Een slimmere en veiliger wereld

Inleiding.

De enorme toename van het aantal transacties dat via netwerken tot stand komt wordt door veel factoren gedreven. De wet van Moore en de wet van Metcalve spreken respectievelijk over het blijvend toenemen van de snelheid van computersystemen en het ontwikkelen van de functionaliteit van netwerken en het internet.

Visies over een “smarter planet” bouwen verder op deze ontwikkelingen en zijn gebaseerd op drie I’s. Als eerste “Instrumented”. Wij zijn in staat om de exacte conditie van ongeveer alles te meten, te voelen en zien. “Interconnected” als tweede, Mensen, systemen en objecten kunnen met elkaar communiceren en interacteren op allerlei nieuwe manieren. En tenslotte “Intelligent”. De mogelijkheid om sneller, precieser en veiliger te kunnen reageren en betere resultaten te verkrijgen en door toekomstige gebeurtenissen beter te kunnen voorspellen.

Het idee van een “smarter planet” heeft wereldwijd weerklank gevonden en heeft een impact die niet alleen ervaren wordt over alle sectoren en industrieën heen maar ook in ons dagelijkse leven.

Van gegevens naar intelligentie.

Een dergelijke geïnstrumentaliseerde en gekoppelde wereld zal geconfronteerd worden met massale hoeveelheden gegevens en transacties. In allerlei formaten; medische gegevens, scans, informatie van beveiligingscamera’s, verkeersbewegingen, betalingen,supply-chain sensoren etc zorgen voor gegevensstromen met een snelheid die we nauwelijks kunnen bijhouden. Nieuwe analystische middelen helpen ons om waarde te onttrekken aan deze overvloed van gegevens. Om patronen en correlaties te ontdekken. We kunnen de maat gaan nemen van alle informatie wereldwijd en daadwerkelijk beginnen met het anticiperen op en het voorspellen van afwijkingen en veranderingen in systemen, bedragen, patronen en gedrag.

Tegen welke prijs?

Al deze technologische ontwikkelingen, met name de toenemende mogelijkheden om de informatie uit meerdere bronnen te combineren en te analyseren zullen de discussie over persoonlijke informatie en het gebruik en misbruik daarvan verder intensiveren.
Het is dan ook de hoogste tijd dat er meer aandacht besteedt wordt aan “identity management” oplossingen. In de private sector sector zien we al veel ontwikkelingen, maar met name bij de overheid zien we nog te weinig activiteiten. Terwijl daar grote kansen liggen, niet alleen op het ontwikkelen van nieuwe en betere diensten maar ook ten aanzien van het herstellen van vertrouwen en het bieden van zekerheid dat de vertrouwelijkheid van persoonlijke gegevens absoluut gegarandeerd is.

De privacy paradox

In deze digitale eeuw zoeken burgers zowel meer gemak als meer zekerheden in hun dagelijkse handelen. Maar al te vaak wordt er daarbij naar de overheid gekeken met de vraag dit ook te gaan realiseren. Aan de andere kant is er sterke oppositie tegen allerlei maatregelen die de overheid wil nemen. Oppositie op basis van privacy argumenten en beroep op burgelijke vrijheid. Dit spanningsveld noemen we de privacy paradox.
Een van de onderliggende elementen hierbij is identiteisbeheer, “identity management”,

Identity Management is een systeem van wetgeving en gebruiken, technologieën en gebruiken die:

- De gemeenschappelijke behoeften van overheid en bedrijfsleven ten aanzien van identiteit bij transacties ondersteunen.
- Transactiekosten verlagen en de dienstverlening verbeteren
- De veiligheid van het publiek vergroten
- De individuele privacy handhaven en verbeteren.

In veel landen zijn wet- en regelgeving maar ook culturele aspecten er de oorzaak van dat er geen betere en effectievere identity management strategie kan worden geïmplementeerd. Op die manier blijft de discussie en samenwerking op het gebied van identy management beperkt tot technische research, expert groepen en standaardisatie activiteiten. En hoe geavanceerd de technologie ook moge zijn, IT alleen is niet voldoende voor het implementeren van privacy-beschermende oplossingen die aan alle verwachtingen van publiek en overheden tegemoetkomen.
Ondanks de beschikbaarheid van de huidige security oplossingen als op smart cards gebaseerde authenticatie, biometrie en op rol en regel gebaseerde gegevensbeveiliging blijkt dat uitgebreide training van medewerkers gecombineerd met security processen op meerdere nivo’s nog steeds het belangrijkste middel is om de bescherming van identity management te realiseren.
De uitdaging voor het bedrijfsleven en de overheid is om effectief gebruik te gaan maken van de hedendaagse security technologieën bij het ontwikkelen en integreren van toepassingen in een open en flexibele architectuur die garant staat voor data security en identity management.
Zo zouden overheden zich moeten realizeren en communiceren naar alle belanghebbenden, dat een goed geregelde security en een verbeterde privacy geen elkaar uitsluitende zaken zijn. Duidelijke doelstellingen zijn daarbij onontbeerlijk. Daarnaast zullen moderne IT oplossingen die zich confirmeren aan compliancy regels en gebruik maken van de facto en de jure standaards samenwerking tussen overheden en het bedrijfsleven faciliteren.
En tenslotte dienen overheden en bedrijfsleven schouder aan schouder te werken om wetgeving en regulering te adopteren en te moderniseren en in een samenhangend identity management proces te formuleren. Maak **vantevoren** afspraken wat mag en wat niet mag. De IT kan alles verwezenlijken, maar wat willen de gebruiker? Wat exact zijn de 'security' eisen? Kortom, afgesproken procedures in de vorm van doctrine en/of SOPs (Standard Operating Procedures) zijn essentieel.
Een goed governance model, waarin alle belanghebbenden vertegenwoordigd zijn en de implementatie van technische werkgroepen zijn voorwaarden voor succes. Synergie zal bereikt kunnen worden door binnen dit governance model de initiatieven op verschillende gouvernementele nivo’s te consolideren via werkgroepen die bestaan uit experts op de onderscheiden gebieden.
Er is werk te doen!

John Post, CTO IBM Benelux