Maar het is wel een mens!

In mijn vorige stukje schreef ik over de enorme mogelijkheden van computers, naar aanleiding van een opmerking over de eerste IBM (speelgoed)computer. 'Maar het is wel een computer!' Onbeperkte mogelijkheden, die uiteraard samengaan met nog onbeperktere problemen. Helaas gaat in onze wereld alleen de zon voor niets op. Ik schreef al dat de nabootsing van de werkelijkheid – de virtuele werkelijkheid – de sterke maar ook de zwakke kant van computers is. Na de sterke kant vorige keer, nu aandacht voor de zwakke kant en voor de mens.

Het is een bekend feit dat elektronische informatie geen identiteit bezit, niet uniek is zoals een mens. Alles wat in elektronische vorm bestaat, is eenvoudig te kopiëren. In de elektronische wereld bestaat geen verschil tussen origineel en kopie, tenzij dat uitdrukkelijk in een attribuut is vastgelegd (dat eenvoudig kan worden veranderd). Dit maakt het mogelijk informatie gemakkelijk te verspreiden en op verschillende manieren weer te geven. Het maakt het ook even gemakkelijk om te frauderen.

Communications Week International van 16 januari jongstleden geeft enkele cijfers. HP-Duitsland verloor eind vorig jaar 400.000 dollar aan 'gestolen' telefoongesprekken in één maand tijd. Men schat de verliezen door 'telecomfraude' in Duitsland op 350 miljoen dollar per jaar. In Europa lopen we achter op de Verenigde Staten, waar men de verliezen door fraude op 5 miljard dollar per jaar schat. Dat is niet gering, want het gaat hier alléén over het door iemand anders laten betalen van internationale gesprekken, niet over computerfraude (het bekijken of veranderen van gegevens in een computer). Met nieuwe mogelijkheden ontstaan steeds meer mogelijkheden voor misbruik – ook wat dat betreft is er niets nieuws onder de zon.

De situatie rond de beveiliging van elektronische informatie is die van een steeds veranderende status quo. Omdat elke vorm van beveiliging helaas ook het gebruik door de legale gebruikers bemoeilijkt, moet een afweging gemaakt worden tussen de beveiliging en de gevaren. Gelukkig werk ik alleen thuis en hoef ik dus niet meer elke twee maanden een nieuw wachtwoord te verzinnen en te onthouden. Zoals een collega het laatst stelde: "Je moet de steeds slimmer wordende boeven proberen voor te blijven door steeds nieuwe maatregelen. Een echte, definitieve oplossing bestaat helaas niet." Dat is jammer, maar dit is de echte werkelijkheid.

Beveiliging hangt natuurlijk ook samen met de nieuwe heilige koe, *privacy*. Allerlei nuttige dingen zijn op dit moment niet meer mogelijk, omdat het onze privacy zou kunnen schaden. Ik heb bezwaar tegen het dragen van een geel oormerk - mijn oren zijn toch al niet zo fraai. Maar ik denk wel eens, waarom implanteren wij niet een unieke chip in ieder mens, die hem of haar een unieke elektronische identiteit geeft? Zoiets werkt fantastisch, heb ik vorig jaar tijdens de wintersport in Zwitserland ontdekt. In plaats van magneetkaarten die je moeizaam in gleuven moet steken, hadden ze daar een soort credit card met een chip (van Nederlands fabricaat) die radiografisch werd uitgelezen als je door een poortje liep. De oplossing kent natuurlijk beperkingen, want met zo'n chip in je bast moet je wel lijfelijk aanwezig zijn om

jezelf te identificeren. Het grote voordeel is eigenlijk alleen dat er geen mensen nodig zijn voor de identificatie. Helaas moet je unieke elektronische identificatie wel gekoppeld worden met je werkelijke naam, adres en banknummer; die koppeling in een computer is natuurlijk eenvoudig te frauderen.
De grote nieuwe rage is een aansluiting op Internet. Voor dergelijke elektronische diensten heeft zo'n chip in je lijf geen zin. Het leuke van Internet is wel dat het, afgezien van enkele snelle verbindingen, geheel bestaat uit lokale netwerken. Je betaalt voor de toegang tot zo'n netwerk, maar niet voor de communicatie over de hele wereld en daarmee kan in principe dus ook niet gefraudeerd worden. Maar omdat er ook bedrijfsnetwerken en -computers aan Internet gekoppeld zijn, schep je voor hackers wel de mogelijkheid om binnen te komen. Ik las in oktober dat de geheimschriftkundige David Chaum elektronisch geld had uitgevonden: E--cash, dat voor een proef nu als speelgoedgeld op Internet gebruikt gaat worden. Een nuttig ontwikkeling, omdat het natuurlijk geen goede zaak is om je creditcardnummer of PIN-code via Internet te versturen. Ik heb er sindsdien niets meer over gelezen, maar je kunt er donder opzeggen dat het systeem nu al gekraakt is. Zo niet, dan komende zomer. Alles wat met computers geschiedt, kan ook door computers worden nagebootst. Veilig en uniek zijn alleen die zaken die opgeslagen zijn in een menselijk brein. Je kunt een mens bedreigen, zelfs martelen, maar als hij of zij die niet wil prijsgeven, blijft de informatie veilig. Aftappen of kopiëren kan niet. Mensen vergeten wel dingen, en soms maken zij fouten. Een accountant van het grootste beleggingsfonds ter wereld (Amerikaans) vergat een min toe te voegen, waardoor een negatief beleggingsresultaat van 1,3 miljard dollar ten onrechte veranderde in een koerswinst van 1,3 miljard. Het goede nieuws is dat de robots van autofabrikant Toyota, eens bejubeld als hèt symbool van verregaande fabrieksautomatisering, worden vervangen door meer flexibele mensen. Mensen hebben wel eens moeite met hun eigen identiteit, maar ze herkennen feilloos die van anderen. Via de elektronische media kunnen ze gemakkelijk voor de gek worden gehouden, maar ze houden wel hun hand op de knip. Misschien moeten we bij het praten over anderen vaker denken: maar het is wel een mens!

Hein van Steenis (Computable 25 februari 1995)