sancties worden opgelegd, komt niet zozeer naar voren in de periode februari 2023 tot op heden. Wellicht dat de grote aandacht voor cyberdreigingen en het belang van security daartoe bijgedragen heeft. Er is in de afgelopen periode immers veel aandacht geweest voor de NIS2, op grond waarvan organisaties die onder de reikwijdte vallen verplicht worden (minimum) beveiligingsmaatregelen te nemen. De elf organisaties die vanaf 2017 door de AP gesanctioneerd zijn, vallen allen onder de reikwijdte van de NIS2 (Cyberbeveiligingswet) zodat er vanuit mag worden gegaan dat zij niet alleen lering hebben getrokken uit de desbetreffende sanctiebesluiten maar zich ook zorgvuldig en tijdig hebben voorbereid op de Cyberbeveiligingswet die binnen afzienbare tijd in werking zal treden.

Met dank aan Marissa Genemans

Natascha van Duuren
is advocaat en partner bij De Clercq advocaten notariaat, gespecialiseerd in IT, privacy en cybersecurity.