Computercriminaliteit

Voorkomen is beter dan genezen!

DRS. J.C. VAN DIJK*

Met het toenemen van het gebruik van de computer neemt ook de computercriminaliteit toe. Daarbij gaat het niet alleen om pure fraude en informatievervalsing, maar ook om diefstal en vernietiging van *programma's en informatiebestanden of chantage door bedreiging daarmee. Hoewel nauwkeurige* cijfers ontbreken, komt computerfraude volgens de auteur veel vaker voor dan dikwijls wordt gedacht. In dit artikel geeft de auteur een overzicht van de verschillende vormen van computercriminaliteit. Tevens gaat hij in op de vraag hoe systematische fraude kan worden voorkomen. De auteur signaleert in veel organisaties een zeer grote naïviteit op het gebied van de computerfraude. Te gemakkelijk denkt men dat het in het eigen bedrijf niet kan voorkomen en verzuimt men adequate voorzorgs- en controlemaatregelen te treffen.

Inleiding

In tegenstelling tot wat de folklore zegt, zijn computersystemen, ook zeer complexe, beheersbaar. Hiermee wil ik niet zeggen dat daarmee ook computercriminaliteit geheel te voorkomen is; wel dat voldoende (meestal eenvoudige en voor de hand liggende) maatregelen te nemen zijn, waardoor *systematische* fraude voorkomen kan worden. De belangrijkste katalysator bij computerfraude is *ongelooflijk grote naïviteit.* Ik kom hier op terug.

Mijn (niet wetenschappelijke) definitie van computercriminaliteit is een wijde: zij omvat niet alleen pure fraude en informatievervalsing, maar ook diefstal, moedwillige beschadiging en vernietiging van computerapparatuur, programma's en informatiebestanden en chantage door bedreiging daarmee.

Als we spreken over illegale economie, moet worden beseft dat de computer met zijn toebehoren volstrekt legaal is, ongeacht de toepassing; het is de *toepasser* die illegaal of crimineel is, als de toepassing dat is; de computer is slechts een passief hulpmiddel.

Wordt computerfraude vergemakkelijkt door de invoering van computers of van meer complexe computersystemen? Het is verleidelijk hier een volmondig „ja" op te zeggen. Dit zou echter een vergaande simplificatie zijn. Laten we het volgende schema bezien:

Schema. Bevordert het computergebruik fraude?

	Ja	Nee
Centrale informatie-opslag	vergroot mogelijk voordeel	vergroot controle- en beschermingsmogelijkheden
Automatische verwerking	vermindert oogtoezicht	vergroot „automatische" controlemogelijkheden
Complexiteit	verkleint ontdekkingskans	verkleint fraudemogelijkheid

Een centrale bewaarplaats van alle vitale informatie van een organisatie vergroot inderdaad de mogelijke „beloning" die een fraudeur te wachten staat; hij hoeft zich slechts op één plaats te concentreren om een „goede" slag te slaan; tegelijkertijd zal het duidelijk zijn dat, als alle informatie op één plaats is opgeslagen, het gemakkelijker en relatief goedkoper wordt afdoende controle- en bewakingsmaatregelen te treffen dan bij verspreide opslag.

Automatische gegevensverwerking vermindert het oogtoezicht dat, als we er over nadenken, bij handmatige gegevensverwerking toch een heel essentiële rol vervulde; hier tegenover geeft het ons de mogelijkheid, automatische controles of geldigheidstoetsen in het computersysteem in te voeren, die bovendien niet afhankelijk zijn van menselijk handelen (attent zijn of even afwezig).

De complexiteit van, met name, de nieuwe computersystemen verkleint de ontdekkingskans: als het eenmaal loopt, dan loopt het en wordt het geacht zich zelf te controleren; het is diezelfde complexiteit die fraude bemoeilijkt, omdat het misbruikers beperkt in hun inzicht in het systeem: zij kunnen moeilijk meer beoordelen wat voor effecten hun ingrepen zullen hebben op het geheel; komt er misschien ergens een rapportering over een ontstane oneigenlijke of onmogelijke situatie?

Samenvattend denk ik te kunnen zeggen dat automatisering de *fraudekans* verkleint, maar, bij geslaagde fraude, de ontdekkingskans eveneens vermindert; waar het slaagt, spreken we vaak over aanzienlijk grotere bedragen dan bij de conventionele handmatige gegevensverwerking van vroeger.

Dit geldt voor fraude; geldt dit ook voor andere vormen van computercriminaliteit, met name „geweldmisdrijven", beschadiging c.q. vernietiging van apparatuur of programmatuur, diefstal van informatiebestanden, chantage met betrekking hiertoe? Hier ligt dit mijns inziens anders. Met name de concentratie

*) De auteur, registeraccountant, is partner bij Coopers en Lybrand en heeft zich gespecialiseerd op het gebied van controle van de automatische gegevensverwerking en risico-analyse. Lezers die interesse hebben voor dit terrein, kunnen hun kennis verrijken door het lezen van *Computer crime* van Gerald McKnight, een Engelse journalist en auteur, of *Crime by computer* van Donn B. Parker, een bekende Amerikaanse auteur op dit gebied; beide boeken zijn helaas nogal gedateerd. Parker heeft recent een nieuwe, zeer lezenswaardige publicatie het licht doen zien: *„Fighting computer crime". Computerworld*, een Amerikaans weekblad, beschrijft vaak actuele interessante gevallen.

van gegevens toont vaak het strategische belang ervan; verspreid kan men met een deel ervan weinig of niets doen, maar de combinatie is waardevol. Bovendien zijn bij met name de moderne produktie- en logistieke besturingssystemen de operationele belangen van een organisatie zo gebonden aan het computersysteem dat het wel heel kwetsbaar wordt. Gelukkig zijn ook hier adequate maatregelen voorhanden. Ik kom ook hier verder op terug.

Omvang

In continentaal Europa, ook in Nederland, is weinig concrete informatie voorhanden over de omvang van computerfraude. Als men probeert te kwantificeren, komt men in de Verenigde Staten of, in veel mindere mate, in het Verenigd Koninkrijk terecht.

In Nederland, maar niet alleen hier, is computerfraude een schande waar men als organisatie niet over spreekt: het toont de kwetsbaarheid en wellicht daardoor impliciet ook het gebrek aan soliditeit van de organisatie aan. Ik ken persoonlijk een geval waarbij een computerfraudeur na ontdekking een zéér royale gouden handdruk wist te bedingen onder de bedreiging dat hij anders zijn ,,werk'' wereldkundig zou maken.

De toegenomen belangstelling voor computercriminaliteit en -fraude kan tot gevolg hebben dat nu meer gegevens voorhanden zijn dan vroeger. Een gerapporteerde stijging is dan ook niet noodzakelijk een indicatie van toename van computerfraude. Anderzijds, computergebruik neemt toe, dus waarom niet computermisbruik.

Uit de Verenigde Staten zijn er rapporten van speciale onderzoeksprojecten van onder meer het Stanford Research Institute en het Ministerie van Justitie. Maar zelfs de gegevens uit deze rapporten zijn op z'n minst zeer onvolledig (zoals door henzelf wordt vermeld). Ik ga dan ook geen statistieken geven; het komt aanzienlijk meer voor dan vaak wordt gedacht; het komt misschien (waarschijnlijk?) ook in uw organisatie voor! Statistieken op dit gebied zijn ook niet belangrijk: computerfraude en computercriminaliteit komen voor, véél vaker dan verondersteld, en erger nog, meestal door medewerking van de eigen organisatie; door misplaatst vertrouwen in medewerkers, door volkomen ongerechtvaardigd vertrouwen in de eigen organisatie; door een gebrek of tekort aan uitgesproken ondernemingsethiek, enz.

Indien u toch wat cijfers wenst, jaren geleden werd door de Amerikaanse Kamer van Koophandel de schade in de VS door computerfraude voor het bedrijfsleven geschat op $ 100 mln. per jaar en door een organisatie van computerbeveiligingsadviseurs op $ 300 mln.

Hierbij moet ik tegelijkertijd zeggen dat, uitzonderingen daargelaten, de omvang van individuele computerfraudes in Europa toch betrekkelijk beperkt lijkt. (Let wel: hier praten we over ontdekte fraudegevallen.) Ik denk dat dit historisch en geografisch is te verklaren.

Ik denk dat de conclusie moet zijn: computerfraude is, net als ,,conventionele'' fraude, een gegeven; het is er en het blijft er, tenzij computergebruikende organisaties het belang van preventie inzien en zich tegelijkertijd realiseren hoe (relatief) goedkoop preventiemogelijkheden zijn. Zulke maatregelen zullen het kwaad niet volledig uitbannen, maar wel adequaat kunnen indammen.

Vormen van computercriminaliteit

Wat is computercriminaliteit nu precies? In welke vornen komt het voor? Laat ik U een paar voorbeelden geven; aan de hand daarvan kunnen we het gebied in kaart brengen en zien hoe we, met redelijke maatregelen, het risico onder controle kunnen brengen. Hierbij zal ik, gezien het thema van deze uitgave, vormen van computercriminaliteit zoals beschadiging of vernietiging van apparatuur, programma's en informatiebestanden buiten beschouwing laten, hoewel het een fenomeen is dat vaker voorkomt dan velen denken.

Frauduleuze programma's

Een bekend voorbeeld van computerfraude is dat van de afronding van renteberekeningen bij banken. Er zijn verscheidene gevallen van ontdekt. De programmeur programmeert het systeem zo dat bij iedere berekening de rente naar beneden wordt afgerond op hele centen, het afrondingsverschil wordt apart geaccumuleerd en bijgeschreven op de rekening van de programmeur. In totaliteit klopt de berekende en geboekte rente en geen enkele rekeninghouder zal tegen de afronding bezwaar maken. Bij een middelgrote Amerikaanse spaarbank met een paar honderdduizend rekeningen met maandelijkse rentebijschrijving, ontvangt de programmeur al gauw zo'n duizend dollar per maand; geen gekke beloning voor relatief weinig werk. (Intussen hebben veel banken hiervan geleerd en doen dit nu zelf!)

Een ander voorbeeld vond plaats bij een Franse bank. Hier was het systeem dusdanig geprogrammeerd dat het saldo van de programmeur onderdrukt werd bij het lijsten van rekeningen die voor meer dan de toegestane limieten rood stonden. Hij kon dat gemakkelijk doen door het inbouwen van een instructie in het programma waardoor zijn rekening werd overgeslagen na herkenning van het rekeningnummer. Op deze manier kon hij, binnen zekere grenzen, zonder toestemming van de bank voor aanzienlijke bedragen in het krijt staan. Dit kan erg lang doorgaan, omdat niemand bij dergelijke lange computerlijsten controleert of het totaal eronder inderdaad het totaal is van de afgedrukte posten.

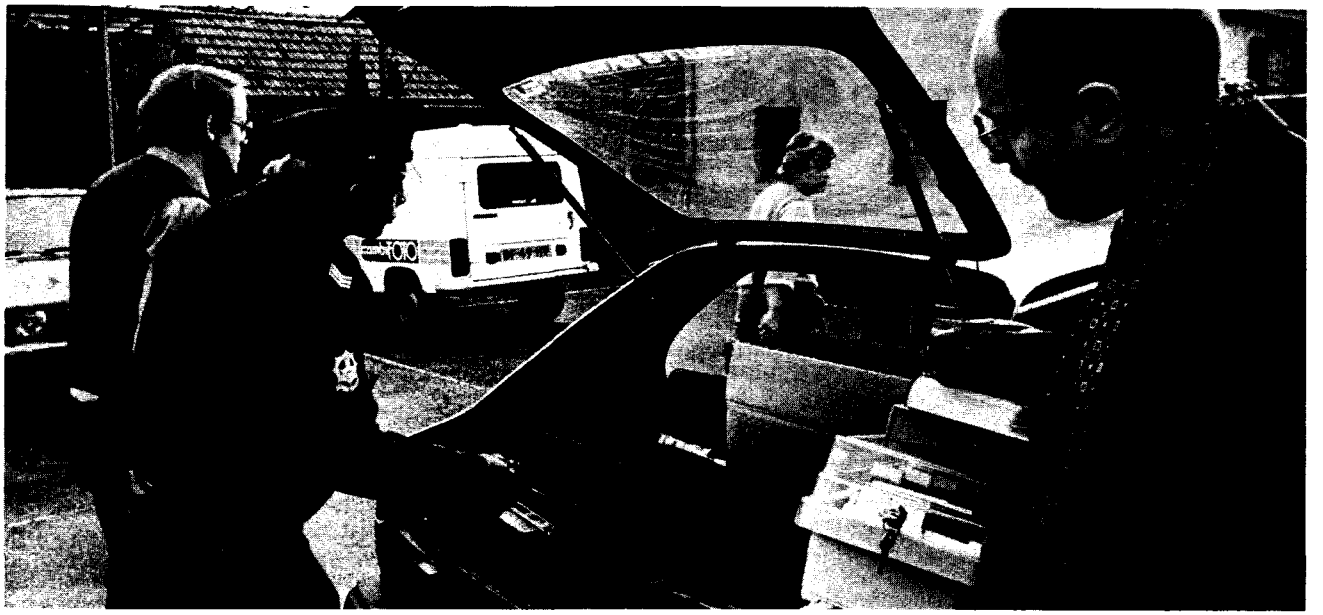
Een geval dat minder bekend is, maar waarvan de potentiële gevolgen veel groter waren, speelde zich af bij een hondenracebaan in de Verenigde Staten. Weddenschappen werden voor drie races vooruit afgesloten. Het computersysteem bepaalde op basis van de inzetten de gewonnen bedragen. Door veranderingen aan het computersysteem konden de fraudeurs, in plaats van drie races vooruit, na afloop van de tweede race (nadat de eerste en tweede winnaar bekend waren) alsnog hun weddenschappen invoeren, met op deze manier een aanzienlijk grotere winstkans. Uiteraard deden zij dit voor aanzienlijke bedragen. Dit werd alleen maar ontdekt omdat de fraudeurs te gretig werden, te grote bedragen gingen invoeren en bij steekproefsgewijze controle op zeer grote winsten tegen de lamp liepen.

Wat hebben deze voorbeelden met elkaar gemeen? Dezelfde organisatorische leemte, nl. dat nieuwe of gewijzigde systemen ,,in produktie'' werden genomen zonder voldoende controle door de gebruikers. Gebruikers, de eigenaars van systemen in wier opdracht ze zijn ontwikkeld, dienen zich hun verantwoordelijkheid bewust te zijn. Zij zijn er voor verantwoordelijk dat nieuwe, of gewijzigde, systemen onder hun toezicht op ten minste twee manieren worden gecontroleerd:

- door het verwerken in het nieuwe systeem van zorgvuldig gekozen testgevallen, die representatief zijn voor elke mogelijke gegevensvariatie die het systeem te verwerken kan krijgen; na verwerking moeten alle uitkomsten worden vergeleken met de vooraf handmatig bepaalde uitkomsten die de testgevallen moeten opleveren;
- door nieuwe systemen gedurende enige tijd simultaan te laten lopen met het voorgaande handmatige of computersysteem; in die tijd moeten de uitkomsten van beide systemen voortdurend worden vergeleken en de ongetwijfeld optredende discrepanties grondig worden uitgezocht door de gebruiker zelf.

Deze twee maatregelen kosten vrij veel geld en tijd; hun kosten zijn echter gering in verhouding tot de totale ontwikkelingskosten van computersystemen en bovendien vallen ze in het niet bij de kosten van systematische fouten of systematische fraudes, die kunnen optreden als men deze maatregelen weglaat.

Bij deze vorm van systematische fraude worden op zich geldige transacties op een niet bedoelde wijze verwerkt ten voordele van niet bedoelde individuen. De techniek komt deze fraudeurs te hulp. Er bestaan programma's, zogenaamde ,,utilities'', waarmee een computeroperator of een systeemprogrammeur tijdens de verwerking wijzigingen, zogenaamde ,,patches'', in programma's kan aanbrengen; deze kunnen na de verwerking weer ongedaan worden gemaakt zonder een spoor achter te laten. Dit soort ,,utilities'' heeft men nodig in grotere computerafdelingen om storingen bij de verwerking te verhelpen. Het zal duidelijk zijn dat bewaring (niet in de gewone programmabibliotheek) en gebruik (nooit zonder toezicht) van deze ,,utilities'' (zoals Zap,



Inbeslagneming van illegaal gekopieerde software onlangs in Uden (ANP-foto)

Superzap, Ditto enz.) goed georganiseerd moeten worden.

Met name door de invoering van telecommunicatie in computersystemen en netwerken kunnen deze fraudes ,,op afstand'' worden uitgevoerd. Goede computersystemen hebben hiertegen ingebouwde controles en beveiligingsmaatregelen. In de praktijk worden deze echter vaak als hinderlijk ervaren door de gebruiker en dan buiten werking gesteld. U zult begrijpen waar men dan om vraagt.

Door handhaving van een goede organisatie bij het ingebruiknemen van systemen, zoals hierboven beschreven, door een goede organisatie van de gegevensverwerking met duidelijke functiescheidingen en controle op de toegang tot actieve programma's en systemen, en een goed systeem van controles in de individuele toepassingen, zijn fraudes van deze soort goed te voorkomen.

De in de aanhef van deze bijdrage genoemde naïviteit komt bij dit soort fraudes om de hoek kijken waar organisaties niet de noodzaak van deze maatregelen onderkennen, vaak onder het motto ,,dat kan ons niet gebeuren''.

Frauduleuze gegevens

Naast bovengenoemde systematische fraudes, zien we ook een vorm van fraude waarbij, in op zich goed functionerende systemen, frauduleuze transacties of gegevens worden ingevoerd. Dit is waarschijnlijk de meest voorkomende vorm van computerfraude. Waarschijnlijk ook alweer omdat organisaties de noodzaak van een behoorlijke organisatie met ingebouwde controles en goedkeuringsprocedures onvoldoende onderkennen. Gelukkig gaat het hierbij meestal (maar niet altijd) om aanzienlijk kleinere bedragen dan bij systematische fraude. Voorbeelden zijn er legio en ze zijn overbekend.

In een verzekeringsmaatschappij veranderde de computeroperator de vaste gegevens van (overleden) verzekerden, waardoor de lijfrente-uitkeringen doorliepen, maar ten gunste van bankrekeningen die de operator had geopend.

Ambtenaren in een stad in Californië produceerden voor fictieve werknemers van de gemeente via de computer loonstrookjes en -cheques, die ze vervolgens zelf incasseerden. Dit werd gedaan door fictieve nieuwe werknemers in het computerbestand in te voeren. (Dit is overigens geen uniek geval; soortgelijke fraudes gebeuren in heel Europa, ook in Nederland, op vrij grote schaal, maar worden niet gepubliceerd.)

Bij de Britse belastingdienst boekte een ambtenaar niet geclaimde belastingrestituties over naar een reeks van andere rekeningen (om het spoor te verduisteren) en uiteindelijk naar zijn eigen rekening.

De EDP-vice-president en een computeroperator bij een bank boekten in ééndrachtige samenwerking geld over van ,,slapende rekeningen'' naar rekeningen die zij zelf openden. Door ,,slepen'' konden ze dit lang volhouden.

Bij een bank in de Verenigde Staten verduisterde een kassier circa $ 1,3 mln. in een periode van drie jaar door correcties te boeken op nieuw geopende rekeningen en deze correcties te incasseren. Bij navraag werd de correctie teruggeboekt en doorgeschoven naar andere rekeningen. Dezelfde activiteit vond plaats bij depositorekeningen.

Een boekhouder bij een cateringbedrijf had de eigenaar van een levensmiddelenbedrijf als medeplichtige. De boekhouder voerde dat bedrijf in het computersysteem in als leverancier en kon daarna facturen (voor niet geleverde goederen) in het systeem invoeren en laten betalen. Uiteraard deelden zij de baten.

Zulke gevallen zijn altijd terug te voeren op twee essentiële tekortkomingen in de betrokken organisaties:

- er waren geen afdoende autorisatieprocedures, of, wat veel vaker voorkomt, autorisatie vond plaats op het verkeerde moment. Autorisatie moet plaatsvinden nadat de volledigheid van de te verwerken transacties is vastgesteld; gebeurt het er voor, dan kunnen voor de volledigheidscontrole geautoriseerde transacties worden vervangen door illegale, waardoor de hele autorisatieprocedure wordt ondermijnd!
- er was onvoldoende controle uitgeoefend of de vaste gegevens in het systeem (zoals het als crediteur ingevoerd zijn van een fictieve leverancier, of de vaste gegevens van de verzekerden, of de fictieve werknemers) juist en volledig zijn en dat ook blijven. Dit kan eenvoudig worden gedaan door deze gegevens periodiek of cyclisch stuk voor stuk te controleren; dat is veel werk, maar het loont de moeite.

Voorbeeld van een ,,geslaagde'' computerfraude

Het risico van fraude is bijzonder groot als zowel de controles over systeem- en programma-ontwikkeling als die over autorisering van vaste en transactiegegevens tekort schieten. Een ,,goed'' voorbeeld hiervan vond plaats in een middelgroot bedrijf, waar de rechterhand van de computermanager onbeperkte toegang had tot een systeem dat hij destijds zelf had ontwikkeld. Hierdoor kende hij het systeem tot in details. Hij had bovendien het toezicht op de dagelijkse werking van het systeem en was verantwoordelijk voor de uitvoering van een groot deel van de gebruikerscontroles in het systeem. Van tijd tot tijd viel hij ook in als computeroperator.

Hij baseerde zijn activiteiten op frauduleuze programma's, die hij laadde wanneer gewenst, in plaats van de oorspronkelijke programma's. In deze situatie kon hij:
- foutieve gegevens invoeren;
- vaste gegevens manipuleren;
- vervalste en echte transactiegegevens verwijderen uit bestanden;
- de controlerekeningen, die ook door de computer werden bijgehouden, aanpassen;
- print-outs van vervalste transacties onderscheppen.

Op deze wijze kon hij door de computer omvangrijke betalingsopdrachten aan zich zelf en aan medeplichtigen laten uitschrijven. Op het eerste gezicht werkten alle controlemaatregelen. Wat niet werkte, was de functiescheiding.

Dit was een zeer omvangrijk en kostbaar fraudegeval, hoewel het slechts door één man werd uitgevoerd (de man werd pas gepakt toen de fiscus naar zijn inkomen begon te informeren). Toch is dit geen theoretische casus; helaas komt dit soort gevallen al te veel voor.

De belangrijkste leemte die de fraude mogelijk maakte, was het ontbreken van de scheiding in verantwoordelijkheid voor integriteitscontroles en applicatiecontroles. Integriteitscontroles zijn die organisatorische en andere maatregelen die de integriteit (de ongestoorde werking) van de computerverwerking als zodanig moeten waarborgen. Bovenstaand voorbeeld illustreert goed het belang van integriteits- en applicatiecontroles en de scheiding in de verantwoordelijkheden ervoor. Inclusief de authenticiteit van de vaste gegevens in het systeem. Applicatiecontroles zijn die maatregelen die per applicatie (toepassing) de ongestoorde verwerking van transacties door het systeem moeten waarborgen.

Het verband tussen integriteits- en applicatiecontroles kan als volgt worden weergegeven:

	Transactie-stroom	Applicatie-controles	Zekerheid over werking der applicatiecontroles
Gebruikersafdeling (b.v. verkoop-afd.)			toezicht en functiescheiding
Computer-afdeling			integriteits-controles
Gebruikers-afdeling (b.v. boekhouding)			toezicht en functiescheiding

Transacties beginnen in een gebruikersafdeling (b.v. verkooporders ontvangen op de verkoopafdeling). Hier moeten dan ook de applicatiecontroles aanvangen (controle op juistheid, volledigheid en autorisatie). Daarna gaan de transacties (de orders) naar de computerafdeling; de applicatiecontroles moeten hier doorwerken (b.v. controle op volledigheid door controle van de nummervolgorde). Na afwerking van de order komt de kopiefactuur op de boekhouding (ook een gebruikersafdeling van de computer). Ook hier moeten de applicatiecontroles doorwerken.

In de gebruikersafdelingen kan door toezicht en functiescheiding zeker worden gesteld dat de applicatiecontroles werken. In de computerafdeling kan dat niet en wordt die taak overgenomen door de ,,integriteitscontroles'', onder andere bestaande uit organisatorische maatregelen en automatische registratie door de computer van alles wat geschiedt.

In het bovenstaande voorbeeld was fraude mogelijk doordat de fraudeur van tijd tot tijd zelf de verwerking der transacties verzorgde (hij viel in als computeroperator) en daarnaast zelf verantwoordelijk was voor de verzorging van een deel der applicatiecontroles en voor de uitvoering van de integriteitscontroles.

Informatievervalsing

Bij informatievervalsing wordt in een meestal op zich goed functionerend systeem op grote schaal onjuiste informatie ingevoerd met het éénduidige doel een aanzienlijk beter beeld te geven van de ,,performance'' van een bedrijf en van de financiële positie. Het zal duidelijk zijn dat dit alleen kan plaats vinden door samenspanning op grote schaal binnen een bedrijf. Het wordt dan ook meestal geïnitieerd door de leiding.

Het klassieke voorbeeld van dit type fraude is wel Equity Funding Corporation of America, een combinatie van beleggingsmaatschappij en verzekeringsmaatschappij. Deze onderneming slaagde erin gedurende een periode van bijna 10 jaar (1964 tot begin 1973) voor een bedrag van meer dan $ 110 mln. aan gefingeerde winsten te boeken ten einde de aandelenprijs op een voor de leiding aantrekkelijk niveau te brengen 2).

Fraudes van deze aard komen gelukkig niet zo vaak voor, hoewel, naar mijn mening, vaker dan wel gedacht wordt. Het grootste probleem is dat zij bij de huidige stand van de computertechnologie moeilijk te ontdekken zijn voor een accountant zonder gedegen computerkennis.

Zoals reeds gezegd, is samenzwering op vrij grote schaal bij deze fraudes noodzakelijk en worden in wezen alle controleprocedures omzeild of buiten werking gesteld. Toch wordt dit soort fraudes waarschijnlijk vergemakkelijkt door computers, doordat met de computer grote hoeveelheden gegevens kunnen worden verwerkt zonder tussenkomst van veel personeel.

Het zal duidelijk zijn dat bij samenzwering op grote schaal weinig te verwachten is van interne preventiemaatregelen. Het is dan aan de externe toezichthoudende instanties, en met name ook aan de externe accountants, om de maatschappij te behoeden voor dit soort calamiteiten. Dit betekent dan automatisch een oproep aan die externe accountants zich grondig in automatiseringsmogelijkheden en daaraan verbonden controletechnieken te verdiepen.

Inbraak en diefstal

Dit is de categorie van computercriminaliteit die het gemakkelijkst de kranten haalt; zij appelleert aan de menselijke verbeeldingskracht; recente bioscoopfilms zijn daar ook een goed bewijs van.

Voorbeelden zijn er te over en soms wordt het ook officieel gesanctioneerd. Een voorbeeld van dit laatste is dat de Amerikaanse marine, leger en luchtmacht elk teams van specialisten hebben die uitsluitend tot taak hebben in te breken in de belangrijkste en gevoeligste computersystemen. Doel is, kritische toegangsmogelijkheden te ontdekken en op die wijze de totale beveiliging van die systemen steeds verder te versterken. Ik praat bij dit soort computerfraude over illegale toegang tot informatiebestanden om informatie te stelen of om de opgeslagen informatie te veranderen.

Enige tijd geleden is een Nederlands constructiebedrijf in de publiciteit gekomen omdat het afluisterapparatuur bij concurrenten had geplaatst. Doel was kennelijk concurrentie-informatie over uit te brengen offertes te verkrijgen. Ik denk dat dit bedrijf een onnodig moeilijke, kostbare en gemakkelijk te ontdekken weg heeft gekozen. Bij de huidige stand van zaken bij de beveiliging van computersystemen in Nederland had men waarschijnlijk gemakkelijker in de computer van de concurrent kunnen inbreken.

Laten we eerlijk zijn: ieder computersysteem dat via een openbaar telefoonnet kan worden bereikt, is kwetsbaar. Telefoonnummers, ook geheime, kunnen worden ontdekt of gekraakt, ,,passwords'' kunnen worden gekraakt, gebruikersprofielen kunnen worden ontdoken of misbruikt. En dit gebeurt in de praktijk.

Studenten aan een Nederlandse universiteit zijn in het computersysteem binnengedrongen en hebben (waarschijnlijk) hun studieresultaten gecorrigeerd; ik zeg waarschijnlijk, omdat het bij mijn weten nooit is bewezen. Overigens was al lang tevoren gewaarschuwd dat het systeem zo lek was als een mandje, naar ik van een ter zake deskundige hoogleraar vernam.

Meestal gebruikt men de telefoon en een eigen micro-computer om zich toegang te verschaffen en snel een grote hoeveelheid informatie te verkrijgen. Dit gebeurde niet zo lang geleden bij

(Vervolg op bladzijde 1231)

1) Diegenen die in details geïnteresseerd zijn, worden verwezen naar de uitgebreide beschrijving die Donn Parker in zijn boek *Crime by computer* heeft gegeven .

(Vervolg van bladzijde 1226)
voorbeeld ook met de concurrentiegegevens van een Amerikaans constructiebedrijf.

Deze voorvallen hebben geleid tot aanzienlijke verrijking van ons taalgebruik: in vakkringen wordt nu gesproken over ,,Trojaanse paarden''; ,,Superzapping''; valluiken of ,,trapdoors''; ,,scavenging'' of wel het rondneuzen in de informatie die na de verwerking in de computer is achtergebleven; aftappen; ,,salami''-techniek, waarbij diefstal (op afstand) in kleine, bijna onmerkbare beetjes plaatsvindt, maar gedurende lange tijd; asynchrone aanval, waarbij bepaalde specifieke eigenschappen van het ,,operating-system'' worden uitgespeeld tegen die van de toepassingsprogrammatuur (eveneens meestal weer op afstand); datalekkage als methode om, op afstand, vertrouwelijke informatie geleidelijk uit een systeem te laten lekken.

Zoals gezegd, spreken dit soort fraudetechnieken aan vanwege het sensatie-element. Inbraak in computersystemen zal op deze manier bijna altijd mogelijk zijn, althans in theorie. Toch moeten we wat dit betreft realistisch blijven. Bij goede beveiligingsmaatregelen (die gewoon mogelijk zijn) vereisen zij een specialistische technische kennis die, zeker in Nederland, slechts weinigen bezitten; de meeste van hen werken bij hardware- en software-leveranciers om beveiligingsmaatregelen en software te ontwerpen.

Redelijke beveiligingsmaatregelen tegen dit soort inbraak en diefstal zijn niet echt zo esoterisch: lokatie en organisatie van het rekencentrum, goede toegangsbeveiliging (zet niet op de toegangsdeur: ,,computercentrum''), goede bibliotheek-software die de toegang tot operationele programma's en gegevensbestanden beschermt, behoorlijke ,,back-up'' en ,,recovery''-procedures, die regelmatig getest worden, en voor gevoelige informatie het gebruik van encryptietechnieken.

Mocht U onverwacht, en bij goede beschermingsmaatregelen onwaarschijnlijk, toch slachtoffer worden van computerinbraak, dan is een goede verzekeringsdekking van nut. Tot mijn niet geringe verbazing leerde ik uit een recent onderzoek van prof. Oonincx (Tilburg) dat meer dan de helft van de Nederlandse computergebruikers niet verzekerd is tegen de gevolgen van moedwillige verstoring van hun computersystemen; kennelijk is slechts één op de vijf gebruikers verzekerd tegen de schade die kan ontstaan door computercriminaliteit. Ook hier ligt mijns inziens een taak voor de externe accountant. Sommige accountantsorganisaties hebben geavanceerde risico-analyse-methodologieën waarmee bedrijven een objectief risicoprofiel aangereikt kunnen krijgen; dit vormt dan een goede basis voor discussie met verzekeringsbedrijven.

Eén vorm van diefstal in dit verband heb ik nog niet genoemd: die van computertijd ten laste van de werkgever maar ten dienste van zich zelf of derden. Het is tegenwoordig al heel gewoon als de penningmeester/boekhouder van een kerk de boekhouding van zijn kerk op de computer van zijn werkgever bijhoudt. Als dit met instemming van de werkgever gebeurt, is het uiteraard geen enkel probleem. Ik vermoed dat die toestemming er niet altijd is. Ook gebeurt het ,,lenen'' van computertijd voor andere, vaak commerciële doeleinden; dan ligt het uiteraard heel anders. Betrekkelijk eenvoudige maatregelen (toegangscontrole en computerlogs) kunnen dit verhinderen.

Conclusie

Welke les is uit het voorgaande te trekken? Allereerst, dat computercriminaliteit voorkomt, vaker dan wordt gedacht. Vervolgens, dat met zindelijke maatregelen (die niet de privacy van individuen behoeven aan te tasten) een redelijke preventie mogelijk is.

Computercriminaliteit is een gegeven; zoals een bedrijf de ingang en uitgang van zijn magazijn bewaakt, behoort het dat ook bij de computer te doen. Dat is mogelijk zonder excessieve kosten. Vertrouwen in eigen organisatie en mensen is heel gezond, maar moet niet leiden tot naïef blindvaren op hen; controle is gezond en heeft niets met wantrouwen te maken.

Organisaties doen er goed aan externe deskundigen, zoals accountants met ervaring in elektronische gegevensverwerking, in te schakelen, enerzijds ter beoordeling van het risicoprofiel en de reeds genomen maatregelen, anderzijds ter advisering bij het opstellen van een beveiligingsactieplan. Zo'n plan moet dan niet blijven stilstaan bij de te nemen maatregelen; het moet ook het regelmatig testen van de genomen beveiligingsmaatregelen inhouden. Voorkomen *is* beter dan genezen!

J.C. van Dijk