

Der Abdruck des folgenden Urteils wird wegen des Umfangs und des sich notwendigerweise einstellenden ersten Eindrucks, daß scheinbar keine neuen Rechtsfragen entschieden werden (daher auch das Fehlen eines Leitsatzes), zunächst Verwunderung hervorrufen. Studiert man das Urteil, so wird man feststellen, daß sein Schwerpunkt im Bereich der Beweiswürdigung liegt. Derartige Passagen werden gegenwärtiger Abdruckpraxis nach drastisch gekürzt, wenn nicht gar ganz gestrichen. Der folgende Abdruck soll diese Praxis in Frage stellen und die Frage aufwerfen, ob uns im EDV-Recht nicht durch diese Bearbeitungspraxis Wesentliches entgeht. Das gilt nicht für die rechtlichen Voraussetzungen des folgenden Urteils. Es geht von der BAG-Rechtsprechung zur Verdachtskündigung aus. Daß der nach diesen Regeln begründete Verdacht (samt Beachtung der anderen nötigen Formalitäten) auf „Implantieren“ eines Virus im Computer des Arbeitgebers ausreicht, die außerordentliche Kündigung zu rechtfertigen, warf keine besonderen Begründungsschwierigkeiten auf. Sorgfältiges Abwägen in tatsächlicher Hinsicht erforderte aber das Umfeld eines Novell-Netzwerkes mit (in Verdacht stehendem) Systemverwalter und mehreren Benutzern (mit abgestuften Berechtigungen) in Kombination mit der Frage, wie Viren in ein derartiges Netz gelangen und sich dort verbreiten können. Folgt man diesen detaillierten Ausführungen des Gerichts, zeichnet sich ein Modell ab, das vorgibt, wie darauf bezogene belastende oder aber auch entlastende Beweisführungen möglich sind. Arbeitgeber wie Systemadministratoren können daraus entnehmen, was sie jeweils zu tun haben, um ihre Interessen in vergleichbarer Lage zu schützen. Weil so „hinter“ der Beweiswürdigung ein normatives Organisationsmodell aufscheint, ist das Urteil durchaus auch von rechtlichem Interesse. Das gilt, obwohl sich sein juristischer Gehalt nicht rechtssatzartig in konventioneller Leitsatzform festhalten läßt. Dies hin und wieder an ausgewählten Beispielen zu demonstrieren, dürfte den Platzverbrauch (der bei sorgfältigen Beweiswürdigungen besonders ausgeprägt sein muß) rechtfertigen  
(mh)

## „Implantierung“ eines Virus als Kündigungsgrund

Landesarbeitsgericht Saarland, Urteil vom 1. Dezember 1993 (2 Sa 154/92) – „Viren-Implantation“

### Tatbestand

Die Parteien streiten über die Rechtswirksamkeit einer außerordentlichen Kündigung.

Der 1954 geborene Kläger war ab dem 15.9.1989 als Praktikant und ab dem 1.1.1990 als EDV- und Büroleiter bei der Beklagten beschäftigt, die einen Fachliteraturdienst mit mehr als 5 Arbeitnehmern außer den Auszubildenden betreibt. Am 18.4.1990 kündigte die Beklagte das Arbeitsverhältnis außerordentlich, wandelte die außerordentliche Kündigung dann aber mit Schreiben vom 27.4.1990 zunächst in eine ordentliche Kündigung zum 30.6.1990 und schließlich zum 30.9.1990 um.

Nach dem 30.9.1990 war der Kläger zunächst nicht mehr bei der Beklagten beschäftigt, wurde aber in der Folgezeit fast täglich in den Betrieb der Beklagten gerufen, um die von ihm aufgebaute und erweiterte EDV-Anlage wieder in Gang zu bringen, bei der es ständig zu Störungen kam.

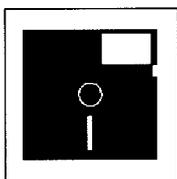
Am 17.12.1990 schlossen die Parteien einen neuen Anstellungsvertrag, wonach der Kläger ab dem 1.1.1991 als EDV-Leiter und Organisationssachbearbeiter bei der Beklagten eingestellt wurde. Das Arbeitsverhältnis war auf den 31.12.1991 befristet und sollte sich jeweils um 12 Monate verlängern, wenn bis zum 30.9. des jeweiligen Kalenderjahres keine Kündigung erfolgt. Als Vergütung war ein Gehalt von 4.500,— DM brutto und eine Leistungszulage von 5 % des monatlichen Firmenergebnisses (Gewinns) vereinbart, auf die eine monatliche Pauschale von 1.000,— DM zusammen mit dem Gehalt ausbezahlt und quartalsweise mit dem tatsächlich errechneten Gewinn abzugleichen war.

Mit Schreiben vom 14.3.1991, das dem Kläger am selben Tag zugegangen ist, kündigte die Beklagte das Arbeitsverhältnis außerordentlich.

*Zum Ablauf der Kündigungen*

*Neuer Anstellungsvertrag*

*Neue außerordentliche Kündigung*



Viren im Netz

Cascade B

Anhörung des Klägers  
Feststellungsklage

Vortrag des Klägers in 1. Instanz

Antrag des Klägers

Antrag der Beklagten

Vortrag der Beklagten

Die Kündigung wird darauf gestützt, daß der Kläger in dem Verdacht stehe, ein Computervirus in das EDV-System der Beklagten implantiert zu haben, um die Beklagte zum Abschluß des neuen Arbeitsvertrages zu veranlassen.

Unstreitig war das EDV-System der Beklagten immer wieder zusammengebrochen. Der Zeuge [] von der Firma [] aus [] hatte bei einer Überprüfung der Hardware-Installation der EDV-Anlage, bei der er keine Mängel feststellen konnte, mit Hilfe eines Virentestprogramms Viren auf dem Netz und auf einzelnen Personalcomputern entdeckt (vgl. seine Angaben gegenüber der Kriminalpolizei).

Daraufhin beauftragte die Beklagte die Firma [] aus [], deren Geschäftsführer, der Zeuge [], die Anlage der Beklagten in der Zeit vom 25.1. bis zum 6.3.1991 überprüfte. Nach dessen Abschlußbericht wurde dabei ein Virus des Typs Cascade B auf dem Fileserver, einem Arbeitsplatz mit Festplatte und einem freistehenden PC entdeckt. Auf dem Fileserver seien die Dateien COMMAND.COM und KEYB.COM von dem Virusbefall betroffen gewesen. Ein Befall mit dem Virustyp Cascade B führe zu einer Vergrößerung der betroffenen Programme und könne in seltenen Fällen dadurch bedingt zu Platzproblemen und damit verbunden zu Störungen im Programmablauf führen. Eine Überprüfung der Zugriffsrechte aller Benutzer habe zu dem Ergebnis geführt, daß lediglich der Benutzer mit dem Benutzercode "SV" das Virus eingeschleust haben könne. Außer dem Kläger selbst habe kein anderer Benutzer über diesen Benutzercode verfügt, so daß der Kläger in dem erheblichen Verdacht stehe, diese Infektion bewußt verursacht zu haben.

Daraufhin wurde der Kläger ab dem 11.3.1991 beurlaubt und am 14.3.1991 angehört. Mit seiner am 21.3.1991 bei dem Arbeitsgericht eingegangenen Feststellungsklage wendet sich der Kläger gegen die ausgesprochene Kündigung. ...

Der Kläger hat im ersten Rechtszug vorgetragen, er habe vor seinem Ausscheiden bei der Beklagten zum 30.9.1990 dem Angestellten [] am 27.8.1990 und der Angestellten [] am 10.9.1990 eine Codeworttabelle übergeben – was insoweit unstreitig ist –. Aus der Codeworttabelle, die er dem Zeugen [] übergeben habe, ergebe sich, daß das Codewort "AAA" gleichbedeutend mit "SV" sei. Damit hätten auch alle anderen Mitarbeiter der Beklagten den Zugang zu dem System gehabt. Da das Virus Anfang 1991, also nach dem 27.8.1990, entdeckt worden sei, könne es von jedem implantiert worden sein, der das Codewort "AAA" gekannt habe. Im Sommer 1990 sei die EDV-Anlage der Beklagten auf Multi-User-Betrieb umgestellt worden, was zu erheblichen Schwierigkeiten in der Arbeitsabfolge geführt habe. Aus diesem Grund habe sich die Beklagte der weiteren Mitarbeit des Klägers versichert, der die Mitarbeiter [] und [] so eingearbeitet habe, daß der Regelbetrieb habe weiterlaufen können. Der Zusammenbruch der EDV-Anlage sei insbesondere durch einen überdurchschnittlichen Datenzuwachs wegen der Geschäftstätigkeit der Beklagten in den neuen Bundesländern verursacht worden.

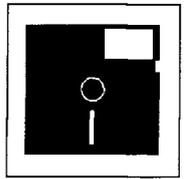
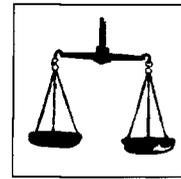
Der Kläger hat beantragt,

1. festzustellen, daß das Arbeitsverhältnis der Parteien durch die fristlose Kündigung der Beklagten vom 14.3.1991 nicht aufgelöst ist, sondern fortbesteht; ...

Die Beklagte hat beantragt,

die Klage abzuweisen.

Die Beklagte hat vorgetragen, nachdem die EDV-Anlage im Juni 1990 grundlegend erweitert worden sei, sei das Datenverarbeitungssystem im Herbst 1990 und auch Anfang 1991 immer wieder zusammengebrochen. Während das von der Beklagten beauftragte Softwareunternehmen nicht in der Lage gewesen sei, die Anlage wieder in Gang zu setzen, habe der Kläger den Fehler immer in kürzester Zeit beseitigen können. Nur der Kläger habe über das Passwort "SV" verfügt, mit dem die Dateien beschrieben und verändert werden könnten. Nur mit diesem Passwort habe man den Zugang zu dem Netzwerk, dem Betriebssystem der Anlage. Mit der Codeworttabelle, die der Kläger den Zeugen [] und [] ausgehändigt habe, bestehe dagegen nur Zugang zu der Anwendersoftware der Anlage. Gegenüber dem Zeugen [] habe der Kläger eingeräumt, daß er das Codewort für das Netzwerk niemandem weitergegeben habe. Der Zeuge habe dem Kläger deswegen Vorhaltungen gemacht. Nachdem der Geschäftsführer den Abschlußbericht des Zeugen [] erhalten habe, habe er den Kläger sofort am 11.3.1991 beurlaubt. Die Mitarbeiter [] und [] seien befragt worden, wobei sich herausgestellt habe, daß beide das Codewort für den Fileserver



nicht gehabt hätten. Als dem Kläger dann bei seiner Anhörung am Morgen des 14.3.1991 die Feststellungen in dem Abschlußbericht des Zeugen [ ] vorgehalten worden seien, insbesondere, daß nur der Kläger das Benutzerwort für den Fileserver gehabt habe, habe der Kläger nur eingewandt, das Virus könne auch von den beiden anderen Mitarbeitern implantiert worden sein. Mit jeder Diskette könne man einen Fehler implantieren. Auf den Vorhalt, Fremdfirmen hätten den Fehler nie gefunden, während er den Fehler immer in kürzester Zeit habe beseitigen können, habe der Kläger nur eingewandt, er kenne die Anlage. Zugang zu dem Betriebssystem habe man jedoch nur, wenn man das Passwort des Supervisors kenne, während die den Zeugen [ ] und [ ] übergebene Codeworttabelle nur den Zugang zu dem Anwendersystem verschaffe. Das werde bestätigt durch einen Vorfall, der sich am 13.3.1991, also einen Tag vor Ausspruch der Kündigung während der Beurlaubung des Klägers abgespielt habe. Der Zeuge [ ] sei von der Beklagten beauftragt worden, den Zeugen [ ] und [ ] das Betriebssystem zu erklären. Die Zeugen [ ] und [ ] hätten jedoch nicht über das dazu erforderliche Passwort verfügt. Die Zeugin [ ] habe daraufhin im Auftrag des Geschäftsführers der Beklagten bei dem Kläger angerufen und nach dem Passwort für das Betriebssystem gefragt. Der Kläger habe sich geweigert, dieses Wort mitzuteilen. Als sich daraufhin der Geschäftsführer der Beklagten telefonisch eingeschaltet und mit einer Strafanzeige gedroht habe, habe der Kläger das Passwort "RRR" mitgeteilt.

Das Arbeitsgericht hat Beweis erhoben aufgrund des Beweisbeschlusses vom 2.8.1991 durch Einholung eines Sachverständigengutachtens.

Der Sachverständige Dipl. Ing. [ ] ist in seinem Gutachten vom 27.5.1992 zu dem Ergebnis gelangt, da das vorgefundene Virus nach seinem beschriebenen Verhalten nicht das Virus Cascade B gewesen sein könne, seien die Folgerungen des Gutachtens der Firma [ ] nicht verifizierbar. Da die Zugriffsrechte des Users "AAA" aus dem Übergabeprotokoll vom 27.8.1990 an den Mitarbeiter [ ] nicht nachvollziehbar seien, liefere das Übergabeprotokoll keine substantiierten Informationen, um den Verdacht zu verifizieren oder zu falsifizieren. Das Virus Cascade B führe nicht zu einer Vergrößerung von COM-Dateien, sondern zu zufallsgenerierten Neustarten (Reboots) des befallenen Computers. Die Folgerungen des Gutachtens der Firma [ ] könnten zwar für das Virus Cascade B korrekt sein. Da aufgrund der vorliegenden Unterlagen aber kein Cascade B Virus vorgelegen habe und das eigentliche Virus unbekannt sei, könne der geäußerte Verdacht nicht verifiziert werden.

Durch Teilurteil vom 28.7.1992 hat das Arbeitsgericht die Klage hinsichtlich des Feststellungsantrags abgewiesen ...

Zur Begründung hat das Arbeitsgericht im wesentlichen ausgeführt, die Beklagte habe alles Zumutbare zur Aufklärung des gegen den Kläger bestehenden Verdachtes unternommen. Das Gutachten der Firma [ ] sei im Ergebnis völlig eindeutig. Der Kläger habe in dem Gespräch mit dem Geschäftsführer der Beklagten und dem Prozeßbevollmächtigten der Beklagten vor Ausspruch der Kündigung sich nicht bemüht, eine Aufklärung herbeizuführen, obwohl er als Fachmann im Computerbereich dazu in der Lage gewesen wäre. Der Kläger habe zwar darauf hingewiesen, daß auch ein anderer das Virus eingepflanzt haben könne, habe aber im übrigen die Feststellungen des Gutachters [ ] nicht in Frage gestellt. Die allgemeine Verteidigung des Klägers habe den bei der Beklagten bestehenden Verdacht der Täterschaft des Klägers nicht ausräumen können. Das Gutachten des Sachverständigen stehe dem nicht entgegen. Aufgrund von Veränderungen im EDV-System der Beklagten sei in der Zwischenzeit nicht mehr festzustellen, welche Virusart tatsächlich vorgelegen habe. Der Sachverständige [ ] habe aber eingeräumt, daß die Folgerungen des Gutachtens [ ] für das Virus Cascade B korrekt sein könnten. Auch wenn der Kläger dem Mitarbeiter [ ] mit der Übergabe der Codeworttabelle am 27.8.1990 möglicherweise auch das Passwort "SV" mitgeteilt habe, sei nicht auszuschließen, daß das Virus bereits vorher eingepflanzt worden sei. ...

Gegen das ihm am 21.9.1992 zugestellte Urteil hat der Kläger am 28.9.1992 Berufung eingelegt und diese nach Verlängerung der Berufungsbegründungsfrist bis zum 25.11.1992 am 24.11.1992 begründet.

Der Kläger trägt vor, es bestünden erhebliche Bedenken dagegen, die ausgesprochene Kündigung als Verdachtskündigung zu bewerten. Die Beklagte habe erst in dem Kündigungsschutzverfahren vortragen lassen, daß es sich um eine Verdachtskündigung handele. Aufgrund des Sachverständigengutachtens [ ] vom 27.5.1992 stehe fest, daß der Vorwurf der Pflichtverletzung durch die Einschleusung eines Virus nicht nachgewiesen sei. Die Beklagte habe nicht alles Zumutbare zur Aufklärung getan. Sie habe mit der Untersuchung ein Unternehmen beauftragt, das selbst derartige Systeme verkaufe und warte und daher ein eigenes Interesse daran besitze, dem Kläger Versäumnisse anzulasten, um selbst mit der weite-

*Sachverständigengutachten*

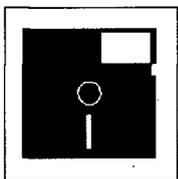
*Der Sachverständige zum Virentyp*

*Urteil des ArbG*

*Begründung des Arbeitsgerichts*

*Berufung durch den Kläger*

*Berufungsvortrag des Klägers*



ren Betreuung der Anlage beauftragt zu werden. Der Kläger sei am 9.3.1991 zu dem Geschäftsführer der Beklagten beordert worden, der ihm aus dem Bericht des Zeugen [] auszugswise vorgelesen habe. Der Kläger habe sofort jegliche Beteiligung abgestritten und erklärt, daß er über schriftliche Beweise verfüge, die den Vorwurf widerlegen würden. Dazu sei dem Kläger aber keine Gelegenheit gegeben worden. Am 11.3.1991 sei der Kläger bis auf weiteres beurlaubt worden. Am 14.3.1991 sei er zu der Beklagten bestellt worden, wo er den Geschäftsführer der Beklagten und dessen Rechtsanwalt vorgefunden habe. Der Rechtsanwalt habe erklärt, der Kläger wisse, was ihm vorgeworfen werde, allein das reiche aus, um ihm frisdos zu kündigen. Eine angebotene einvernehmliche Lösung des Arbeitsverhältnisses habe der Kläger abgelehnt, woraufhin ihm die fristlose Kündigung ausgehändigt worden sei. Der Kläger habe die von den übrigen Mitarbeitern unterzeichneten Übergabeprotokolle vorgelegt, aus denen ersichtlich sei, daß außer dem Kläger auch diese Mitarbeiter Zugang zu dem System gehabt hätten. Ergänzend werde die eidesstattliche Erklärung des Mitarbeiters [] vom 12.8.1992 vorgelegt, wonach dieser vor dem Ausscheiden des Klägers im September 1990 von diesem das Codewort „AAA – SSS“ erhalten habe und damit vollen Zugang zu dem Netzwerk der Beklagten gehabt habe und somit alle Netzwerkoperationen eigenständig habe durchführen können. Die Zeugin [] habe am 11.8.1992 eidesstattlich erklärt, daß sie vor dem Ausscheiden des Klägers im September 1990 von diesem das Codewort „EEE – SSS“ erhalten habe und das Übergabeprotokoll vom 10.9.1990 korrekt gewesen sei. Durch das Gutachten des Sachverständigen sei der Verdacht hinsichtlich der Täterschaft des Klägers ausgeräumt. Der Sachverständige habe nämlich ausgeschlossen, daß es sich um das Virus Cascade B gehandelt habe. Da der Verdacht von dem Zeugen [] ausschließlich darauf gestützt worden sei, daß das Computersystem von dem Virus Cascade B verseucht worden sei, sei von dem in dem Gutachten des Zeugen [] geäußerten Verdacht nichts mehr übrig geblieben. Das Virus habe unbewußt durch eine oder mehrere verseuchte Disketten übertragen werden können. Dafür kämen alle Mitarbeiter in Betracht, die über die Rechte eines „Supervisors“ verfügten, also der Kläger, der Zeuge [] und die Zeugin [] für den Server und für den anderen PC alle übrigen Mitarbeiter. ...

### Berufungsantrag des Klägers

Der Kläger beantragt,

*unter Abänderung des Teilurteils des Arbeitsgerichts Neunkirchen vom 28.7.1992, Az.: 3 Ca 378/91,*

1. festzustellen, daß das Arbeitsverhältnis der Parteien durch die fristlose Kündigung der Beklagten vom 14.3.1991 nicht aufgelöst worden ist, sondern fortbesteht; ...

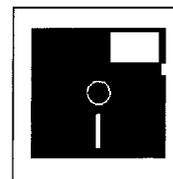
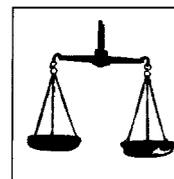
Die Beklagte beantragt,

### Berufungsantrag der Beklagten

*die Berufung zurückzuweisen.*

### Berufungsvortrag der Beklagten

Die Beklagte trägt vor, mit der Codeworttabelle, die der Kläger unstreitig den Zeugen [] und [] vor seinem Ausscheiden am 30.9.1990 ausgehändigt habe, habe man nur Zugang zu der Anwendersoftware, nicht zu dem Netzwerk, dem Betriebssystem der Anlage. In das Netzwerk (Betriebssystem) der Computeranlage gelange man nur mit dem sogenannten Passwort, und zwar zusammen mit dem sogenannten User-Code. Als der Kläger der Zeugin [] die Codeworttabelle übergeben habe, habe die Zeugin sich zunächst geweigert diese Tabelle anzunehmen, aus Angst, sie könne eventuell Netzwerkdaten vernichten. Der Kläger habe sie daraufhin beruhigt und erklärt, mit diesen Codewörtern könne sie nur auf einzelne Stationen, aber nicht in das Netzwerk gelangen. Am 12.8.1992 sei der Kläger ohne jegliche Voranmeldung in der Wohnung der Zeugin [] erschienen und habe der Zeugin eine eidesstattliche Erklärung zur Unterschrift vorgelegt mit der Begründung, der Geschäftsführer der Beklagten bestreite, daß der Kläger ihr die Codeworttabelle übergeben habe. Beim Durchlesen habe die Zeugin festgestellt, daß in der vorbereiteten Erklärung die Sätze gestanden hätten, daß sie damit vollen Zugang zum Netzwerk der Beklagten gehabt und alle Netzwerkoperationen habe durchführen können. Als die Zeugin den Kläger darauf hingewiesen habe, daß sie diese Erklärung so nicht unterzeichnen werde, weil sie falsch sei, seien die entsprechenden Sätze gestrichen worden. Dem Zeugen [] habe der Kläger am selben Tag ebenfalls die gleiche vorbereitete eidesstattliche Erklärung mit der gleichen Begründung vorgelegt. Der Zeuge [] habe die eidesstattliche Erklärung ungeprüft unterschrieben, was er in seiner eidesstattlichen Erklärung vom 30.11.1992 bestätigt habe. Das User-Wort habe damals wie heute „SV“ gelautet. Das dazu gehörige Passwort für das Betriebssystem



stem habe damals „BBB“ gelautet. Als die Anlage der Beklagten nach dem Ausscheiden des Klägers im September 1990 wieder einmal abgestürzt sei, habe die Beklagte die Firma [ ] eingeschaltet, um den Schaden zu beheben. Die Zeugin [ ] von der Firma [ ] habe die beiden Zeugen [ ] und [ ] gebeten, ihr das Passwort für das Betriebssystem auszuhändigen, woraufhin beide ihr die Codeworttabelle gegeben hätten. Der Zeugin [ ] sei es nicht gelungen, mit der Codeworttabelle in das Betriebssystem zu gelangen. Am nächsten Tag sei der Kläger im Betrieb der Beklagten erschienen und habe den Schaden in kürzester Zeit behoben. Nachdem der Kläger gegenüber dem Zeugen [ ] eingeräumt habe, daß nur er das Passwort habe, habe der Zeuge [ ] dem Kläger deshalb Vorhaltungen gemacht. Bei dem festgestellten Virus habe es sich um ein Virus des Typs Cascade B gehandelt. Aus dem englischen Text mit den Angaben der Symptome dieses Virus, der dem Gutachten als Anhang 1 beigefügt gewesen sei, ergebe sich eindeutig, daß zu den Symptomen auch eine Vergrößerung der Dateien („Com-file growth“) gehöre. Der Zeuge [ ] von der Firma [ ] habe als Erster das Virus entdeckt und dies auch dem Zeugen [ ] mitgeteilt. Dabei habe sich herausgestellt, daß der Zeuge [ ] das Virus nicht überall gelöscht gehabt habe. Der Zeuge [ ] habe das Virus daher selbst eindeutig identifizieren können. Das Virus könne auch nicht unbeabsichtigt durch Benutzung einer mit dem Virus befallenden Diskette in das Betriebssystem der Anlage gelangt sein, weil das Sicherheitssystem der Firma [ ] das verhindere.

Dem Kläger sei seit dem 9.3.1991 bekannt gewesen, welche Vorwürfe gegen ihn durch den Zeugen [ ] erhoben worden seien. Er sei deshalb ab dem 11.3.1991 beurlaubt worden. Bei der Anhörung, zu der der Kläger auf den 14.3.1991 geladen worden sei, sei der Vorwurf nochmals wiederholt worden, so wie es der Zeuge [ ] in seinem Gutachten ausgeführt habe. Der Kläger habe darauf hingewiesen, daß auch andere Personen die Möglichkeit gehabt hätten, das Virus zu installieren. Daraufhin sei dem Kläger vorgehalten worden, daß nur er über das Passwort für den Fileserver verfügt habe. Der Kläger habe geantwortet, daß man mit jeder Diskette Fehler einpflanzen könne. Auf den Widerspruch angesprochen, daß Fremdfirmen den Fehler nicht hätten beheben können, während der Kläger dazu sofort in der Lage gewesen sei, habe der Kläger nur erwidert, daß er sich ja in der Anlage auskenne. Man habe dem Kläger gesagt, daß seine Angaben nicht ausreichen und gravierende Verdachtsmomente übrigblieben, daß nur er das Virus eingepflanzt haben könne.

Das erkennende Gericht hat Beweis erhoben aufgrund der Beweisbeschlüsse vom 10.3.1993 durch Vernehmung der Zeugen [ ] und [ ] und vom 24.3.1993 durch Einholung eines Sachverständigengutachtens. Wegen des Ergebnisses der Beweisaufnahme wird auf die Sitzungsniederschrift vom 10.3.1993 und das Gutachten des Sachverständigen Dipl. Ing. [ ] Bezug genommen.

*Zur Anhörung*

## Entscheidungsgründe

Die zulässige Berufung des Klägers hat keinen Erfolg.

Das Arbeitsgericht hat zu Recht festgestellt, daß das Arbeitsverhältnis der Parteien durch die außerordentliche Kündigung der Beklagten vom 14.3.1991 aufgelöst worden ist ...

*Erfolglosigkeit der Berufung*

1. Der Beklagten hat ein wichtiger Grund im Sinne des § 626 Abs. 1 BGB zum Ausspruch einer außerordentlichen Kündigung zur Seite gestanden.

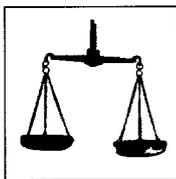
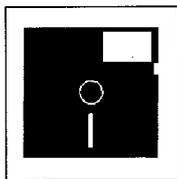
*Wichtiger Grund*

Der Kläger steht in dem dringenden Verdacht, ein Computervirus in die EDV-Anlage der Beklagten implantiert zu haben, um die Beklagte zum Abschluß des Arbeitsvertrages vom 17.12.1990 zu bewegen.

*Dringender Verdacht*

Nach der ständigen Rechtsprechung des Bundesarbeitsgerichts kann nicht nur eine erwiesene Vertragsverletzung, sondern schon der Verdacht einer strafbaren Handlung oder einer sonstigen schweren arbeitsvertraglichen Verfehlung des Arbeitnehmers einen wichtigen Grund im Sinne des § 626 Abs. 1 BGB für eine außerordentliche Kündigung darstellen, wenn gerade der Verdacht das zur Fortsetzung des Arbeitsverhältnisses notwendige Vertrauen des Arbeitgebers in die Redlichkeit des Arbeitnehmers zerstört oder zu einer unerträglichen Belastung des Arbeitsverhältnisses geführt hat (vgl. BAG, Urt. v. 4.6.1964 AP Nr. 13 zu § 626 BGB Verdacht strafbarer Handlung u. v. 27.1.1972 AP Nr. 2 zu § 626 BGB Ausschlussfrist). Gegenüber dem Vorwurf, der Arbeitnehmer habe eine Vertragsverletzung begangen, stellt der Verdacht einer strafbaren Handlung oder einer sonstigen schweren arbeitsvertraglichen Verfehlung des Arbeitnehmers einen eigenständigen Kündigungsgrund dar, der in dem Tatvorwurf nicht enthalten ist. Die Gerichte für Arbeitssachen können eine Kündigung daher nur dann unter dem Gesichtspunkt der Verdachtskündigung beurteilen,

*BAG zur Verdachtskündigung*



*Strenge Maßstäbe*

wenn der Arbeitgeber die Kündigung gerade auf den Verdacht stützt, was sowohl bei Ausspruch der Kündigung als auch während des Kündigungsschutzprozesses in der Tatsacheninstanz geschehen kann (vgl. BAG, Urt. v. 3.4.1986 u. v. 26.3.1992 AP Nr. 18 u. 23 zu § 626 BGB Verdacht strafbarer Handlung).

An die Zulässigkeit einer Verdachtskündigung sind strenge Maßstäbe anzulegen, da die Gefahr groß ist, einen Unschuldigen zu treffen. Der Verdacht muß daher objektiv durch bestimmte Tatsachen begründet und dringend sein (BAG, Urt. v. 8.8.1968 AP Nr. 57 zu § 626 BGB). Der Arbeitgeber muß alle zumutbaren Anstrengungen zur Aufklärung des Sachverhalts unternommen haben. Dazu gehört insbesondere, den Arbeitnehmer vor Ausspruch einer Verdachtskündigung zu den gegen ihn erhobenen Vorwürfen zu hören. Verletzt der Arbeitgeber die ihm obliegende Anhörungspflicht schuldhaft, so ist die auf den Verdacht gestützte Kündigung unwirksam (vgl. BAG, Urt. v. 11.4.1985 AP Nr. 39 zu § 102 BetrVG 1972 u. v. 30.4.1987 AP Nr. 19 zu § 626 BGB Verdacht strafbarer Handlung).

*Fristlauf*

Die Ausschlußfrist des § 626 Abs. 2 BGB beginnt in dem Zeitpunkt, in dem der Kündigungsberechtigte den Sachverhalt soweit mit Sicherheit kennt, daß er sich ein Urteil über den Verdacht, seine Tragweite und seine Auswirkungen bilden und daraufhin die Entscheidung gemäß § 626 Abs. 1 BGB treffen kann (vgl. BAG, Urt. v. 27.1.1972 AP Nr. 2 zu § 626 BGB Ausschlußfrist).

*Zu berücksichtigen:  
Entlastungsbeweise im  
Verfahren*

Stellt sich im Verlauf des Kündigungsrechtsstreits die Unschuld des verdächtigten Arbeitnehmers heraus, so ist dies noch zu seinen Gunsten zu berücksichtigen. Deshalb hat das Gericht etwaigen Entlastungsbeweisen des Arbeitnehmers während des Kündigungsrechtsstreits nachzugehen (vgl. BAG, Urt. v. 4.6.1964 AP Nr. 13 zu § 626 BGB Verdacht strafbarer Handlung).

*Dringender Verdacht objektiv  
begründet*

2. Der dringende Verdacht gerade gegen den Kläger ist objektiv durch bestimmte Tatsachen begründet.

*Definition:  
Systemabsturz*

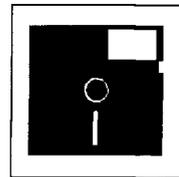
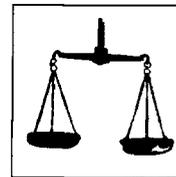
Die EDV-Anlage der Beklagten, die von dem Kläger aufgebaut und im Juni 1990 wesentlich erweitert worden ist, ist unstreitig häufig abgestürzt, so daß der Kläger nach seinem Ausscheiden bei der Beklagten zum 30.9.1990 fast täglich in den Betrieb der Beklagten gerufen worden ist, um die Anlage wieder in Gang zu setzen. Unter einem Systemabsturz versteht man nach den überzeugenden Ausführungen in dem Gutachten des Dipl. Ing. □ vom 19.9.1993 allgemein einen undefinierten Programmabbruch oder Programmneustart, wobei der Programmabsturz meist dadurch gekennzeichnet ist, daß der Rechner auf keinerlei Bedieneingabe mehr reagiert.

*Viren „Jerusalem“ und „Vanilla“*

Die Beklagte beauftragte die Firma □ mit der Überprüfung der Hardware. Wie sich aus der glaubhaften Aussage des Zeugen □, eines Büroinformationselektronikermeisters, der bei der Firma □ für die Hardware zuständig ist, bei seiner Vernehmung vor dem erkennenden Gericht ergibt, hat der Zeuge am 11.1.1991 die Hardware der Anlage überprüft, ohne einen Fehler festzustellen. Der Zeuge hat sich deshalb so genau an das Datum seiner Untersuchung erinnern können, weil es sich aus einem mitgebrachten Arbeitsbericht ergibt. Der Zeuge hat weiter bekundet, daß er daraufhin die Anlage der Beklagten mit einem mitgeführten Virussuchprogramm überprüft habe, das 27 Virustypen erfasse, während es über 100 Typen gebe. Nach seiner Aussage hat er an verschiedenen Stellen Viren des Typs Jerusalem und Vanilla gefunden, u.a. in dem Server, und zwar entweder auf der Festplatte oder auf der Diskette, mit der der Server gestartet wird. Er hat das Virus nach seiner Aussage beseitigt, soweit er es gefunden und an die Disketten herangekommen ist. Der Zeuge hat nicht ausschließen können, daß danach noch ein Virus vorhanden gewesen ist. Die Aussage des Zeugen erscheint glaubhaft. Der Zeuge hat bei seiner Aussage betont, daß er damals zum ersten Mal in seinem Leben ein Virus entdeckt habe und daß er kein Fachmann auf diesem Gebiet sei. Seine Aussage stimmt überein mit seinen Angaben vom 26.4.1991 gegenüber der Kriminalpolizei. Die Aussage wird weiter bestätigt durch die Angaben des Zeugen in dem Arbeitsbericht vom 11.1.1991, wonach nach dem Entfernen des Virus der Fehler immer noch vorhanden gewesen ist.

*Virus „Cascade B“*

Nach dem Abschlußbericht des Zeugen □ von der Firma □ aus □, der die Anlage der Beklagten unstreitig in der Zeit vom 25.1. bis zum 6.3.1991 überprüft hat, war die Anlage von einem Virus des Typs Cascade B befallen, wobei auf dem Fileserver die Dateien COMMAND.COM sowie KEYB.COM betroffen waren. In dem Abschlußbericht zu Ziffer 3.1 wird darauf hingewiesen, daß der Virusbefall von Herrn □ entdeckt und zu einem großen Teil beseitigt worden sei, während der Zeuge □ den Rest beseitigt habe.



Diese Angaben in dem Abschlußbericht des Zeugen [ ] werden durch das Gutachten des Sachverständigen [ ] vom 27.5.1992 nicht widerlegt. Der Sachverständige hat zwar ausgeführt, das Virus Cascade B führe nicht zu einer Vergrößerung von COM-Dateien, sondern zu zufallsgenerierten Neustarten (Reboots) des befallenen Computers, so daß das vorgefundene Virus nach dessen beschriebenem Verhalten nicht Cascade B gewesen sein könne, wobei der Sachverständige auf eine beigefügte Beschreibung des Virus in englischer Sprache im Anhang seines Gutachtens Bezug genommen hat. Diese Angaben des Sachverständigen beruhen jedoch auf einem offensichtlichen Irrtum. Wie sich bereits aus der dem Gutachten beigefügten Beschreibung der Symptome des Virus Cascade B in englischer Sprache ergibt, gehört zu den Symptomen nicht nur das zufallsgenerierte Neustarten („Reboot“), sondern auch eine Vergrößerung von Com-Dateien („Com:file growth“). Darauf hat die Beklagte bereits im ersten Rechtszug hingewiesen. Der Sachverständige [ ] hat das in seinem Gutachten vom 19.9.1993 eindeutig bestätigt. Danach ist die Vergrößerung der Dateien eines der auffälligsten und typischen Merkmale für eine Vireninfektion. Diese Eigenschaft treffe nicht nur für das Virus Cascade B und das Virus Jerusalem, sondern für die größte Zahl aller anderen bekannten Viren zu. Das Virus Cascade vergrößere Dateien um 1.701 oder 1.704 Bytes, wobei ein typisches Erscheinungsbild sei, daß Zeichen auf dem Bildschirm herunterfielen, weshalb das Virus auch vielfach als Herbstlaubvirus bezeichnet werde. Darüber hinaus führe dieses Virus zu sporadischem Neustarten (Reboot) des Rechners, was einem Systemabsturz gleichkomme, da dabei alle im Speicher befindlichen Daten verloren gingen, die noch nicht auf einer Festplatte abgespeichert seien.

Das stimmt überein mit der Aussage des Zeugen [ ] bei seiner Vernehmung vor dem ererkennenden Gericht. Wie sich aus dieser Aussage ergibt, hat der Zeuge vor der Überprüfung der Anlage von dem Geschäftsführer der Beklagten erfahren, daß der Zeuge [ ] ein Virus gefunden hatte. Der Zeuge hat nach seiner Aussage das gesamte System noch einmal überprüft, und zwar mit einem Viren-Scanner der Marke Mc-Afee, der damals auf dem neuesten Stand gewesen sei, und dessen Programm das Virus Cascade B identifiziert habe. Dem steht die Aussage des Zeugen [ ] nicht entgegen. Der Zeuge [ ] der nach seiner eigenen Einschätzung kein Fachmann auf diesem Gebiet ist, hat mit einem Virensuchprogramm gearbeitet, das lediglich etwa 27 Virentypen erfaßt, also nur einen Bruchteil der tatsächlich existierenden Typen. Der Zeuge [ ] hat nicht ausschließen können, daß nach seinem Versuch, das Virus zu beseitigen, noch ein Virus vorhanden gewesen ist. Soweit der Zeuge [ ] ein Virus vom Typ Jerusalem entdeckt haben will, kann das mit seinem eingeschränkten Virensuchprogramm zusammenhängen, zumal das Virus Jerusalem nach den Angaben des Sachverständigen [ ] ähnliche Symptome aufweist wie das Virus Cascade B. Soweit der Zeuge [ ] ein Virus vom Typ Vanilla entdeckt haben will, das nach den Angaben des Sachverständigen [ ] in der internationalen Literatur unbekannt ist, handelt es sich möglicherweise um eine Verwechslung mit dem ähnlich klingenden Virus Vaesina, das nach den Angaben des Sachverständigen [ ] ebenfalls ähnliche Symptome ausweist wie das Virus Cascade B. Es ist nicht auszuschließen, daß der Zeuge [ ] bei seiner Vernehmung sich nicht an die richtige Bezeichnung erinnern konnte und eine ähnlich klingende Bezeichnung genannt hat.

Nach dem Ergebnis der im zweiten Rechtszug durchgeführten Beweisaufnahme muß davon ausgegangen werden, daß die EDV-Anlage der Beklagten bei der Untersuchung durch den Zeugen [ ] am 11.1.1991 und der Untersuchung durch den Zeugen [ ] in der Zeit vom 25.1. bis zum 6.3.1991 von dem Virus Cascade B befallen war.

Nach den zutreffenden Feststellungen des Sachverständigen Dipl. Ing. [ ] in seinem Gutachten vom 19.9.1993, die von den Parteien in der Verhandlung über das Ergebnis der Beweisaufnahme nicht angezweifelt worden sind, kann ein derartiges Virus Programmstörungen, z. B. ein Abstürzen der EDV-Anlage verursachen.

Zugang zu dem Netzwerk der EDV-Anlage der Beklagten hatte nur der Kläger. Mit den Passwörtern der Codeworttabelle, die der Kläger unstreitig am 27.8.1990 dem Mitarbeiter [ ] und am 10.9.1990 der Mitarbeiterin [ ] übergeben hat, bestand entgegen der Darstellung des Klägers nur Zugang zu den Anwendungsprogrammen, nicht zu dem Netzwerk der Anlage.

Wie sich aus den Erläuterungen des Sachverständigen [ ] in seinem Gutachten vom 19.9.1993 ergibt, erfordert ein Mehrplatzsystem oder Netzwerk bei einer EDV-Anlage einen Systemverwalter, der die zentralen Aufgaben in dem System (z. B. die Konfiguration des Netzwerks, das Einrichten von Benutzern, die Programmpflege usw.) wahrnimmt. Dieser Systemverwalter wird im Englischen, aber auch in der EDV-Umgangssprache meist Supervisor genannt. Der Supervisor, der Systemverwalter, hat in den verschiedenen Softwaresystemen unterschiedliche Benutzernamen. In der bei der Beklagten verwandten

Was tut Cascade B  
(= Herbstlaub)?

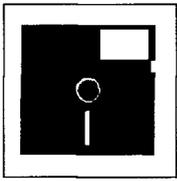
Vanilla oder Vaesina?

Ergebnis:  
Virenbefall mit Cascade B

Vom Virus bewirkt:  
Absturz

Alleinzugang des Beklagten  
zum Netzwerk

Die Rolle des Systemverwalters



*„Systemverwalter für  
Anwendungsprogramme“*

*COMMAND.COM und  
KEYB.COM*

*Die Bekundung der mit der  
Buchhaltung befaßten Zeugin*

*Die Bekundung des für das  
Bestell- und Rechnungswesen  
zuständigen Zeugen*

Netzwerk-Software netware der Firma [] hat der Benutzer, der die Funktion des Supervisors ausübt, auch den Benutzernamen „SV“. Der Supervisor ist der Benutzer mit den höchsten Rechten, der anderen Benutzern Rechte zuweisen oder wegnehmen kann. Viele Funktionen in dem Netzwerk lassen sich nur von dem Supervisor oder einem anderen Benutzer mit den gleichen Rechten ausführen.

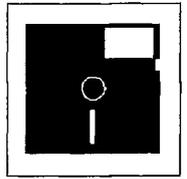
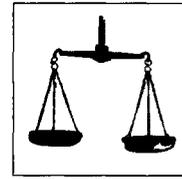
Auch in vielen Anwendungsprogrammen ist nach den Erläuterungen des Sachverständigen [] ein Systemverwalter vorgesehen, der das System betreut und Rechte innerhalb des Systems vergibt, wobei es auch hier nicht üblich ist, daß alle Benutzer die gleichen Rechte bezüglich einzelner Programme oder Dateien haben. Der Systemverwalter für ein Anwenderprogrammssystem wird im üblichen Sprachgebrauch ebenfalls oft Supervisor genannt. Vielfach hat der Systemverwalter in Anwendungsprogrammen keinen fest definierten Benutzernamen; vielmehr kann dieser bei der Installation des Programms frei gewählt werden.

Nach den Feststellungen in dem Abschlußbericht des Zeugen [] hat nur der Kläger über das Passwort für den Benutzercode „SV“ verfügt, womit das Recht eingeräumt sei, die Dateien COMMAND.COM und KEYB.COM auf dem Fileserver zu beschreiben bzw. zu verändern. Diese Feststellungen beruhen nach dem Abschlußbericht auf einer Überprüfung der Zugriffsrechte aller Benutzer und auf den eigenen Angaben des Klägers gegenüber dem Zeugen [].

Die Feststellungen in dem Abschlußbericht des Zeugen [] sind durch die Beweisaufnahme bestätigt worden.

Die Zeugin [], eine gelernte Rechtsanwaltsgehilfin, die seit Mai 1989 bei der Beklagten als kaufmännische Angestellte beschäftigt und für das Telefon, die Kundenbetreuung und Reklamationen zuständig ist, sich aber zur Zeit im Erziehungsurlaub befindet, hat bei ihrer Vernehmung vor dem erkennenden Gericht bekundet, als ihr der Kläger die Codeworttabelle am 10.9.1990 habe übergeben wollen, habe sie diese Tabelle zunächst nicht haben wollen, aus Angst, sie könne etwas zerstören. Der Kläger habe sie jedoch mit dem Hinweis beruhigt, daß sie mit diesen Codewörtern nicht in das Netzwerk gelangen könne. Mit dem Codewort „MMM“ habe sie in die Anwendersoftware der Anlage gelangen können. Der Kläger habe ihr damals erklärt, daß sie mit dem Codewort „EEE SSS“ in die Bereiche der Anlage gelangen könne, die sonst für sie gesperrt seien, z.B. in die Buchführung und den Tagesabschluß. Der Kläger habe ihr nicht gesagt, daß man mit dem Codewort „EEE SSS“ Netzwerkoperationen durchführen könne. Der Unterschied zwischen Netzwerkoperationen und dem Zugriff zu Anwenderprogrammen sei ihr bekannt. Bei Netzwerkoperationen könne man das Programm verändern; der Zugriff zur Buchhaltung sei eine Anwenderfrage. Als ihr der Kläger die eidesstattliche Erklärung vom 12.8.1992 vorgelegt habe, habe sie deshalb veranlaßt, daß die Wendung „... und damit vollen Zugang zum Netzwerk der Firma [] hatte. Ich konnte alle Netzwerkoperationen eigenständig durchführen“ gestrichen werden, weil ihr von dem Kläger seinerzeit gesagt worden sei, daß sie mit diesen Codewörtern nicht in das Netzwerk komme.

Die Aussage der Zeugin [] wird im wesentlichen bestätigt durch die Aussage des Zeugen []. Der Zeuge [], der seit etwa 5 Jahren als Bürokaufmann bei der Beklagten beschäftigt und für Kundenanfragen, Bestellwesen und kaufmännische Rechnungen zuständig ist, hat bekundet, er wisse nicht mehr, ob ihm der Kläger bei der Übergabe der Codeworttabelle am 27.8.1990 genau erklärt habe, warum er diese Codeworttabelle erhalte. Mit seinem Codewort „CCC-BBB“ gelange man lediglich in die Anwendersoftware mit Ausnahme der Finanzbuchhaltung. Er wisse nicht, was der Satz „Das Codewort AAA ist gleichbedeutend mit SV“ bedeuten solle. Im Nachhinein habe er gehört, er wisse nicht mehr, von wem, daß man mit diesem Codewort in das Betriebssystem gelangen könne. Er habe es jedoch nie ausprobiert. Als ihn der Kläger am 12.8.1992 wegen der eidesstattlichen Erklärung zu Hause aufgesucht habe, habe er ihm erklärt, es gehe lediglich um die Bestätigung, daß er – der Zeuge – die Codeworttabelle erhalten habe, was angezweifelt würde. Er habe noch gefragt, ob die Zeugin [] ebenfalls eine solche Erklärung unterschrieben habe, was ihm der Kläger bestätigt habe. Wenn ihm vorgehalten werde, daß die Zeugin [] in ihrer eidesstattlichen Erklärung etwas durchgestrichen habe, so möchte er bekunden, daß er damals nur habe bestätigen wollen, daß er die Codeworttabelle erhalten habe. Er habe von dem Kläger eine Durchschrift der eidesstattlichen Erklärung vom 12.8.1992 erhalten und beim Durchlesen wenige Tage später festgestellt, daß er einen Fehler gemacht habe. Er sei später von dem Geschäftsführer der Beklagten zu der von ihm abgegebenen eidesstattlichen Erklärung befragt worden.



Die Zeugin [], die als Vertriebsbeauftragte bei der Firma [] [] in Kaiserslautern beschäftigt ist, hat ausgesagt, sie sei seinerzeit von der Beklagten wegen einer Störung in der EDV-Anlage angerufen worden. Auf ihrem Weg von ihrem Wohnort bei Saarbrücken zur Zentrale in Kaiserslautern sei sie bei der Beklagten vorbeigefahren und habe zusammen mit einem Kollegen in Kaiserslautern, mit dem sie telefonisch verbunden gewesen sei, versucht, die Anlage wieder in Ordnung zu bringen. Ihr sei damals eine Codeworttabelle übergeben worden, sie wisse nicht mehr, ob von der Zeugin [] oder dem Zeugen [] []. Sie könne sich an diese Codeworttabelle nicht mehr genau erinnern. Wenn ihr die Codeworttabellen Blatt 67 und 68 der Akten vorgehalten würden, könne sie nicht mehr angeben, ob die ihr übergebene Codeworttabelle mit diesen Codeworttabellen identisch sei. An die Wörter „SSS“ und „GGG“ könne sie sich dunkel erinnern. Sie wisse noch, daß alle Wörter auf der ihr übergebenen Codeworttabelle unseriös, zum Schmunzeln gewesen seien. Mit den ihr übergebenen Codewörtern seien sie und ihr Kollege aus Kaiserslautern nicht in das Betriebssystem der Anlage gelangt. In der Anwendersoftware könne man nicht erkennen, warum eine Anlage abgestürzt ist. Auf ihre Fragen hätten ihr die Zeugen [] und [] seinerzeit bestätigt, daß sie nicht in das Betriebssystem hätten hineinkommen können. Ihrer Auffassung nach seien die beiden Zeugen als Anwender auch nicht in der Lage, in das Betriebssystem zu gelangen; das sei nicht so einfach. Sie habe vorher schon öfter mit den beiden Zeugen Anwendungsprobleme besprochen und habe dazu sehr genaue Erklärungen abgeben müssen. Sie habe seinerzeit dem Geschäftsführer der Beklagten, der sich an diesem Tag nicht im Betrieb aufgehalten habe, telefonisch erklärt, daß sie mit allen vorhandenen Codewörtern nicht in das Betriebssystem habe gelangen können.

Schließlich hat der Zeuge [] der Geschäftsführer der Firma [] aus [], der die EDV-Anlage der Beklagten unstreitig in der Zeit vom 25.1. bis zum 6.3.1991 überprüft hat, bei seiner Vernehmung vor dem erkennenden Gericht seine Aussage dahingehend gemacht, die Codeworttabellen Blatt 67 und 68 der Akten seien ihm seit jener Überprüfung Anfang 1991 bekannt. Mit den Codewörtern, die in diesen Tabellen aufgeführt seien, habe man nicht in das Netzwerk der Anlage der Beklagten gelangen können. Das gelte auch für die Wörter „AAA SSS“ und „EEE SSS“. Die aufgeführten Namen hätten einen unterschiedlichen Zugriff auf die Daten in der Anwendersoftware ermöglicht. Es gebe unterschiedliche Zugangsberechtigungen zu dem Netzwerksystem und dem Anwendersystem der Anlage. Der Kläger habe ihm gegenüber seinerzeit eingeräumt, daß er der einzige sei, der über das Passwort für das Netzwerksystem verfüge. Er habe dem Kläger deshalb damals Vorhaltungen gemacht.

Die Zeugen [] und [] haben weiter die Darstellung der Beklagten hinsichtlich des Vorfalles vom 13.3.1991 bestätigt.

Die Zeugin [] hat dazu bekundet, sie könne sich an ein Telefongespräch erinnern, das sie im Auftrag des Geschäftsführers der Beklagten mit dem Kläger geführt habe. Das Gespräch habe etwa zur Zeit der Entlassung des Klägers stattgefunden, jedenfalls noch vor dem Betriebsausflug am 15.3.1991. Sie habe das Passwort für das Betriebssystem von dem Kläger erfahren wollen, da der Geschäftsführer der Beklagten das Passwort für den Zeugen [] gebraucht habe. Der Kläger habe sich ihr gegenüber geweigert, das Wort mitzuteilen, mit der Begründung, ihr gebe er das Passwort schon gar nicht an, weil sonst die Gefahr bestehe, daß jemand mit dem Passwort etwas anstellen könne und er wieder daran Schuld sei. Der Kläger habe nicht eingewandt, daß sie das Passwort doch bereits habe, da er es ihr mit der Codeworttabelle übergeben habe. Sie habe den Kläger dann mit dem Geschäftsführer der Beklagten verbunden. Dieser habe ihr kurz danach mitgeteilt, er habe jetzt das Passwort. An das Wort selbst könne sie sich nicht erinnern.

Der Zeuge [] hat dazu ausgesagt, er könne sich an das fragliche Gespräch genau erinnern. Er habe das Passwort gebraucht, um in das System zu gelangen. Er habe beide Gespräche auf seiten der Zeugin [] bzw. des Geschäftsführers der Beklagten verfolgen können, allerdings ohne zu hören, was der Kläger jeweils gesagt habe. Der Geschäftsführer der Beklagten sei bei dem Gespräch laut geworden. Er habe offenbar das Passwort von dem Kläger erfahren, das seiner Erinnerung nach „BBB“ gelautet habe. Mit diesem Passwort habe er die volle Zugangsberechtigung zu dem ganzen Netzwerksystem gehabt.

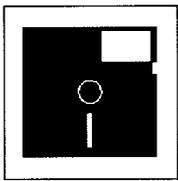
Die Aussagen der Zeugen, mit gewissen Einschränkungen auch die Aussage des Zeugen [], sind glaubhaft. Die Aussagen sind in sich schlüssig. Sie widersprechen sich nicht. Sie stimmen mit dem unstreitigen Tatbestand und mit den Feststellungen des Sachverständigen [] überein.

*„daß alle Wörter auf der ihr übergebenen Codeworttabelle unseriös, zum Schmunzeln gewesen seien ...“*

*Ergebnisse der Systemüberprüfung*

*Ein Telefongespräch mit dem Kläger in Sachen Paßworte*

*Würdigung der Zeugenaussagen*



*Prüfung auf: Interessenlage und  
Widerspruchsfreiheit*

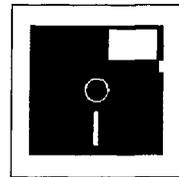
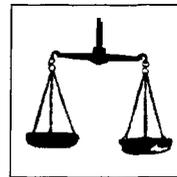
Die Tatsache allein, daß die Zeugin [], bei der Beklagten beschäftigt ist, spricht noch nicht gegen ihre Glaubwürdigkeit. Das muß um so mehr gelten, als sich die Zeugin zur Zeit im Erziehungsurlaub befindet und noch nicht einmal feststeht, ob sie das Arbeitsverhältnis mit der Beklagten fortsetzt. Das Aussageverhalten der Zeugin war sehr sicher und überzeugend. Die Zeugin war in ihren Antworten völlig offen. Sie ist keiner Frage ausgewichen. Für die Richtigkeit ihrer Aussage spricht insbesondere der Umstand, daß sie sich bei der Entgegennahme der Codeworttabelle am 10.9.1990 bei dem Kläger vergewissert hat, daß sie mit den darin aufgeführten Passwörtern, und zwar auch mit dem Passwort „EEE SSS“ nicht in das Netzwerk, sondern lediglich in die ihr normalerweise gesperrten Anwendungsprogramme gelangen kann. Konsequenterweise hat die Zeugin auch bei der Vorlage der eidesstattlichen Erklärung vom 12.8.1992 durch den Kläger veranlaßt, daß die entsprechenden Streichungen vorgenommen werden. Diese eidesstattliche Erklärung ist von dem Kläger mit den Streichungen in dem vorliegenden Rechtsstreit vorgelegt worden. Es trifft zwar zu, daß die Zeugin in dieser eidesstattlichen Erklärung auch erklärt hat, sie habe eine mehrseitige deutsche Anleitung zur Fehlerbeseitigung innerhalb des Netzwerks erhalten. Das hat die Zeugin bei ihrer Aussage auch bestätigt. Der Kläger hat nach dem Beweisaufnahmetermin vom 10.3.1993 mit Schriftsatz vom 9.8.1993 Fotokopien „Handbuch für Operator Fa. [] Stand 3.7.1990“ vorgelegt, bei denen es sich um diese Fehlerbeseitigungsanweisung handeln soll. Dazu hat der Sachverständige Z. in seinem Gutachten von 19.9.1993 ausgeführt, die übergebene Fehlerbeseitigungsanweisung enthalte nur solche Vorgänge, die jeder Benutzer ausführen könne, ohne daß es dazu der besonderen Rechte des Supervisors bedürfe. Dort wo spezielle Kenntnisse oder Berechtigungen erforderlich seien, werde in diesem Dokument ausdrücklich darauf verwiesen, daß ein spezieller Mitarbeiter bei der Firma [] für die Fehlerbeseitigung anzurufen sei. Aus der Kenntnis dieser Fehlerbeseitigungsanweisung könnten daher keine Rückschlüsse auf spezielle Zugangsberechtigungen hergeleitet werden. Diesen überzeugenden Feststellungen des Sachverständigen ist der Kläger nicht mehr entgegengetreten. Widersprüche in der Aussage der Zeugin [] sind somit nicht ersichtlich.

*Prüfung auf:  
Erinnerungsgenauigkeit*

Auch bei der Zeugin [] ist kein eigenes Interesse am Ausgang des Rechtsstreits erkennbar. Die Tatsache, daß sie als Vertriebsbeauftragte bei der Firma [] aus [] beschäftigt ist, welche die Software in der EDV-Anlage der Beklagten zumindest teilweise entwickelt hat, also mit der Beklagten in Geschäftsverbindung steht, spricht nicht gegen ihre Glaubwürdigkeit. Die Zeugin erschien in ihrem Aussageverhalten völlig unvoreingenommen. Sie hat sofort eingeräumt, daß sie sich an die ihr übergebene Codeworttabelle nicht mehr genau erinnern könne. Andererseits erscheint es durchaus glaubhaft, daß der Zeugin noch in Erinnerung war, daß alle Wörter unseriös, also irgendwie zum Schmunzeln gewesen waren. Das trifft aber auf die in den Codeworttabellen vom 27.8.1990 bzw. 10.9.1990 aufgeführten Codewörter wie „SSS“, „GGG“, „YYY“ und „BBB“ durchaus zu. An derartig auffallende Wörter erinnert man sich erfahrungsgemäß leichter. Der Umstand, daß die Zeugin ausgesagt hat, ihrer Erinnerung nach handele es sich um einen kleinen handgeschriebenen Zettel, fällt demgegenüber weniger ins Gewicht. Die der Zeugin [] am 10.9.1990 übergebene Codeworttabelle ist jedenfalls von Hand geschrieben. An die Wörter „SSS“ und „GGG“ konnte sich die Zeugin jedenfalls dunkel erinnern. Das Format des handgeschriebenen Zettels fällt demgegenüber weniger ins Gewicht.

*Das Verhalten des Klägers  
gegenüber den Zeugen*

Es trifft zu, daß der Zeuge [] bei seiner Vernehmung vor dem erkennenden Gericht einen sehr unsicheren Eindruck gemacht hat. Der Zeuge hat sich in Widersprüche verstrickt. Ihm mußten wiederholt Vorhaltungen gemacht werden. Dieses Aussageverhalten hängt möglicherweise damit zusammen, daß der Zeuge am 12.8.1992 die ihm von dem Kläger zu Hause vorgelegte eidesstattliche Erklärung unterschrieben hat, ohne – wie die Zeugin [] – bestimmte Wendungen durchzustreichen. Der Zeuge hat unter dem 30.11.1992 offensichtlich auf Veranlassung der Beklagten eine von der Beklagten vorgelegte Anmerkung zu seiner eidesstattlichen Erklärung vom 12.8.1992 abgegeben, in der er diese eidesstattliche Erklärung praktisch widerrufen hat. Dadurch hat der Zeuge naturgemäß unter einem gewissen Druck gestanden. Der Zeuge hat auch nach wiederholtem Vorhalt eingeräumt, daß er von dem Geschäftsführer der Beklagten zu der von ihm abgegebenen eidesstattlichen Erklärung „be-fragt“ worden sei. Zu Gunsten des Klägers kann durchaus davon ausgegangen werden, daß dem Zeugen dabei Vorwürfe gemacht worden sind. Andererseits ist zu bedenken, daß der Zeuge offensichtlich geistig wenig beweglich erscheint und Schwierigkeiten hatte, den Fragen intellektuell zu folgen. Dem Zeugen war nur mit Mühe zu vermitteln, daß in der eidesstattlichen Erklärung der Zeugin [], die dem Zeugen vorgehalten wurde, zwei Sätze gestrichen waren. Der Zeuge hat dazu bekundet, daß ihm das seinerzeit nicht aufgefallen sei, er



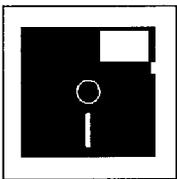
es aber gemerkt hätte, wenn dort etwas durchgestrichen gewesen wäre. Das könnte aber nur zutreffend sein, wenn der Kläger dem Zeugen die Erklärung der Zeugin [] ohne diese Streichungen vorgelegt hätte, was von keiner Seite behauptet worden ist. Der Zeuge ist offensichtlich von dem Kläger mit der eidesstattlichen Erklärung vom 12.8.1992 überrumpelt worden unter dem Vorwand, es gehe lediglich um die Bestätigung, daß er die Codeworttabelle erhalten hätte. Den Empfang dieser Codeworttabellen hatten die Zeugen [] und [] aber bereits am 27.8.1990 bzw. am 10.9.1990 unterschriftlich bestätigt. Wie sich aus der Aussage des Zeugen [] ergibt, waren diesem Zeugen die Codeworttabellen zumindest seit Anfang 1991 bekannt. Die Parteien haben in dem Kammertermin vom 2.8.1991 vor dem Arbeitsgericht unstreitig gestellt, daß dem Geschäftsführer der Beklagten das Übergabeprotokoll vom 27.8.1990 an den Mitarbeiter [] vor Ausspruch der Kündigung bekannt gewesen ist. Für den Kläger bestand also keinerlei Veranlassung, sich den Erhalt der Codeworttabelle am 12.8.1992, also nach der Verkündung des Urteils des Arbeitsgerichts vom 28.7.1992, noch einmal bestätigen zu lassen. In Wirklichkeit ist es dem Kläger natürlich um die Bestätigung gegangen, daß man mit den Codewörtern in das Netzwerk gelangen konnte. Bei dem Zeugen [] hatte er damit Erfolg, bei der Zeugin [] nicht. Dabei ist bemerkenswert, daß der Kläger die Streichungen in der vorformulierten Erklärung durch die Zeugin [] hingenommen hat. So wie sich der Zeuge bei seiner Vernehmung dargestellt hat, erscheint es jedenfalls als glaubhaft, daß der Zeuge nie ausprobiert hat, mit einem Codewort der ihm übergebenen Codeworttabelle in das Netzwerk der EDV-Anlage der Beklagten zu gelangen, weil er dazu auch gar nicht in der Lage wäre. Das entspricht auch der Einschätzung des Zeugen [] durch die Zeugin [] nach mehreren Besprechungen. Es erscheint auch als glaubhaft, wenn der Zeuge bekundet hat, er wisse nicht, was der Satz *„Das Codewort AAA ist gleichbedeutend mit SV.“* in der ihm übergebenen Codeworttabelle bedeuten solle. Nach den Feststellungen des Sachverständigen [] handelt es sich nämlich bei *„AAA“* offensichtlich nicht um ein Codewort, sondern um einen Benutzernamen.

Auch wenn man ein gewisses eigenes Interesse des Zeugen [] am Ausgang des Rechtsstreits nicht völlig ausschließen kann, weil der Zeuge in seinem Abschlußbericht einen Verdacht gegen den Kläger ausgesprochen hat und daher möglicherweise sich zu rechtfertigen versucht, erscheint seine Aussage doch als glaubhaft. Es gibt keine Anhaltspunkte dafür, daß der Zeuge [] von der Beklagten den Auftrag hatte, den Kläger zu überführen, nachdem der Zeuge [] von der Firma [] den Virusbefall festgestellt hatte. Gegen eine derartige Annahme spricht gerade der Umstand, daß der Zeuge [] in seinem Abschlußbericht Vorschläge für eine Verbesserung der Anlage unterbreitet hat, zu deren Realisierung naturgemäß auch sein eigenes Unternehmen in Betracht gekommen wäre. Andererseits wäre bei einer Realisierung dieser Vorschläge die Position eines EDV-Leiters und Organisationssachbearbeiters nicht unbedingt entfallen, da nach den Ausführungen des Sachverständigen [] eine EDV-Anlage mit einem Mehrplatzsystem einen Systemverwalter braucht. Hinsichtlich des gefundenen Virus ist die Aussage des Zeugen [] jedenfalls durch die Bekundung des Zeugen [] bestätigt worden. Auch in seiner übrigen Aussage finden sich keine Widersprüche. Das gilt auch für seine Bekundung hinsichtlich des sogenannten Aktivitäts-Log. Der Zeuge hat ausgesagt, bei dem System der Firma [] gebe es kein sogenanntes Aktivitäts-Log, mit dem man alle Aktivitäten der Anlage durch einen Ausdruck erfassen könne. Dieser Teil der Aussage wird bestätigt durch das Gutachten des Sachverständigen [] wonach die bei der Beklagten verwandte Netzwerksoftware lediglich über ein Abrechnungssystem (Accounting-System) verfügt, das aber lediglich gewisse auswählbare Aktionen wie das sogenannte Login und das sogenannte Logout protokolliert, nicht jedoch, welche Dateien geöffnet oder verändert werden.

Entscheidend für die Richtigkeit der Zeugenaussagen spricht das Gutachten des Sachverständigen []. Danach handelt es sich bei den von dem Kläger den Zeugen [] und [] am 27.8. bzw. 10.9.1990 übergebenen Codeworttabellen eindeutig um die Codewörter oder Passwörter für die Benutzer der Anwendungssoftware. Auf der linken Seite dieser Tabellen steht jeweils ein Name, auf der rechten Seite ein Passwort. In der Codeworttabelle für die Zeugin [] sind die beiden Rubriken auch ausdrücklich unter den Bezeichnungen *„Name“* und *„Passwort“* aufgeführt. Der Satz in der Codeworttabelle für den Zeugen [] *„Das Codewort AAA ist gleichbedeutend mit SV“* kann nach den Feststellungen des Sachverständigen [] nur so verstanden werden, daß AAA der Name des Systemverwalters oder Supervisors der Anwendungssoftware ist. Das dazugehörige Passwort lautet *„SSS“*. AAA ist nicht etwa ein Passwort, sondern eindeutig ein Benutzername, der in beiden Tabellen in der linken Spalte steht, während SSS in der selben Zeile auf der rechten Spalte aufgeführt ist. Bei den Passwörtern auf der jeweils rechten Spalte der beiden Tabellen handelt es sich um Passwörter.

*Abschlußbericht und  
Eigeninteresse des Berichtenden*

*Das entscheidende  
Sachverständigen Gutachten und  
die Codeworttabellen*



*Kritisch betrachtet:  
Der Vortrag des Klägers zur  
Paßwortentwicklung*

ter für die Anwendungssoftware, nicht für das Netzwerk der EDV-Anlage der Beklagten. Ein deutlicher Hinweis dafür ist für den Sachverständigen, daß der Benutzername „SV.“ in der Tabelle nicht auftaucht. In der von der Beklagten verwandten Netzwerksoftware der Firma Novell hat aber der Benutzer, der die Funktion des Supervisors ausübt, auch den Benutzernamen „SV“. Auch das Passwort für den Netzwerk-Supervisor „XXX“ bzw. „YYY“ taucht in den beiden Tabellen nicht auf.

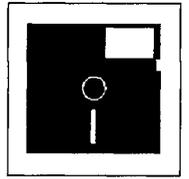
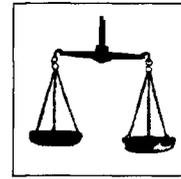
Der Kläger hat zwar nachträglich behauptet, das Passwort für das Netzwerk der EDV-Anlage der Beklagten sei später geändert worden, setzt sich damit aber mit seinem bisherigen prozessualen Verhalten in beiden Instanzen in Widerspruch. Zwischen den Parteien war immer unstrittig, daß das Passwort für den Netzwerk-Supervisor „RRR“ bzw. „BBB“ gelautet hat. Das ist von der Beklagten während des ganzen Rechtsstreits so vorgetragen worden, ohne daß es von dem Kläger bestritten worden wäre. Bereits in dem Abschlußbericht des Zeugen [], auf den sich die Beklagte bezogen hat, war ausgeführt worden, ein Mitarbeiter einer Firma [] sei zwar im Sommer 1990 bereits einmal im Besitz des damals gültigen Passworts gewesen, dieses Passwort sei jedoch danach geändert worden, nur der Kläger selbst kenne und benutze dieses Passwort. In den Schriftsätzen vom ... (folgt Aufzählung, red.) hat die Beklagte immer wieder vorgetragen, daß das Passwort für den Supervisor des Netzwerks „RRR“ bzw. „BBB“ gelautet habe, ohne daß der Kläger dem substantiiert entgegengetreten wäre. In der Berufungsbegründung vom 23.11.1992 und im Schriftsatz vom 19.2.1993 hat der Kläger lediglich die Frage aufgeworfen, wieso der Sachverständige [] bei dem Ortstermin am 10.2.1992, also fast 1 Jahr nach der streitbefangenen Kündigung, keine Übereinstimmung zwischen den Eintragungen der Codetabelle in der Maschine und den Übergabeprotokollen habe feststellen können. In diesem letzten Schriftsatz hat der Kläger die Behauptung aufgestellt, SSS sei ein weiterer Benutzername für den Mitarbeiter [], wobei das dazugehörige Passwort „AAA“ laute, mit dem es dem Zeugen [] möglich gewesen sei, alle Bedürfnisse des Netzwerks zu bearbeiten. Im Termin zur Beweisaufnahme vor dem erkennenden Gericht am 10.3.1993, in welchem u. a. über den Vorfall vom 13.3.1991 Beweis erhoben worden ist durch Vernehmung der Zeugen [] und [] hat der anwesende Kläger bei der Vernehmung dieser Zeugen nicht den Vorhalt gemacht, daß das Passwort für den Netzwerk-Supervisor geändert worden sei. Auch in der anschließenden Verhandlung über das Ergebnis der Beweisaufnahme hat der Kläger nicht darauf hingewiesen. In seinen zusätzlichen Beweisanträgen durch Einholung eines Sachverständigengutachtens ist diese Behauptung nicht enthalten. Es trifft zwar zu, daß die in der Anlage der Beklagten verwandte Netzwerksoftware netware ELS II 2.12, die der Zeuge [] unstrittig vorgefunden hat, als er mit der Überprüfung der Anlage begonnen hat, noch während der bis zum 6.3.1991 dauernden Untersuchung durch den Zeugen [] auf den neuesten Stand gebracht worden ist, indem die Version 2.15 installiert worden ist (vgl. den Bericht des Zeugen []), eine Version, die der Sachverständige [] offensichtlich noch bei seinem Ortstermin am 10.2.1992 vorgefunden hat (vgl. dessen Gutachten). Das bedeutet jedoch nicht, daß auch das Passwort für den Supervisor des Netzwerks geändert worden wäre. Es muß vielmehr als eine reine Schutzbehauptung des Klägers angesehen werden, wenn er vorträgt, daß das Passwort für das Netzwerk der Anlage, das er in dem Telefongespräch am 13.3.1993 nicht der Zeugin [] [], sondern nur dem Geschäftsführer der Beklagten mitgeteilt hat, das Passwort für die geänderte Netzwerksoftware darstellt, während die Supervisorrechte in dem Netzwerk in der vorherigen Netzwerksoftware dem Kläger selbst und den Benutzern AAA und EEE zugestanden hätten. Denn der Kläger hat nicht angegeben, wie das Passwort für den Netzwerksupervisor in der früheren Version der Netzwerksoftware gelautet haben soll. AAA und EEE sind Benutzernamen. Der Benutzername in der Netzwerksoftware netware der Firma [] ist als „SV“ festgelegt, taucht aber – wie bereits ausgeführt – in den Codeworttabellen für die Zeugen [] und [] nicht auf.

*Ergebnis hinsichtlich des  
Supervisor-Paßworts*

Nach dem Ergebnis der Beweisaufnahme muß demnach mit dem Sachverständigen [] davon ausgegangen werden, daß es sich bei den Passwörtern „SSS“ und „GGG“ in den Codeworttabellen, die der Kläger unstrittig am 27.8.1990 bzw. 10.9.1990 den Zeugen [] und [] übergeben hat, um Passwörter für die Benutzer der Anwendungsprogramme handelt. Mit diesen Passwörtern war es den Zeugen [] und [] nicht möglich, die Funktion eines Supervisors auszuüben. Dafür war ein besonderes Passwort erforderlich: das Passwort für den Netzwerk-Supervisor.

*Virusinfektion und  
Benutzerrechte*

Nach den Feststellungen des Sachverständigen [] kann ein Programm grundsätzlich nur dann von einem Virus infiziert werden, wenn der Benutzer, welcher ein infiziertes Programm benutzt, auch das Schreibrecht für die „zu infizierende“ Datei hat. Das Schreibrecht, die Zugangsberechtigung „W“ (Abkürzung für Write, englisch = schreiben), für die



Systemdateien COMMAND.COM und KEYB.COM auf dem Fileserver der EDV-Anlage der Beklagten, auf denen der Zeuge [ ] nach seinem Abschlußbericht und nach seiner glaubhaften Aussage vor dem erkennenden Gericht das Virus Cascade B gefunden hat, hat nach den Feststellungen des Sachverständigen [ ] [ ] nur der Benutzer "SV", also der Netzwerksupervisor, bzw. ein Benutzer mit Supervisor-Rechten. Mit den Passwörtern "SSS" und "GGG" war dagegen kein Benutzer der EDV-Anlage der Beklagten in der Lage, im Netzwerk die Funktionen eines Supervisors auszuüben oder Programme zu verändern.

Das entspricht offensichtlich auch der Auffassung des Klägers, wenn der Kläger darauf abstellt, daß alle Mitarbeiter der Beklagten in Betracht kämen, die über die Rechte eines "Supervisors" verfügten, also der Kläger selbst sowie die Zeugen [ ] und [ ]. Für diese Einschätzung des Klägers spricht auch die vorformulierte eidesstattliche Erklärung vom 12.8.1992, die er den Zeugen [ ] und [ ] zur Unterschrift vorgelegt hat. Wie bereits ausgeführt, hatten aber die Zeugen [ ] und [ ] nicht die Rechte des Netzwerksupervisors.

Das erkennende Gericht ist auch der Frage nachgegangen, ob das Virus unbeabsichtigt durch die Benutzung einer mit dem Virus befallenen Diskette auf einer Workstation Dateien auf dem Fileserver infizieren kann oder ob dieser Infektionsweg durch ein besonderes Sicherheitssystem der bei der Beklagten verwandten Netzwerksoftware der Firma [ ] ausgeschlossen ist.

Der Sachverständige [ ] der zur Vorbereitung Auskünfte von der Firma [ ], der Herstellerin der bei der Beklagten verwandten Netzwerksoftware netware, eingeholt hat, hat sein Gutachten dahingehend erstattet, daß ein Programm zwar grundsätzlich nur dann von einem Virus infiziert werden könne, wenn der Benutzer, der ein infiziertes Programm benutzt, auch das Schreibrecht für die "zu infizierende" Datei hat. Es könne jedoch nicht mit Sicherheit ausgeschlossen werden, daß ein Virus, das über eine Diskette in eine Workstation eingeschleust worden sei, unbeabsichtigt auch Dateien auf dem Fileserver wie die Systemdateien COMMAND.COM und KEYB.COM infiziert, für die nur der Netzwerksupervisor bzw. ein Benutzer mit Supervisorrechten Schreibrechte habe. In den von der Firma [ ] übersandten Berichten werde beschrieben, wie ein Virus über eine Diskette, die in einer Arbeitsstation unbeabsichtigt eingelesen werde, in eine Systemdatei im Fileserver gelangen könne. Verkürzt wiedergegeben sei folgender Ablauf möglich: In der Arbeitsstation werde eine verseuchte Diskette eingelesen. Diese infiziere Programme auf der Arbeitsstation. Nach Ausführung eines Programms, zu welchem alle Benutzer Zugriff hätten, würden weitere Programme infiziert. Wenn sich nun der Benutzer "Supervisor" in das System einbuche (Login), könne das Virus unbeabsichtigt Dateien infizieren, zu denen nur der Supervisor Schreibrechte habe. Das Einloggen des Supervisors könne z.B. erfolgen, um Systemarbeiten durchzuführen, aber auch speziell, um die von dem noch nicht erkannten Virus verursachten Störungen zu überprüfen. Bei dem Sicherheitssystem der Netzwerksoftware komme es darauf an, wie dessen Möglichkeiten im konkreten Fall eingesetzt würden. Auch der beschriebene mögliche Infektionsweg könne verhindert oder zumindest weiter erschwert werden, indem die besonders zu schützenden Dateien mit dem Attribut "Read Only" (nur lesen) versehen würden. Im Streitfall lasse sich heute nicht mehr mit Sicherheit rekonstruieren, welche Zugriffsrechte zu welchen Verzeichnissen oder Dateien für welche Benutzer bestanden und welche Attribute die einzelnen Dateien gehabt hätten. Daher könne nicht mit Sicherheit ausgeschlossen werden, daß auch Dateien, zu denen nur der Netzwerksupervisor das Schreibrecht gehabt habe, unbeabsichtigt von einem Virus infiziert worden sei, welches ebenfalls unbeabsichtigt über eine Diskette in eine Workstation gelangt sei.

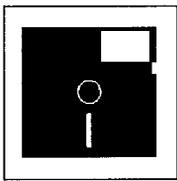
Damit ist der gegen den Kläger bestehende Verdacht nicht ausgeräumt. Die EDV-Anlage der Beklagten ist unstreitig von dem Kläger aufgebaut und erweitert worden. Unstreitig sind die Systemdateien COMMAND.COM und KEYB.COM auf dem Fileserver der Anlage befallen gewesen. Der Kläger hat nicht dargelegt, welche Sicherheitsattribute er als EDV-Leiter diesen Systemdateien verliehen hat. Die abstrakt bestehende Infektionsmöglichkeit ist daher nicht geeignet, den gegen den Kläger bestehenden Verdacht auszuräumen. Dieser Verdacht hat bereits bei Zugang der außerordentlichen Kündigung der Beklagten vom 14.3.1991 bestanden. Das von dem Kläger aufgebaute und später erweiterte EDV-System der Beklagten war immer wieder zusammengebrochen. Das von der Beklagten beauftragte Softwareunternehmen, die Firma [ ] aus [ ] war nicht in der Lage, den Fehler zu beseitigen. Aus diesem Grund war der Kläger nach seinem Ausscheiden zum 30.9.1990 fast täglich in den Betrieb der Beklagten gerufen worden, um die Anlage wieder in Gang zu bringen. Das ist dem Kläger offensichtlich immer wieder in kürzester Zeit gelungen. Der Zeuge [ ] von der Firma [ ] aus [ ] hat bei seiner Überprüfung der Anlage am 11.1.1991 keine

*Frage:  
Infektion von einer Workstation aus?*

*Antwort:  
Möglicherweise ja.*

*Trotzdem:  
Verdacht nicht ausgeräumt.*

*Verdacht bereits im Zeitpunkt der außerordentlichen Kündigung*



Mängel in der Hardware, also an den eingesetzten Computern, Servern und ihrer Verbindung, festgestellt, hat aber entdeckt, daß die Anlage von einem Virus befallen war. Der Zeuge □ selbst scheidet als Täter offensichtlich aus, da der Zeuge nach der eigenen Darstellung des Klägers das Virus im Beisein des Klägers entdeckt hat. Das war zu einem Zeitpunkt, bevor der Zeuge □ die Anlage in der Zeit vom 25.1. bis zum 6.3.1991 überprüft hat, so daß auch der Zeuge □ nicht in Betracht kommt, auf den der Kläger zunächst den Verdacht zu lenken versucht hat. Auch wenn das Virus erstmals am 11.1.1991 entdeckt worden ist, so ist damit nicht gesagt, wann das Virus implantiert worden ist. Das kann vor dem Ausscheiden des Klägers zum 30.9.1990 gewesen sein, aber auch danach. Denn auch nach dem 30.9.1990 hat sich der Kläger fast täglich im Betrieb der Beklagten aufgehalten. Ein derartiges Virus kann zu Programmstörungen, insbesondere zu sogenannten Programmabstürzen führen. Um ein Virus auf Systemdateien des Fileservers wie den von dem Virus befallenden Dateien COMMAND.COM und KEYB.COM zu □ implantieren, braucht man grundsätzlich das Passwort des Netzwerksupervisors, über das alleine der Kläger verfügt hat. Das hat der Kläger gegenüber dem Zeugen □ auch eingeräumt. Mit den Passwörtern der Codeworttabellen, die der Kläger unstreitig vor seinem Ausscheiden zum 30.9.1990 den Zeugen □ und □ übergeben hatte und die dem Zeugen □ bei seiner Überprüfung bekannt waren, gelangt man dagegen nicht in das Netzwerk der EDV-Anlage, so daß auch die Zeugen □ und □ jedenfalls für eine bewußte Implantierung des Virus ausscheiden. Es kann zwar nicht völlig ausgeschlossen werden, daß ein Virus unbeabsichtigt über eine verseuchte Diskette auf einer Arbeitsstation Dateien des Netzwerks befällt, für die nur der Netzwerksupervisor Schreibrechte hat. Durch Sicherheitsvorkehrungen des □ Sicherheitssystems kann dieser Infektionsweg aber zumindest bis zu einem gewissen Grad verhindert werden. Der gegen den Kläger bestehende Verdacht, den der Zeuge □ in seinem Abschlußbericht im einzelnen aufgezeigt hat, ist durch den Vorfall bei dem Telefonat am 13.3.1991 noch verstärkt worden. Die Interessenlage des Klägers spricht nicht gegen den dringenden Verdacht. Es trifft zwar zu, daß die Parteien am 17.12.1990 einen neuen Anstellungsvertrag geschlossen haben, nachdem das Arbeitsverhältnis zunächst zum 30.9.1990 aufgelöst worden war, und daß dieser neue Arbeitsvertrag dem Kläger günstige Arbeitsbedingungen, insbesondere eine nach seiner eigenen Einschätzung gute Vergütung und eine lange Vertragsdauer ohne Probezeit mit vorteilhafter Kündigungsregelung gebracht hat. Diese Vertragsgestaltung bestätigt aber gerade den gegen den Kläger bestehenden Verdacht. Geht man davon aus, daß das Virus bereits vor Vertragsschluß implantiert worden ist, wofür alle Indizien sprechen, so konnte der Kläger kein Interesse daran haben, daß die Programmstörungen plötzlich mit dem Vertragsschluß aufhören, ohne daß die Konfiguration der Anlage verändert worden wäre.

*Entlastungsbeweise erhoben*

Der demnach gegen den Kläger zum Zeitpunkt des Zugangs der Kündigung vom 14.3.1991 bestehende dringende Verdacht konnte auch während des Kündigungsrechtsstreits durch Entlastungsbeweise, denen das Gericht nachgegangen ist, nicht entkräftet werden.

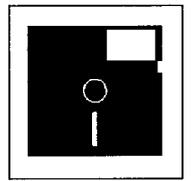
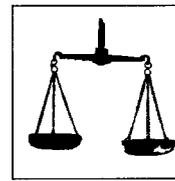
3. Die Beklagte hat vor Ausspruch der Kündigung alle zumutbaren Anstrengungen zur Aufklärung des Sachverhalts unternommen.

*Ausreichende  
Aufklärungsbemühungen der  
Beklagten*

Nachdem das EDV-System der Beklagten immer wieder zusammengebrochen war und der Zeuge □ am 11.1.1991 erstmalig den Virusbefall entdeckt hatte, hat die Beklagte die gesamte Anlage und den organisatorischen Ablauf durch die Firma □ □ aus □ in der Zeit vom 25.1.1991 bis zum 6.3.1991 überprüfen lassen, die darüber einen Abschlußbericht gefertigt hat. Im Laufe dieser Überprüfung hat der Kläger bereits gegenüber dem Zeugen □ von der Firma □ zugegeben, daß er allein über das Passwort des Netzwerksupervisors verfügt. Das ist durch das Telefonat vom 13.3.1991 bestätigt worden. Die Codeworttabellen, die der Kläger am 27.8.1990 bzw. am 10.9.1990 den Zeugen □ und □ übergeben hatte, haben dem Zeugen □ bei dieser Überprüfung vorgelegen, wobei nach den Feststellungen des Zeugen mit den darin enthaltenen Passwörtern ein Zugang zu dem Netzwerk der EDV-Anlage nicht möglich gewesen ist. Der Geschäftsführer der Beklagten hat vor Ausspruch der Kündigung die Zeugen □ und □ befragt, was die Zeugen bei ihrer Vernehmung bestätigt haben. Nach ihrer Aussage sind die Zeugen insbesondere danach gefragt worden, ob sie Disketten, z. B. Spieldisketten, in das Unternehmen der Beklagten gebracht hätten, was die Zeugen verneint haben.

*Kein Aktivitätslog vorhanden*

Die Behauptung des Klägers, die in der EDV-Anlage der Beklagten verwandte Netzwerksoftware der Firma □ verfüge über eine Art „Black Box“, vergleichbar einem Flugschreiber, mit der man alle Aktivitäten der Anlage durch einen Ausdruck hätte erfassen können, so



daß man den Hergang des Virusbefalls hätte herausfinden können, ist durch die Beweisaufnahme eindeutig widerlegt worden. Der Sachverständige [ ] hat in seinem Gutachten dazu ausgeführt, die Netzwerksoftware verfüge nicht über ein Aktivitäts-Log, mit dem alle Aktivitäten der Anlage erfaßt und ausgedruckt werden könnten. Vielmehr bestehe nur die Möglichkeit, ein Accountingsystem (Abrechnungssystem) laufen zu lassen, dessen Log-Datei beim Einschalten durch den Supervisor gewisse anwählbare Aktionen wie das Login und das Logout, die benutzte Speicherkapazität und die Anzahl der Lese-/Schreibzugriffe automatisch protokolliert. Dieses System protokolliert jedoch nicht, welche Dateien geöffnet oder verändert worden sind und auch nicht, wer, wann und was an den Zugriffsrechten geändert hat. Aus diesem Grund reichen die Angaben des Accountingsystem nach den Feststellungen des Sachverständigen nicht aus, um eine erfolgte Virusinfektion identifizieren zu können. Diesen in sich schlüssigen, zutreffenden Feststellungen des Sachverständigen ist der Kläger nicht mehr entgegengetreten.

4. Der Kläger ist auch vor Ausspruch der außerordentlichen Kündigung zu den gegen ihn erhobenen Vorwürfen ordnungsgemäß gehört worden.

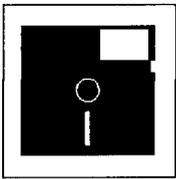
*Anhörung des Klägers*

Nach seiner eigenen Einlassung ist der Kläger bereits am 9.3.1991 zu dem Geschäftsführer der Beklagten gerufen worden, der ihm aus dem Abschlußbericht des Zeugen [ ] auszugsweise vorgelesen habe. Zu diesem Zeitpunkt war dem Kläger bereits bekannt, daß der Zeuge [ ] am 11.1.1991 im Beisein des Klägers den Virusbefall entdeckt hatte. Dem Kläger war weiter bekannt, daß ihm der Zeuge [ ] Vorhaltungen gemacht hatte, weil der Kläger alleine über das Passwort des Netzwerksupervisors verfügt hat. Die Vorwürfe in dem Abschlußbericht des Zeugen [ ] können den Kläger daher nicht unvorbereitet getroffen haben. Bei den schriftlichen Beweisen, auf die der Kläger nach seiner Darstellung bei der Unterredung am 9.3.1991 hingewiesen hat und die den Vorwurf widerlegen sollen, kann es sich nur um die Übergabeprotokolle mit dem Codeworttabellen gehandelt haben, die der Kläger unstreitig am 27.8.1990 und am 10.9.1990 den Zeugen [ ] und [ ] übergeben hat. Andere schriftliche Beweise hat der Kläger auch in dem vorliegenden Rechtsstreit nicht vorgebracht. Den Angaben in den Codeworttabellen, die bereits dem Zeugen [ ] bei seiner Untersuchung vorgelegen haben, ist die Beklagte aber nachgegangen. Eine Endastung des Klägers hat sich daraus nicht ergeben. Am 11.3.1991 ist der Kläger dann bis auf weiteres beurlaubt worden. Als der Kläger von dem Geschäftsführer der Beklagten zu einer formellen Anhörung auf den 14.3.1991 bestellt worden ist, mußte dem Kläger klar gewesen sein, daß es um den in dem Sachbericht des Zeugen [ ] angesprochenen Verdacht geht. Es ist auch nicht ungewöhnlich, daß bei einem derartigen Gespräch ein Zeuge zugegen ist. Die Tatsache, daß es sich vorliegend um den (späteren) Prozeßbevollmächtigten der Beklagten gehandelt hat, ändert daran nichts. Nach den zutreffenden Feststellungen des Arbeitsgerichts hat der Kläger die detaillierte Darstellung der Beklagten über den Hergang des Gesprächs vom 14.3.1991 nicht mehr substantiiert bestritten. Dazu genügt es nicht, wenn der Kläger vorträgt, die Beklagte habe sich bei diesem Gespräch augenscheinlich der Mittel der Inquisition bedient, zumal der Kläger noch mit einem Rechtsanwalt konfrontiert worden sei, was gelinde gesagt äußerst ungewöhnlich sei. Im Rahmen eines Verhörs unter Hinzuziehung eines Rechtsanwalts gedeihe schwerlich ein vernünftiges Gespräch, um Mißverständnisse auszuräumen. Es trifft demnach gerade nicht zu, daß dem Kläger keine Gelegenheit gegeben worden wäre, den Vorwurf zu widerlegen. Die angeblichen schriftlichen Beweise, auf die sich der Kläger nach seiner eigenen Einlassung bereits in dem Gespräch vom 9.3.1991 berufen hat, können jedenfalls nur die Übergabeprotokolle vom 27.8.1990 und 10.9.1990 gewesen sein, die der Beklagten unstreitig bereits bekannt gewesen sind und deren Richtigkeit bereits von dem Zeugen [ ] überprüft worden war. Es muß vielmehr davon ausgegangen werden, daß der Kläger offensichtlich von vorneherein nicht bereit gewesen ist, sich zu den Verdachtsgründen substantiiert zu äußern.

5. Der Beklagten war es bei Ausspruch der Kündigung nicht mehr zumutbar, das Arbeitsverhältnis bis zum Ablauf der Kündigungsfrist bzw. zu der vereinbarten Beendigung des Arbeitsverhältnisses, d. h. bis zum 31.12.1991 fortzusetzen.

Wie bei jeder außerordentlichen Kündigung aus wichtigem Grund sind auch bei einer außerordentlichen Verdachtskündigung die gesamten für und gegen eine sofortige Beendigung des Arbeitsverhältnisses sprechenden Umstände erschöpfend zu würdigen und gegeneinander abzuwägen.

*Erforderlich:  
Gesamt abwägung*



*Die beteiligten Interessen*

## Viren-„Implantierung“ als Kündigungsgrund

Gegen den Kläger besteht – wie bereits im einzelnen dargelegt – aufgrund bestimmter Tatsachen der dringende Verdacht, ein Computervirus in die EDV-Anlage der Beklagten implantiert zu haben, um die Beklagte zum Abschluß des Arbeitsvertrages vom 17.12.1990 zu bewegen, nachdem alles Zumutbare zur Aufklärung des Sachverhalts geschehen ist. Die Verfehlung, deren der Kläger verdächtigt wird, erscheint als gravierend. Die Beklagte, die einen Fachliteraturdienst betreibt, ist in ihren unternehmerischen Aktivitäten von dem reibungslosen Funktionieren ihrer EDV-Anlage abhängig, über die sie ihre Aufträge abwickelt. Dabei handelt es sich um den Kernbereich ihrer unternehmerischen Tätigkeit, der bei Störungen nicht einfach zu Fremdfirmen ausgelagert werden kann wie etwa eine Buchhaltung, die von einem Steuerberaterbüro durchgeführt wird. Der Verdacht einer derartig gravierenden Verfehlung ist an sich geeignet, einen wichtigen Grund zum Ausspruch einer außerordentlichen Kündigung darzustellen. Dabei kann dahinstehen, ob der Kläger zugleich in dem Verdacht einer strafbaren Handlung steht (vgl. §§ 303 a u. 303 b StGB). Der Verdacht dieser schweren Verfehlung gerade gegen den Kläger hat das Vertrauen der Beklagten in die Redlichkeit des Klägers zerstört und zu einer unerträglichen Belastung des Arbeitsverhältnisses geführt. Obwohl alles Zumutbare zur Aufklärung des Sachverhalts geschehen ist, konnte der gerade gegen den Kläger bestehende Verdacht nicht ausgeräumt werden. Bei der Entscheidung gemäß § 626 Abs. 1 BGB, ob der Beklagten die Fortsetzung des Arbeitsverhältnisses zugemutet werden kann, war zu berücksichtigen, daß das Arbeitsverhältnis der Parteien nach dem Arbeitsvertrag vom 17.12.1990 auf den 31.12.1991 befristet war und sich jeweils um 12 Monate verlängern sollte, wenn nicht bis zum 30.9. eine Kündigung erfolgt. Die Beklagte hätte das Arbeitsverhältnis also bis zum 31.12.1991, d.h. länger als 3/4 Jahr fortsetzen müssen. Das ist ihr angesichts der schweren Verfehlung, deren der Kläger verdächtigt ist, und der erheblichen Schäden, die ihr bei einer Weiterbeschäftigung des Klägers drohen, nicht zuzumuten. Zum maßgeblichen Zeitpunkt des Zugangs der Kündigung war der Kläger erst etwa 37 Jahre alt, so daß ihm im Hinblick auf sein Lebensalter der Arbeitsmarkt nicht versperrt ist. Der Kläger ist offensichtlich nur gegenüber seiner Ehefrau zum Unterhalt verpflichtet. Zu Lasten des Klägers war weiter zu berücksichtigen, daß das Arbeitsverhältnis zum Zeitpunkt des Zugangs der Kündigung erst kurze Zeit bestanden hat. Das Interesse der Beklagten an der sofortigen Beendigung des Arbeitsverhältnisses überwiegt demnach das Interesse des Klägers an dessen Fortbestand.