WYNIA'S WEEK

Niet alles wat technisch mogelijk is, is maatschappelijk verstandig. Dat geldt ook voor de digitale EU-identiteit

Posted on 12 maart 2026 by Gastauteur

*Door Eric Zaat**

De recente ophef rond datalekken en hacks bij commerciële bedrijven, zoals het incident bij telecomprovider Odido, laat zien hoe groot de maatschappelijke onrust kan zijn wanneer persoonsgegevens op straat belanden. Terecht: niemand wil dat zijn gegevens rondzwerven.

Zulke incidenten zijn, hoe vervelend ook, meestal herstelbaar. Accounts kunnen worden geblokkeerd, wachtwoorden gewijzigd en contracten worden aangepast. De impact kan groot zijn voor individuele slachtoffers, maar zelden ontwrichtend voor de samenleving als geheel. Bij een digitale kernidentiteit ligt dat echter fundamenteel anders: dan raakt een incident niet een losse dienst, maar de

toegangspoort zelf.

In de Europese plannen voor een digitale identiteit, de *EU Digital Identity Wallet* (EUDI), onderdeel van de eIDAS 2.0-verordening, gaat het niet om een gewone database of een los account, maar om een digitale kernidentiteit: een infrastructuurlaag waarop toegang tot tal van maatschappelijke systemen wordt gebaseerd. En juist dat maakt het risico van een beveiligingsinbreuk van een geheel andere orde.

100 procent veilig bestaat niet

Dit is geen mening, maar een basisprincipe uit de informatica en cybersecurity. Elk systeem dat bestaat, gebruikt wordt en verbonden is met andere systemen heeft een aanvalsvlak. Een systeem is alleen volledig veilig als het niet wordt gebruikt, niet bekend is en volledig is losgekoppeld (*air-gapped*). En zulke systemen bestaan alleen in militaire kluizen of laboratoria, niet in een digitale samenleving.

Cybersecurity gaat daarom nooit over absolute veiligheid, maar over risicomanagement. En daarbij geldt een eenvoudige regel: hoe groter de mogelijke schade, hoe kleiner het risico dat je kunt accepteren.

Bij een digitale kernidentiteit gaat het niet om een losse applicatie, maar om een sleutel tot verschillende domeinen van de samenleving. Denk aan financiële dienstverlening, overheidsvoorzieningen, identificatie in de zorg en juridische en administratieve processen.

Een beveiligingsinbreuk van zo'n systeem betekent dus niet alleen een datalek. Het raakt het vertrouwen in de infrastructuur waarop economie, zorg en rechtsstaat functioneren. Daarmee ontstaat een nieuw type kwetsbaarheid: als de identiteitslaag wankelt, wankelen opeens meerdere vitale sectoren tegelijk.

Juist daarom vormt zo'n infrastructuur een aantrekkelijk doelwit voor statelijke actoren. Waar cybercriminelen doorgaans uit zijn op financieel gewin, richten staten zich eerder op strategische ontwrichting: het verstoren van vertrouwen in systemen die essentieel zijn voor het functioneren van een samenleving.

In het publieke debat wordt cybersecurity vaak teruggebracht tot het beeld van hackers die van buitenaf een systeem binnendringen. In werkelijkheid is dat slechts

één van de mogelijke aanvalsvectoren, en lang niet altijd de meest effectieve. Veel succesvolle aanvallen op kritieke infrastructuur verlopen via andere routes: infiltratie van organisaties die systemen bouwen of beheren, compromittering van leveranciers in de softwareketen, manipulatie van updates of het langdurig positioneren van insiders met toegang tot gevoelige systemen.

Juist statelijke actoren maken gebruik van dergelijke methoden. Zij opereren vaak over langere tijd, met geduld en strategische doelstellingen. In plaats van snel financieel gewin na te jagen, proberen zij posities te verwerven binnen organisaties met kernsystemen die later, indien nodig, kunnen worden gemanipuleerd of verstoord. Bij een digitale kernidentiteit, die toegang kan geven tot grote delen van de maatschappelijke infrastructuur, maakt dat soort langdurige infiltratie het risico fundamenteel anders dan bij gewone datalekken of cybercriminaliteit.

De mythe van decentralisatie

Een veelgehoord argument is dat de digitale EU-identiteit 'gedecentraliseerd' en '*user-centric'* zou zijn. In technische zin is dat deels waar: de *wallet*-app op de telefoon van de gebruiker kan bepaalde gegevens lokaal opslaan. Maar dat zegt weinig over de onderliggende architectuur. Zulke systemen blijven afhankelijk van centrale of semi-centrale bronnen, registers, *trusted lists* en identiteitsproviders, waar identiteitsgegevens en attributen worden uitgegeven, gevalideerd en bijgewerkt. *Wallets* moeten met deze systemen synchroniseren om betrouwbaar te blijven.

Met andere woorden: ergens in de infrastructuur bestaat altijd een plek waar de referentiegegevens worden beheerd, waar uiteindelijk 'de waarheid' staat waarop alle *wallets* vertrouwen. Juist die vertrouwenslaag vormt het strategische doelwit voor aanvallers.

Wanneer een digitale kernidentiteit op grote schaal wordt gemanipuleerd of gecompromitteerd, is het doel van een aanval waarschijnlijk niet het leegroven van individuele bankrekeningen. De impact ligt eerder in het ontwrichten van vertrouwen in maatschappelijke systemen. Enkele realistische scenario's illustreren dat.

Scenario 1: Na manipulatie van identiteitsattributen slaan compliance- en fraudedetectiesystemen bij banken massaal op tilt. Grote groepen burgers en

bedrijven krijgen tijdelijk geen toegang tot rekeningen of betalingsverkeer, omdat de betrouwbaarheid van de identiteitslaag niet meer kan worden vastgesteld. Pinnen bij de supermarkt, salarisbetalingen en internationale transacties lopen vast of worden preventief geblokkeerd. Het gevolg is onmiddellijke economische frictie en verlies van vertrouwen in het financiële stelsel.

Scenario 2: Aanvallers manipuleren de koppelingen waarmee zorgverleners identiteiten verifiëren voor toegang tot medische dossiers. Ziekenhuizen en apotheken schakelen noodprocedures in omdat niet langer duidelijk is wie toegang mag hebben tot welke gegevens. Herhaalrecepten, verwijzingen en medicatiecontroles worden trager en foutgevoeliger, terwijl personeel meer tijd kwijt is aan administratieve checks. De zorg valt niet stil, maar wordt trager, foutgevoeliger en administratief zwaar belast.

Scenario 3: Door manipulatie van status- en autorisatiegegevens raken juridische en administratieve processen verstoord. Burgers kunnen tijdelijk geen toegang krijgen tot bepaalde overheidsdiensten of procedures, terwijl controlesystemen niet langer zeker weten welke identiteitsstatus betrouwbaar is. Dat kan betekenen dat iemand geen paspoort kan aanvragen, geen bezwaar kan indienen of geen recht op een uitkering kan laten vaststellen. Zelfs beperkte manipulatie kan zo institutionele onzekerheid veroorzaken.

Meer dan een technisch probleem

Deze voorbeelden illustreren een belangrijk punt: dergelijke aanvallen zijn niet primair gericht op financieel gewin, maar op het ondermijnen van vertrouwen in de digitale infrastructuur waarop economie, zorg en rechtsstaat steunen. In moderne samenlevingen draait macht niet alleen om geld of grondgebied, maar ook om controle over systemen van vertrouwen. Wie de digitale identiteit kan manipuleren, kan in principe bepalen wie toegang heeft tot geld, zorg, diensten en rechten. De vraag wie de identiteitslaag beheert en kan ingrijpen bij verstoringen, is daarmee geen puur technische vraag meer, maar een vraag over machtsverdeling en publieke legitimiteit.

Uiteindelijk gaat het hier dus niet alleen om technologie, maar om vertrouwen. Een samenleving waarin burgers niet meer zeker weten of hun digitale identiteit nog klopt, is een samenleving waarin economische transacties, zorgverlening en rechtsbescherming zelf onzeker worden.

Natuurlijk zijn er maatregelen denkbaar om risico's te verkleinen zoals segmentatie, minimale koppeling tussen domeinen, sterke *offline-fallbacks*, maar de Europese *digital-identity*-richting stuurt juist op brede inzetbaarheid en hergebruik van identiteitsattributen over sectoren heen en dat vergroot de potentiële impact als er toch iets misgaat.

De ongemakkelijke vraag

De vraag die daarom gesteld moet worden is niet alleen of we zo'n systeem technisch kunnen bouwen. De vraag is of het verstandig is om een digitale infrastructuur te creëren waarvan de onvermijdelijke faalmodi zo'n brede maatschappelijke impact kunnen hebben. Politiek en samenleving moeten expliciet afwegen hoeveel concentratie van digitale macht acceptabel is, en welke noodremmen dan nodig zijn, vóórdat de infrastructuur onomkeerbaar is uitgerold. Niet alles wat technisch mogelijk is, is maatschappelijk verstandig om te bouwen.

*****Eric Zaat*** *is onafhankelijk strategisch adviseur op het gebied van informatievoorziening, IT-architectuur en governance.*

Wynia's Week *verschijnt 156 keer per jaar en wordt* ***volledig mogelijk gemaakt*** *door de donateurs. Doet u mee?* ***Doneren kan zo****.* ***Hartelijk dank!***