

Inloggen met vingerafdruk of irisscan? Beter van niet

Posted on 14 augustus 2024 by Rik Smits

Biometrisch inloggen is hip en gemakkelijk, maar zit vol duistere kanten en regelrechte gevaren. Dan toch maar liever een wachtwoord.

Uit het niets werd mijn schoonvader getroffen door een kanjer van een herseninfarct. De schade zat links, wat onder meer betekende dat zijn rechterhand buiten dienst was en zijn spraak verdwenen. Letterlijk, er kwam de eerste dagen geen geluid meer uit. Terwijl we als een razende logopedie voor hem regelden – je moet er in zulke gevallen snel bij zijn om te redden wat er te redden valt – ontdekten we ook ineens hoe afhankelijk we allemaal geworden zijn van computersystemen en identificatieprocedures. Want wat waren zijn inloggegevens bij de bank, en wat was zijn pincode, en die van zijn scannertje? Wat was de toegangscode van zijn eigen pc? Hij wist het allemaal nog wel, zo zou weken later blijken, maar vooralsnog kon hij het niet zeggen of opschrijven, en een toetsenbord zei hem even helemaal niks meer.

Zo kan het moderne leven zomaar veranderen in een gekmakende hordenloop

tussen kastjes en muren. Zo ontdek je hoe vaak je je tegenwoordig moet identificeren, op hoeveel manieren dat kan en hoeveel verschillende eisen allerlei bedrijven en instanties eraan stellen.

Onlangs ventileerde NWO-voorzitter Marcel Levi in *Het Parool* nog maar eens zijn diepe frustratie over dit dagelijkse digitale ongemak, waardoor hij bijvoorbeeld ook al met drie verschillende laptops moet rondsjouwen, omdat de instanties erachter uit veiligheidsoverwegingen maar één specifiek type apparaat contact met hun diensten laten maken. Dat is, hoe je het ook bekijkt, contraproductieve waanzin. Al evenzeer leed hij onder de terreur van instanties die ingewikkelde wachtwoorden eisen, die ook nog eens regelmatig veranderd moeten worden. Hoe kan een mens dat allemaal onthouden?

Biometrie heeft nadelen

Kun je dat nu niet veel eenvoudiger aanpakken, met één simpele identiteitscheck die precies vertelt wie je bent? Ja, dat kan, met biometrie. Dat wordt bijvoorbeeld nu in het paranoïde Amerika bepleit om fraude bij verkiezingen uit te sluiten: 'Een belangrijke stap voorwaarts is het controleren van biometrische eigenschappen als vingerafdrukken, het gezicht en de iris. Wanneer die gebruikt worden in combinatie met automatische controle van NAW-achtige gegevens, kan dat resulteren in een uitzonderlijk hoge mate van accuratesse en betrouwbaarheid', zo meldt de *Electronic Insight Newsletter*.

Het klinkt logisch en efficiënt, en smartphonefabrikanten en bedrijfsbeveiligers maken er al duchtig gebruik van. Toch kleven er grote nadelen en risico's aan biometrische toegangscontrole.

De grootste makke is misschien wel dat grootschalig gebruik ervan inhoudt dat delen van ieders intiemste en meest particuliere gegevens, namelijk die over het eigen lichaam, zonder dwingende reden op enorm veel verschillende plaatsen worden opgeslagen en bewaard. Al die verzamelingen kunnen worden verhandeld en naar eigen goeddunken gebruikt door hun eigenaren, BigTech voorop. Ze kunnen ook worden gehackt door onverlaten en overheden.

Dat is geen kattenpis. De ervaring van alledag leert dat geen enkele grote databank inbraakvrij is. Vergeet ook niet dat, zelfs in een keurige, stevig gewortelde rechtsstaat als de onze, de overheid verreweg de machtigste en gevaarlijkste partij

is waar je als burger in je leven mee te maken krijgt.

De risico's van biometrische gegevens in verkeerde handen zijn bovendien onberekenbaar. Je kunt natuurlijk denken 'ach, wat kun je nou helemaal uit zo'n irisscan afleiden?' maar dat is struisvogelpolitiek. Dit soort biotechnologie ontwikkelt zich razendsnel, dus niemand weet wat er over tien of twintig jaar allemaal mee kan. En eens gegeven blijft gegeven, je leven lang. Biometrische gegevens zijn niet alleen uniek, maar ook onveranderlijk. Ze behoren onverbrekelijk tot de essentie van wie je bent. Daar wil je graag zeggenschap over houden.

Daarnaast is de technologie voor ons, de gecontroleerden, niet inzichtelijk. We weten daarom nooit zeker wat er allemaal gescand wordt. Wie nu je iris scant, kan over een paar jaar misschien zomaar het netvlies even meenemen, bepaalde bloedwaarden meten en wie weet wat nog meer.

Wie is rechthebbend?

Dat klinkt als wel heel veel datageweld voor zoiets banaals als een telefoon of webaccount ontgrendelen, en dat is het ook. In de meeste gevallen is het biometrische sop de kool niet waard, het gaat immers niet om absolute veiligheid. We willen het indringers alleen maar zo moeilijk maken dat ze liever iets anders gaan doen. Bovendien werkt biometrische identificatie meestal met een verkeerd type gegevens. De reden is dat biometrische data van alles vertellen over wie je bent, terwijl meestal alleen relevant is wat je bent.

Wie je bent, is enorm belangrijk als je bijvoorbeeld een partner zoekt. Dan gaat het om iemands stem, geur, motoriek en de blik in zijn of haar ogen. Om de dingen waar je spiegelneuronen op aanslaan, om al die trekjes en eigenschappen die die ene persoon nu juist zo verrukkelijk onderscheiden van alle andere. Voor vrienden maken geldt iets dergelijks, maar verder is wie je bent voornamelijk van belang als het gaat om de inhoud van je medisch dossier, en voor overheidsdiensten die hun pappenheimers terdege in de gaten en op het juiste pad wensen te houden. Denk bijvoorbeeld aan de Chinese staat en, niet te vergeten, de ordediensten van Rusland.

In bijna alle andere gevallen doet wie je bent niet terzake, het gaat slechts om wat je bent. Daarmee bedoelen we: ben je een rechthebbende? Behoor je bijvoorbeeld tot degenen die mogen stemmen, een bepaalde krant, databank of bankrekening mogen inzien, of hotelkamer 213 mogen betreden? In dat laatste geval noem je bij

de receptie je naam, en krijg je een kamersleutel of pasje. Bij vertrek lever je die sleutel weer in en klaar is Kees. In de digitale wereld noem je je accountnaam en is je kamersleutel een vooraf afgesproken wachtwoord.

Bij verkiezingen in wat primitievere landen neemt men op het stembureau vaak een vingerafdruk van de stemmer, maar dat is allerminst een vorm van biometrische identificatie. Die hele vingerafdruk kan zo de vuilnisbak in. Waar het om gaat is de zwarte vingertop die de kiezer eraan overhoudt. Zo wordt voorkomen dat mensen dubbel stemmen: alleen wie schone vingers heeft, krijgt een stembiljet. Simpel, en bij ontbreken van een hoogwaardig bevolkingsregister zo waterdicht als maar kan. In zo'n geval is een schone vingertop dus de sleutel.

Een gebruikersnaam plus wachtwoord is als het gaat om wat je bent zowel simpeler als veiliger dan biometrische identificatie. Wachtwoorden kun je naar believen veranderen, en ook aan een ander overdragen. Je kunt bijvoorbeeld met diens pinpas een boodschap doen voor een zieke ander, zoals mijn schoonvader. Met biometrie kan dat allemaal niet. Ook bevatten wachtwoorden geen enkele gevoelige informatie, bij biometrie is dat per definitie wel zo. Ook is iets als een vingerafdruk gemakkelijker met drang of geweld af te dwingen dan een wachtwoord.

En verder is de inlogprocedure met een wachtwoord volstrekt transparant – er kunnen niet stiekem allerlei zaken gescand, gelezen en aan anderen verklapt worden. Als het heel belangrijk is, zoals bij een bankrekening, volgt een extra controle op je sleutel: bij pinnen moet je behalve je fysieke bankpasje ook je pincode opgeven, en anders moet je na je wachtwoord ook een wisselende inlogcode vanaf je rekeningscanner of via een sms-je intypen.

Niet perfect, wel goed genoeg

Dat is vrijwel waterdicht. Een wachtwoordsysteem heeft maar één echte vijand: de slordige, goedgelovige en luie gebruiker zelf. Noteer op kantoor geen wachtwoorden op gele briefjes aan je monitor of onder je toetsenbord, en laat je machine niet openstaan als je koffie haalt. Gebruik niet de verjaardag van je kind als wachtwoord, enzovoort. Maar hou privé wel nauwgezet een lijst van uw eigen wachtwoorden bij, bewaar die goed en laat een vertrouwd iemand weten waar de boel in geval van nood te vinden is.

Als nu nog fabrikanten en ict-afdelingen ophouden met het stellen van overdreven

eisen aan de vorm van wachtwoorden en ons niet langer dwingen tot het even zinloze als hinderlijke periodiek wisselen van wachtwoord, hebben we tot de quantumcomputer misschien alles kraakbaar maakt een alleszins redelijk beveiligde omgang tussen particulier en machine. Niet perfect, maar wel goed genoeg, en daar gaat het om.

Rik Smits *is taalkundige en wetenschapsjournalist.*

Wynia's Week *wordt mogelijk gemaakt door de lezers, kijkers en luisteraars. Bent u al donateur? Hartelijk dank!*