

Baas, pas op voor fraude

Niet iedere baas neemt de beveiliging van zijn bedrijfsnetwerk even serieus. Het zal zo'n vaart niet lopen, is de gedachte. Maar dat doet het dus wel: 80 procent van het misbruik wordt van binnenuit gepleegd, door het personeel.

DOOR YVETTE BENNINGSHOF

Wie kent het niet: bij het per ongeluk openen van een besmette e-mail of bijlage wurmt een computervirus zich in het netwerk. Erg vervelend - het kan veel ongemak en schade veroorzaken - maar het is een ongelukje. Schokkender is het bewust stelen van vertrouwelijke bedrijfsinformatie.

Dat deed een werknemer van MCI Communications, een Amerikaans telecombedrijf. Hij werd gearresteerd voor het ontvreemden van 60.000 telefoonkaartnummers die op de bedrijfscomputers stonden opgeslagen. De kaartnummers verkocht hij aan een internationale criminele bende. Dat kostte het bedrijf meer dan 50 miljoen dollar.

Chris Verhoef, hoogleraar Informatica aan de Vrije Universiteit in Amsterdam, geeft nog een voorbeeld van interne computerfraude. Na bijna twee jaar onderzoek door de FBI bij de Amerikaanse belastingdienst bleek dat de volledige salarishistorie van iedere willekeurige Amerikaan voor 175 dollar bij *information brokers* te koop was. Vooral onder werkgevers vonden de gegevens gretig aftrek. Aan de hand van gestolen informatie kon een chef een nietsvermoedende sollicitant een heel scherp salarisbod doen, waarvan ze al bij voorbaat wisten dat het geen cent te veel was.

Verhoef: „In dit geval hadden laagbetaalde werknemers van de overheid heel simpel toegang tot zeer gevoelige informatie op de

computers. Een aantal van hen was ontvankelijk voor omkoping. Jouw privacy gooiden ze voor 25 dollar te grabbel. Want dat was het bedrag dat de information brokers betaalden aan belastingmedewerkers.” De belastingdienst heeft nu een systeem ingebouwd dat automatisch precies bijhoudt welke werknemer toegang heeft

tot welke data. Sommige fraudepraktijken in Amerika zijn beter gedocumenteerd dan in andere landen, maar ook in de Verenigde Staten probeert men de kaken stijf op elkaar te houden als het gaat om het buitenhangen van de vuile was.

Dat betekent bepaald niet dat interne fraude in ons land nauwelijks voorkomt. Toch lopen bedrijven niet direct warm voor investeringen in de beveiliging van hun

Personeel pleegt 80 procent van computer-misbruik

computernetwerk, want het gevaar is niet direct aan de oppervlakte zichtbaar. Door 11 september 2001 begint daar wel verandering in te komen, merkt Gilbert Houtekamer van Consul Risk Management, een bedrijf dat 'zijn klanten helpt een veilige IT-omgeving te creëren en te be-

houden’.

Houtekamer weet uit onderzoek dat 80 procent van de fraude van binnenuit komt. „Het besef begint nu pas door te dringen dat IT een business is die je moet managen en beveiligen”, zegt Houtekamer. „Toen ik in '86 met Consul begon, ging mijn aandacht vooral naar grote bedrijven. Vaak zagen ook die de noodzaak niet in van het belang van een goede beveiliging.”

Een baas die zijn personeel scherp in de gaten wil houden, heeft tegenwoordig de keuze uit diverse softwareprogramma's die al het verkeer op een computernetwerk registreren, zoals eAudit van Consul. Dit meet- en managementsysteem kan op verschillende controleniveaus worden ingesteld. Zo is het ook geschikt voor de Nederlandse markt, want het is hier volgens de wet niet toegestaan alle handelingen op het werkstation van een personeelslid te volgen. Dat is schending van de privacy. Verhoef: „Het gevaar bestaat anders dat de werknemer kan worden afgerekend op zijn productiviteit. Want dat is allemaal te achterhalen aan de hand van zijn verrichtingen op het

computernetwerk. De vraag is of dat wel zo gewenst is.”

In hoeverre een baas het nodig vindt zijn netwerk tot in de puntjes te controleren hangt af van de bedrijfscultuur. En: hoe belangrijk privacy en tolerantie binnen dat bedrijf zijn. Verhoef: „Volgens de Nederlandse wet moet de privacy zo min mogelijk geschonden worden. Als er voor een probleem een minder privacy-gevoelige oplossing is, moet voor die variant gekozen worden.”

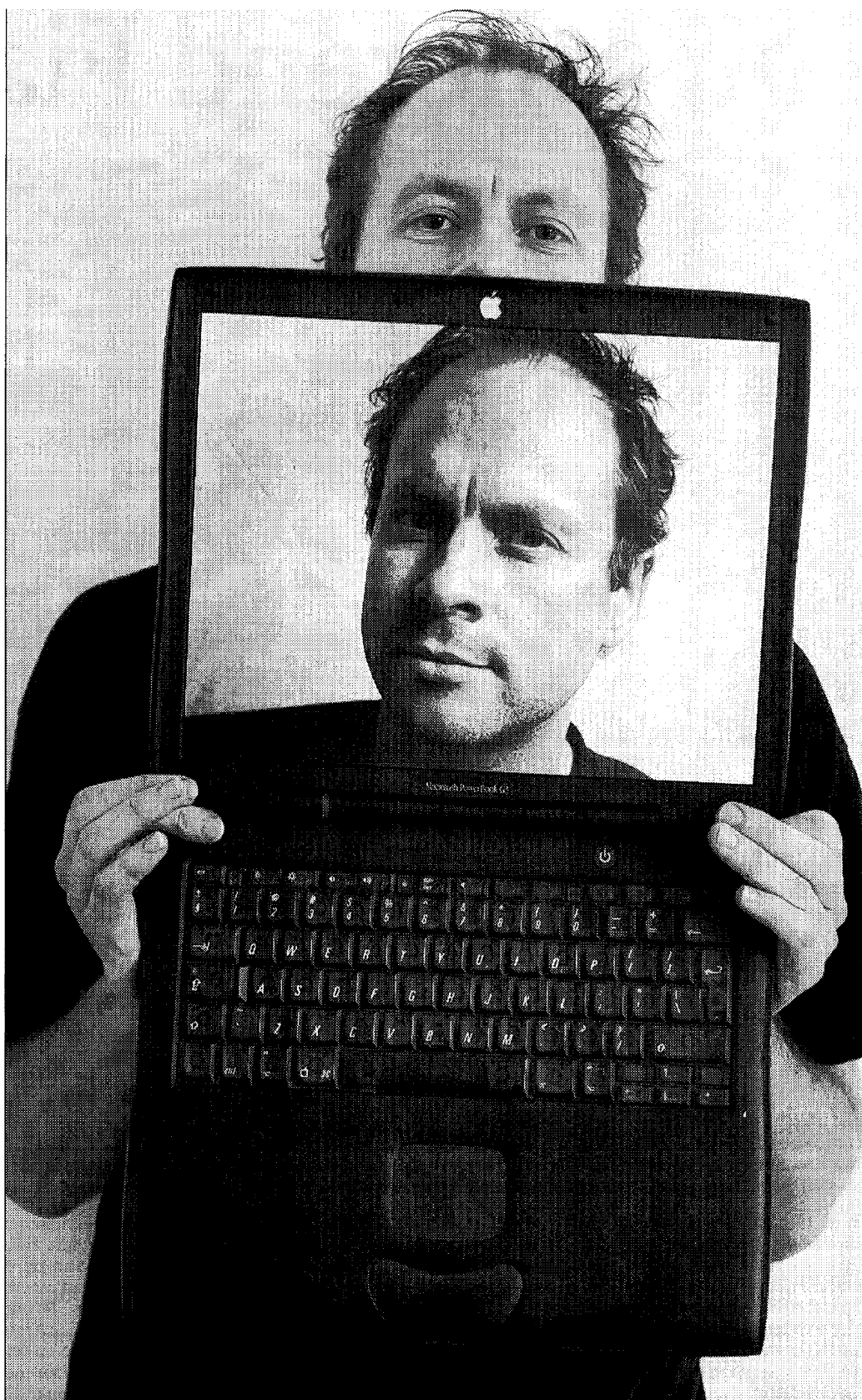
Volgens Verhoef moet de bedrijfstop beveiliging serieus nemen en het niet als een lastige kostenpost zien waar je op kunt bezuinigen als het economisch minder goed gaat. „Je kunt beter je data goed beschermen, zodat van binnenuit frauderen veel moeilijker wordt.”



i Meer informatie op:
[www.fibrechannel.org/
solutions/Continuity/](http://www.fibrechannel.org/solutions/Continuity/)

Continuity.pdf

@punt@ad.nl



Alles wat een werknemer op het toetsenbord doet, is te achterhalen, aldus hoogleraar Chris Verhoef.

FOTO MARCO OKHUIZEN