# BUNDESPATENTGERICHT

## IM NAMEN DES VOLKES

## URTEIL

Verkündet am
29. November 2018
…

2 Ni 53/16 (EP)

**(Aktenzeichen)**

**In der Patentnichtigkeitssache**

…

ECLI:DE:BPatG:2018:291118U2Ni53.16EP.0

**betreffend das europäische Patent 0 965 094**
**(DE 697 39 021)**

hat der 2. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 29. November 2018 unter Mitwirkung des Vorsitzenden Richters Guth sowie der Richterinnen Hartlieb und Dipl. Phys. Dr. Thum-Rung und der Richter Dipl. Phys. Dr. Forkel und Dipl.-Ing. Hoffmann

für Recht erkannt:

I. Das europäische Patent 0 965 094 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland im Umfang seiner Patentansprüche 1, 2, 7, 8, 9, 10 und 26 für nichtig erklärt.

II. Die Kosten des Rechtsstreits trägt die Beklagte.

III. Das Urteil ist gegen Sicherheitsleistung in Höhe von 120% des zu vollstreckenden Betrages vorläufig vollstreckbar.

## Tatbestand

Mit ihrer Klage begehrt die Klägerin die Nichtigerklärung des europäischen Patents 0 965 094 im Umfang der Patentansprüche 1, 2, 7, 8, 9, 10 und 26 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland. Die Beklagte ist Inhaberin des am 6. November 1997 in englischer Sprache angemeldeten, am 1. Oktober 2008 veröffentlichten und durch Zeitablauf erloschenen europäischen Patents **EP 0 965 094 B1** mit der deutschen Bezeichnung „System und Verfahren zum Schutz eines Computers und eines Netzes gegen feindliche herunterladbare Programme“, das auf die PCT-Anmeldung mit der Veröffentlichungsnummer **WO 1998/021683 A2** zurückgeht und die Priorität der provisorischen

US-Anmeldung 60/030,639 vom 8. November 1996 in Anspruch nimmt. Dessen deutscher Teil wird vom Deutschen Patent- und Markenamt unter der Nummer **697 39 021.7** geführt.

Das Streitpatent umfasst 58 Patentansprüche. Der Patentanspruch 1 ist auf ein „Verfahren zum Betreiben eines Computersystems, welches ein internes Netzsicherheitssystem umfasst“ gerichtet, die Patentansprüche 2 bis 27 sind hiervon abhängige Patentansprüche.

Der **erteilte Patentanspruch 1** des Streitpatents lautet in der Verfahrenssprache Englisch (mit einer an die Gliederung aus dem Schriftsatz der Klägerin vom 24. November 2016 angelehnten Gliederung versehen):

**M1** A method of operating a computer system comprising

**M2** an internal network security system (110) coupling at least one client computer with an external network (105),

**M3** the method comprising

**M3a** receiving, by said internal network security system, from said external network, executable application programs, herein referred to as Downloadables (602) addressed to said client computer,

**M3b** checking said Downloadables and

**M3c** passing or discarding said Downloadables

characterised in that

**M4** the method includes

**M4a** examining said Downloadables according to a security policy defined by at least one test,

**M4b** the method including conducting said test, by said internal network security system,

- on a received Downloadable addressed to said client computer,
- with reference to a Downloadable security profile, herein also referred to as a DSP, comprising a list of suspicious computer operations that the received Downloadable may attempt if executed,

**M4c** determining, by said internal network security system, that said security policy has been violated if the Downloadable fails said test, and

**M4d** discarding the Downloadable and thereby preventing the Downloadable from passing to said client computer if the internal network security system determines that said security policy has been violated.

In Anlehnung an die von der Klägerin vorgeschlagene Merkmalsgliederung lautet der **erteilte Patentanspruch 1** in der deutschen Übersetzung:

**m1** Verfahren zum Betreiben eines Computersystems,

**m2** welches ein internes Netzsicherheitssystem (110) umfasst, das mindestens einen Client-Computer mit einem externen Netz (105) koppelt,

**m3** das Verfahren umfassend

**m3a** das Empfangen, durch das interne Netzsicherheitssystem, von dem externen Netz, von an den Client-Computer adressierten ausführbaren Anwendungsprogrammen, die im Folgenden als Downloadables (602) bezeichnet werden,

**m3b** das Überprüfen der Downloadables und

**m3c** das Weitergeben oder das Verwerfen der Downloadables,

dadurch gekennzeichnet, dass

**m4** das Verfahren einschließt

**m4a** das Untersuchen der Downloadables entsprechend einer Sicherheitsrichtlinie, die durch mindestens einen Test definiert ist,

**m4b** das Verfahren einschließend das Durchführen dieses Tests, durch das interne Netzsicherheitssystem,

- an einem empfangenen Downloadable, das an den Client-Computer adressiert ist,
- unter Bezugnahme auf ein Downloadable-Sicherheitsprofil, das im Folgenden auch als ein DSP bezeichnet wird, welches eine Liste mit verdächtigen Computeroperationen umfasst, die das empfangene Downloadable möglicherweise versucht auszuführen,

**m4c** das Ermitteln, durch das interne Netzsicherheitssystem, dass die Sicherheitsrichtlinie verletzt wurde, wenn das Downloadable den Test nicht besteht, und

**m4d** das Verwerfen des Downloadables und dadurch das Verhindern, dass das Downloadable an den Client-Computer weitergegeben wird, wenn das interne Netzsicherheitssystem ermittelt, dass die Sicherheitsrichtlinie verletzt wurde.

Diesem Anspruch schließen sich die rückbezogenen Ansprüche 2 bis 27 an.

Der **Patentanspruch 2** lautet in der Verfahrenssprache Englisch:

„The method of claim 1, further comprising the step of decomposing, by the internal network security system (110), the Downloadable (602) into said DSP (628), this step including disassembling Downloadable code by the internal network security system."

und in der deutschen Übersetzung:

> „Verfahren gemäß Anspruch 1, des Weiteren umfassend den Schritt des Zerlegens des Downloadables (602), durch das interne Netzsicherheitssystem (110), in das DSP (628), dieser Schritt einschließend das Disassemblieren des Downloadable-Codes durch das interne Netzsicherheitssystem."

Der **Patentanspruch 7** lautet in der Verfahrenssprache Englisch:

> „The method of claim 1, wherein the Downloadable includes a Java applet."

und in der deutschen Übersetzung:

> „Verfahren gemäß Anspruch 1, wobei das Downloadable ein Java-Applet einschließt."

Der **Patentanspruch 8** lautet in der Verfahrenssprache Englisch:

> „The method of claim 1, wherein the Downloadable includes an ActiveX control."

und in der deutschen Übersetzung:

> „Verfahren gemäß Anspruch 1, wobei das Downloadable ein ActiveX-Steuerelement einschließt."

Der **Patentanspruch 9** lautet in der Verfahrenssprache Englisch:

„The method of claim 1, wherein the Downloadable includes a JavaScript script.“

und in der deutschen Übersetzung:

„Verfahren gemäß Anspruch 1, wobei das Downloadable ein JavaScript-Skript einschließt.“

Der **Patentanspruch 10** lautet in der Verfahrenssprache Englisch:

„The method of claim 1, wherein the Downloadable includes a Visual Basic script.“

und in der deutschen Übersetzung:

„Verfahren gemäß Anspruch 1, wobei das Downloadable ein Visual Basic-Skript einschließt.“

Der **Patentanspruch 26** lautet in der Verfahrenssprache Englisch:

„The method of claim 1, wherein said security policy comprises an access control list (410) which contains criteria indicating whether to pass or fail a Downloadable (602) and the method further comprises the step of comparing the DSP, for an incoming Downloadable (602), against said access control list (630), to determine whether the Downloadable should be passed or discarded.”

und in deutscher Übersetzung:

„Verfahren gemäß Anspruch 1, wobei die Sicherheitsrichtlinie eine Zugriffsteuerungsliste (410) umfasst, welche Krite-

rien enthält, die angeben, ob ein Downloadable (602) bestehen oder durchfallen soll, und das Verfahren des Weiteren den Schritt des Vergleichens des DSP, für ein eingehendes Downloadable (602), mit der Zugriffsteuerungsliste (630) umfasst, um zu ermitteln, ob das Downloadable weitergegeben oder verworfen werden soll."

Hinsichtlich des Wortlauts der weiteren Patentansprüche wird auf die Patentschrift EP 0 965 094 B1 verwiesen.

Die Beklagte verteidigt die angegriffenen Ansprüche des Streitpatents in vollem Umfang gemäß **Hauptantrag** in der erteilten Fassung und hilfsweise mit 14 Hilfsanträgen.

**Patentanspruch 1** gemäß **Hilfsantrag 1** unterscheidet sich von Patentanspruch 1 gemäß Hauptantrag in der eingereichten englischsprachigen Fassung durch Merkmal **MX1**, das auf Merkmal **M4b** folgt:

**MX1** „by comparing the DSP against the security policy,"

Patentanspruch 1 gemäß **Hilfsantrag 2** unterscheidet sich von Patentanspruch 1 gemäß Hilfsantrag 1 in der eingereichten englischsprachigen Fassung durch Merkmal **MY1**, das auf Merkmal **M4d** folgt:

**MY1** „wherein the list of suspicious computer operations includes registry operations."

Patentanspruch 1 gemäß **Hilfsantrag 3** unterscheidet sich von Patentanspruch 1 gemäß Hilfsantrag2 in der eingereichten englischsprachigen Fassung durch Merkmal **MY2**, das an die Stelle von Merkmal **MY1** tritt:

**MY2** „wherein the list of suspicious computer operations includes registry operations and network operations."

Patentanspruch 1 gemäß **Hilfsantrag 4** unterscheidet sich von Patentanspruch 1 gemäß Hilfsantrag 3 in der eingereichten englischsprachigen Fassung durch Merkmal **MY3**, das Merkmal **MY2** ersetzt:

**MY3** „wherein the list of suspicious computer operations includes file operations, network operations, registry operations and operating system operations"

Patentanspruch 1 gemäß **Hilfsantrag 5** unterscheidet sich von Patentanspruch 1 gemäß Hauptantrag in der eingereichten englischsprachigen Fassung durch Merkmal **MX2**, das sich an Merkmal **M4b** anschließt:

**MX2** „by retrieving, if the DSP of the received Downloadable is known, the DSP from a security database (240) including DSPs corresponding to known Downloadables and comparing the DSP against the security policy,"

Patentanspruch 1 gemäß **Hilfsantrag 6** beinhaltet gegenüber Patentanspruch 1 gemäß Hilfsantrag 5 noch Merkmal **MY2**, das an Merkmal **M4d** angefügt ist:

**MY2** „wherein the list of suspicious computer operations includes registry operations and network operations."

Patentanspruch 1 gemäß **Hilfsantrag 7** beinhaltet gegenüber Patentanspruch 1 gemäß Hilfsantrag 6 das Merkmal **MY3**, das Merkmal **MY2** ersetzt:

**MY3** „wherein the list of suspicious computer operations includes file operations, network operations, registry operations and operating system operations."

Patentanspruch 1 gemäß **Hilfsantrag 8** beinhaltet gegenüber Patentanspruch 1 gemäß Hauptantrag das Merkmal **MX3**, das zwischen den Merkmalen **M4b** und **M4c** eingefügt ist sowie das Merkmal **MZ**, das sich an Merkmal **M4d** anschließt:

**MX3** „by retrieving, if the DSP of the received Downloadable is known, the DSP from a security database (240) including DSPs corresponding to known Downloadables, forwarding the DSP to an ACL comparator, and comparing, by the ACL comparator, the DSP against the security policy,"

**MZ** „wherein said security policy comprises an access control list (410) which contains criteria indicating whether to pass or fail a Downloadable (602), wherein comparing the DSP against the security policy comprises the step of comparing, by the ACL comparator, the DSP of the received downloadable against said access control list (630)."

Patentanspruch 1 gemäß **Hilfsantrag 9** beruht auf Patentanspruch 1 gemäß Hilfsantrag 8, wobei das Merkmal **MY2** nach Merkmal **MZ** angefügt ist:

**MY2** „wherein the list of suspicious computer operations includes registry operations and network operations."

Patentanspruch 1 gemäß **Hilfsantrag 10** beruht auf Patentanspruch 1 gemäß Hilfsantrag 9, wobei Merkmal **MY3** das Merkmal **MY2** ersetzt:

**MY3** „wherein the list of suspicious computer operations includes file operations, network operations, registry operations and operating system operations."

Patentanspruch 1 gemäß **Hilfsantrag 11** unterscheidet sich von Patentanspruch 1 gemäß Hauptantrag durch Merkmal **MX4**, das zwischen die Merkmale **M4b** und **M4c** eingefügt ist, Merkmal **MZ** folgt auf Merkmal **M4d**:

**MX4** „by retrieving, if the DSP of the received Downloadable is known, the DSP from a security database (240) including DSPs corresponding to known Downloadables, forwarding the DSP to an ACL comparator, otherwise decomposing, by a code scanner, the Downloadable into the DSP, and comparing, by the ACL comparator, the DSP against the security policy,"

**MZ** „wherein said security policy comprises an access control list (410) which contains criteria indicating whether to pass or fail a Downloadable (602), wherein comparing the DSP against the security policy comprises the step of comparing, by the ACL comparator, the DSP of the received downloadable against said access control list (630)."

Patentanspruch 1 gemäß **Hilfsantrag 12** unterscheidet sich von Patentanspruch 1 gemäß Hilfsantrag 11 durch Merkmal **MX5**, das an die Stelle von Merkmal **MX4** tritt:

**MX5** „by retrieving, if the DSP of the received Downloadable is known, the DSP from a security database (240) including security policies, known Downloadables, known Certificates and DSPs corresponding to the known Downloadables, forwarding the DSP to an ACL comparator, otherwise decomposing, by a code scanner, the Downloadable into the DSP, and comparing, by the ACL comparator, the DSP against the security policy,"

Patentanspruch 1 gemäß **Hilfsantrag 13** beinhaltet gegenüber Patentanspruch 1 gemäß Hilfsantrag 12 noch Merkmal **MY2**, das sich an Merkmal **MZ** anschließt:

**MY2** „wherein the list of suspicious computer operations includes registry operations and network operations."

Patentanspruch 1 gemäß **Hilfsantrag 14** basiert auf Patentanspruch 1 gemäß Hilfsantrag 13, wobei Merkmal **MY2** durch Merkmal **MY3** ersetzt ist:

**MY3** „wherein the list of suspicious computer operations includes file operations, network operations, registry operations and operating system operations."

Wegen des Wortlauts der weiteren Ansprüche der von der Beklagten in der mündlichen Verhandlung gestellten Hilfsanträge 1 bis 14 wird auf die mit Schriftsatz vom 21. September 2018 eingereichten Hilfsanträge verwiesen.

Die Klägerin greift das Streitpatent im Umfang der Patentansprüche 1, 2, 7, 8, 9, 10 und 26 an und macht den Nichtigkeitsgrund der unzulässigen Erweiterung geltend, da der Gegenstand der angegriffenen Patentansprüche über den Inhalt der früheren Anmeldung in der ursprünglichen eingereichten Fassung hinausgehe und stützt sich weiter auf den Nichtigkeitsgrund der fehlenden Patentfähigkeit, weil der Gegenstand der angegriffenen Patentansprüche nicht neu sei, jedenfalls aber nicht auf erfinderischer Tätigkeit beruhe.

Zur Stützung ihres Vorbringens nennt die Klägerin u. a. folgende Dokumente:

| | |
|---|---|
| **K1** | Verletzungsklage vor dem LG Düsseldorf |
| **K2** | Auszug aus dem Patentregister |
| **K3** | EP 0 965 094 B1 (Streitpatent) |
| **K3a** | WO 98/021683 A2 |

| | |
|---|---|
| **K3b** | US 60/30639 P |
| **K4** | ESaSS B.V.: „ThunderBYTE Anti-Virus Utilities“, User manual, 1995 |
| **K5** | EP 0 636 977 A2 |
| **K6** | US 5 319 776 A |
| **K7** | WO 97/12321 A1 |
| **K8** | Morton Swimmer et al.: „Dynamic Detection and Classification of Computer Viruses using General Behaviour Patterns“, Virus Bulletin Conference, September 1995 |
| **K9** | WO 95/33237 A1 |
| **K10** | David M. Martin Jr. et al.: „Blocking Java Applets at the Firewall”, IEEE, 10-11 Februar 1997 |
| **K11** | „Firewalls”, September 1996 |
| **K12** | US 6 092 194 A |
| **K13** | US 5 412 717 A |
| **K14** | Gliederung des Patentanspruchs 1 |
| **K15** | Eingabe der Anmelderin im Prüfungsverfahren am Europäischen Patentamt |
| **K16** | Prüfungsbescheid des Europäischen Patentamts |
| **K17** | Wikipedia-Artikel „Virensignatur“ |
| **K18** | Wikipedia-Artikel „EICAR-Testdatei“ |
| **K19** | Eingabe der Beklagten im Nichtigkeitsverfahren vor dem USPTO |
| **K20** | Auszug aus „The Computer Desktop Encyclopedia“, 1996 |
| **K21** | Auszug aus „Computer Dictionary“, 1991 |
| **K22** | Gutachten von Dr. C… im Verletzungsstreit am LG Düsseldorf |
| **K23** | Wikipedia-Artikel „EICAR test file“ |
| **K24** | „File Management Functions” unter Windows |
| **K25** | „Registry Functions“ unter Windows |
| **K26** | Virus Bulletin, Juni 1994 |

**K27** PC Magazin, November 1995

**K28** Virus Bulletin, September 1997

Die **Klägerin** ist der Ansicht, insbesondere die Merkmale eines „Client Computers“ sowie die Merkmale **M3a** bis **M3c** sowie **M4a bis M4d** des erteilten Patentanspruchs 1 seien nicht ursprünglich offenbart. Patentanspruch 1 könne auch nicht die Priorität der provisorischen US-Anmeldung 60/030,639 vom 8. November 1996 in Anspruch nehmen. Bei dem Client Computer und dem internen Netzsicherheitssystem handele es sich sowohl nach dem Wortlaut als auch nach der Lehre des Streitpatents um zwei getrennte Hardwaresysteme.

Der Gegenstand des erteilten Patentanspruchs 1 sei nicht neu gegenüber den Druckschriften **K4**, **K5** und **K6**, wenn die Auslegung der Beklagten der Nichtigkeitsklage im parallelen Verletzungsprozess zugrunde gelegt werde, wonach als „Client-Computer“ im Sinne des Streitpatents auch ein Browser und als „internes Netzsicherheitssystem“ eine integrierte Softwareanwendung angesehen werden könne.

Lege man Patentanspruch 1 aber dahingehend aus, dass das interne Netzsicherheitssystem lediglich als Gatewayserver beansprucht werde und ein Client Computer der Zielcomputer sei, so sei der Gegenstand des Patentanspruchs 1 nicht neu gegenüber Druckschrift **K7**, die Stand der Technik gemäß Art. 54 Abs. 3 EPÜ sei, sowie gegenüber den Druckschriften **K8**, **K9** und **K10**.

Jedenfalls aber liege der Gegenstand von Patentanspruch 1 gegenüber einer oder einer Kombination einzelner der Druckschriften **K4** bis **K12** nahe.

Auch seien die Gegenstände der **Hilfsanträge 1 bis 14** unzulässig erweitert, könnten die Priorität nicht in Anspruch nehmen und seien durch den Stand der Technik neuheitsschädlich vorweggenommen oder jedenfalls nahegelegt.

Die Klägerin stellt den Antrag,

> das europäische Patent 0 965 094 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland im Umfang seiner Patentansprüche 1, 2, 7, 8, 9, 10 und 26 für nichtig zu erklären.

Die Beklagte stellt den Antrag,

> die Klage abzuweisen,
> hilfsweise unter Klageabweisung im Übrigen das europäische Patent 0 965 094 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland im Umfang seiner Patentansprüche 1, 2, 7, 8, 9, 10 und 26 dadurch für nichtig zu erklären, dass diese Ansprüche die Fassung gemäß eines der Hilfsanträge 1 bis 14 gemäß Anlage zum Schriftsatz vom 21. September 2018, in dieser Reihenfolge, erhalten.

Die **Beklagte**, die die angegriffenen Patentansprüche in vollem Umfang und mit 14 Hilfsanträgen beschränkt verteidigt, tritt der Argumentation der Klägerin in vollem Umfang entgegen.

Patentanspruch 1 verlange nicht, dass Client-Computer und internes Netzsicherheitssystem auf getrennter Hardware liefen, da die Lehre der Erfindung auch durch in einen normalen Computer integrierte, funktional bestimmte oder virtualisierte Komponenten – z. B. auch Softwarekomponenten – ausgeführt werden könne.

Die öffentliche Zugänglichkeit der Druckschrift **K4** sei nicht hinreichend belegt. Außerdem verwende Druckschrift **K4** kein Downloadable-Sicherheitsprofil.

Druckschrift **K7** sei kein relevanter Stand der Technik, da die Priorität des Streitpatents wirksam in Anspruch genommen werde. Sie verwende außerdem einen anderen Typ eines Virenscanners als das Streitpatent.

Die Veröffentlichung der Druckschrift **K8** sei ebenfalls nicht belegt. Druckschrift **K8** umfasse außerdem insbesondere kein DSP mit einer Liste von verdächtigen Computeroperationen, die das empfangene Downloadable möglicherweise versuche auszuführen, was ebenso für Druckschrift **K9** gelte.

Druckschrift **K10**, deren Veröffentlichung bestritten werde, offenbare lediglich einen einfachen Signaturenscanner, der nach einer einzigen Signatur suche, die keine Computeroperationen enthalte.

Es sei auch kein Anlass ersichtlich, ausgehend von einer der Entgegenhaltungen oder durch ihre Kombination zur Lehre des Streitpatents zu gelangen.

Jedenfalls aber sei das Streitpatent in der Fassung der **Hilfsanträge 1 bis 14**, die die Bedenken des Senats berücksichtigten, bestandsfähig.

Die Beklagte stützt ihr Vorbringen u. a. auf folgende Dokumente:

| | |
|---|---|
| **LM1** | Definition Virus Signature (Webopedia) |
| **LM2** | Definition Virus Signature (Techopedia) |
| **LM3** | Definition Virus Signature (PC Magazin) |
| **LM4** | Definition Virus Signatur von Bitdefender |
| **LM5** | Antrag auf Eintritt in die regionale Phase vor dem EPA für WO 97/12321 |
| **LM6** | Auszug Register EPA für EP 0 852 762 (Übersicht) |
| **LM7** | Auszug Register EPA für EP 0 852 762 (Rechtsstand) |
| **VP17** | Anlagenkonvolut mit Veröffentlichungen von „VIRUS BULLETIN“ |
| **LM8** | Wikipedia-Artikel „Firewall“-Versionsgeschichte |

| | |
|---|---|
| **LM9** | RASMUSSON, L.; JANSSON, S.: Simulated Social Control for Secure Internet Commerce, 1996 |
| **LM10** | Wikipedia-Artikel “Java applet” |
| **LM11** | Wikipedia Artikel Maschinensprache |
| **LM12** | Entscheidung vom 24. September 2015 des US PTAB (Patent Trial and Appeal Board) |
| **LM13** | Entscheidung vom 10. Januar 2018 des United States Court of Appeals |
| **LM14** | Webpage von ESET |
| **LM15** | Entscheidung vom 28. Januar 2016 des US PTAB |

Wegen der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

## Entscheidungsgründe

### I.

Die Klage, mit der die Nichtigkeitsgründe der unzulässigen Erweiterung gemäß Art. II § 6 Abs. 1 Nr. 3 IntPatÜG, Art. 123 Abs. 2, Art. 138 Abs. 1, lit. c) EPÜ sowie der fehlenden Patentfähigkeit im Sinne der Art. 138 Abs. 1, lit. a) in Verbindung mit Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, weil der Gegenstand der angegriffenen Patentansprüche nicht neu sei (Art. 54 Abs. 1 und 2 EPÜ), jedenfalls aber nicht auf erfinderischer Tätigkeit beruhe (Art. 56 i. V. m. Art. 54 Abs. 2 EPÜ), geltend gemacht werden, ist zulässig.

Die Klage ist auch begründet. Das Streitpatent ist im Umfang seiner Patentansprüche 1, 2, 7, 8, 9, 10 und 26 für nichtig zu erklären, weil der Gegenstand des Streitpatents insoweit weder in der erteilten Fassung, die mit dem Hauptantrag verteidigt wird, noch in der mit den Hilfsanträgen 1 bis 14 verteidigten Fassung

der genannten Patentansprüche patentfähig ist; denn die darin beanspruchte Lehre ist für den Fachmann durch den Stand der Technik nahegelegt.

Es bedarf daher keiner Entscheidung, ob dem Streitpatent in den nach dem Hauptantrag und den Hilfsanträgen 1 bis 14 verteidigten Fassungen auch der weiterhin geltend gemachte Nichtigkeitsgrund der unzulässigen Erweiterung (Art. II § 6 Abs. 1 Nr. 3 IntPatÜG, Art. 123 Abs. 2, Art. 138 Abs. 1, lit. c) EPÜ) entgegensteht.

**1.** Das Streitpatent befasst sich mit dem Schutz von einzelnen Computern und Computernetzwerken vor Schadprogrammen, die aus dem Internet heruntergeladen werden und im Streitpatent als „Downloadables“ bezeichnet werden (Streitpatent, Absatz [0001]). Da das Internet allgemein zugänglich ist, hat es sich zur Quelle für viele Schadprogramme wie z. B. Viren entwickelt.

Das Streitpatent geht insbesondere von einem Stand der Technik aus, wie er in der Patentanmeldung US 5 412 717 A beschrieben wird. Diese offenbart ein System und Verfahren für eine in Echtzeit erfolgende Steuerung eines Programms, bei der das Programm in Quarantäne genommen wird und in einem „Isolationsmodus“ innerhalb einer „safety box“ abläuft, wobei es nicht in der Lage ist, die Ressourcen des Computers zu schädigen. Das ausführbare Programm wird durch Programmautorisierungsinformationen *(program authorization information PAI)* gesteuert. Solche bekannten Sicherheitssysteme können allerdings nur Programme untersuchen, die bereits im Dateisystem des Computers gespeichert sind. Mit Entwicklung von Scripts und Applet Bytecode können Programme aber auch durch Webbrowser unmittelbar ohne lokale Speicherung auf einem Computer ausgeführt werden (Streitpatent, Absatz [0002]).

Die vorbekannten Sicherheitssysteme sind laut Streitpatent nicht in der Lage, Computerviren zu erkennen, die sich in „Downloadables“ verbergen, d. h. in ausführbaren Anwendungen, die während der Nutzung des Internets von einem Quellcomputer heruntergeladen worden sind und auf dem Zielcomputer ablaufen.

Ein „Downloadable“ wird typischerweise durch einen Internetbrowser oder eine Web Engine angefordert und kann Java Applets, JavaScript Scripts, ActiveX Steuerelemente oder Visual Basic Anwendungen beinhalten (Streitpatent, Absatz [0004]).

**2.** Ausgehend vom bekannten Stand der Technik adressiert das Streitpatent das Problem, ein System und Verfahren bereitzustellen, welche ein Netzwerk vor schädlichen „Downloadables“ schützen können (Streitpatent, Absätze [0004], Spalte 2, Zeilen 4 bis 6; [0005], Spalte 2, Zeilen 10 bis 11; [0007], Spalte 2, Zeilen 41 bis 43).

**3.** Die oben genannte Aufgabe soll durch das Verfahren nach dem erteilten Patentanspruch 1 gelöst werden.

**4.** Dem erteilten Patentanspruch 1 lässt sich in Verbindung mit der Beschreibung und den Figuren 1 bis 8 folgende Lehre entnehmen:

Zusammengefasst lehrt der Patentanspruch 1 ein Sicherheitsverfahren bzw. -system, das der Überprüfung von herunterladbaren Anwendungsprogrammen, sogenannten „Downloadables“ dient.

Merkmal **M1** betrifft ein Verfahren zum Betreiben eines Computersystems. Laut Merkmal **M2** zeichnet sich das Computersystem dadurch aus, dass es eine Schnittstelle beinhaltet, welche ein externes Netzwerk mit mindestens einem Client-Computer verbindet. Diese Anordnung wird in Figur 1 des Streitpatents veranschaulicht. Das Netzwerk (100) verfügt über ein externes Computernetzwerk (105), wie etwa ein Weitverkehrsnetz (WAN), z. B. das Internet, das über eine Kommunikationsverbindung (125) mit einem internen Netzsicherheitssystem (110) verknüpft ist. Das Netzwerk (100) umfasst weiterhin ein internes Computernetzwerk (115), wie etwa ein unternehmensweites lokales Netzwerk (LAN), das über einen Kommunikationsweg (130) an das interne Netzsicherheitssystem (110) angebunden ist (Streitpatent, Absatz [0010]). In Patentanspruch 1 tritt

anstelle des internen Computernetzwerkes ein einzelner oder mehrere Computer.

Entsprechend Merkmal **M3a** aus dem Merkmalskomplex **M3** empfängt das interne Netzsicherheitssystem von dem externen Netzwerk ausführbare Anwendungsprogramme, sogenannte „Downloadables“, die an den wenigstens einen Client-Computer adressiert sind. In den Merkmalen **M3b** und **M3c** ist vorgesehen, die „Downloadables“ zu überprüfen und diese entweder an das interne Computernetzwerk weiterzugeben oder aber zu verwerfen.

Im Merkmalskomplex **M4** wird die Analyse der „Downloadables“ konkretisiert. Laut Merkmal **M4a** werden sie vom Sicherheitssystem auf Einhaltung einer Sicherheitsrichtlinie überprüft. Bei der Überprüfung der Einhaltung der Sicherheitsrichtlinie wird ein Test herangezogen. Merkmal **M4b** besagt, dass dieser Test durch das interne Netzsicherheitssystem an einem empfangenen, an den Client-Computer adressierten „Downloadable“ durchgeführt wird, wobei der Test eine Bezugnahme auf ein Downloadable-Sicherheitsprofil (Downloadable Security Profile „DSP“) beinhaltet. Jedes „DSP“ enthält gemäß Merkmal **M4b** eine Liste mit verdächtigen Computeroperationen, die das jeweilige „Downloadable“ bei seiner Ausführung möglicherweise auszuführen versucht. In Absatz [0023] der Streitpatentschrift ist ein Beispiel für eine Liste mit verdächtigen Operationen angeführt. Der Fachmann versteht die in Merkmal **M4b** genannte Liste daher so, dass in ihr Aktionen wie das Lesen und Schreiben von Dateien, Lese- und Schreibvorgänge in der Systemregistrierung, das Senden und Empfangen von Daten, Aktionen auf Betriebssystemebene oder beanspruchte Ressourcen genannt werden. Weiterhin entnimmt der Fachmann der Beschreibung des Streitpatents (Absatz [0022]), dass zu jedem „Downloadable“ ein „DSP“ gehört. Gemäß Absatz [0025] der Streitpatentschrift besteht der im Merkmalskomplex **M4** beschriebene Test darin, die Liste eines „DSP“ mit der Sicherheitsrichtlinie bzw. deren Zugriffssteuerungsliste ACL zu vergleichen. Es findet eine Gegenüberstellung der einzelnen, in der Liste genannten Aktionen mit der zuvor definierten Sicherheitsrichtlinie statt.

Wenn das „Downloadable“ den Test nach den Merkmalen **M4a** und **M4b** nicht bestanden hat, wird laut Merkmal **M4c** festgestellt, dass die Sicherheitsrichtlinie verletzt worden ist. Wenn das interne Netzsicherheitssystem ermittelt, dass die Sicherheitsrichtlinie verletzt worden ist, der Test also als nicht bestanden gilt, wird verhindert, dass das „Downloadable“ an den Client-Computer weitergegeben wird, indem es verworfen wird (Merkmal **M4d**). Im Ergebnis wird dadurch unterbunden, dass ein Schadprogramm auf den Client-Computer gelangt.

**5.** Als **Fachmann**, der mit der Aufgabe betraut wird, ein Verfahren bzw. System zum Schutz eines Computersystems vor Schadprogrammen zu verbessern, sieht der Senat einen Diplominformatiker mit Universitätsabschluss an, der über eine mehrjährige Berufserfahrung auf dem Gebiet der Sicherheitstechnik für Computer und Computernetzwerke besitzt.

**6.** Einige Begriffe des Streitpatents bedürfen der Erläuterung.

Bei der Interpretation eines erteilten Patentanspruchs ist zu berücksichtigen, dass die im Patentanspruch verwendeten Begriffe im Zweifel so zu verstehen sind, dass sämtliche Ausführungsbeispiele zu ihrer Ausfüllung herangezogen werden können *(BGH GRUR 2015, 972 - Kreuzgestänge)*.

Zu den Begriffen *Client-Computer* und *internes Netzsicherheitssystem*
Der Fachmann wird in dem anspruchsgemäßen *Client-Computer* ein Computersystem in einem Netzwerk erkennen, das bestimmte Dienste von anderen Computersystemen in Anspruch nehmen kann.
Bei Berücksichtigung des Ausführungsbeispiels des Streitpatents ist damit unter dem *internen Netzsicherheitssystem* in Merkmal **M2** und in den Merkmalsgruppen **M3** und **M4** des erteilten Patentanspruchs 1 eine Schnittstelle zwischen mindestens einem *Client-Computer* und einem externen Netzwerk zu verstehen, die von dem externen Netzwerk an den *Client-Computer* adressierte Anwendungsprogramme erhält, diese mittels eines Tests überprüft und entsprechend dem Testergebnis entweder weitergibt oder aber verwirft, wobei

das *interne Netzsicherheitssystem* derart zu interpretieren ist, das es auch den Übergang zu einem internen Computernetzwerk (z. B. ein LAN, üblicherweise bestehend aus mehreren PCs) herstellen und zu diesem Zweck eine eigenständige Hardwarekomponente bilden kann.

Der Begriff *internes Netzsicherheitssystem* ist aber nicht auf dieses Beispiel beschränkt:
Der erteilte Patentanspruch 1 verlangt *nicht*, dass im Fall lediglich eines einzigen zu schützenden *Client-Computers* das *interne Netzsicherheitssystem* dem einzelnen Computer als eigenständige Hardwarekomponente vorgeschaltet sein muss; der Patentanspruch 1 schließt nicht aus, dass das *interne Netzsicherheitssystem* als Softwarelösung im *Client-Computer*, also dem Zielcomputer für das Anwendungsprogramm implementiert ist. Nach dem Verständnis des Fachmannes kann zum Schutz des *Client-Computers* ein *Netzsicherheitssystem* in gleichwirkender Weise sowohl auf einem eigenständigen Rechner (ähnlich einem Router oder einer Hardware-Firewall) untergebracht sein als auch in Gestalt eines virtuellen Computers im realen *Client-Computer* emuliert werden. Unter den Begriff „*internes Netzsicherheitssystem“* fallen somit auch beliebige Techniken, die ein Anwendungsprogramm in einer von den anderen Systemressourcen des zu schützenden *Client-Computers* isolierten Laufzeitumgebung ausführen und analysieren, so dass dessen Start auf dem realen *Client-Computer* erst dann erfolgt, wenn im virtuellen Umfeld keine als verdächtig einzustufenden Aktionen entdeckt worden sind.

Die Merkmalsgruppe **M3** verlangt im Wesentlichen, dass das *interne Netzsicherheitssystem* an den *Client-Computer* adressierte Anwendungsprogramme empfängt, diese überprüft und danach an den (Client) entweder weitergibt oder aber verwirft. Da die Auslegung eines Patentanspruchs an seinen Wortlaut gebunden ist, so wie ihn der Fachmann versteht, ist die Merkmalsgruppe so zu verstehen, dass ein analysiertes Anwendungsprogramm entsprechend dem Resultat der Überprüfung entweder an den *Client-Computer*

*zur Ausführung übergeben* oder aber unwirksam gemacht wird. Der erteilte Patentanspruch 1 schließt hierbei nicht aus, dass die Übergabe des Anwendungsprogramms von einem virtuellen an einen realen Computer stattfindet, wobei Programmstart und -ausführung nicht bereits im virtuellen Umfeld sondern erst später auf dem realen *Client-Computer* erfolgen, wo dann auch ein Zugriff auf reale Systemressourcen zugelassen wird.

Zum Begriff *Downloadable security profile DSP*
In Merkmalsgruppe **M4** wird festgelegt, dass ein Test „unter Bezugnahme auf ein Downloadable-Sicherheitsprofil“ *DSP* durchgeführt wird, „welches eine Liste mit verdächtigen Computeroperationen umfasst.“ Demnach verlangt Patentanspruch 1 nur eine irgendwie geartete Bezugnahme auf eine Liste mit verdächtigen Computeroperationen. Patentanspruch 1 lässt somit völlig offen, wie diese Liste erzeugt oder wie mit ihr im Test umgegangen wird. Außerdem ist Patentanspruch 1 nicht auf eine Liste beschränkt, die nur verdächtige Computeroperationen beinhaltet.

Ferner ist der Begriff „*Liste§* breit auszulegen. Demnach ist - einem Alltagsverständnis folgend - unter einer *Liste* ganz allgemein eine Sammlung von Informationen zu verstehen, die in einer einheitlichen, sich ständig wiederholenden Form dargestellt wird. Aber auch eine dynamische Datenstruktur zum Speichern von Datenelementen, z. B. eine sequentielle Datei fällt unter den Begriff „*Liste“*.

## 7. Zum Hauptantrag

Das Streitpatent kann in der nach dem **Hauptantrag** verteidigten Fassung keinen Bestand haben, da der Gegenstand des erteilten Patentanspruchs 1 nicht auf erfinderischer Tätigkeit beruht.

**7.1** Von besonderer Bedeutung sind die Druckschriften **K9 / Schnurer** und **K4 / ThunderByte**, an deren Vorveröffentlichung der Senat keinen Zweifel hegt. Mit Rücksicht auf den daraus bekannten Stand der Technik fehlt es dem Gegen-

stand des erteilten Patentanspruchs 1 an der für die Patentfähigkeit erforderlichen erfinderischen Tätigkeit.

**7.1.1** Bei der Druckschrift **K4** handelt es sich um ein Benutzerhandbuch für verschiedene Antivirenmodule des Unternehmens ThunderByte, das einen Copyright-Vermerk von 1995 trägt, was vor dem Prioritätsdatum des Streitpatents liegt. Demnach bildet das Handbuch unabhängig von der Frage der Wirksamkeit der Priorität des Streitpatents Stand der Technik nach Art. 54 Abs. 2 EPÜ. Die Einschätzung des Senats steht in Einklang mit der herrschenden Meinung, nach der grundsätzlich davon ausgegangen werden kann, dass der auf der Druckschrift angegebene Zeitpunkt (copyright notice) mit der öffentlichen Zugänglichkeit identisch ist, da Druckschriften nach der Lebenserfahrung in unmittelbarem Anschluss nach der Herstellung auch verteilt zu werden pflegen (vgl. Schulte, Patentgesetz, 10. Auflage 2017, § 3, Rd. 42 und 45; vgl. auch BPatGE 1991, 821 - Hochspannungstransformator).
Aus dem Anlagenkonvolut VP17 mit verschiedenen Ausgaben von *VIRUS BULLETIN* geht zudem hervor, dass der Virenscanner *ThunderBYTE*, auf den sich das Benutzerhandbuch **K4** bezieht, im Jahr 1995 existierte, getestet wurde und käuflich erworben werden konnte (Seite 18, links unten der Ausgabe Januar/1995; Seite 18, rechts unten der Ausgabe Juli/1995; Seite 19, links oben der Ausgabe Januar/1996; Seite 19, links unten der Ausgabe Januar/1995).
Damit ist selbstverständlich auch das zugehörige Benutzerhandbuch im Jahr 1995 erhältlich gewesen.
Dass die Druckschrift **K4** somit vor dem Prioritätsdatum des Streitpatents publiziert wurde, steht nach allem außer Zweifel.

**7.1.2** Die Druckschrift **K9** wurde am 7. Dezember 1995, also vor dem Prioritätsdatum des Streitpatents veröffentlicht, so dass die Frage, ob der erteilte Patentanspruch 1 die im Streitpatent angegebene Priorität wirksam in Anspruch nehmen kann, dahinstehen kann.
Sie führt den Fachmann zu einer Computervirenfalle *(computer virus trap)*. Das bekannte System stellt einem Virus eine virtuelle Umgebung bereit, die der des

Computers, auf dem der Virus aktiv werden soll, gleicht. In dieser virtuellen Umgebung werden Dateien auf mögliche Viren untersucht und anschließend entfernt, bevor der Virus auf dem eigentlichen Computersystem aktiv werden kann (Abstract). Folglich offenbart die Druckschrift **K9** ein Verfahren zum Betreiben eines Computersystems (Merkmal **M1**).

Weiterhin beschreibt sie ein Computersystem, welches ein internes Netzsicherheitssystem umfasst. Als internes Netzsicherheitssystem fungiert nach der Lehre der Druckschrift **K9** eine Virenfalle 10, die wenigstens einen Client-Computer *(workstation 38)* mit einem externen Netz *(34)* verknüpft (Seite 12, zweiter Absatz; Fig. 4 - Merkmal **M2**).

In Figur 4 werden sämtliche Datenströme, die ein Netzwerk 34 durchqueren, vor Computerviren geschützt. Der ganze Datenverkehr zwischen den an das Netzwerk 34 angebundenen Workstations 38 und einem Mainframe Dateiserver 30 wird ständig auf Viren überprüft, da er über die Virenfalle 10 geleitet wird (Seite 11, erster Absatz). Ausführbare Dateien, die die Virenfalle 10 als internes Netzsicherheitssystem über das Netzwerk 34 empfangen hat, werden im Emulator 48 *(emulation box)* zur Ausführung gebracht und analysiert (Seite 12, dritter Absatz). Die Übertragung von Anwendungsprogrammen an ein internes Netzsicherheitssystem und deren anschließende Überprüfung sind damit in der Druckschrift **K9** offenbart (Merkmale **M3a**, **M3b**).

Wird das Anwendungsprogramm als schädlich eingestuft, so werden Maßnahmen gegen Virenaktivität eingeleitet. U. a. kann die Datei dann gelöscht werden; andernfalls wird das Anwendungsprogramm als unbedenklich eingestuft und weitergegeben (Seite 14, erster Absatz, Fig. 6C – Merkmal **M3c**).

Das Entdecken eines Virus ist gleichbedeutend damit, dass eine Sicherheitsrichtlinie in der Virenfalle verletzt worden ist und die Datei den Test nicht bestanden hat. In einem solchen Fall wird die Datei verworfen und nicht an den Client-Computer *(workstation 38)* weitergegeben (Seite 14, erster Absatz). Die Merkmale **M4c** und **M4d** sind in der Lehre der Druckschrift **K9** verwirklicht.

Zwar offenbart das Verfahren der Druckschrift **K9** kein Sicherheitsprofil mit einer Liste von verdächtigen Computeroperationen, jedoch können die durchgeführten zyklischen Redundanzprüfungen zumindest nachweisen, ob bei der Emulation

eines Anwendungsprogramms verdächtige Computeroperationen stattgefunden haben: so können z. B. verdächtige Veränderungen an einer Konfigurationsdatei, der *IRQ table* entdeckt werden (Seite 12, letzter Absatz).

Weiterhin offenbart auch die Druckschrift **K4** ein Verfahren zum Betreiben eines Computersystems, bei dem heruntergeladene ausführbare Programmdateien, also Downloadables, im Hinblick auf Virenaktivitäten überprüft werden. Das bekannte Verfahren ist als Antivirensoftware *ThunderBYTE (TBAV)* implementiert, die über mehrere Module verfügt. Dabei ist das Modul *TbScan* dazu ausgelegt, an ausführbaren Programmdateien sowohl Signaturscans als auch heuristische Analysen vorzunehmen (Seite 1, letzter Absatz bis Seite 2, erster Absatz; Seite 57, Absatz *Configure executable extensions*). Weiterhin umfasst *TBAV* das Programm *TbScanX*, eine speicherresidente Variante von *TbScan*, die Dateien untersucht, während sie aus einem Netzwerk auf ein Computersystem heruntergeladen werden (Seite 2, dritter Absatz; Seiten 84 bis 91). Hinsichtlich ihrer Funktionalität sind die beiden Module *TbScan* und *TbScanX* praktisch identisch (Seite 84, Abschnitt 3.4). Die Merkmale **M1** und **M3b** sind damit in der Lehre der Druckschrift **K4** verwirklicht. Insbesondere beschreibt die Druckschrift **K4**, wie mittels heuristischer Analyse verdächtige Computeroperationen, die die jeweilige Programmdatei versucht auszuführen, entdeckt werden. Die Datei wird zerlegt (*disassembling)* und hieraus ermittelte Computeroperationen *(instructions)* werden untersucht (Seite 56; Seite 153, Abschnitt 4.3 bis Seite 154, dritter Absatz; Seite 155, Abschnitt 4.3.2, erster Absatz).
Verdächtige Computeroperationen werden mit einem *heuristic flag* gekennzeichnet (Seite 155, Abschnitt 4.3.2), das den jeweiligen Typ von Computeroperation näher umschreibt (Seite 180ff, Appendix B). Laut Druckschrift **K4** ergibt jedes gefundene *heuristic flag* eine Punktzahl *(score)*. Die Heuristik untersucht den Code der Programmdatei und erhöht einen „Verdächtigkeitszähler“ für die Datei, wenn sie eine verdächtige Computeroperation erkennt. Wenn der Wert des Zählers nach Untersuchung des Codes einen vordefinierten Grenzwert überschreitet, geht *TbScan* bzw. *TbScanX* davon aus, dass die untersuchte Datei einen Virus beinhaltet (Seite 155, Abschnitt 4.3.2, erster Absatz). *TbScan* erzeugt für Pro-

grammdateien Listen solcher *heuristic flags*, die für verdächtige Computeroperationen stehen. Die Listen können während der Analyse sowohl an einem Computerbildschirm ausgegeben als auch in eine Logdatei geschrieben werden (Seiten 73, 74, siehe „scanning window“ und „Notice the following example“, siehe „heuristic flags“; Seite 155, oben, siehe z. B. „FILE4.EXE scanning … FRALM# …“; Seite 60, siehe „Output to logfile“; Seite 61, siehe „Append to existing log“). Der Fachmann liest an dieser Stelle mit, dass die während eines Scanvorgangs – also zur Laufzeit von *TbScan* und *TbScanX* – erkannten verdächtigen Computeroperationen bzw. deren *flags* inklusive Trefferanzahl zumindest temporär in geeigneten (idealerweise dynamischen) Datenstrukturen als Listen gespeichert werden müssen, um sie einer anschließenden Auswertung zuführen zu können.

Die Druckschrift **K4** lehrt nach allem eine Prüfung auf Einhaltung einer Sicherheitsrichtlinie, die auf der Durchführung eines Tests beruht, welcher die Erzeugung von Listen mit verdächtigen Computeroperationen in Gestalt von *heuristic flags*, die Ermittlung von deren *scores* und als Virenkriterium die erreichten *scores* relativ zu einem vordefinierten Grenzwert vorsieht. Die Merkmale **M4a** und **M4b** sind daher in der Druckschrift **K4** offenbart.

**7.1.3** Der Gegenstand des Patentanspruchs 1 nach **Hauptantrag** ist durch den aus den Druckschriften **K9** und **K4** bekannten Stand der Technik nahegelegt und beruht daher nicht auf erfinderischer Tätigkeit.

Da der Fachmann angesichts wachsender Bedrohung durch Schadprogramme stets bestrebt ist, Sicherheitslücken in Computernetzwerken zu schließen, hatte er ausgehend von der Lösung der Druckschrift **K9** die Veranlassung, überall dort nach weiteren Maßnahmen zur Verbesserung der Informationssicherheit zu suchen, wo effektive Virenschutzprogramme entwickelt, getestet und angewandt werden. Hierbei konnte er auf das Benutzerhandbuch **K4** stoßen, das die Handhabung der Anti-Virensoftware *ThunderBYTE (TBAV)* beschreibt und ähnlich wie Druckschrift **K9** eine proaktive/heuristische Methode zur Entdeckung von Viren

lehrt. Im Vergleich hierzu erweist sich die auf dem Emulationspuffer mit zyklischer Redundanzprüfung (CRC) basierende Methode der Druckschrift **K9** als ressourcenintensiver, weil für die Analyse eine virtuelle Umgebung erforderlich ist.
Dem Fachmann bot es sich daher an, zur weiteren Erhöhung der Sicherheit in einem Computernetzwerk das aus der Druckschrift **K9** bekannte Verfahren bzw. System dahingehend zu erweitern, dass die wenig performante und ressourcenintensive Emulation zusätzlich mit einem Signaturenscanner und einem heuristischen Scanner nach dem Vorbild des speicherresidenten Programms *TbScanX* aus Druckschrift **K4** kombiniert wird (vgl. K4 Seite 1, letzter Absatz), welches sich insbesondere durch hohe Geschwindigkeit und überdurchschnittliche Erkennungsraten bei der Entdeckung von Viren auszeichnet (vgl. Anlagenkonvolut VP17, Virus Bulletin Januar 1996, Seite 19, linke Spalte, oben; vgl. K4 Seite 47, Mitte) und darüber hinaus Schadprogramme bereits beim Herunterladen erkennt.

Durch die geschilderten Überlegungen konnte der Fachmann zum Gegenstand des Patentanspruchs 1 nach **Hauptantrag** gelangen, ohne dabei erfinderisch tätig zu werden.

**7.1.4** Die Beklagte führt aus, dass schon alleine vom sprachlichen Verständnis heraus der Begriff *Downloadable security profile* so auszulegen sei, dass das DSP nicht sämtliche Computeroperationen eines Downloadables umfasse, sondern lediglich auf die *verdächtigen Computeroperationen* beschränkt sei.
Aus den Absätzen [0040] und [0041] sowie der Figur 7 des Streitpatents werde klar, dass bei der Erstellung des DSPs nicht beabsichtigt sei, alle Operationen eines Downloadables in die Liste von verdächtigen Operationen aufzunehmen, sondern Operationen in dem Downloadable, die als verdächtig angesehen würden. Die verdächtigen Computeroperationen seien eine Untermenge aller Computeroperationen. So werde in Schritt 715 der Figur 7 überprüft, ob eine Operation verdächtig sei. Nur falls dies zutreffe, werde eine solche Computeroperation in ein Downloadable Sicherheitsprofil aufgenommen. Allerdings könne ein DSP

zusätzlich zur Liste mit verdächtigen Computeroperationen auch andere Informationen enthalten, z. B. eine Liste von allen Dateien, auf die durch den Downloadable-Code zugegriffen werde (Streitpatent, Absatz [0022]). Eine solche DSP sei weder aus Druckschrift **K9** noch **K4** bekannt.

Dem Einwand der Beklagten kann nicht gefolgt werden. Die Beschränkung einer DSP auf eine Liste, die nur verdächtige Computeroperationen beinhaltet, wird durch den breit formulierten Anspruchswortlaut nicht gestützt; denn „ein Ausführungsbeispiel erlaubt regelmäßig keine einschränkende Auslegung eines die Erfindung allgemein kennzeichnenden Patentanspruchs“ (BGH, GRUR 2004, 1023 - Bodenseitige Vereinzelungseinrichtung). Somit fallen unter die anspruchsgemäße *list of suspicious computer operations* auch solche Listen, die neben verdächtigen auch nicht-verdächtige Computeroperationen mit umfassen.
Listen mit verdächtigen Computeroperationen treten bei der heuristischen Analyse der Druckschrift **K4** sowohl bei der Ausgabe der *heuristic flags* als auch bei deren temporärer Speicherung in Datenstrukturen auf (siehe oben).

**7.1.5** Die Beklagte argumentiert, dass es sich bei den im Patentanspruch 1 verwendeten *Computeroperationen* um „higher level“ Operationen und nicht etwa um Instruktionen auf niedriger Codeebene handle. Sie beruft sich dabei auf die in Absatz [0023] des Streitpatents aufgezählten Operationen, die keine „lower level“ Codeinstruktionen sondern „higher level“ Operationen seien. Außerdem verweist sie auf eine Entscheidung des PTAB (Patent Trial and Appeal Board) in Bezug auf das Patent US 8 677 494 B2, einem Familienmitglied des Streitpatents, wo zwischen einer Computeroperation, die sich aus der Ausführung von als möglicherweise feindlich geltenden Instruktionen ergeben könne, und der Instruktion selbst unterschieden werde. Die Druckschrift **K4** befasse sich allenfalls mit der Analyse von „lower level“ Codeinstruktionen und nicht etwa mit Computeroperationen.

Der Vortrag der Beklagten ist nicht überzeugend. Weder ist Patentanspruch 1 auf „higher level“ Operationen eingeschränkt, noch kann der Begriff der Be-

schreibung des Streitpatents unmittelbar entnommen werden. Vielmehr umfasst der Begriff „*Computeroperation“* sämtliche Vorgänge, die auf einem Computer ausgeführt werden und nach festgelegten Regeln aus gegebenen Operanden Resultate erzeugen. Ein solcher Vorgang beruht auf einer Sequenz von Instruktionen bzw. Befehlen, die elementare Operationen, deren Operanden und die Abfolge der Verarbeitung festlegen. Ein Befehlscode stellt dabei eine Gruppe von Bits dar, die den Computer anweisen, einen bestimmten Teil des Vorgangs auszuführen. Dieses Verständnis des Begriffs „*Computeroperation“* steht auch mit der Beschreibung des Streitpatents in Einklang. So weist ein Downloadable als ausführbare Programmdatei üblicherweise Maschinen- bzw. Binärcode auf, der wiederum Instruktionen auf Prozessorebene, d. h. „lower level instructions“ beinhaltet. Der Maschinencode wird streitpatentgemäß von einem Scanner zerlegt, und der zerlegte Code wird dann in ein DSP geschrieben (vgl. Streitpatent, Absatz [0022]). In der Druckschrift **K4** finden sich *verdächtige Computeroperationen* u. a. in der Beschreibung der *heuristic flags* (Seite 180 ff., siehe z. B. *F-Suspicious file access* auf Seite 182).

**7.1.6** Die Beklagte argumentiert, dass es sich bei dem speicherresidenten Modul *TbScanX* ausschließlich um einen Signaturenscanner handle, der über keinerlei Heuristik verfüge. Sie verweist dabei auf die Seite 2, dritter Absatz sowie die Seiten 90, 91 (Abschnitt 3.4.4) der Druckschrift **K4**, die belegten, dass *TbScanX* lediglich dazu ausgelegt sei, verdächtige Signaturen aufzuspüren. Hierfür spreche auch der gegenüber dem Modul *TbScan* vergleichsweise geringe Speicherbedarf (siehe Seiten 147, 148, Abschnitt 4.1.1), der darauf hindeute, dass *TbScanX* keine heuristische Analyse für unbekannte Schadprogramme anbiete.

Der Einwand greift nicht durch. So geht aus den oben genannten Textstellen der Seiten 2, 90 und 91 nicht hervor, dass es sich bei *TbScanX* nur um einen Signaturenscanner handelt, der verdächtige Signaturen („suspicious signatures“) erkennt. Vielmehr geht aus Seite 91, letzter Absatz hervor, dass *TbScanX* selbst dann noch Schadprogramme erfasst, wenn gar kein Zugriff auf die Signaturdatei

*TBSCAN.SIG* mehr besteht, was wiederum für die Implementierung einer Heuristik spricht („… If for any reason *TbScanX* cannot access this file, it still detects viruses, …“). Die auf Seite 147 der Druckschrift **K4** angegebenen Unterschiede in den Werten für den jeweiligen Speicherbedarf von *TbScan* und *TbScanX* erklären sich in erster Linie daraus, dass *TbScanX* gewöhnlich nur ein Kilobyte an Arbeitsspeicher ausnutzt und die Option anbietet, erweiterten Speicher zu adressieren, um Daten per Swapping aus dem Arbeitsspeicher auszulagern (Seite 2, dritter Absatz; Seite 148, erster Absatz, siehe „You can swap to EMS und XMS memory.“).
Im Übrigen ist davon auszugehen, dass beim Modul *TbScanX*, das speicherresident im Hintergrund abläuft, auf die Gestaltung einer aufwändigen, speicherlastigen Benutzerschnittstelle, wie sie etwa bei *TbScan* Verwendung findet, weitgehend verzichtet wurde, da sie überflüssig ist.

**7.1.7** Nach allem ergeben sich die Merkmale des Gegenstandes nach dem Patentanspruch 1 gemäß Hauptantrag in naheliegender Weise aus dem in den Druckschriften **K9** und **K4** aufgezeigten Stand der Technik. Dem Gegenstand des erteilten Patentanspruchs 1 fehlt es an der für die Patentfähigkeit erforderlichen erfinderischen Tätigkeit.

**7.2** Mit dem Patentanspruch 1 fällt der gesamte Antrag.

**7.3** Dass die zusätzlichen Merkmale der Unteransprüche zu einer anderen Beurteilung der Patentfähigkeit führen könnten, wurde weder geltend gemacht, noch ist es ersichtlich.

## 8. Zu den Hilfsanträgen 1 bis 14

Das Streitpatent kann in den jeweiligen nach den **Hilfsanträgen 1 bis 14** verteidigten Fassungen keinen Bestand haben, da die jeweiligen Gegenstände ihres Patentanspruchs 1 mangels erfinderischer Tätigkeit nicht patentfähig sind.

**8.1** **Hilfsantrag 1** bleibt ohne Erfolg, weil sein Patentanspruch 1 nichts Zusätzliches enthält, was eine Patentfähigkeit tragen könnte.

Das neu hinzugekommene Merkmal **MX1** konkretisiert, dass beim Durchführen des Tests das Downloadable Sicherheitsprofil DSP mit der Sicherheitsrichtlinie verglichen wird.

Der Vergleich eines Sicherheitsprofils mit einer Sicherheitsrichtlinie geht aber aus Druckschrift **K4** hervor.

So werden in der Lehre der Druckschrift **K4** die in einer Liste angeordneten *heuristic flags* ausgewertet und mit einer Sicherheitsrichtlinie verglichen, die die Summe der Punktzahlen erkannter *flags* im Vergleich zu einem Schwellwert als Kriterium vorsieht (vgl. K4, Seite 155, Abschnitt 4.3.2, erster Absatz). Merkmal **MX1** ist damit in der Lehre der Druckschrift **K4** verwirklicht.

Demnach ist Patentanspruch 1 gemäß Hilfsantrag 1 nicht günstiger zu beurteilen als der erteilte Patentanspruch 1.

Mit dem Patentanspruch 1 fällt der gesamte Antrag.

**8.2** Dem **Hilfsantrag 2** kann nicht stattgegeben werden, weil der Gegenstand seines Patentanspruchs 1 nicht auf erfinderischer Tätigkeit beruht.

Patentanspruch 1 gemäß Hilfsantrag 2 enthält neben den Merkmalen des Patentanspruchs 1 gemäß Hilfsantrag 1 das Merkmal **MY1**, dass das Downloadable Sicherheitsprofil DSP Registry-Operationen *(registry operations)*, also Operationen auf einer Windows-Konfigurationsdatenbank enthält.

Dieses Merkmal kann jedoch das Vorliegen einer erfinderischen Tätigkeit nicht begründen.

Da im Virenscanner *(TBAV)* der Druckschrift **K4** verdächtige Lese- und Schreiboperationen auf Dateien erkannt und in eine Liste geschrieben werden (vgl. K4 Seite 182 *F-Suspicious file access*), werden dementsprechend auch verdächtige Operationen auf der üblicherweise über mehrere Dateien gespeicherten Registrierungsdatenbank erfasst, wenn das betreffende Downloadable solche Vorgänge beinhaltet. Damit ergibt sich Merkmal **MY1** aus der Druckschrift **K4**.

Die Beklagte führt aus, die Software *TBAV* sei nicht in der Lage, verdächtige Computeroperationen auf einer Windows Registrierungsdatenbank zu erkennen. Dementsprechend würden im Benutzerhandbuch **K4** auch keine solchen Instruktionen angesprochen.

Dem kann nicht gefolgt werden.
Bereits aus Seite 86, dritter Absatz geht hervor, dass *TBAV* als Vollversion eines speicherresidenten Virenscanners auch für Windows verfügbar ist. Weiterhin ist auf Seite 122, dritter Absatz offenbart, dass *TBAV* bzw. sein Modul *TbDisk* die 32-Bit Version von Windows unterstützt. In diesem Zusammenhang ist dem Fachmann geläufig, dass die Windows Registry bereits 1992 mit Windows 3.1 auch im Bereich der Consumerbetriebssysteme eingeführt worden ist. Demnach ist die Analyse verdächtiger Computeroperationen auf der Windows Registry durch die Software *TBAV* gewährleistet, da diese dazu ausgelegt ist, mittels Heuristik jedwede Art verdächtiger Schreibzugriffe auf Dateien zu erkennen (Seite 182, *F-Suspicious file access*).

Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 2 beruht somit nicht auf erfinderischer Tätigkeit.

Mit dem Patentanspruch 1 fällt der gesamte Hilfsantrag.

**8.3** Der **Hilfsantrag 3** kann nicht günstiger beurteilt werden, weil das zum Patentanspruch 1 hinzugekommene Merkmal ausgehend von Druckschrift **K9** zumindest nahegelegt ist.

Patentanspruch 1 gemäß Hilfsantrag 3 enthält zusätzlich zu den Merkmalen des Patentanspruchs 1 gemäß Hilfsantrag 2 das Merkmal, dass das Downloadable Sicherheitsprofil DSP Netzwerkoperationen umfasst.

Auch dieses Merkmal kann das Vorliegen einer erfinderischen Tätigkeit nicht begründen.

Bereits die Druckschrift **K9** lehrt eine Überwachung von Programmen bzw. Operationen der *network shell* (vgl. K9, Seite 12, letzter Absatz bis Seite 13, erster Absatz), die bekanntlich das Konfigurieren von lokalen und entfernten Netzwerkeinstellungen ermöglichen und durch die z. B. die IP-Konfiguration geändert werden kann. Hiervon ausgehend war es für den Fachmann zumindest naheliegend, in die aus der Druckschrift **K4** bekannte Liste verdächtiger Computeroperationen neben Operationen auf der Registrierungsdatenbank auch solche Netzwerkoperationen mit aufzunehmen, falls diese beim heuristischen Scanvorgang als schädlich eingestuft werden. Dies gilt umso mehr, als dass bereits in der Lehre der Druckschrift **K4** verdächtige Schreibvorgänge erkannt werden (siehe oben), bei denen es sich z. B. auch um eine unerwünschte Konfiguration von Schnittstellen zu Netzwerken handeln kann.
Merkmal **MY2** ist nach allem ausgehend von Druckschrift **K9** zumindest nahegelegt.

Die Beklagte argumentiert, dass die Lehre der Druckschrift **K9** davon ausgehe, dass Computerviren vornehmlich durch den Austausch von Datenträgern verbreitet würden. Sie verweist dazu auf eine Textstelle der Seite 5, dritter Absatz („The majority of viruses are spread through diskettes.“). Dementsprechend sei die bekannte Lehre auch nicht dazu ausgelegt, Netzwerkoperationen zu analysieren. In Hinblick auf die Druckschrift **K4** führt die Beklagte aus, dass das der Anwendung *TBAV* unterlegte Betriebssystem MS-DOS nicht geeignet sei, Netzwerkoperationen zu überwachen.

Der Einwand greift nicht durch. So erfüllt die Virenfalle der Druckschrift **K9** gerade den Zweck, aus einem Netzwerk heruntergeladene Dateien per Emulation zu untersuchen (Seite 12, zweiter Absatz u. a.). Folgerichtig finden u. a. auch Computeroperationen aus der *network shell*, also Netzwerkoperationen in der Virenanalyse Berücksichtigung (Seite 12, letzter Absatz bis Seite 13, erster Absatz). Ferner geht aus dem Benutzerhandbuch **K4** hervor, dass die Module *TbScan* und *TbScanX* nicht nur das Betriebssystem Windows unterstützen (u. a. Seite 181, *w-Windows or OS/2 header*) sondern auch netzwerktauglich sind (u. a. Seite 186, vorletzter Absatz, siehe „Problem: You are running a network …“) und damit grundsätzlich in der Lage sind, Computeroperationen zu überwachen, die den Datenaustausch im Netzwerk oder aber die Konfiguration von Netzwerkschnittstellen betreffen.

Da Merkmal **MY2** aus dem aufgezeigten Stand der Technik ableitbar ist und damit auch der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 3 nicht auf erfinderischer Tätigkeit beruht, fällt der gesamte Hilfsantrag.

**8.4 Hilfsantrag 4** bleibt ohne Erfolg, weil sein Patentanspruch 1 nichts Zusätzliches enthält, was eine Patentfähigkeit tragen könnte.

Patentanspruch 1 gemäß Hilfsantrag 4 enthält neben den Merkmalen des Patentanspruchs 1 gemäß Hilfsantrag 3 das Merkmal, dass das Downloadable Sicherheitsprofil DSP Datei- und Betriebssystem-Operationen umfasst.

Das neue Merkmal kann die Patentfähigkeit der Lehre nach Patentanspruch 1 gemäß Hilfsantrag 4 nicht begründen.

So ergeben sich Dateioperationen *(file operations)* und Betriebssystemaufrufe *(operating system operations)* i. S. d. Merkmals **MY3** direkt aus der Aufzählung der *heuristic flags* im Benutzerhandbuch **K4** (Seite 182, *F – Suspicious file access;* Seite 184, *U-Undocumented system call*).

Unter Berücksichtigung der Ausführungen zu Hilfsantrag 2 und 3 ist Merkmal **MY3** somit zumindest nahegelegt. Mit Rücksicht auf den den Druckschriften **K9** und **K4** entnehmbaren Stand der Technik beruht die Lehre nach Patentanspruch 1 gemäß Hilfsantrag 4 nicht auf erfinderischer Tätigkeit.

Mit dem Patentanspruch 1 fällt der gesamte Antrag.

**8.5** **Hilfsantrag 5** ist nicht günstiger zu beurteilen, da der Gegenstand seines Patentanspruchs 1 nicht auf erfinderischer Tätigkeit beruht.

Gemäß **Hilfsantrag 5** wird der Patentanspruch 1 gemäß Hauptantrag durch Merkmal **MX2** eingeschränkt. Darin wird präzisiert, dass wenn das DSP des Downloadables bekannt ist, dieses aus einer Datenbank abgerufen wird, welche DSPs von bekannten Downloadables enthält und dass das DSP mit einer Sicherheitsrichtlinie verglichen wird.

Merkmal **MX2** kann eine Patentfähigkeit der Lehre nach Patentanspruch 1 gemäß Hilfsantrag 5 nicht begründen.

Zwar ist das Erhalten eines DSPs aus einer Sicherheitsdatenbank, wenn das DSP des empfangenen Downloadables bekannt ist, aus der Druckschrift **K9** nicht ableitbar.
Allerdings ergibt sich Merkmal **MX2** aus dem Benutzerhandbuch **K4**. Dieses offenbart die Software *TbScan* und deren speicherresidente Variante *TbScanX*, die sowohl über einen schnellen Signaturenscanner als auch einen heuristischen Scanner verfügen (Seite 1, letzter Absatz bis Seite 2, erster Absatz; Seite 47, Abschnitt „Fast Scanning“; Seite 84, Abschnitt „Using *TbScanX*). Als Signaturdatei nutzen sowohl *TbScan* als auch *TbScanX* eine codierte *TBSCAN.SIG* Datei, die im Notfall vom Nutzer aktualisiert werden kann und die als Sicherheitsdatenbank fungiert (Seite 1, letzter Absatz; Seite 91, letzter Absatz). Der Fachmann wird in den in der *TBSCAN.SIG* Datei gespeicherten Signaturen fortlaufende Sequenzen von Bytes erkennen, die für ein bestimmtes Schadprogramm

bzw. schädliches Downloadable normal sind und die nichts anderes als Listen schädlicher Computeroperationen, d. h. DSPs repräsentieren. Nur die in der *TBSCAN.SIG* Datei enthaltenen und bekannt gewordenen Signaturen bzw. DSPs werden von *TbScan* bzw. *TbScanX* nacheinander abgerufen, um sie mit dem Codemuster des jeweils empfangenen Downloadables zu vergleichen. Die Gegenüberstellung selbst stellt die Anwendung einer Sicherheitsrichtlinie dar, die – falls die bekannte Signatur im Downloadable tatsächlich gefunden wird – ggfs. zum Verwerfen des Downloadables führt. Dabei ist unmittelbar klar, dass eine Liste verdächtiger Computeroperationen in Gestalt einer Signatur überhaupt nur dann in einem heruntergeladenen Downloadable ermittelt werden kann, wenn sie zuvor in der Sicherheitsdatenbank *TBSCAN.SIG* hinterlegt und infolgedessen als bekannt ausgewiesen ist bzw. wenn sie sich unter den bereits bekannten DSPs befindet.
Merkmal **MX2** ist sonach in der Lehre der Druckschrift **K4** verwirklicht.

Die Beklagte führt aus, das Benutzerhandbuch **K4** offenbare lediglich Signaturen, die nicht zu einem bestimmten Downloadable gehörten.

Dem kann nicht gefolgt werden. So geht aus Abschnitt 4.5.2 (Seiten 165, 166) hervor, dass eine benutzerdefinierte Signatur, d. h. eine Sequenz schädlicher Computeroperationen mit speziellen Flags (z. B. EXE, COM, INF; vgl. Seite 169, Abschnitt „Using Item Keywords“) und einer Bezeichnung für das jeweilige Schadprogramm versehen wird, aus dem sie gewonnen worden ist (z. B. „TEST VIRUS“, „NEW VIRUS“; vgl. Seite 173 „Haifa.Mozkin“). Mittels des Signaturdatei-Compilers *TbGenSig* werden die Informationen in die Signaturdatei *TBSCAN.SIG* überführt (Seite 165, Abschnitt 4.5.1, fünfter Absatz). Der Fachmann wird somit erkennen, dass die Signaturdatei *TBSCAN.SIG* nicht nur irgendwelche aneinandergereihten Signaturen umfasst, sondern auch über Zuordnungen der jeweiligen Signaturen zu Bezeichnungen für Schadprogramme verfügt, von denen sie eigentlich herrühren bzw. zu denen sie gehören.

Demnach ergibt sich der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 5 in naheliegender Weise aus dem den Druckschriften **K9** und **K4** entnehmbaren Stand der Technik.

Damit hat auch Hilfsantrag 5 keinen Erfolg.

**8.6** Die **Hilfsanträge 6** und **7** sind nicht günstiger zu beurteilen, weil der jeweilige Gegenstand ihres Patentanspruchs 1 mit Rücksicht auf den den Druckschriften **K9** und **K4** entnehmbaren Stand der Technik nahegelegt ist.

In Patentanspruch 1 gemäß Hilfsantrag 6 bzw. 7 wurden die Merkmale des jeweiligen Patentanspruchs 1 gemäß Hilfsantrag 3 und 5 bzw. 4 und 5 miteinander kombiniert.
Patentanspruch 1 gemäß Hilfsantrag 6 bzw. 7 ist nicht günstiger zu beurteilen als Patentanspruch 1 gemäß Hilfsantrag 5. Zur Vermeidung von Wiederholungen sei auf die Ausführungen zu Hilfsantrag 5 und 3 bzw. 4 verwiesen.

**8.7** Dem **Hilfsantrag 8** kann nicht stattgegeben werden, weil die im Patentanspruch 1 neu hinzugekommenen Merkmale eine erfinderische Tätigkeit nicht begründen können.

Patentanspruch 1 gemäß Hilfsantrag 8 enthält neben den Merkmalen des Patentanspruchs 1 gemäß Hilfsantrag 5 noch das Merkmal, wonach das DSP zu einem ACL Komparator weitergeleitet wird, der das DSP mit einer Sicherheitsrichtlinie vergleicht. Außerdem soll die Sicherheitsrichtlinie eine Zugriffssteuerungsliste (*access control list*) umfassen, die Kriterien angibt, wann ein Downloadable den Test besteht oder aber durchfällt. Dabei besteht der Vergleich des DSPs mit der Sicherheitsrichtlinie darin, dass der ACL Komparator das DSP des empfangenen Downloadables mit der Zugriffssteuerungsliste (*access control list*) vergleicht.
Der Fachmann wird aber erkennen, dass der in *TbScan* bzw. *TbScanX* der Druckschrift **K4** enthaltene schnelle Signaturenscanner als Komparator bzw.

Vergleicher i. S. d. Merkmals **MX3** fungiert. Unter Verweis auf die Ausführungen zum Hilfsantrag 5 geht Merkmal **MX3** aus der Druckschrift **K4** hervor.

Merkmal **MZ** bedeutet allenfalls, dass die angewandte Sicherheitsrichtlinie über Regeln verfügt, die darüber entscheiden, wann ein Downloadable einen Test bestanden hat oder aber durchgefallen ist und dass ein DSP des Downloadables gegen diese Regeln verglichen wird. Dies entspricht aber im Wesentlichen dem der Druckschrift **K4** entnehmbaren Vergleich zwischen bekannten Signaturen und dem Codemuster eines empfangenen Downloadables: falls eine der Signaturen im Code des Downloadables auftaucht, wird u. a. angezeigt, um welchen Typ von Schadprogramm es sich dabei handelt (Seite 74 Mitte bis Seite 75 Mitte; Seiten 90, 91 Abschnitt 3.4.4, siehe „TBAV interception“), z. B. einen harmlosen *Joke* oder einen sicherheitskritischen Trojaner *(Trojan)*. Im weiteren Verlauf kann das entdeckte Schadprogramm dann umbenannt oder gelöscht werden (Seite 69, erster und zweiter Absatz).
Die Merkmale **MX3** und **MZ** sind damit aus der Druckschrift **K4** bekannt.

Dem Einwand der Beklagten, Merkmal **MZ** sei nicht auf den Signaturenscanner der Druckschrift **K4** anwendbar, kann nicht gefolgt werden. Der von dem Signaturenscanner durchgeführte Vergleich zwischen der aus der Signaturdatei abgerufenen Signatur und dem Code der zu analysierenden Programmdatei ist immer zugleich verknüpft mit Regeln bzw. Kriterien, nach denen die Datei verworfen oder aber durchgelassen wird. Eine solche Regel ergibt sich im einfachsten Fall bereits daraus, dass wenn eine Signatur an irgendeiner Stelle im Code der Programmdatei ermittelt wird, die betreffende Datei grundsätzlich gelöscht wird. In anderen Fällen reicht es für ein Verwerfen der Programmdatei aus, wenn die Signatur an ganz bestimmten Stellen des Programmcodes (z. B. am Einsprungpunkt „entry-point“) auftritt, die mittels *Position keywords (UATE., ATE., XHD.)* in der Signaturdatei kenntlich gemacht werden (Seiten 170 bis 172, Abschnitt „Position keywords“). In diesem Sinne fungiert die Signaturdatei *TBSCAN.SIG* auch als Zugriffssteuerungsliste bzw. *access control list*, aus der für die jeweilige Sig-

natur Kriterien zur Handhabung der heruntergeladenen Programmdatei abgeleitet werden können.

Nach allem erlauben die hinzugekommenen Merkmale keine Änderung der Beurteilung für den Patentanspruch 1.

Demnach hat auch Hilfsantrag 8 keinen Erfolg.

**8.8** Die **Hilfsanträge 9** und **10** bleiben ohne Erfolg, weil der jeweilige Gegenstand ihres Patentanspruchs 1 durch den den Druckschriften **K9** und **K4** entnehmbaren Stand der Technik nahegelegt ist.

In Patentanspruch 1 gemäß Hilfsantrag 9 bzw. 10 wurden die Merkmale des jeweiligen Patentanspruchs 1 gemäß Hilfsantrag 3 und 8 bzw. 4 und 8 miteinander kombiniert.
Unter Berücksichtigung der Ausführungen zu Hilfsantrag 8 und 3 bzw. 4 ist Patentanspruch 1 gemäß Hilfsantrag 9 bzw. 10 nicht günstiger als Patentanspruch 1 gemäß Hilfsantrag 8 zu beurteilen.

**8.9** Dem **Hilfsantrag 11** kann nicht stattgegeben werden, weil die Einschränkungen gegenüber Hilfsantrag 8 durch den Stand der Technik nahegelegt sind.

Patentanspruch 1 gemäß Hilfsantrag 11 enthält gegenüber Patentanspruch 1 gemäß Hilfsantrag 8 zusätzlich das Merkmal, dass falls das DSP eines empfangenen Downloadables nicht bekannt ist, das Downloadable durch einen Codescanner in ein DSP zerlegt wird und dieses DSP gegen die Sicherheitsrichtlinie verglichen wird.

Die Zerlegung einer ausführbaren Datei in eine Liste verdächtiger Computeroperationen durch einen Codescanner ist aber durch den heuristischen Scanner von *TbScan* bzw. *TbScanX* aus der Druckschrift **K4** gegeben (Seiten 153-155, Abschnitt 4.3.1 u. a.). Eine Liste verdächtiger Computeroperationen ergibt sich hier

als eine Folge von *heuristic flags*, wie sie auf Seite 155 oben oder im Informationsfenster der Seite 73 dargestellt wird. Dass die so erzeugten Listen in einer geeigneten Datenstruktur zumindest zwischengespeichert werden müssen, damit anschließend ein Vergleich mit einer Sicherheitsrichtlinie stattfinden kann, ist aus Sicht des Fachmannes trivial. Ferner ist die Anwendung einer solchen Sicherheitsrichtlinie auf der Seite 155 (Abschnitt 4.3.2) beschrieben. Dass bei kombiniertem Signatur- und heuristischem Scan durch *TbScan* und *TbScanX* (vgl. Seite 1, letzter Absatz – Seite 2, erster Absatz) insbesondere dann eine Zerlegung von ausführbaren Dateien stattfindet, wenn der schnelle Signaturscanner für diese keine Übereinstimmung mit einer der bekannten Virensignaturen gefunden hat, stellt für den Fachmann eine Selbstverständlichkeit dar.
In Hinblick auf Merkmal **MZ** ist anzumerken, dass natürlich auch der heuristische Scanner der Druckschrift **K4** auf Sicherheitsrichtlinien mit entsprechenden Kriterien angewiesen ist, die auf die Liste der verdächtigen Computeroperationen in Gestalt der *heuristic flags* angewendet werden (Seite 155, Abschnitt 4.3.2).
Unter Berücksichtigung der Ausführungen zu Hilfsantrag 8 sind die Merkmale **MX4** und **MZ** in der Lehre der Druckschrift **K4** verwirklicht.

Die Beklagte argumentiert, die anhand der Druckschrift **K4** vorgenommene Auslegung des Downloadable Sicherheitsprofils DSP als Liste von *heuristic flags* einerseits und als Signatur (d. h. als Bytecode einer Instruktionssequenz) andererseits sei in sich widersprüchlich. Vielmehr müsse das anspruchsgemäße DSP einheitlich interpretiert werden.

Dem Einwand ist nicht zuzustimmen, da der Patentanspruch 1 allenfalls fordert, dass das Downloadable Sicherheitsprofil DSP eine (irgendwie geartete) Liste mit verdächtigen Computeroperationen umfasst. Da weder festgelegt wird, welcher Typ von Liste gemeint ist noch auf welche Art die anspruchsgemäßen verdächtigen Computeroperationen repräsentiert sind, umfasst ein DSP sämtliche Datenstrukturen, deren Elemente verdächtige Computeroperationen in irgendeiner Darstellung beinhalten (z. B. als Bytecode, Assemblercode, *heuristic flags* oder Quellcode). Patentanspruch 1 verlangt hierbei nicht, dass es sich bei den be-

kannten DSPs aus der Sicherheitsdatenbank und den aus der Disassemblierung gewonnenen DSPs um ein und dieselben Datenstrukturen handeln muss.

Damit ist auch der Patentanspruch 1 in der Fassung des **Hilfsantrags 11** nicht patentfähig. Mit dem Patentanspruch 1 fällt der gesamte Hilfsantrag.

**8.10 Hilfsantrag 12** bleibt ohne Erfolg, weil sein Patentanspruch 1 nichts Zusätzliches enthält, was eine Patentfähigkeit tragen könnte.

In Patentanspruch 1 gemäß Hilfsantrag 12 wird gegenüber Patentanspruch 1 gemäß Hilfsantrag 11 präzisiert, dass in der Sicherheitsdatenbank *(security database)* Sicherheitsrichtlinien, bekannte Downloadables, bekannte Zertifikate *(certificates)* und DSPs abgelegt sind, welche den bekannten Downloadables entsprechen.

Aus der Druckschrift **K4** geht hervor, dass bekannte Virensignaturen, also DSPs in der *TBSCAN.SIG* Datei hinterlegt sind (Seite 1, letzter Absatz). In der *ANTI-VIR.DAT* Datenbank befinden sich Informationen, die die Integrität von Systemdateien belegen können („fingerprints“) und die somit als Zertifikate fungieren (Seite 20, zweiter Absatz; Seite 33, Abschnitt 3.1.1; Seite 42 erster Absatz; Seite 92, Abschnitt 3.5.1, erster Absatz). Aus dem Format von benutzerdefinierten Signaturen (z. B. Seite 166), die in die Datei *TBSCAN.SIG* importiert werden, wird klar, dass die Signaturdatei *TBSCAN.SIG* auch Bezeichnungen von bekannten schädlichen Downloadables enthält (z. B. NEW VIRUS). Dass auch die jeweiligen Regeln des heuristischen Scanners in einer Datei bzw. einer Datenbank hinterlegt sein müssen, liest der Fachmann u. a. in Abschnitt 4.3.2 der Seite 155 mit. Merkmal **MX5** geht damit aus der Druckschrift **K4** hervor.

Der Einwand der Beklagten, die aus der Druckschrift **K4** bekannte Datei *ANTI-VIR.DAT* habe mit einem Zertifikat nichts zu tun, ist nicht überzeugend. Die Datensätze der Datei *ANTI-VIR.DAT* enthalten Informationen zu jeder ausführbaren Datei eines Verzeichnisses, z. B. Dateigröße und Prüfsumme. In Verbindung mit

dem speicherresidenten Modul *TbCheck* können die in ANTI-VIR.DAT hinterlegten Informationen mit dem tatsächlichen Dateistatus verglichen werden, wodurch Änderungen an Dateien automatisch erfasst werden, einschließlich die von Computerviren verursachten Beschädigungen (Seite 92, Abschnitt 3.5; Seite 20, Abschnitt 1.4.1; Seite 34, zweiter Absatz). Insoweit handelt es sich bei den Einträgen der Datei *ANTI-VIR.DAT* ganz allgemein um digitale Zertifikate bzw. digitale Datensätze, die bestimmte Eigenschaften ausführbarer Dateien (und auf die kommt es an) bestätigen und deren Integrität geprüft werden kann.

Demnach ist auch Merkmal **MX5** aus der Druckschrift **K4** ableitbar, so dass unter Berücksichtigung der Ausführungen zu Hilfsantrag 11 der Gegenstand nach Patentanspruch 1 gemäß Hilfsantrag 12 aus dem aufgezeigten Stand der Technik nahegelegt ist.

Mit dem Patentanspruch 1 fällt der gesamte Hilfsantrag.

**8.11** Die **Hilfsanträge 13** und **14** bleiben ohne Erfolg, weil ihr jeweiliger Patentanspruch 1 nichts Zusätzliches enthält, was eine Patentfähigkeit tragen könnte.

In Patentanspruch 1 gemäß Hilfsantrag 13 bzw. 14 wurden die Merkmale des jeweiligen Patentanspruchs 1 gemäß Hilfsantrag 3 und 12 bzw. 4 und 12 miteinander kombiniert.
Es gelten die Ausführungen zu den Hilfsanträgen 3, 4 und 12. Damit ist auch der Patentanspruch 1 in der jeweiligen Fassung der **Hilfsanträge 13** und **14** nicht patentfähig. Mit dem Patentanspruch 1 fällt jeweils der gesamte Hilfsantrag.

**8.12** Einen eigenen erfinderischen Gehalt der jeweiligen Unteransprüche der **Hilfsanträge 1** bis **14** hat die Beklagte nicht geltend gemacht. Ein solcher ist auch für den Senat nicht erkennbar.

**9.** Das Streitpatent hat demnach weder in der Fassung des Hauptantrags noch in einer der Fassungen der Hilfsanträge 1 bis 14 Bestand.

**II.**

Die Kostenentscheidung beruht auf § 84 Abs. 2 PatG i. V. m. § 91 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 99 Abs. 1 PatG i. V. m. § 709 Satz 1 und 2 ZPO.

**III.**

Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung gemäß § 110 PatG gegeben.

Die Berufungsfrist beträgt einen Monat. Sie beginnt mit der Zustellung des in vollständiger Form abgefassten Urteils, spätestens aber mit dem Ablauf von fünf Monaten nach Verkündung. Die Berufung ist durch einen in der Bundesrepublik Deutschland zugelassenen Rechtsanwalt oder Patentanwalt schriftlich beim Bundesgerichtshof, Herrenstraße 45a, 76133 Karlsruhe, einzulegen.

Die Berufungsschrift muss

- die Bezeichnung des Urteils, gegen das die Berufung gerichtet ist, sowie
- die Erklärung, dass gegen dieses Urteil Berufung eingelegt werde,

enthalten. Mit der Berufungsschrift soll eine Ausfertigung oder beglaubigte Abschrift des angefochtenen Urteils vorgelegt werden.

Guth Hartlieb Dr. Thum-Rung Dr. Forkel Hoffmann

Pr