

Geautomatiseerd toegangb

Veelvuldig openen wij afgesloten deuren en identificeren wij ons op allerlei informatiesystemen en apparatuur waaronder smartphones en computers. Zou het niet prettig zijn als wij in deze dagelijkse bezigheden net zo snel en gemakkelijk of zelfs beter herkend zouden kunnen worden, zoals mensen elkaar herkennen? In mijn droom loop ik naar een kamer of computer en word ik - zonder dit te beseffen - biometrisch herkend op het moment dat ik de kamer betreed of de computer ga gebruiken, zodat ik kan doen wat ik wil gaan doen.

B iometrie biedt nu al vele mogelijkheden en gaat ons nog veel verder brengen in (automatische) persoonsherkenning. Onder biometrie versta ik het biometrisch herkennen van mensen aan een lichaamskenmerk met gebruikmaking van informatietechnologie. Biometrie is een volgende stap in toegangsbeheer. Zonder biometrie zie ik ons niet aan de toekomstige eisen van toegangscontrole, informatiebeveiliging en gebruiksgemak voldoen. Vooral deze laatste drijfveer ('hoe onthoud ik toch al die wachtwoorden?') is de afgelopen tijd sterk in belang toegenomen. ICT maakt onder andere plaats- en tijdonafhankelijk werken en nieuwe communicatievormen mogelijk. Wij zijn voortdurend bezig werkprocessen te automatiseren, zoals iemand toegang verlenen tot een specifieke ruimte. In het huidige informatietijdperk willen wij - eigenlijk net als voorheen maar wel steeds vaker - weten of wij met de juiste persoon te maken hebben. Het besef van het belang van een betrouwbare identiteit van een persoon is groeiende in de elektronische en virtuele wereld. De economische belangen van adequaat identiteitsmanagement (fysiek, administratief, elektronisch en in combinatie) zijn aanzienlijk.

Vriend en vijand Biometrische systemen benaderen het meest de mens bij het herkennen van 'vriend en vijand'. Ik verwacht daarom veel van biometrie, ook en vooral in toegangsbeheer.

Onderschat echter nooit de impact van biometrie. Introductie brengt vaak veel verandering met zich mee. Deze innovatie biedt organisaties nieuwe kansen en vereist tegelijkertijd de nodige tijd en aandacht, maar ook voldoende mate van bewustzijn.

Een groot voordeel van het gebruik van biometrie is dat men de 'sleutel' altijd bij zich heeft. Hierdoor kunnen een aantal veelvoorkomende problemen in de praktijk voorkomen worden. Sleutels of pasjes gaan bijvoorbeeld vaak van hand tot hand, pasjes of pincodes worden verloren of vergeten, pasjes of sleutels zijn lastig terug te vorderen en het beheer van pasjes is een substantiele kostenpost. Het principe is simpel en beproefd. De uitslag van biometrische herkenning bij de ingang bepaalt of (automatisch) toegang tot de betreffende ruimte wordt verleend.

Ontwikkelingen Verschillende biometriesystemen worden al langere tijd succesvol toegepast en hebben hun waarde bewezen. Handgeometrie is één van de eerste goed werkende technieken en leent zich goed voor minder schone omgevingen. De nauwkeurigheid is wat gering. Van oudsher is de vingerafdruk bekend en daarmee vaak een voordelige keuze (uitgaande van elektronische afbeeldingen en niet inkt en papier). Als sleutel voor fysieke toegang kan de vingerafdruk prima ingezet worden tot ongeveer tienduizend gebruikers. Irisherkenning gaat ook al langere tijd mee en biedt een hogere nauwkeurigheid. Ontwikkelingen zijn

succesvol gaande om een iris (of retina) te scannen op een afstand van één tot tientallen meters tijdens het voorbij wandelen. Gelaatsherkenning is vaak eenvoudig en snel. Een tweedimensionaal beeld levert op zichzelf beperkte nauwkeurigheid en wordt daarom vaak in combinatie met een ID-pas gebruikt. 3D-opnames van het gezicht leveren meer unieke kenmerken op en zijn reden van lopende technologische ontwikkelingen. Gezichtsherkenning in consumentensoftware is een extra stimulans. Patroonherkenning van de aders in de vinger of de handpalm heeft zich snel ontwikkeld vanwege de hoge nauwkeurigheid en de mogelijkheid om contactloos biometrische kenmerken af te nemen.

Multimodaliteit Bovengenoemde biometrische technieken hebben zich de afgelopen jaren gestaag doorontwikkeld. Systemen, groot en klein, zijn sterk verbeterd. Biometrische sensoren zijn kwalitatief verbeterd en tegelijkertijd beter betaalbaar geworden. Er bestaat meer inzicht in de mogelijkheden en beperkingen. Multimodaliteit zoals gelaat- en stemherkenning samen of vingerafdruk- en aderherkenning samen zijn in opkomst. Welke vorm van biometrie het beste ingezet kan worden bij het verlenen van fysieke toegang, kan het beste per situatie bekeken worden. Wees bewust dat biometrie vaak meer biedt dan in eerste instantie gedacht wordt, zoals operationele informatie als aanwezigheidsregistratie, track & trace van personen en lagere beheerkosten.

heer met jezelf als sleutel



Informatiebeveiliging Bij identity & access management hanteert men gezien vanuit informatiebeveiliging de opvolgende stappen identificatie, authenticatie en autorisatie. Biometrie kan een versterkende rol van betekenis spelen in identificatie en authenticatie. Wees overigens alert op spraakverwarring vanwege andere begrippen of betekenis van deze termen in het biometriejargon. Ook in de informatietechnologie moeten we erop kunnen vertrouwen dat wij met de juiste persoon te maken hebben. Hier ligt een enorme uitdaging voor deze elektronische en virtuele wereld. Gebruikersnaam en wachtwoord zijn geen probleem bij minimale betrouwbaarheid. Elektronische diensten vereisen zwaardere middelen zoals biometrie als het om beperkte, redelijke of hoge betrouwbaarheid van persoons-

herkenning gaat. Vanzelfsprekend zijn gebruiks- en beheergemak ook essentieel. Voor de biometriewereld ligt er anderzijds ook de enorme uitdaging om aan de behoefte van informatiebeveiliging te voldoen. Ik ben zeer benieuwd hoe deze twee werelden elkaar zullen beïnvloeden.

Elektronische oplossingen In eerste instantie heeft de informatietechnologie voornamelijk naar elektronische oplossingen voor betrouwbaardere herkenning gezocht zoals tokens, smartcards, usb-sticks en dergelijke. Einstein heeft ooit al verteld dat wij een probleem niet oplossen met waarmee wij het gecreëerd hebben. Biometrie wordt als reële oplossing gezien, wat ik vanuit mijn gezichtsveld volledig onderschrijf. Ik ken echter geen panklare oplossing.

In mijn beeld dient enerzijds de informatietechnologie zich meer bewust te worden van de complexiteit van betrouwbare persoonsherkenning. Anderzijds dient biometrie geïntegreerd te worden met moderne informatietechnologie. De smartphone en tablet zijn momenteel belangrijke apparaten voor identificatie en authenticatie (en daarmee voor verschillende autorisaties). Dit soort apparaten bevatten allerlei onderdelen om gegevens van verschillende biometrische kenmerken te verwerven. Denk aan een microfoon voor stemherkenning, camera voor gezichts- en mogelijk oogherkenning. Recente smartphones bevatten ook een lezer voor een vingerafdruk. Allerlei smart technology kan gekoppeld worden, of staat op de rit om biometrische kenmerken als hartslag, bewegingsritme en dergelijke te registreren. ▶



Onderhuidse chip Ik verwacht dat de uitlezing en verwerking van de biometrische kenmerken nog aan kwaliteit moet winnen. Zeker als hoge betrouwbaarheid vereist is, bijvoorbeeld als ik gegevens in mijn persoonlijke medische dossier zou willen aanpassen. Hoe dan ook, de smartphone (of tablet) heeft het in zich om zowel aan multimodale biometrische herkenning als multifactorauthenticatie te doen. Wat je weet, wat je hebt en wat je bent worden in of via één apparaat gebundeld. Misschien is het een handig (en veiliger) vooruitzicht, maar wel een met een duidelijk 'single point of failure'.

In kantooromgevingen met computers en notebooks ligt het voor de hand om biometrie meer toe gaan passen als de betrouwbaarheidseisen hiertoe aanzetten. Dit kan bij de ingang van de ruimte(s) of het apparaat. Automatisch inloggen en aanwezigheidscontrole kan ik mij met biometrie-sensoren eventueel in combinatie met andere elektronica voorstellen. Of dit soort oplossingen in Nederland gebruikt worden, weet ik niet. Ik verwacht wel dat zij er zullen komen, zodra informatiebeveiliging, gebruiksgemak en toegangbeheer hierbij gebaat zijn. Eventueel kunnen wij de biometrie in de toekomst nog kunstmatig helpen door een onderhuidse RFID-chip, een op ons lichaam geplakte biostamp of een ingeslikte wachtwoordpil. Gemak dient de mens, maar de balans met privacy blijft een aandachtspunt.

■ Ruud Huijts
Voorzitter Vereniging Voor Biometrie & Identiteit (VVBI)

Deze bijdrage is een weerslag van een persoonlijke visie van dit moment. Het beeld is gevormd in contacten met kenniswerkers uit het biometrieveld en e-herkenning en met leden van de Vereniging Voor Biometrie & Identiteit (VVBI).

'Een enkele verwijzing naar de Algemene Voorwaarden op uw website of factuur werkt niet altijd.'

mr. Carolien Brederije
www.valegis.com
c.brederije@valegis.com
Twitter:
@valegislawyers



Gastcolumn

Algemene Voorwaarden

In de ideale situatie zijn er nooit problemen met klanten over de dienstverlening. Alle facturen worden op tijd betaald en er wordt nooit geklaagd over de geleverde dienst. Tot zover de ideale wereld. In die wereld zijn Algemene Voorwaarden niet nodig. Helaas is de praktijk vaak anders. Stel dat de klant zijn rekening niet wil betalen of u wordt aansprakelijk gesteld. In zo'n situatie bieden Algemene Voorwaarden uitkomst. Het gebruik van Algemene Voorwaarden is wijdverbreid en voor bijvoorbeeld het verkrijgen van een keurmerk van de Nederlandse Veiligheidsbranche zelfs vereist.

Belangrijk is ervoor te zorgen dat de Algemene Voorwaarden ook daadwerkelijk van toepassing worden verklaard op de overeenkomst. Als dat niet goed gebeurt, kan u er mogelijk géén beroep op doen. Hoe Algemene Voorwaarden van toepassing te verklaren? Een enkele verwijzing naar de voorwaarden op uw website of factuur werkt niet altijd. Belangrijk is dat Algemene Voorwaarden voorafgaand aan het sluiten van het contract ter hand worden gesteld en van toepassing worden verklaard. Hoe doet u dat? Stuur de Algemene Voorwaarden altijd vooraf aan de klant toe en zorg dat u van de ontvangst bewijs hebt.

Het deponeren van uw Algemene Voorwaarden bij de griffie van de rechtbank of bij de Kamer van Koophandel kan ook nuttig zijn. Anders dan veel wordt gedacht neemt deponeren echter niet weg, dat er een plicht is om de voorwaarden ter hand te stellen. Ook moet rekening worden gehouden met wel- en niet wettelijk toegestane bepalingen in de tekst. Sommige bepalingen zijn niet toegestaan. Dat speelt met name bij transacties met particulieren.

Kortom: Algemene Voorwaarden zullen hun nut pas bewijzen als ze van toepassing zijn verklaard en (bewijsbaar) ter hand gesteld. Wie weet hoeft u er nooit een beroep op te doen, maar zoals ook in de beveiliging geldt: 'voorkomen is beter dan genezen'!

Opinie@beveiliging.nl