

Samenvatting

Binnen de informatiebeveiliging is de exclusiviteit van gegevens een belangrijk kwaliteitsaspect. De belangen van een bedrijf of van een persoon kunnen ernstig geschaad worden als onbevoegden toegang kunnen krijgen tot informatie. Het controleren van de toegang tot informatie is dan ook cruciaal. Hiervoor is het nodig om te weten wie toegang probeert te krijgen: wat is de identiteit van de persoon (identificatie) en kan deze identiteit bevestigd worden door vergelijking met een ander betrouwbaar gegeven (authenticatie).

Handelingen waarbij vroeger de betrokken personen fysiek aanwezig waren, worden tegenwoordig via computers en netwerken verricht. Dit is vaak een economische en efficiënte manier van zaken doen, maar het nadeel is dat je er moeilijk zeker van kunt zijn met wie men eigenlijk zaken doet. De huidige vormen van identificatie en authenticatie zijn immers fraudegevoelig. Vaak wordt gebruik gemaakt van authenticatie door middel van een voorwerp, bijvoorbeeld een pasje, of iets wat alleen de juiste persoon behoort te weten, bijvoorbeeld een wachtwoord. Geen van deze methoden is volledig persoonsgebonden. Een pasje of code kan immers worden overgedragen of in handen van onbevoegden komen. Hierbij valt te denken aan het aannemen van valse identiteiten of het gebruik van andermans PIN-code. Het gebruik van biometrie kan de kwaliteit van de identificatie en authenticatie verhogen, omdat lichaamskenmerken immers nagenoeg uniek zijn en niet overdraagbaar aan derden.

Vormen van biometrische identificatie

Biometrie is een verzameling van technieken gebaseerd op het meten van kenmerken die uniek kunnen worden toegeschreven aan de drager daarvan. Het unieke van deze kenmerken maakt deze geschikt voor identificatie, het vaststellen van iemands identiteit, en authenticatie, het vaststellen dat iemand is wie hij of zij claimt te zijn.

Op het moment zijn de meest geavanceerde toepassingen het gebruik van vingerafdruk, netvlies en iris, gezichtsvorm, hand- en vingergeometrie. Uit andere kenmerken, zoals lichaamsgeur of het DNA-profiel kan eveneens de identiteit van een persoon worden bepaald. De inzet van deze middelen voor toegangscontrole is echter vooralsnog niet aan de orde. Wel worden bepaalde gedragskenmerken voor identificatie gebruikt. Voorbeelden hiervan zijn de herkenning van de stem, de manier waarop iemand een handtekening zet, of de specifieke aanslag van het toetsenbord.

Het proces van biometrische identificatie en authenticatie kent een aantal stappen. Er moet altijd sprake zijn van een eerste vastlegging. In principe is dit een eenmalige gebeurtenis, waarbij het biometrische gegeven gemeten wordt

en toegeschreven aan de juiste persoon. Dit oorspronkelijke gegeven wordt nu vastgelegd in een template, bijvoorbeeld in een database of op een chipcard. Overigens zal dit template doorgaans geen 'afbeelding' van het lichaamskenmerk zijn, maar bestaan uit een aantal specifieke meetpunten.

In de gebruiksfase presenteert iemand zijn lichaamskenmerk aan een sensor. Het lichaamskenmerk wordt gemeten en vergeleken met het template. De meting zal altijd een zekere onnauwkeurigheid hebben en daarom afwijken van het template. Wanneer de overeenkomst tussen de meting en template groter is dan een van tevoren gespecificeerde drempel, zal de persoon worden geauthenticeerd.

Biometrische identificatie en privacy

Bij alle voordelen als beveiligingsmiddel kent biometrie voor identificatie ook een keerzijde. Juist de belangrijke eigenschap van lichaamskenmerken, namelijk dat ze uniek verwijzen naar een persoon, zorgen ervoor dat de privacy van die persoon in het geding komt. Wanneer immers verschillende gegevens over die persoon op verschillende plekken zijn opgeslagen kan aan de hand van het biometrische kenmerk worden achterhaald dat die gegevens allemaal bij die persoon horen. Door samenvoeging van de bestanden kan een gedetailleerder beeld ontstaan, zonder dat de betrokkene dat weet of daarvoor toestemming heeft gegeven. Wanneer dezelfde biometrische gegevens worden gebruikt voor allerlei verschillende handelingen, wordt het mogelijk om iemands leven voor een groot deel te traceren. Zeker bij toepassingen in de relatie overheid-burger is dit een punt van zorg omdat meestal de burger geen alternatief heeft. Bijvoorbeeld bij het plan om het paspoort uit te rusten met een biometrische kenmerk zal hier terdege rekening mee moeten worden gehouden.

Een ander punt van aandacht is dat biometrische gegevens vaak meer informatie bevatten dan direct voor identificatie of authenticatie nodig. Zo is het soms mogelijk om uit de lichaamskenmerken ook iets af te leiden over de gezondheidstoestand, of over het ras. Ook kan, bijvoorbeeld uit de stem of bij gezichtsherkenning, informatie worden afgeleid over de emotionele toestand. Dit laatste, het principe van de aloude leugendetector, zou gebruikt kunnen worden als hulpmiddel bij verkoop of afstand, waarbij de emoties geanalyseerd worden om het verkoopproces te stimuleren. In dergelijke gevallen kan meer informatie worden afgeleid dan waar iemand toestemming voor heeft gegeven.

Wettelijk kader voor de inzet van biometrische identificatie

Er is in Nederland (nog) geen speciale wetgeving over biometrische identificatie. Er is echter wel algemene wet- en regelgeving die bepaalt aan

welke voorwaarden biometrische identificatiesystemen moeten voldoen. Hierna wordt heel beknopt ingegaan op drie aspecten van deze regelgeving.

persoonsgegevens

Ten eerste zijn biometrische gegevens *persoonsgegevens*, primair omdat ze bedoeld zijn om mensen van elkaar te onderscheiden, en vallen derhalve onder de daarvoor relevante wetgeving. Op het moment geldt de Wet persoonsregistraties (Wpr) waarin de omgang met persoonsgegevens geregeld wordt. Er is een nieuwe wet in behandeling, de Wet Bescherming Persoonsgegevens (WBP). Gelet op de parlementaire behandeling is de verwachting dat deze rond de jaarwisseling in werking zal treden. De nieuwe wet is in grote lijnen gelijk aan de Europese richtlijn van 24 oktober 1995. Op hoofdlijnen kan uit de richtlijn daarom bepaald worden aan welke eisen biometrische identificatie in ieder geval moet voldoen. Bijvoorbeeld geldt het volgende algemene beginsel:

Artikel 6 van de richtlijn:

De Lid-Staten bepalen dat de persoonsgegevens:

- (a) eerlijk en rechtmatig moeten worden verwerkt;
- (b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

Artikel 6(a) betekent bijvoorbeeld dat het verwerken en verzamelen van gegevens op een eerlijke manier dient te gebeuren. Mensen moeten dus weten dat er biometrische identificatie plaatsvindt. Artikel 6 (b) betekent bijvoorbeeld dat wanneer biometrische gegevens worden ingewonnen om vast te stellen of iemand bevoegd is tot toegang tot een systeem, het onverenigbaar met dat doel zou zijn als deze gegevens gebruikt worden om de emotionele toestand of het ras van de betrokkene te bepalen.

Overigens zijn er bepaalde gevallen denkbaar waarbij de richtlijn niet van toepassing is. Artikel 3 (2) van de richtlijn luidt: De bepalingen zijn niet van toepassing op de verwerking van persoonsgegevens die door een natuurlijke persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden worden verricht.

Als het dus een puur persoonlijke activiteit betreft, dan is de richtlijn niet verder van toepassing, ook al gaat het om een persoonsgegeven. In dit verband kan de authenticatiemethode van belang zijn. Zo zijn er prototypen van een flinterdunne vingerafdruklezer, ingebed in een chipkaart. Bij deze opzet komt de vingerafdruk dus noch tijdens de eerste vastlegging van de gegevens, noch tijdens de gebruiksfase buiten de kaart. De kaart geeft alleen een signaal af: de juiste persoon houdt de kaart vast, ja of nee. Het is te vergelijken met het openen van een huis met de goede sleutel. In dat geval kan gesteld worden dat

de persoonsgegevens in het persoonlijke domein blijven en de richtlijn niet verder van toepassing is.

bijzondere gegevens

Het tweede belangrijke aspect in de regelgeving is die van de *bijzondere gegevens*. Bijzondere gegevens zijn bijvoorbeeld gegevens over iemands ras of gezondheid. De basisregel is dat de verwerking van bijzondere gegevens verboden is. Er moet dus ook nagegaan worden of de specifieke toepassing van biometrie die wordt gebruikt ervoor kan zorgen dat een persoonsgegeven een bijzonder gegeven wordt.

Artikel 8 (1) van de Richtlijn luidt:

De Lid-Staten verbieden de verwerking van persoonlijke gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen.

Vormt dit nu een wezenlijk beletsel voor inzet van biometrische identificatie? Als uit een template geen volledig signaal meer is af te leiden (het algoritme kan niet 'terugrekenen' en het volledige oorspronkelijk (analoge) signaal reconstrueren), geldt dat het template wel als persoonsgegevens maar misschien niet als een bijzonder gegeven is aan te merken.

beveiliging

Het derde aspect in de regelgeving dat van belang is voor het verwerken van biometrische gegevens, is *beveiliging*. Artikel 17 van de richtlijn geeft aan dat persoonsgegevens moeten worden beschermd tegen allerlei vormen van onrechtmatig of onzorgvuldig gebruik. Deze wettelijke verplichting tot het nemen van beveiligingsmaatregelen geldt op grond van de classificatie als persoonsgegevens uiteraard ook voor biometrische gegevens.

Biometrie verantwoord toepassen

De invoering van biometrie betekent kansen en bedreigingen. Hoe kan hier op een verantwoorde manier mee worden omgegaan? Allereerst moeten de wettelijke randvoorwaarden, zoals hierboven uiteengezet, in het oog worden gehouden. Maar het is ook belangrijk dat de techniek voor biometrische identificatie zodanig wordt ingezet dat de privacy zo min mogelijk bedreigd wordt. De Registratiekamer hanteert het begrip Privacy Enhancing Technologies (PET) als verzamelnaam voor technische maatregelen om het gebruik van persoonsgegevens te vermijden of te beperken.

Als eerste moet altijd onderzocht worden of er voor het beoogde doel nodig is om personen te identificeren of dat een authenticatie volstaat. In veel gevallen is het immers helemaal niet noodzakelijk dat iemand zijn identiteit prijs geeft. Soms kan het voldoende zijn om vast te stellen dat iemand inderdaad degene

is die een bepaald recht mag uitoefenen, bijvoorbeeld een lidmaatschap. Daarnaast kan er gezorgd worden voor een decentrale opslag van templates. Ook de cryptografische beveiliging van gegevens verdient aandacht.

Op hoofdlijnen gelden voor verantwoord biometrie de volgende vragen:

- 1 Welke gegevens zijn echt nodig voor het doel?
- 2 Worden de gegevens rechtmatig ingewonnen? Is de betrokken persoon geïnformeerd?
- 3 Is er sprake van 'bijzondere gegevens'?
- 4 Wat gebeurt er met de oorspronkelijke biometrische gegevens? Worden deze verwijderd?
- 5 Zijn de biometrische gegevens zo opgeslagen dat ze niet meer terug te voeren zijn tot de oorspronkelijke gegevens?
- 6 Is het mogelijk om de meting van de gegevens en de verificatie decentraal te laten plaatsvinden?
- 7 Is de beveiliging van templates voldoende?
- 8 Rechtvaardigt het doel een eventuele centrale opslag van biometrische gegevens?

Conclusie

De komst van biometrische identificatie is een belangrijke trend binnen de beveiliging. Verantwoorde inzet van biometrische identificatie betekent dat rekening wordt gehouden met de wetgeving voor de bescherming van persoonsgegevens. Ook is het belangrijk dat een identificatiesysteem technisch zo worden ingericht dat een minimale hoeveelheid persoonsgegevens wordt ingewonnen, en dat de verspreiding van die gegevens voorkomen wordt.