NIEUWS

Contactloze toegangscontrole via biometrie

21 april 2020

Wanneer je als bedrijf gespecialiseerd bent in hoogwaardige securityoplossingen, moet je de beveiliging van je eigen terreinen en gebouwen uiteraard feilloos op orde hebben. Dat is bij Idemia Nederland in Haarlem zeker het geval. De marktleider op het gebied van 'augmented identity' maakt voor de toegangscontrole in haar hoofdkantoor in Parijs en haar productielocatie in Haarlem gebruik van een contactloos vingerafdruksysteem. Een toepassing die organisaties met een hoog beveiligingsprofiel in staat stelt de optimale balans te vinden tussen gemak en security.

Rob Jastrzebski

Het vingerafdruksysteem MorphoWave is een van de producten die Idemia tot koploper in de wereld maakt op het gebied van contactloze identiteits- en toegangscontrole via biometrie. Maar Idemia doet meer. Het bedrijf is wereldwijd actief en levert hoogwaardige security- en identiteitscontroleproducten aan overheden en het bedrijfsleven. Zo produceert het voor de Nederlandse overheid paspoorten, identiteitskaarten en de Rijkspas.

Fysieke toepassingen voor toegangscontrole en het vaststellen van identiteit die Idemia levert, zijn onder andere controlepoortjes op stations en luchthavens, vingerafdruksystemen voor forensische opsporingsdoeleinden door politiediensten en chips voor de beveiliging van slimme apparaten binnen het Internet of Things. Een groeimarkt in een steeds verder digitaliserende wereld, waarin ook apparaten hun identiteit onomstotelijk moeten aantonen.

Soepele toegang en optimale beveiliging

Met zo'n bedrijfsprofiel is het logisch dat het hoofdkantoor in Parijs en de productievestiging in Haarlem fysiek en digitaal 'vestingen' zijn, waar qua toegangsautorisatie de lat bijzonder hoog ligt. Security & compliance officer *Coen Postma* en senior pre-sales manager *Edwin Faber*, leggen uit hoe dankzij slimme biometrische oplossingen soepele toegang en optimale beveiliging toch samen kunnen gaan.

Digimagazine Toegangscontrole & Inbraakbeveiliging »

Balans tussen gemak, kosten en beveiliging

"De basis van elke security-oplossing is een grondige risico- en impactanalyse", begint Faber. "Een kwestie van de balans zoeken tussen gemak, kosten en beveiliging. De oplossing moet passen bij het afbreukrisico dat een organisatie loopt als gevolg van het betreden van een gebouw of terrein door ongeautoriseerde personen. Als ergens een deur in zit, kun je naar binnen, dus het vaststellen van de identiteit is een belangrijke stap in het beveiligingsproces. Maar dat moet wel efficiënt, want elke beveiligingsstap werkt vertragend. Voor het ene bedrijf is dat erger dan voor het andere bedrijf. Op een grote internationale luchthaven bijvoorbeeld, kost elke seconde dat een controlepoort langer dan nodig dicht blijft heel veel geld. Hoe slimmer je het vaststellen van de identiteit inricht, hoe minder tijd verloren gaat met autorisatie om toegang te krijgen. Daarin spelen onze biometrische oplossingen een grote rol."

>> LEES OOK: Horen toegangscontrole en inbraakbeveiliging bij elkaar?

> *"Het volstaat om de vingers in een soepele beweging door een optische scanner te 'vegen'"*

Optische scanner

Waarvan akte in de zwaar beveiligde productielocatie in Haarlem, met de slimme contactloze vingerafdrukscanner MorphoWave (verkrijgbaar bij Aras Security). Daarmee wordt van alle medewerkers bij toegang tot het gebouw de identiteit vastgesteld. Anders dan bij de reguliere vingerafdrukscanner, waarbij mensen ter identificatie één of vier vingers op een scanner moeten leggen, volstaat het bij deze oplossing om de vingers in een soepele beweging door een optische scanner te 'vegen'. Die handeling, in combinatie met een aan de persoon gebonden toegangspas, bevestigt de identiteit. Stemt de vingerscan overeen met de gegevens op de pas, dan mag de medewerker passeren.

Contactloze vingerafdrukscan met MorphoWave.

Balans tussen hospitality en security

Postma: “In vergelijking met traditionele toegangspoorten, hanteert het hoofdkantoor in Parijs bij deze identiteitscheck een bijzondere systematiek. Traditioneel zijn toegangspoorten gesloten en gaan ze open op het moment dat het toegangssysteem vaststelt dat de persoon is wie hij zegt te zijn. Bij ons hoofdkantoor staan de poortjes standaard open en gaan ze onverbiddelijk dicht als de identiteitsgegevens bij de scan niet blijken te kloppen. Dit scheelt tijd en bevordert een snelle doorstroom. Een voorwaarde in situaties met grote aantallen personen die via zo’n toegangspoort een beveiligd gebied in moeten. Deze werkwijze is natuurlijk niet overal toepasbaar. Het hang af van het risicoprofiel van de te beveiligen omgeving. Op ons hoofdkantoor is dit een uitstekende balans tussen hospitality en security.”

>> LEES OOK: Trends in toegangscontrole

Toegangssluis

Voor omgevingen met een extra hoog beveiligingsregime kunnen vingerafdrukscanners worden ingebouwd in een beveiligde eenpersoons toegangssluis. Een combinatie die volgens Postma fraude en misbruik voorkomt, zoals het meelopen door onbevoegden, al dan niet onder bedreiging. “De medewerker biedt eerst zijn pas aan bij de toegangssluis en stapt naar binnen, waarna de deur achter hem sluit. Er is in de sluis ruimte voor slechts één persoon, wat ook nog gecontroleerd wordt door sensoren. Als vervolgens de vingers door de scanner gaan, weet het identificatiesysteem honderd procent zeker dat de medewerker dezelfde persoon is die buiten de sluis de pas aanbood en dat er geen anderen bij hem zijn. Daarop gaat de tweede deur van de sluis open. Deze combinatie biedt maximale zekerheid dat alleen geautoriseerde personen de beveiligde ruimte betreden.”

Contactloze vingerafdrukscan met MorphoWave.

Beperking privacy risico

Dat het vaststellen van identiteit een privacygevoelig issue is, daarvan is men zich bij Idemia als specialist in identiteitscontrole als geen ander bewust. De combinatie van vingerafdrukscan en persoonlijke toegangspas maakt deze securitytoepassing volgens Postma tot een veilig systeem dat ongevoelig is voor fraude of diefstal van identiteitsgegevens.

> *"Wat we niet bewaren kunnen we ook niet kwijtraken"*

"Want de vingerafdrukgegevens van de medewerkers staan uitsluitend op de persoonlijk uitgereikte toegangspassen, waarvoor zij zelf verantwoordelijkheid dragen. Er vindt geen centrale registratie plaats in een database. Daardoor zijn deze toepassingen volledig compliant met de regelgeving onder de AVG. Het geeft ons als organisatie ook een veilig gevoel. Immers, wat we niet bewaren kunnen we ook niet kwijtraken. Maar voor organisaties die goed in staat zijn een beveiligde database met biometrie op te leveren, is het gebruikersgemak van alleen de Wave zonder toegangspas wellicht een aanlokkelijke oplossing. Onze Franse collega's zijn vol trots over deze vorm van toegangsverlening tot hun hoofdkantoor, net zoals ik trots ben op onze lokale high security oplossing"

De kracht van biometrie

Faber en Postma zien een sterke opmars van biometrie in identiteits- en toegangscontroleregimes. De toekomst is volgens Faber dat identiteitscontroles van bijvoorbeeld reizigers op vliegvelden automatisch op afstand op basis van gezichtskenmerken plaatsvindt. Idema heeft hiervoor de 'MorphoFace' toepassing ontwikkeld. Geen

tijdverlies meer in wachtrijen, dankzij biometrische gegevens die op het paspoort of de ID-kaart zijn opgeslagen en die op afstand worden ingelezen. In combinatie met de gezichtsscan, om vast te stellen dat de aanbieder van het identiteitsdocument ook daadwerkelijk de eigenaar is. Ook is een applicatie voor mobiele telefoons ontwikkeld, waarmee reizigers zelf deze verificatie met behulp van de camera in hun eigen telefoon kunnen uitvoeren.

Nieuw: Digimagazine Cameratoezicht »

Faber: "Zo'n oplossing zou heel goed kunnen werken voor zogenaamde 'frequent travelers', die heel vaak op luchthavens door paspoortcontroles moeten. Als je zulke 'bekende en vertrouwde' reizigers via een geautomatiseerd contactloos identiteitscontrolesysteem kunt laten autoriseren, scheelt dat veel wachttijd en kunnen toezichthoudende autoriteiten zich meer concentreren op afwijkende profielen die mogelijk een risico vormen."

Welke securityrisico's wil je afdekken?

Biometrie in de vorm van gezichtskenmerken, irisscan of vingerafdrukken is volgens Faber een ijzersterk security-instrument. "Het is wel zo dat elke oplossing moet zijn afgestemd op het bedrijfsprofiel en het beveiligingsrisico. Welke securityrisico's wil je afdekken? En hoe kan zo'n systeem goed geïmplementeerd worden? Daar moeten bedrijven goed over nadenken. Wat in de ene omgeving wel werkt, is in een andere omgeving wellicht contraproductief. Een systeem als de MorphoWave bijvoorbeeld, zul je niet snel gebruiken in een ziekenhuisomgeving. Zo'n instelling wil openheid uitstralen. Maar in gevoelige overheidsgebouwen en bijvoorbeeld gesloten zorgafdelingen, zijn deze voorzieningen uitstekend toepasbaar."

> *"Biometrie bij identificatie en toegangscontrole levert een zeer hoog securityniveau door de hoge betrouwbaarheid"*

Uitdagingen

Toch zijn er volgens Postma nog wel uitdagingen. Hij wijst op de steeds beter wordende 3D-technieken voor beeldmanipulatie, in combinatie met steeds betere kwaliteit van camera's in mobiele telefoons. "In de opmars van biometrie voor identificatiedoeleinden, moeten we voortdurend bewaken dat met dergelijke slimme beeldmanipulatie de hoge beveiligingsgraad van contactloze biometrische scans niet wordt omzeild. Bijvoorbeeld door een foto- of video-opname te misbruiken voor gezichtsherkenning. Slimme functionaliteiten, die bijvoorbeeld bij een vingerafdruk aan de hand van temperatuur kunnen vaststellen dat een echte vinger door de scanner gaat, beperken dat manipulatierisico. In onze visie waarborgt biometrie bij identificatie en toegangscontrole een zeer hoog securityniveau door de hoge betrouwbaarheid en zullen deze toepassingen steeds meer worden toegepast."

Rob Jastrzebski is freelance journalist