Zeitschrift: Wechselwirkung : Technik Naturwissenschaft Gesellschaft
Herausgeber: Wechselwirkung
Band: 2 (1980)
Heft: 7

Artikel: "Der Vandalismus nimmt im allgemeinen zu" : alltäglicher Widerstand oder Computerstürmerei?

Autor: Onlein, Ferdinand

DOI: https://doi.org/10.5169/seals-653432

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 17.05.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Ferdinand Onlein

„Der Vandalismus nimmt im allgemeinen zu"*

Alltäglicher Widerstand oder Computerstürmerei?

Ein von 21 großen Firmen und Universitäten benutztes Computersystem hat ein bisher noch unbekannter New Yorker Oberschüler fast vollständig zerstört. Wie die Nachrichtenagentur apf meldet, wruden große Teile des gespeicherten Datenmaterials von dem Computersystem „Datapac" beschädigt bzw. gelöscht. Dem Computer-Killer ist es demnach gelungen, von einem in einer privaten Oberschule im Nobelviertel Upper East Side stehenden Computer-Terminal aus, das System zu entschlüsseln und lahmzulegen.

Warum eine solche Fragestellung?

In diesem WW-Heft wird in dem Artikel *Sesam öffne dich* u.a. der Anteil der Datenverarbeitung an Herrschaft untersucht. Datensammlungen im Sozialbereich und Personalinformationssysteme bilden weitere Schwerpunkte. Alles in allem soll sich dabei ein Bild dessen ergeben, was ist.
Was fehlt bzw. völlig unterentwickelt ist, ist die Untersuchung der tatsächlichen Reaktionen von Ingenieuren, Technikern und Naturwissenschaftlern an ihrem DV-Arbeitsplatz auf die Arbeitsbedingungen, auf die zunehmende Taylorisierung.[1]
Absicht dieses Artikels ist es, eine Beschreibung bestimmter (unbewußter und bewußter) Widerstandsformen gegen die (Auswirkungen der) Datenverarbeitung zusammenzustellen. Der angepaßte, sich dreinschickende Angestellte wird nicht betrachtet. Vielmehr das nonkonforme, „kriminelle" Verhalten derer, bei denen Konsum, Geld, Karriere oder Faszination durch die Maschine nicht reibungslos integrierend wirken. Mich interessierte dabei besonders, ob sich die im folgenden stichwortartig angedeuteten Verhaltensweisen, die mir aus meinem Kollegen- und Freundeskreis bekannt sind, allgemeiner – gesellschaftlich relevanter – wiederfinden:

* Vortäuschen von Arbeit, um bequem „über die Runden zu kommen;
* Gegenmaßnahmen gegen die Intensivierung der Arbeit: Quatschen, Kaffeepausen ...;
* viel zu hohe Zeitvorgaben durchsetzen, den eigenen Arbeitsbereich möglichst unbestimmbar (nicht meßbar) zu halten;
* Einbau von Fehlern in Programme, ein kleiner Fußtritt, Sabotage;
* Krankfeiern, Verweigerung der Arbeit, „Aussteigen;

Kurz:
Zeigt der DV-Angestellte überhaupt „Unmutsäußerungen"?
und:
Wie reagieren Unternehmer und Staat?

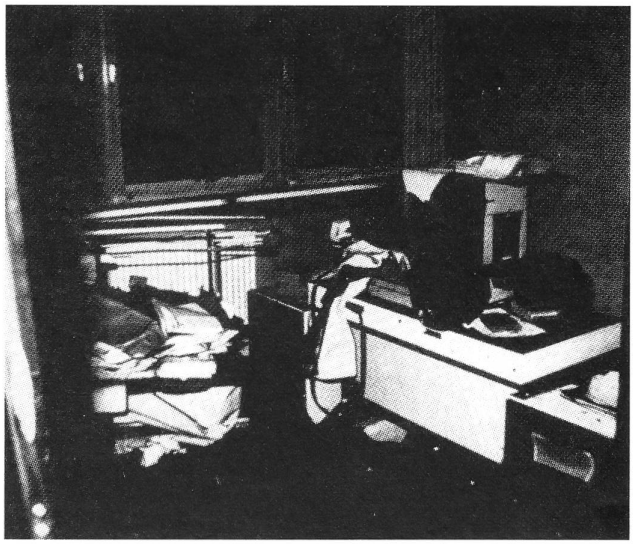
Das herkömmliche Medienbild zeigt den DV-Mitarbeiter als jungen, dynamischen Mann, der über seine Arbeit mit der hochentwickelten DV-Technologie am gesellschaftlichen Fortschritt aktiv mitwirkt und entsprechende gesellschaftliche Anerkennung und gute Bezahlung genießt. Ein Leitberuf sozusagen. Woher sollte da auch nur ein Gedanke an Widerstand kommen?

Die Unternehmerseite jedoch sieht ernste Probleme. So schreibt die *Computerwoche* in einer Extra-Beilage zum Thema: Safety first in der Datenverarbeitung:
„... empfiehlt es sich angesichts der Millionenwerte, die in einem Rechenzentrum stecken, und der teuren Terminals [...], *alle Sicherheitsmaßnahmen nach einer ‚Bedrohungsmatrix' einzurichten.*
Bei der RZ-Planung muß gefragt werden: Wer könnte ein Interesse an einer Missetat haben? Was könnte einer tun? Unter welchen Umständen kann er es heute tun?"[2]
Und bedauernd wird anschließend festgestellt, daß die Sicherheitskalkulation für die Zukunft Spekulation bleiben wird, *„weil das Spektrum der Gefahren so breit wie die Phantasie des Täters und die Sicherheitslücken im Betrieb sind. Bei der krimonologischen Auswertung* [...] *haben sich in der jüngeren Vergangenheit zwei Tendenzen herausgeschält: Erkennbar waren es in jüngster Zeit mehr Insider-Anschläge. Oft Affekt-Taten, bei dem einer nach wiederholter Wartezeit und blinkendem Terminal mit dem Fuß dagegentrat. Zunehmend aber spielt Brandstiftung eine Rolle und spielen Anschläge auf die Stromversorgung und die Nachrichtenkabel der Datenverarbeitung eine Rolle."*[3]
Der Dipl.-Kfm. von zur Mühlen beschreibt in seinem Buch *Computer-Kriminalität Gefahren und Abwehrmaßnahmen* diverse Beispiele aus dem Bereich der Computer„kriminalität". Sabotage und Zeitdiebstahl (Erlangung von Rechenzeit, ohne zu bezahlen) kommen dabei ebenso vor wie Wirtschaftsspionage und allein 20 verschiedene Arten von Manipulation.[4]
Die *Autonomie* dokumentierte in ihrer Ausgabe vom September 1978 mehrere Fälle von EDV-Sabotage, die dem Unternehmerorgan *Sicherheitsberater Informationsdienst zu Problemen der Sicherheit im Betrieb, Unternehmen und Verwaltung* aus dem Handelsblatt-Verlag entnommen wurden:
„Ein Brandstifter legte am 8.10.1977 das Rechenzentrum eines norddeutschen Versicherungsunternehmens mit einem gezielten Anschlag still. Die EDV-Anlage im Wert von 3,5 Mio. DM muß als Totalschaden abgeschrieben werden, Datenträger und der Maschinenraum sind stark in Mitleidenschaft gezogen. [...]
Sabotagehandlung mit Wasser – Wasser bewirkte Schmorschaden an der Zentraleinheit des Computers – zwölf Tage Betriebsunterbrechung [...] *Ein metallverarbeitender Mittelbetrieb erlitt in der letzten Zeit wiederholt erhebliche Schäden aufgrund von Produktionsausfällen. Ein Saboteur entwendete innerhalb eines dreiviertel Jahres sechzehnmal Lochstreifen, die für die Steuerung automatischer Werkzeugmaschinen benötigt wurden."*[5]

* Feststellung der *Computerwoche* zur Computerkriminalität

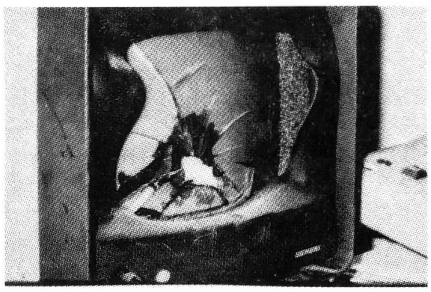
Da fragt man sich doch, wie denn wohl rundum zufriedene Mitarbeiter zu solchen Handlungen kommen. Ohnmächtige Wut, ziellose Aggression als Ausdruck der entfremdeten Arbeitssituation? Reaktion auf die Tendenz zu jeglicher Eliminierung des menschlichen Faktors in der und durch die Datenverarbeitung? Gar Computerstürmerei?

Meine **These**:
Je mehr die Datenverarbeitung in den nächsten Jahren als Rationalisierungsinstrument vor allem im Büro eingesetzt wird und je mehr Automatisierung in der Datenverarbeitung selbst stattfindet, umso mehr werden individuelle, aggressive Aktionen gegen DV-Anlagen samt Zubehör zunehmen!
Der Schweizer Computerspezialist Emil Zopfi beschreibt in seinem Roman *Jede Minute kostet 33 Franken* sehr eingängig die Arbeitssituation von Operatoren und Programmierern im Rechenzentrumsschichtdienst. Gewaltphantasien gegen die Maschine tauchen bei mehreren Mitarbeitern auf:
„Greif in die Eingeweide der Maschine hinein. Reiß an den Drähten und Kabeln. Zerr das Zeug ans Licht. Trample den Haufen zusammen. Die gedruckten Schaltungen, Stecker, Bandkabel, Speicherplatten. Reiß die Bänder von den Spulen. Aufreizend knistern sie unter den Sohlen, wenn sie zerknittern und all die fürchterlichen Daten, die sie enthalten, kaputt gehen. Irgendwann vor Jahren hat er das geträumt."[6]
Die Feststellung, daß *„der Vandalismus allgemein zunimmt"*, sieht die *Computerwoche* durch Berichte der TELA-Versicherung dokumentiert. Diese schilderte u.a. einen Fall, *„... bei dem Einbrecher den Geldschrank eines größeren Handwerksbetriebs aufstemmten, und weil sie von der ‚geringen' Beute von 20 000 Mark nicht satt wurden, ließen sie die Safetür mitgehen und legten Feuer, das die MDT-Anlage des Betriebs zerstörte."*[7]



In der Ausgabe der *Computerwoche* vom 25.4.1980 beschäftigt sich der Wissenschaftsjournalist Egon Schmidt mit der Frage *„Warum und von wem werden Computer ‚geknackt'?"* Solche Fragestellungen in unternehmernahen Zeitschriften häufen sich. In den USA existiert ein nationales Zentrum für Computer-Crime. Das läßt den Schluß zu, daß es nicht um einzelne Fälle, sondern schon um ein soziales Phänomen geht. Egon Schmidt stützt sich bei der Beantwortung seiner Frage auf Untersuchungen des US-nationalen Computer-Crime-Zentrums. Er kommt zu einer Unterteilung in sieben Haupttypen:

1. Täter, die den Rechner nüchtern als Werkzeug betrachten: vom „Telefon-Freak", der zu Gratistelefonaten kommen will, bis zum Held, der per Computer Tausende manipulierter Versicherungspolicen anfertigte; also typische Kriminelle;
2. die Gruppe jener Angestellten, die einmal zufällig auf eine Schwachstelle stoßen und nun den Rechner zugunsten des eigenen Kontos wirken lassen;
3. zielstrebiger sucht jene Gruppe Täter nach Lücken in der Computersicherheit, deren Angehörige vielleicht Schulden haben, spielen und wetten, erpreßt werden oder auch drogenabhängig sind;



4. die Gruppe der typischen Problemlöser, die vom logisch-technischen Reiz der Datenverarbeitung herausgefordert werden, die Befriedigung, das Problem gelöst zu haben, ist dabei oft wichtiger als das Geld;
5. jene Mitarbeiter, die gedanklich nie über ihr Keyboard hinausblicken. Sie wurden schon dazu verleitet, mal eben eine Million fehlzuleiten, um einem Kollegen einen Streich zu spielen;
6. die von Datenverarbeitungsneuerungen sich attackiert fühlenden Angestellten, für die der Computer eine Art Kampfplatz in der Auseinandersetzung mit ihrem Arbeitgeber ist; sie begehen gern Sabotage, gehen physisch gegen Hardware vor, ändern Programme;
7. ein verwandter Typus von Computer-Gangster ist jener, der die Automation an sich attackiert. Er will die verhaßte Maschine als solche lahmlegen. Auch mit revolutionären Ideologien werden derartig motivierte Sabotageakte oft verknüpft.

Schmidt spricht den letzten beiden Gruppen eine Art politische Begründung für ihre Taten zu und führt schließlich als Resumée seiner „Typologie der Computergaunerei" aus:
„Wer sich mit Datensicherheitsproblemen herumzuschlagen hat, sieht nun wohl klarer, wo der ‚Feind' steht und welche Charakteristika ihn auszeichnen."[8]
Auch wenn in den letzten Jahren ein regelrechter Rummel um den Schutz personenbezogener Daten veranstaltet wurde, die Datensicherheit – sprich der Schutz der Daten vor den Personen – ist für die Unternehmer das eigentliche Problem. Schmidts Resumée ist ein weiterer Beleg dafür.
Aber die einschlägigen Kenner der Computer„kriminalität" bleiben nicht bei Typisierungen stehen. Gegenmaßnahmen sind für die Unternehmerseite äußerst wichtig. Die *Computerwoche* hat entsprechende Tips parat:
„Da nach den vorliegenden Erkenntnissen in einer Reihe von Fällen Mitarbeiter, und zwar solche, die Zugang zum unmittelbaren Sicherheitsbereich hatten, die Täter gewesen sein müssen, gewinnt hier vor allem der ***Aspekt der menschlichen Qualifikation*** *zunehmendes Gewicht. Allgemein klagen beispielsweise die Sachversicherer, daß die Achtung vor fremdem Eigentum geringer geworden ist: Der ‚Bootstrap' wird schon mal öfter in wütend zerstörerischer Absicht geführt. Von zur Mühlen plädiert denn auch dafür, bei der Personalauswahl bedingungslos* ***labile Typen*** *[...] nicht im DV-Bereich einzusetzen [...] Die Sicherheitsexperten müssen überlegen, ob sich unter den Kolle-*

gen des Terminal-Sachbearbeiters einer findet, dessen ***kriminelle Intelligenz*** *zur Gefahr für geheimschutzbedürftiges Material werden kann. Auch wenn es vielleicht Diskussionen mit dem Betriebsrat geben wird: Gleichlaufend proportional mit der Intelligenz der Technik müssen Kenntnisse und* ***charakterliche Qualifikation*** *der Mitarbeiter steigen. Am Einzelarbeitsplatz liegt die psychologische Sperre, ‚mal eben seiner Aggression freien Lauf zu lassen', wesentlich niedriger als innerhalb eines Gruppenarbeitsplatzes* [...] *Die schädliche Energie entlädt sich in einem Fluch."*[9]

Der *Sicherheitsberater* gibt seinen Lesern nach Schilderung des Problemfalles einen detaillierten Maßnahmenkatalog an, um im eigenen Unternehmen solche „Delikte" möglichst zu verhindern.

Die oben aufgeführten Zitate und Beispiele sollen keinesfalls eine radikale Angestelltenbewegung oder eine politische motivierte Computerstürmerei vortäuschen. Aber sie zeigen doch, daß die Verhaltensweisen der DV-Angestellten nicht nur aus Anpassung, Norm und Wohlverhalten bestehen können. **Individueller** Widerstand ist existent, fernab von ideologischen Rechtfertigungen. Die persönlichen Bedürfnisse, Phantasien, Träume lassen sich nicht so einfach wegrationalisieren.

Die zitierten Äußerungen zeigen ferner, daß die Unternehmer solche „Fälle" für gefährlich halten und damit zu kämpfen haben. Ihre Methoden unterscheiden sich dabei nicht wesentlich von Auseinandersetzungen in anderen Bereichen. Typisch die Polizeisprache und der permanente sprachliche Versuch der Kriminalisierung. *„Kriminell", „schädlich", „wütend zerstörerisch"* sind die *„Missetaten". „Kriminelle Intelligenz", „Aggression"* und *„Vandalismus"* – so lauten die Begriffe für die Verhaltensbeschreibungen der „Täter".

Wie aber sollen wir als Linke solche individuellen Verhaltensweisen bewerten? Ich würde K.H. Roth zustimmen, wenn er in einem Gespräch mit der Zeitschrift *Alternative* behauptet, daß die bisherigen Klassenkampfformen des Marxismus bzw. Neo-Leninismus gegen die automatisierte Fabrik mit all ihren Auswirkungen, gegen die perfektionierte Überwachung versagt haben. Auchd die herkömmliche Gewerkschaftsarbeit nimmt den Angriff auf die Identität der Mitarbeiter durch die Automatisierung, nimmt ihre Aggressivität und Frustration nicht auf. Als Reaktion auf diese Frustration sieht Roth *„so etwas wie eine neue Form von Maschinenstürmerei. Und da fangen die Probleme des Marxismus an, oder genauer: da hört der Marxismus auf und beginnt die soziale Revolution – auch in diesem Bereich."*[10]

Eine der Hauptgruppen in Egon Schmidts o.a. Computerkriminalitätstypologie bildeten jene Angestellte, die ihre Sabotageakte mit revolutionären Ideologien motivieren. Ein spektakuläres Beispiel dieser Art hatte die *Hamburger Morgenpost* im Frühjahr dieses Jahres zu berichten:

„Sie verabscheuen Computer als Instrument der Mächtigen und nennen sich ‚wütende Schafe' [...] *eröffneten ihre Offensive über Ostern mit einem großen Knall, als sie das Computer Service Center von Philips in Toulouse in die Luft sprengten. Dabei wurden die gesamten Daten-Anlagen und alle Magnetbänder zerstört.* [...] *das ‚Komitee zur Vernichtung der Computer' – kurz CLODO – erklärte jüngst in einem Pariser Untergrundblatt: ‚Wir sind durchweg Computerfachleute und daher in der Lage, die Gefahren, die von diesem Industriezweig ausgehen, in besonderem Maße zu erkennen. Der Computer ist das Lieblingsinstrument der Mächtigen. Er dient der totalen Kontrolle und der Unterdrückung."*[10]

Doch alle Aktionen dieser Art können nur Teil einer Hinhaltetaktik sein: denn Maschinen und Programme werden nach einiger Zeit neu installiert, und die Datenbestände sind heutzutage durchweg mehrfach an verschiedenen Orten aufbewahrt.

Widerstand – ein Computerspiel?

Die Abhängigkeit von Unternehmen und staatlichen Institutionen vom Personal im DV-Bereich zeigt sich sehr deutlich dann, wenn kollektive Aktionen – wie z.B. Streiks – stattfinden. Vor einigen Jahren schon reagierten Politiker und Medien hektisch auf die ständischen Forderungen der Fluglotsen. Die Kommentare anläßlich des ersten Streiks in einem Rechenzentrum der BRD 1979 waren ähnlich besorgt:

„Im August dieses Jahres fand im Rechenzentrum der Landesversicherungsanstalt Rheinprovinz in Düsseldorf der erste Streik von Spezialisten der elektronischen Datenverarbeitung in Deutschland statt. In Frankreich gab es schon einige Streiks von EDV-Personal im Bankenbereich, und in England drohte vor einigen Monaten das EDV-Personal des Schatzministeriums mit Streik. Mit dem von der Gewerkschaft ÖTV in Düsseldorf ausgerufenen Streik wurden zwei zusätzliche Freischichten für das Rechenzentrumspersonal erkämpft, das Schichtarbeit leisten muß [...] *In einer Umfrage der ‚Computerwoche' machen mehrere Verantwortliche keinen Hehl aus ihrer Furcht vor einem solchen Wanken der Basis ihrer Macht. ‚Ein umfassender Streik des EDV-Personals wäre ein Alptraum* [...] *und würde die Wurzeln der sozialen Marktwirtschaft erschüttern', sagt Manager G. Brussmann."*[12]

Anmerkungen

1 In WECHSELWIRKUNG Nr. 2 wird im Schwerpunkt *Ingenieure im Beruf* eine „Entwicklung zum Lohnarbeiter" konstatiert, d.h. die Arbeitsbedingungen der Ingenieure gleichen sich denen der Lohnarbeiter an. Die Kontrolle über die Arbeit werde mit Hilfe von rechnerunterstützten Arbeitsplätzen, Arbeitsplatzbewertungsverfahren, Stechuhr und Zeiterfassungsbogen durchgeführt: Taylorisierung der geistigen Arbeit.
2 Computerwoche 14/1979, S. IV
3 Computerwoche 14/1979, S. IV
4 Rainer von zur Mühlen, Computerkriminalität – Gefahren und Abwehrmaßnahmen, Luchterhand 1973
Für weitere Anregungen vgl. auch: Pflasterstrand, Nr. 79 , S. 20 f.
5 Autonomie, Nr. 12, S. 107 f.
6 Emil Zopfi, Jede Minute kostet 33 Franken, Zürich: Limmat-Verlag, S. 132
7 Computerwoche 14/1979, S. V
8 Computerwoche vom 25.4.1980, S. 33
9 Computerwoche 14/1979, S. V
10 Alternative, Nr. 119, S. 89
11 Hamburger Morgenpost vom 30.4.1980, S. 10
12 Die Tageszeitung vom 28.9.1979