ZATERDAGS
NRC HANDELSBLAD

8 OKTOBER 1983
BIJVOEGSEL

OP ZOEK NAAR EEN RAMPENPLAN VOOR DE KWETSBARE SAMENLEVING

Frank Kuitenbrouwer

EEN computerkraak is kinderspel. Dat is de afgelopen zomer weer eens bewezen door een groepje scholieren in de Amerikaanse stad Milwaukee die op afstand vanachter hun computereindstations spelenderwijs inbraken bij ogenschijnlijk zwaarbeschermde databanken.
In een hoofdartikel zag de *Washington Post* hierin vooral het teken van een generatiekloof. De vanzelfsprekendheid waarmee jongeren opgroeien met de computer leidt tot meesterschap waar ouderen slechts intimidatie voelen, zo constateerde het gezaghebbende dagblad ietwat afgunstig. Het legde de caesuur bij vijfendertig jaar.
In werkelijkheid was aan beide zijden van deze leeftijdsgrens verbijstering troef. 'Ik schrok me een hoedje toen ik hoorde dat het om kankerpatiënten ging', zei Neal Patrick (17 jaar) die was binnengedrongen in de databank van het Memorial Sloan-Kettering kankerinstituut in New York. Hij en zijn makkers hadden zich niet gerealiseerd wat ze uitgericht hadden tot ze werden gewaarschuwd door alarmsignalen uit het gekraakte systeem en via de nieuwsberichten.
Omgekeerd signaleerde de computer van Sloan-Kettering wèl dat er opeens vijf nieuwe gebruikers waren zonder behoorlijke legitimatie. Maar waar ze vandaan kwamen kon het systeem met al zijn ingebouwde zekeringen niet achterhalen. 'Wij zouden vooral willen weten hóé ze in het systeem zijn binnengekomen', was de eerste reactie van het hoofd van het rekencentrum.
Het is dit wederzijdse karakter van het blindemanspelletje dat de episode pas echt griezelig maakt. Niemand zal verlangen dat computers waterdicht veilig zijn. Dat geldt per slot van rekening ook niet voor de belastingen, het verkeer en het gemiddelde huishoudkastje. Maar als aanvaller en verdediger over en weer compleet in het duister tasten, geeft dat toch te denken over de kwaliteit van de moderne informatiesystemen.
Die informatiesystemen zijn géén kinderspel. Met name de steeds groeiende computernetwerken vormen het zenuwstelsel van de hedendaagse maatschappij. *Telematica* (de combinatie van computers en telecommunicatie) is aan de orde van de dag. Zijn we als samenleving niet bezig ons té afhankelijk te maken van moderne informatietechnologieën.

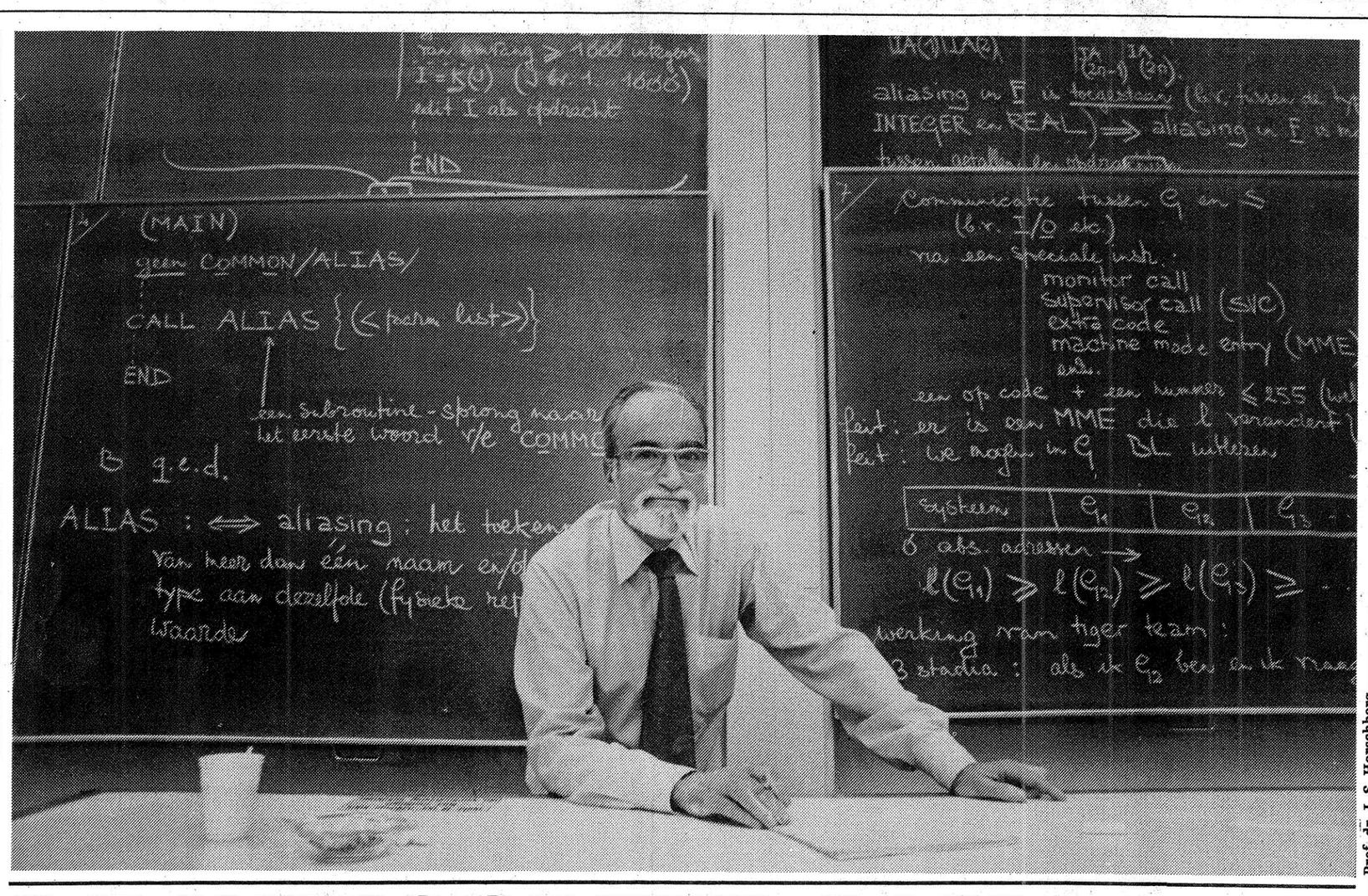
Mankementen

Zweden heeft als eerste de kat de bel aangebonden. In 1979 rapporteerde daar een speciale staatscommissie: 'De kwetsbaarheid van de hedendaagse computersamenleving is onaanvaardbaar hoog'. De commissie inventariseerde niet minder dan vijftien afzonderlijke kwetsbaarheidsfactoren.
Deze varieerden van gebrekkige systeemdocumentatie (zodat het bijvoorbeeld bij panne moeilijker wordt te achterhalen waar mogelijke groeistuipen zitten) tot computermisdaad en het afsnijden van buitenlandse aanvoerlijnen.
De toenemende centralisatie en integratie van geautomatiseerde gegevensverwerking is volgens de Zweden het grootste afzonderlijke risico. Netwerkbouw brengt het gevaar mee dat fouten of ongelukken een 'watervaleffect' hebben tot ver buiten hun bron. Ook de pure omvang (en ingewikkeldheid) van steeds meer databanken is riskant.
Computermalheur kan er inderdaad flink inhakken. Een electronische storing maakte onlangs dat de effectenbeurs van Stockholm voor het eerst sinds de crisis van de jaren dertig moest sluiten. 'Het is een schandaal', zei een verontwaardigde effectenmakelaar, 'je kunt je effecten niet krijgen én je kunt je geld niet krijgen.'
Een computerfout bij het verlengen van het huurcontract van een federaal kantorencomplex in San Francisco, die vorige herfst aan het licht kwam, is de Amerikaanse belastingbetaler op miljoenen dollars schade komen te staan. Aanloopmoeilijkheden met de computers van de staat New York brachten aannemers van werk, tehuizen voor geestelijk gehandicapten en zelfs volksvertegenwoordigers in geldnood.
'Als zo'n systeem niet uitbetaalt ben je inderdaad nog niet jarig,' zegt een hoge Nederlandse ambtenaar *off the record*. 'Er kan in Amsterdam bijvoorbeeld van alles mis gaan, maar als de computer van de Sociale Dienst het echt laat afweten is dat een geheid recept voor revolutie.'

Kwetsbaarheid

De gevaren blijven natuurlijk altijd betrekkelijk. Zelfs een spectaculaire electriciteitsstoring als de *black out* van New York in 1977 leidde niet tot ineenstorting van het computerverkeer aan de Amerikaanse Oostkust. En wellicht is ook hier het geluk enigszins met de goddelozen; slechts 10 tot 25 procent van de Amerikaanse bedrijven die sterk afhankelijk zijn van computers heeft een behoorlijk rampenplan, meldde de *International Herald Tribune*.
De Zweedse regering was in elk geval voldoende onder de indruk om in 1981 een *Särbarhetsberedningen* (Raad voor de veiligheid) in te stellen. Deze heeft een serie vervolgonderzoeken op touw gezet en praat met het bedrijfsleven om de bewustwording te bevorderen. Tot de opties behoort een vergunningenstelsel met 'robuustheidseisen' voor vitale computersystemen.
Eerder heeft Zweden ons het leerstuk van openbaarheid van bestuur gebracht. In 1973 liep het voorop met wetgeving op de 'computer privacy'. Wordt nu een nieuwe trend ingeluid?
De OESO (Organisatie voor economische samenwerking en ontwikkeling) pikte de issue van de kwetsbare computersamenleving snel op. In 1981 belegde zij in het Spaanse plaatsje Siguënza een conferentie over de risico's die afhankelijkheid van informatietechnologie meebrengt voor 'gelijkberechtiging van groepen burgers, de sociale stabiliteit en de nationale soevereiniteit'.
Mede op verzoek van Nederland is een commissie van de OESO nu bezig deze ruim bemeten agenda verder uit te werken.
De Verenigde Staten — die zichzelf met enige reden als het computercentrum van de wereld beschouwen — waren niet overtuigd. Een zware commissie uit de overkoepelende organisatie van genootschappen voor informatieverwerking AFIPS kwam eind vorig jaar met een tegenrapport onder de uitdagende titel: 'De veerkracht van de informatiemaatschappij'.
Hebben de Zweden, en in commissie de OESO, er dus niets van begrepen? Dat kan zeker niet gezegd worden, want het hangt er nogal van af van welke kant van de oceaan men tegen de kwestie aankijkt. De Zweedse studie gebeurde in opdracht van het ministerie van defensie en werd in de eerste plaats ingegeven door overwegingen van neutraliteitspolitiek: de afhankelijkheid van het buitenland op computergebied.
Die afhankelijkheid is voor verschillende landen een probleem, zo geeft het AFIPS-rapport ook eerlijk toe. Het onderkent zorg over een gebrek aan evenwicht in de internationale telematica ten gunste van de VS. Omgekeerd hoeft Amerika, met zijn onmiskenbare informatie-overwicht zich daar niet zoveel zorgen over te maken.
De kwetsbaarheid van de een is de veerkracht van de ander. Amerika is er juist bezorgd over dat beschermende maatregelen inbreuk maken op het zozeer gekoesterde beginsel van *free flow of information* in de wereld. — óók in het computertijdperk. De

Vervolg op pagina 2

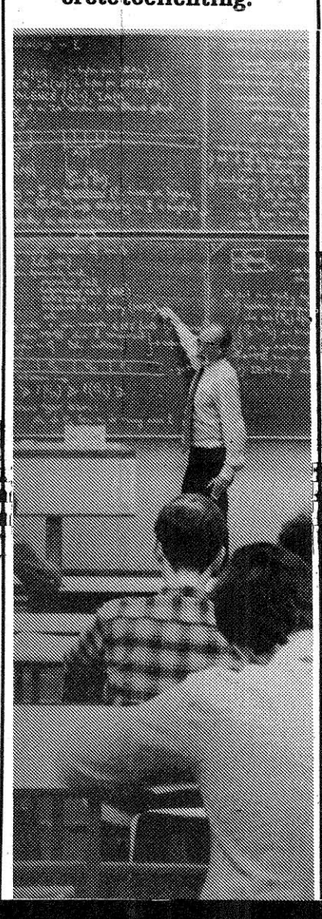


Prof. dr. I. S. Herschberg

FOTO'S LEO VAN VELZEN

DE INDISCRETE COMPUTER

Computerkraken beginnen ook in Nederland de gemoederen meer en meer bezig te houden. Komende week is dit een thema van de ASI-leergangen 1983, een co-productie van het Koninklijk Instituut van Ingenieurs en het Nederlands Genootschap voor Informatica. De titel van de leergang, 'In de ban van de Fout', is ontleend aan de Delftse oratie van dr. I. S. Herschberg, een befaamd systeemkraker. Hij spreekt over 'Misbruik, vervuiling en ondoordringbaarheid' van computers. Een andere inleider is NRC Handelsblad-commentator mr. F. Kuitenbrouwer, die het daar (en ook alvast hieronder) heeft over 'De kwetsbare computermaatschappij'. Cas de Stoppelaar geeft aan de hand van de onoorbare praktijken enige concrete toelichting.



TIPS VAN EEN MEESTERKRAKER

Cas de Stoppelaar

HET was op een woensdag niet lang geleden, 's morgens om vijf voor half elf, aan het einde van een twee uur durend college in de informatica aan de TH Delft. De studenten van de hooggeleerde meesterkraker prof. dr. I.S. Herschberg, die zijn sporen op het gebied van computerbeveiliging bij Unilever heeft verdiend en inmiddels een reputatie heeft opgebouwd om iedere computer te kunnen 'binnenkomen' met programmeertrucs, spitsen hun oren wanneer de kleine professor met twinkelende ogen zegt: 'En nu zal ik tot slot u nog een tip geven hoe u zonder veel moeite de *useridentity* en het *password* van iemand anders te weten kan komen.' (De useridentity — gebruiksnummer — en het daarbij behorende password — wachtwoord — zijn de codes, op grond waarvan een computer weet of hij de juiste man aan de lijn heeft).
Herschberg vervolgt: 'U schrijft een klein programmaatje, waarin u *simuleert* of u de computer bent. Dus u zorgt dat de volgende woorden op de *terminal* verschijnen bij degene wiens codes u wilt ontfutselen: "Here is your system XYZ, Please log on".
Hij legt uit hoe het werkt: ieder computer-systeem maakt zich op deze wijze bekend, en na de woorden *log on* moet de gebruiker zich melden met een gebruiksnummer van bijvoorbeeld een letter en vijf cijfers en een codewoord van zes symbolen; dit kan zijn (heel voor de hand liggend en daarom zo makkelijk te raden door spelende schooljongens): 'geheim', maar ook '$&!!A'. Een slimme code is, wegens het oneindige aantal variaties, niet te raden. 'Dan', vervolgt Herzberg, 'komt het te bestelen slachtoffer binnen. Hij wil aan het werk en ziet tot zijn vreugde op het beeldscherm dat de computer zich al heeft gemeld. Hij tikt onder de text zijn user-identity en password. Wat gebeurt er dan? Het door de kraker opgestelde programma slaat deze gegevens op en tikt op het scherm: "Mismatch. Please log on again". De inmiddels bestolene denkt dat hij iets fout heeft getikt en probeert het opnieuw, waarna hij *wel* contact krijgt met de computer. En dit, mijn heren, is hoe u codes kunt verzamelen en in computers kunt inbreken."
De zaal met studenten lacht, de klok slaat half elf en ieder stroomt zijn weegs.
Een student, die stage loopt bij een grote Nederlandse instelling, gaat 's middags achter zijn toetsenbord zitten en schrijft het programma zoals zijn professor het die morgen heeft verteld. Om half vijf die middag heeft hij al 17 geheime toegangssleutels tot de computer en de volgende dag heeft hij ze allemaal — althans van iedere medewerker in het bedrijf die op de computer heeft zitten werken. In principe zit nu alle informatie van de computer voor hem 'onder de toetsen'. Hij stelt de directie op de hoogte en men schrikt. Niemand had iets gemerkt, zoals zijn professor eerder voorspelde.

Bit-niveau

Herschberg zit nu in zijn kale kamer aan de TH, onder een met geheime formules volgeschreven bord en verlustigt zich in het opsommen van meer trucs, die wat lastiger zijn en 'afdalen tot op het bit-niveau'. Hij verschafte zich met een *basic*-programma toegang tot *assembler*, een programmeertaal die de machine op een dieper niveau bestuurt en geen beveiligingen heeft zodat hij de computer alle opdrachten kon geven die hij wilde. Ook kent hij een geval waarin een student op zijn huiscomputer de op *floppy disc* opgeslagen informatie uit een grote computer kon lezen — en wijzigen. Hij kwam er achter dat hij maar 1 bit in een bepaalde code hoefde te veranderen en de grote computer deed alles wat hij zei. Zo zijn er vele voorbeelden, en beveiliging daartegen is zo ingewikkeld dat Herschberg zegt: 'Zelfs de door mijzelf voorgestelde verbeteringen in het systeem kon ik uiteindelijk zonder moeite kraken'.
In zijn tijd bij Unilever had hij zich eens toegang verschaft tot de computer van hun grootste wasmiddelen-concurrent Procter and Gamble. 'Daar stonden we. Moesten we hun *five years program* opvragen of niet?'

Wat deed u?

Met zedig neergeslagen ogen zegt hij: 'Niet'. Inmiddels zijn mij uit betrouwbare bron — vanzelfsprekend anoniem — verhalen ter ore gekomen over bedrijfsspionage waarin deze beslissing duidelijk *positief* uitviel. Een met zonnebril bedekte informant, die in zijn zakelijk leven automatiserings-opperhoofd is bij een belangrijk telecommunicatiebedrijf, vertelde me zojuist dat hij eens toevalligerwijs terecht kwam achter de computer van een collega in een concurrerend bedrijf. Hij probeerde als password de naam van diens secretaresse en BLIEB, de gehele voorraad gegevens viel als guldens uit een Jackpot in zijn schoot. Het was ten tijde van een belangrijke concurrentieslag in Saoedi Arabië en je zou toch ook gek zijn als je niet dóórvroeg, nietwaar?

Er dient, technisch gezien, een onderscheid gemaakt te worden tussen een 'volledige kraak' en een 'beperkte kraak'. In het eerste geval heeft de inbreker toegang tot alle opgeslagen informatie, kan hij deze bovendien wijzigen (ook uitwissen), en laat hij bijvoorbeeld de rekening van de gebruikte computertijd op iemand anders' naam zetten. Hij hoeft geen sporen na te laten, zeker geen sporen die naar hemzelf wijzen. Er is dus een kans dat de inbraak niet gemerkt wordt. Bij een beperkte kraak zijn de mogelijkheden van de dief geringer.
Er verschijnen de laatste tijd in de pers allerlei avonturen van knaapjes die inbreken in computers, zoals van het Los Alamos National Laboratory (waar — koren op de molen van de mensen die nog *bang* zijn van computers — kernwapengegevens te halen zouden zijn) en in het Sloan-Kettering Cancer Centre waar ze bestralingsgegevens van kankerpatiënten te pakken kregen. Het blijken scholieren, die een beetje zitten te stoeien achter hun beeldscherm — een eigentijds soort krijgertje, dat volgens een verhaal in het weekblad Newsweek van vorig jaar hen een speciaal soort *kick* geeft getuige een 13 jarige *whizkid*: 'Man, het gevoel in je vingertoppen... de macht over het systeem... het is *the sensation of power man*, die ik alleen ervaar als ik achter het scherm ga zitten, nergens anders.'
Het belang van deze gevallen is niet de ramp die geschiedt (er gebeurde tot op heden eigenlijk niks) maar het bewijs hoe lek beveiligingssystemen zijn. 'Als een vergiet', zei Herschberg in een symposium over dit onderwerp dit voorjaar. Hij vervolgde toen: 'En bij een vergiet weet je tenminste waar de gaten zitten, maar bij computers niet.'
Hoe heeft het zo ver kunnen komen?
Er zijn meerdere redenen voor. In de eerste plaats was het wereldje van programmeurs 20 jaar geleden als een grote familie. Ik herinner me de gewijde sfeer rond de 'nieuwe' IBM in het Centraal rekeninstituut te Leiden. Men fluisterde uit eerbied voor De Computer, kende en vertrouwde elkaar, terminals stonden *in* het gebouw en misbruik was uitgesloten.

Misdaad

Nu is dat anders. Een groot bedrijf heeft tientallen, of honderden, terminals buiten de deur. Een luchtvaartmaatschappij heeft er duizenden over de hele wereld. Weliswaar hebben deze maatschappijen 'huurlijnen' in plaats van 'kieslijnen' (dat zijn gewone telefoonlijnen die iedereen kan draaien als hij het nummer van de computer heeft). In een huurlijn breek je niet makkelijk in, tenzij je de draad aftapt,

Vervolg op pagina 2