"Der Computer-Kriminelle [...]"

„Der Computer-Kriminelle ...

ist für ein Unternehmen u.U. gefährlicher als einer, der sich mit einer entsicherten Pistole im Betrieb aufhält." (Computerwoche Nr. 35/81.)

Aber woran erkennt man als sorgengeplagter Kapitaleigner denn eigentlich einen solchen Saboteur, und was macht man gegen ihn?
Jay Becker, Direktor des US-amerikanischen Zentrums für Computerkriminalität, hat eine „wissenschaftliche" Typenbeschreibung ausgearbeitet:
Ihr zufolge muß man auf der Hut sein, sollen doch 80% der Delikte im EDV-Bereich von den eigenen Mitarbeitern ausgehen. Aufpassen sollte man, seine Untergebenen nicht durch eine rigide Betriebspolitik zu verärgern oder zu enttäuschen. Können sie ihre Kritik nicht konstruktiv innerhalb der betrieblichen Strukturen äußern, werden Mitarbeiter unsachlich und beschädigen möglicherweise Daten, Programme und Maschinen.
So ist es vorgekommen, daß Systemprogrammierer einen Kündigungsschutz in ihre Programme eingebaut haben. Diese arbeiten nur solange richtig, wie die Namen der Urheber in der Beschäftigtenliste der betroffenen Firma aufgeführt sind . . . Für die Gruppe der **Problemlöser** ist es nicht das ausgesprochene Ziel ihres Tuns, möglichst viel Unheil anzurichten. Vielmehr fühlen sie sich geradezu herausgefordert von der bloßen Existenz eines technischen Systems und wollen es unbedingt überlisten. Dabei entsteht Schaden gewissermaßen nur zufällig und nebenbei; jedoch teilweise in sehr beachtlicher Größenordnung.
Stanley Rifkin z.B. hatte einfach nichts vorbereitet, um die 10 Millionen US-Dollar langfristig zu verstecken, die er 1978 einer Bank in Los Angeles durch Computermanipulation entlockte. Lächelnd ließ er sich verhaften, war doch seine Festnahme für ihn der wichtigste Beweis, daß seine Tricks wirklich funktionierten . . .

Hier hilft soziale Kontrolle am besten. Die Motivation, sich auf den geistigen Zweikampf mit der Maschine einzulassen, steigt mit den Möglichkeiten, einfach unbeobachtet rumspielen und ausprobieren zu können.
Natürlich gibt es auch die ganz **gewöhnlichen Kriminellen**. Sie benutzen den Computer systematisch nur als ein weiteres Werkzeug in ihrem Vorratskästchen, um sich „unrecht Gut" anzueignen. Dabei wollen sie dem armen Rechner selbst überhaupt nichts antun.
Der intensive Versuch, solche Leute bei ihrer anstrengenden Arbeit zu stören, behindert meist auch den eigenen Betriebsablauf. Und zusammen mit den Kontrollauflagen wächst die Phantasie der Mitarbeiter, um diese Auflagen alltäglich umgehen zu können. Am sinnvollsten ist auch hier die soziale Kontrolle, stets mehrere Leute ein Problem durchschauen zu lassen und sich nicht auf einen einzelnen zu verlassen. Das bewußt planende und versierte Übeltätertum ist hiermit allerdings keineswegs gänzlich zu stoppen.
Andere haben einfach pauschal etwas gegen Technik. Sie sehen in einem Computer nicht etwa die Lösung ihrer Probleme – sondern gar den Anfang all dieser. Sie wollen dem Kapitaleigner selbst vielleicht gar nicht soviel Böses, aber eben dieser verflixten Maschine. Dann treten sie gegen ihr Terminal, schmeißen es zu Boden, kippen Bier hinein, ja manchmal erschießen sie sogar den Rechner. Und zum Teil gehen sie dann auch noch straffrei aus, weil sie meinten, im Affekt handeln zu müssen. – Bloß weil die Maschine mal ein paar Stunden lang nicht korrekt arbeitete und ein wenig Geduld und Verständnis erforderte.
Solche Leute darf man grundsätzlich nicht wieder an verantwortungsvolle Aufgaben heranlassen. Auch sollte man sich ihre Namen merken und sie gegebenenfalls anderen sagen, die einem mit ähnlich wertvollen Tips unter die Arme greifen können. Außerdem gilt: Die Leute reißen sich mehr zusammen, wenn sie nicht unbeobachtet und alleine arbeiten.
Bleiben noch **politisch motivierte Personen**. Sie sehen den Computer als das Lieblingsspielzeug der Mächtigen zur Ausbeutung und Denunziation, zur sozialen Kontrolle und Unterdrückung an. Sie tun alles, um diese Maschinen anzugreifen, sie außer Betrieb zu setzen oder zu demontieren.
Wie z.B. die französische Gruppe CLODO, das Komitee zur Zerstörung oder Entführung von Computern. Die Leute sind vom Fach, sie wissen, was sie tun. Framatome (französische Atomindustrie), Air France, Philips und andere haben schon hautnahen Kontakt mit ihnen gehabt.
Diesen Personen kann man laut Becker nur auf breitester Front begegnen: soziale Kontrolle im eigenen Betrieb, Zugangskontrollen, Warnanlagen, Gebäudeschutz und Werkschutz, neuerdings auch mit Versicherungspolicen.

Als erstes Bundesland: Niedersachsen richtet Beratungsstelle für vorbeugenden Sabotageschutz ein

Als erstes Bundesland hat Niedersachsen eine Beratungsstelle für den vorbeugenden materiellen Sabotageschutz eingerichtet. Wie der Sprecher des Innenministeriums am Freitag in Hannover mitteilte, erarbeitet diese Beratungsstelle auf Wunsch von lebens- und verteidigungswichtigen Einrichtungen Schwachstellen-Analysen der sicherheitsempfindlichen Bereiche. Seit Herbst letzten Jahres können sich die betreffenden Betriebe mit der von einem Diplom-Ingenieur geleiteten und in der Verfassungsschutzabteilung des Innenministeriums angesiedelten Stelle in Verbindung setzen. Die Adresse lautet: Niedersächsischer Minister des Innern, Abteilung 4, Postfach 4420, 3000 Hannover 1.

Aus: „Die Polizei".