BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

X ZR 36/19

Verkündet am:
13. April 2021
Zöller
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

ECLI:DE:BGH:2021:130421UXZR36.19.0

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 13. April 2021 durch den Vorsitzenden Richter Dr. Bacher, die Richter Dr. Grabinski, Hoffmann und Dr. Deichfuß sowie die Richterin Dr. Marx

für Recht erkannt:

Auf die Berufung der Beklagten wird das Urteil des 2. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 29. November 2018 abgeändert.

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits hat die Klägerin zu tragen.

Von Rechts wegen

Tatbestand:

1 Die Beklagte ist Inhaberin des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 965 094 (Streitpatents), das am 6. November 1997 angemeldet worden ist und eine US-Priorität vom 8. November 1996 in Anspruch nimmt. Das Streitpatent betrifft ein Verfahren und ein System zum Schutz eines Computers und eines Netzes gegen feindliche herunterladbare Programme. Patentanspruch 1, auf den 26 weitere Ansprüche zurückbezogen sind, lautet in der Verfahrenssprache:

> A method of operating a computer system comprising an internal network security system (110) coupling at least one client computer with an external network (105), the method comprising 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, checking said Downloadables and passing or discarding said Downloadables characterised in that the method includes examining said Downloadables according to a security policy defined by at least one test, 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, determining, by said internal network security system, that said security policy has been violated if the Downloadable fails said test, and 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.

2 Die Klägerin, die wegen Verletzung des Streitpatents gerichtlich in Anspruch genommen wird, hat das Schutzrecht im Umfang der Ansprüche 1, 2, 7 bis 10 und 26 angegriffen und geltend gemacht, der angegriffene Gegenstand gehe über den Inhalt der ursprünglich eingereichten Unterlagen hinaus und sei nicht patentfähig. Die Beklagte hat das Schutzrecht in der erteilten Fassung und hilfsweise in vierzehn geänderten Fassungen verteidigt.

3 Das Patentgericht hat das Streitpatent im beantragten Umfang für nichtig erklärt. Hiergegen richtet sich die Berufung der Beklagten, die das Streitpatent mit ihren erstinstanzlichen Anträgen und einem zusätzlichen Hilfsantrag verteidigt. Die Klägerin tritt dem Rechtsmittel entgegen.

Entscheidungsgründe:

4 I. Die Berufung ist zulässig und hat auch in der Sache Erfolg.

5 1. Das Streitpatent befasst sich mit dem Schutz eines Computers und eines Computernetzes vor Schadprogrammen, die aus dem Internet heruntergeladen werden.

In der Beschreibung des Streitpatents wird ausgeführt, herkömmliche Programme würden als lokale Anwendungen auf einzelnen Computern betrieben. Zum Schutz vor Schadprogrammen sei aus dem US-amerikanischen Patent 5 412 717 (K13) ein System bekannt, bei dem der Benutzer Operationen festlegen könne, die einem Programm erlaubt oder verboten seien. Das untersuchte Programm werde in Quarantäne genommen und laufe zunächst in einem Isolationsmodus ab. Solche bekannten Sicherheitssysteme könnten nur Programme untersuchen, die bereits im Dateisystem des Computers gespeichert seien, nicht aber Scripts und Applets, die ein Webbrowser ohne lokale Speicherung auf einem Computer ausführe (Abs. 2).

6 2. Vor diesem Hintergrund betrifft das Streitpatent das technische Problem, Computer und Netzwerke gegen Schadprogramme zu schützen, die ohne lokale Speicherung ausgeführt werden.

7 3. Zur Lösung dieses Problems schlägt das Streitpatent in Patentanspruch 1 ein Verfahren mit folgenden Merkmalen vor:

8

1	A method of operating a computer system comprising	Verfahren zum Betreiben eines Computersystems,
2	an internal network security system (110) coupling at least one client computer with an external network (105),	mit einem internen Netzsicherheitssystem (110), das mindestens einen Client-Computer mit einem externen Netz (105) koppelt.
3	the method comprising	Das Verfahren umfasst
3a	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,	das Empfangen von an den Client-Computer adressierten ausführbaren Anwendungsprogrammen (602) aus dem externen Netz durch das interne Netzsicherheitssystem,
3b	checking said Downloadables and	das Überprüfen und
3c	passing or discarding said Downloadables;	das Weitergeben oder das Verwerfen dieser Programme;
4	the method includes	das Verfahren umfasst ferner
4a	examining said Downloadables according to a security policy defined by at least one test,	das Untersuchen der Programme anhand einer Sicherheitsrichtlinie, die durch mindestens einen Test definiert ist,
4b	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,	wobei der Test durch das interne Netzsicherheitssystem erfolgt, und zwar - an einem empfangenen Programm, das an den Client-Computer adressiert ist, und - unter Bezugnahme auf ein Sicherheitsprofil für empfangbare Programme (DSP), das eine Liste mit verdächtigen Computeroperationen umfasst, die das Programm nach Aufruf möglicherweise auszuführen versucht,

4c	determining, by said internal network security system, that said security policy has been violated if the Downloadable fails said test, and	die Feststellung durch das interne Netzsicherheitssystem, dass die Sicherheitsrichtlinie verletzt worden ist, wenn das Programm den Test nicht besteht, und
4d	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.	das Verwerfen des Programms und damit das Unterbinden von dessen Weitergabe an den Client-Computer, wenn das interne Netzsicherheitssystem eine solche Verletzung der Sicherheitsrichtlinie feststellt.

9 4. Im Hinblick auf einige Merkmale bedarf der Anspruch der Erläuterung.

10 a) Entgegen der Auffassung der Beklagten und des Patentgerichts muss das interne Netzsicherheitssystem im Sinne von Merkmal 2 auf einem von dem ebenfalls in Merkmal 2 vorgesehenen Client-Computer verschiedenen Gerät angesiedelt sein.

11 aa) Bei dem in der Beschreibung des Streitpatents geschilderten Ausführungsbeispiel ist das Sicherheitssystem als Verbindungsstelle zwischen dem externen und dem internen Netz ausgestaltet. Dies ist in der nachfolgend wiedergegebenen Figur 1 wie folgt dargestellt:

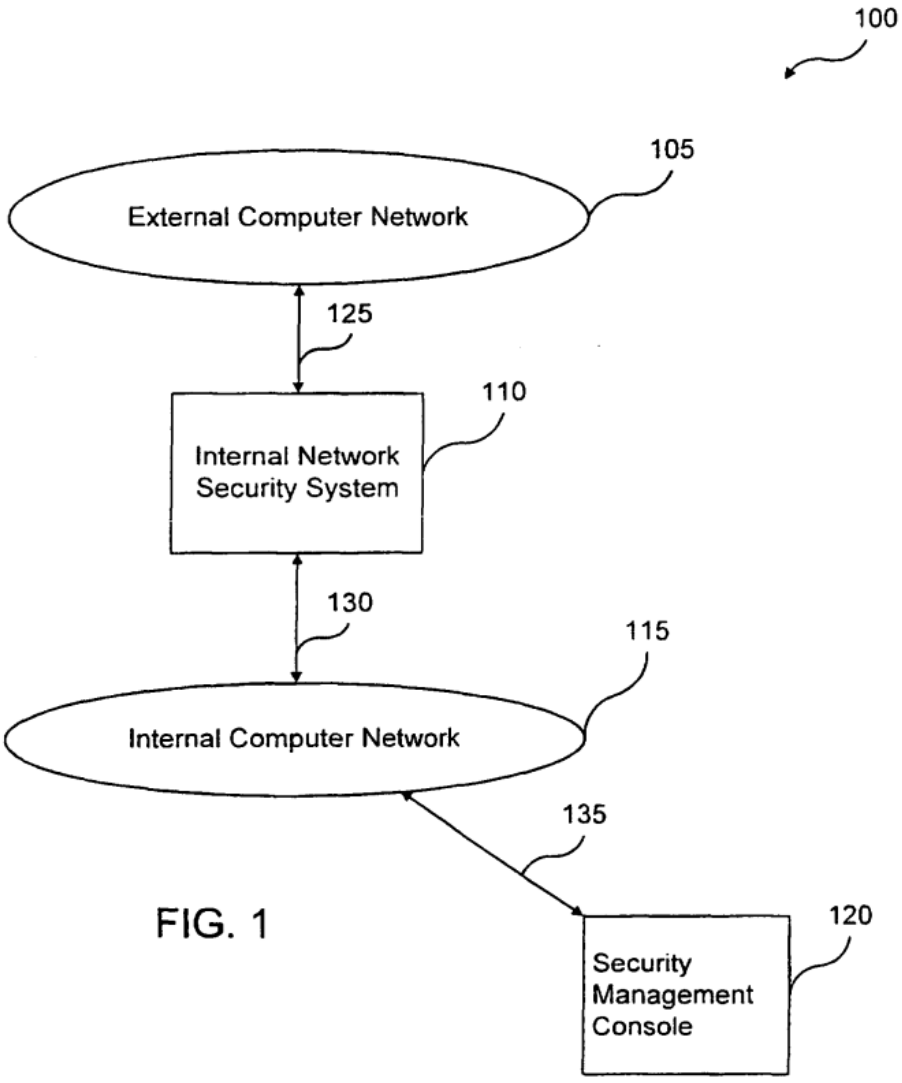


FIG. 1

12 Das Sicherheitssystem (110) ist über einen Kommunikationskanal (125) mit dem externen Netz (105) und über einen Kommunikationskanal (130) mit dem internen Netz (115) verbunden (Abs. 10). Es verhindert, dass verdächtige Programme das interne Netz (115) erreichen (Abs. 11). Ein untersuchtes Programm, das als unbedenklich eingestuft worden ist, wird an den vorgesehenen Empfänger weitergeleitet (Abs. 39 Z. 13-16).

13 bb) Ob die damit beschriebenen Funktionen auch dadurch verwirklicht werden können, dass das Sicherheitssystem als Softwarekomponente in einer isolierten Laufzeitumgebung auf dem Client läuft und nur Programme, die den Test bestehen, an die für den realen Betrieb vorgesehene Laufzeitumgebung

desselben Clients weitergegeben werden, bedarf keiner abschließenden Entscheidung. Selbst wenn dies zu bejahen wäre, fiele eine solche Ausgestaltung nicht unter den Wortsinn von Patentanspruch 1.

14 (1) Patentanspruch 1 sieht vor, dass das Sicherheitssystem ein an den Client-Computer adressiertes Programm aus dem externen Netz empfängt (Merkmal 3a) und dieses nur dann an den Client-Computer weitergibt (Merkmal 3c), wenn es sich beim Test als unbedenklich erwiesen hat (Merkmal 4d).

15 Nach dem Wortlaut dieser Merkmale genügt es nicht, wenn das Testergebnis für die Weitergabe an eine bestimmte Softwarekomponente oder Laufzeitumgebung auf dem Client-Computer maßgeblich ist. Vielmehr muss es für die Weiterleitung des Programms an den Computer selbst ausschlaggebend sein.

16 (2) Dieses Verständnis steht in Einklang mit den oben aufgezeigten Ausführungen in der Beschreibung des Streitpatents, die die in K13 offenbarte Vorgehensweise, ein als schädlich eingestuftes Anwendungsprogramm auf dem Computer, auf dem es ausgeführt werden soll, unter Quarantäne zu stellen, als nicht mehr zeitgemäß bezeichnen.

17 Die Untersuchung eines Programms vor dessen Weiterleitung an den Zielrechner gehört zu den Merkmalen, mit denen sich das Streitpatent von diesem Stand der Technik abgrenzt.

18 (3) Dieser Bedeutungsgehalt steht zudem in Einklang mit dem oben dargestellten Ausführungsbeispiel, bei dem das Sicherheitssystem an einer anderen Stelle der Netzwerkumgebung angesiedelt ist als die zum internen Netzwerk gehörenden Client-Computer.

19 (4) Eine andere Beurteilung ergibt sich nicht daraus, dass es nach Merkmal 2 ausreicht, wenn das Sicherheitssystem einen einzigen Computer mit einem externen Netz koppelt.

20 Auch für diese Konstellation gelten die oben aufgezeigten Vorgaben, wonach ein Programm vor der Weiterleitung an den Zielcomputer zu untersuchen ist.

21 (5) Aus den Ausführungen am Ende der Beschreibung, wonach die Erfindung auch in einem System für den Schutz eines individuellen Computers verwirklicht sein kann und ihre Bestandteile wahlweise durch einen programmierten Universalcomputer, durch anwendungsspezifische integrierte Schaltkreise oder durch ein Netzwerk aus miteinander verbundenen konventionellen Komponenten und Schaltkreisen implementiert werden können (Abs. 43), ergibt sich vor diesem Hintergrund ebenfalls keine abweichende Beurteilung.

22 Dass die Funktion des Systems sich auf den Schutz eines einzelnen Computers beschränken kann, ist im Wortlaut von Merkmal 2 ausdrücklich vorgesehen. Wie bereits oben dargelegt wurde, muss auch in dieser Konstellation die Prüfung erfolgen, bevor das zu untersuchende Programm an den Zielrechner weitergeleitet wird. Bei dieser Ausgangslage ergibt sich auch aus den Ausführungen zu den unterschiedlichen Arten von Hardware, mit denen die Erfindung ausgeführt werden kann, kein hinreichend deutlicher Hinweis darauf, dass diese Hardware mit dem Zielrechner eine Einheit bilden kann.

23 cc) Angesichts dessen kann den Merkmalen 2, 3a, 3c und 4d auch dann kein weitergehender Bedeutungsgehalt beigemessen werden, wenn eine Anordnung des Sicherheitssystems in einer gesicherten Laufzeitumgebung als gleichwirkend anzusehen ist, wie dies das Patentgericht angenommen hat. Eine solche Auslegung fände nur dann eine Stütze in der Beschreibung, wenn dieser Hinweise darauf zu entnehmen wären, dass die Begriffe "Netzsicherheitssystem" und "Client-Computer" lediglich Funktionen beschreiben, nicht aber voneinander getrennte und in unterschiedlichen Bereichen der Netzwerkumgebung angesiedelte Geräte. Solche Hinweise enthält die Beschreibung nicht.

24 Ob eine Ausgestaltung in dem zuletzt genannten Sinne als Verwirklichung mit äquivalenten Mitteln anzusehen wäre, ist für das Nichtigkeitsverfahren nicht von Bedeutung.

25 b) Ein herunterladbares Programm (Downloadable) im Sinne von Merkmal 3a ist eine Software, die nicht schon im Voraus auf dem zur Ausführung bestimmten Computer gespeichert wird, sondern unmittelbar vor der Ausführung aus einem externen Netzwerk angefordert und heruntergeladen wird, typischerweise durch einen Internetbrowser oder eine Web-Engine. Als Beispiele nennt die Streitpatentschrift Java-Applets, JavaScript-Skripte, ActiveX-Steuerelemente und Visual-Basic-Programme (Abs. 4).

26 c) Zentrale Bedeutung kommt dem in Merkmal 4b vorgesehenen Test anhand eines Sicherheitsprofils (downloadable security profile, DSP) zu.

27 aa) Das Sicherheitsprofil umfasst gemäß Merkmal 4b eine Liste mit verdächtigen Computeroperationen, die das untersuchte Programm nach seinem Start möglicherweise auszuführen versucht.

28 Zu Recht ist das Patentgericht zu dem Ergebnis gelangt, dass als verdächtig in diesem Sinne nicht nur solche Operationen anzusehen sind, die zur Verwerfung des Programms führen. Die Liste darf vielmehr auch solche Operationen enthalten, die zwar potentiell schädlich sind, bei einer nachfolgenden Überprüfung aber aufgrund der im jeweiligen Kontext geltenden Sicherheitsvorgaben doch akzeptiert werden.

29 (1) Die Funktion des Sicherheitsprofils besteht nach der Beschreibung des Streitpatents nicht darin, dass ein Eintrag in der Liste zwingend zum Ausschluss des Programms führt. Die Liste mit verdächtigen Programmoperationen

dient vielmehr als Grundlage für einen Abgleich mit Zugangslisten (access control lists, ACL 410), die in der jeweils herangezogenen Sicherheitsrichtlinie (security policy 305) enthalten sind (Abs. 25 Z. 35-43).

30 Hierzu sind in einer Datenbank unterschiedliche Sicherheitsrichtlinien und Regeln zu deren Auswahl hinterlegt. So können zum Beispiel besondere Richtlinien für einzelne Nutzer, Nutzergruppen oder Programme definiert sein (Abs. 18). Je nach den Umständen kann die Zugangsliste etwa vorsehen, dass Programme, die die Operation WRITE ausführen, nicht zugelassen werden. Dann werden Programme zurückgehalten, deren Sicherheitsprofil diese Operation enthält (Abs. 25 Z. 43-47).

31 In Einklang damit sieht die Beschreibung vor, dass in das Sicherheitsprofil alle potentiell feindlichen und schädlichen Computeroperationen aufgenommen werden (Abs. 16). Dies können alle Operationen sein, die unter irgendeinem Gesichtspunkt als potentiell feindlich angesehen werden könnten (Abs. 22 Z. 56 ff.).

32 (2) Merkmal 4b greift diese Funktion auf.

33 Anders als die Beschreibung stellt Merkmal 4b zwar nicht auf potentiell feindliche, sondern nur auf verdächtige Operationen ab. Hieraus ergibt sich aber schon deshalb kein abweichender Sinngehalt, weil die Beschreibung diese Begriffe als Synonyme gebraucht.

34 Darüber hinaus sieht Merkmal 4b vor, dass der Test unter Bezugnahme auf ein Sicherheitsprofil erfolgt. Dies steht in Einklang mit den Ausführungen in der Beschreibung, wonach das Sicherheitsprofil dem Abgleich mit einer vorgegebenen Zugangsliste dient, ein Eintrag im Sicherheitsprofil also nur dann zum Ausschluss des untersuchten Programms führt, wenn er mit den im Einzelfall maßgeblichen Vorgaben nicht vereinbar ist.

35

bb) Merkmal 4b setzt voraus, dass das Sicherheitsprofil erstellt worden ist, ohne das zu untersuchende Programm auf dem Sicherheitssystem (110) oder dem Zielrechner auszuführen.

36 Nach der Beschreibung des Streitpatents sind die Sicherheitsprofile für bereits bekannte Programme im System hinterlegt. Steht ein solches Profil nicht zur Verfügung, wird es mit Hilfe eines Codescanners (325) erstellt. Dieser nutzt bekannte Suchtechniken, um den Programmcode zu zerlegen (Abs. 22 Z. 41-50).

37 Diese Details haben in Patentanspruch 1 zwar keinen Niederschlag gefunden. Die darin definierte Anforderung, wonach das Sicherheitsprofil Operationen auflistet, die das Programm nach Aufruf (if executed) möglicherweise auszuführen versucht, bringt aber zum Ausdruck, dass die Liste schon vor dem Aufruf erstellt worden ist (Abs. 8 Z. 50-56 und Abs. 11 Z. 43-46).

38 cc) Ob als Computeroperationen im Sinne von Merkmal 4b nur Befehle anzusehen sind, die ähnlich wie die in der Beschreibung angeführten Beispiele Read a file, Listen on a Socket, Read a registry item oder Exit Windows auf einer höheren Ebene angesiedelt sind, oder ob auch einzelne Befehle auf der Ebene der Maschinensprache in Betracht kommen, ist für die Entscheidung über den Rechtsbestand des Streitpatents nicht von Bedeutung.

39 II. Das Patentgericht hat seine Entscheidung im Wesentlichen wie folgt begründet:

40 Der Gegenstand von Patentanspruch 1 beruhe ausgehend von der internationalen Anmeldung WO 95/33237 (K9) in Verbindung mit dem Benutzerhandbuch zu der Software ThunderBYTE der ESaSS B.V. (K4) nicht auf erfinderischer Tätigkeit.

41

K9 betreffe ein Verfahren zum Betreiben eines Computerprogramms in einer virtuellen Umgebung, um Dateien auf mögliche Computerviren zu untersuchen und gegebenenfalls zu entfernen, bevor sie auf dem eigentlichen Computersystem aktiv werden könnten. Zwar offenbare K9 kein Sicherheitsprofil mit einer Liste verdächtigter Computeroperationen. Die durchgeführten zyklischen Redundanzprüfungen könnten aber nachweisen, ob bei der Emulation des Programms verdächtigte Computeroperationen stattgefunden hätten.

42 K4 offenbare eine Antivirensoftware mit mehreren Modulen. Ein Modul TbScan sei dazu ausgelegt, an ausführbaren Programmdateien Signaturscans und heuristische Analysen vorzunehmen. Ein speicherresidentes Modul TbScanX untersuche Dateien, während sie aus dem Netzwerk heruntergeladen würden. Die Dateien würden zerlegt und auf verdächtige Computeroperationen untersucht. Hierzu würden Kennzeichnungen (heuristic flags) eingesetzt, denen jeweils eine Punktzahl zugeordnet sei. Wenn die ermittelte Punktzahl einen vordefinierten Grenzwert überschreite, werde das untersuchte Programm als virusbehaftet betrachtet. TbScan erzeuge Listen solcher Kennzeichnungen, die während der Überprüfung am Bildschirm gelesen oder in eine Logdatei geschrieben werden könnten.

43 Der Fachmann, ein Informatiker mit Hochschulabschluss, der über mehrjährige praktische Erfahrung auf dem Gebiet der Sicherheitstechnik für Computer und Computernetzwerke verfüge, sei angesichts wachsender Bedrohung durch Schadprogramme bestrebt gewesen, Sicherheitslücken in Computernetzwerken zu schließen. Daher habe er ausgehend von K9 Anlass gehabt, nach weiteren Maßnahmen zum Virenschutz zu suchen. Zur Erhöhung der Sicherheit in einem Computernetzwerk habe es nahegelegen, die wenig performante und ressourcenintensive Emulation der K9 zusätzlich mit einem Signaturscanner und einem heuristischen Scanner nach dem Vorbild des speicherresidenten Moduls TbScanX der K4 zu kombinieren.

44

Die mit den Hilfsanträgen verteidigten Gegenstände beruhten ebenfalls nicht auf erfinderischer Tätigkeit.

45 III. Diese Beurteilung hält den Angriffen der Berufung in einem entscheidenden Punkt nicht stand.

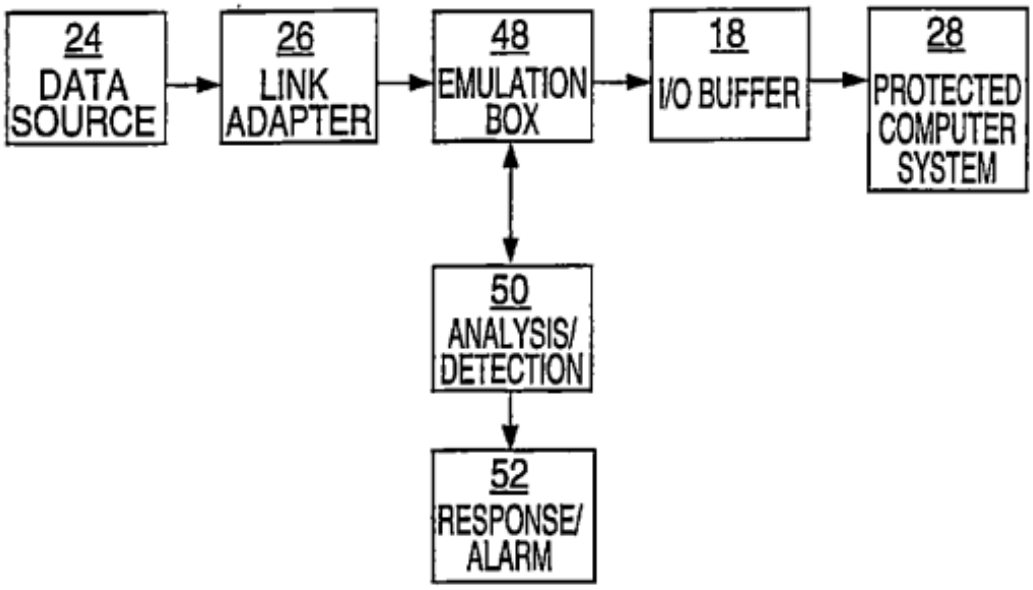
46 1. Zutreffend hat das Patentgericht entschieden, dass der Gegenstand von Patentanspruch 1 in der erteilten Fassung neu ist.

47 a) In K9 sind die Merkmale von Patentanspruch 1 nicht vollständig offenbart.

48 aa) K9 betrifft ein Verfahren und eine Vorrichtung zum Detektieren von Viren.

49 Nach der Beschreibung von K9 bestand die gebräuchlichste Methode zur Erkennung von Computerviren darin, Datenträger auf bekannte Muster zu untersuchen. Dies sei nachteilig, weil die zum Vergleich benötigten Daten ständiger Aktualisierung bedürften. Außerdem müsse das Programm häufig aufgerufen werden, insbesondere dann, wenn Daten über Disketten eingespielt würden. Darüber hinaus bestehe die Gefahr, dass das Programm nicht ordnungsgemäß funktioniere, wenn der Rechner, auf dem es laufe, bereits infiziert sei (S. 3 unten bis S. 4 unten).

50 Zur Lösung schlägt K9 vor, die zu untersuchenden Daten zunächst einem anderen Computer zuzuführen, der mit einem anderen Betriebssystem läuft als der Zielrechner, aber dessen Betriebssystem emuliert. Hierdurch soll ein Virus veranlasst werden, seine Aktivitäten zu entfalten (S. 5 unten bis S. 8 oben). Der Aufbau einer solchen Virenfalle (virus trapping device) ist in der nachfolgend wiedergegebenen Figur 1 schematisch dargestellt.



51 Die Vorrichtung nimmt Daten, die für einen anderen Computer bestimmt sind, über eine oder mehrere Quellen (24) entgegen. Die zu untersuchenden Daten werden in die Emulationsumgebung (48) geladen. Dadurch wird dem Virus der Eindruck vermittelt, er befinde sich auf dem Zielcomputer (S. 6 Abs. 2, S. 9). Er kann seine Aktivitäten innerhalb der Emulationsumgebung frei entfalten, wird aber durch das Betriebssystem der Virenfalle an einem Zugriff auf andere Rechner gehindert (S. 11 Abs. 2).

52 Um unerwünschte Aktivitäten erkennen zu können, werden für alle Dateien in der Emulationsumgebung, für die Tabelle der Unterbrechungsanforderungen (interrupt request table, IRQ table) und für die Dateizuordnungstabelle (file allocation table, FAT) mittels zyklischer Blockprüfung (Cylic Redundancy Check, CRC) Prüfsummen erstellt. Diese werden außerhalb der Emulationsumgebung gespeichert. Danach wird das zu untersuchende Programm gestartet. Wenn es Änderungen an IRQ table, FAT oder anderen kritischen Daten vornimmt, wird es als Virus eingestuft (S. 12 f.). Dann wird ein Alarm ausgelöst (S. 14 oben). Wenn kein Virus entdeckt worden ist, wird das untersuchte Datenpaket für den Zielcomputer freigegeben (S. 14 unten).

53 bb) Damit sind, wie das Patentgericht zutreffend und unangegriffen angenommen hat, die Merkmale 1 bis 4a und das Merkmal 4d offenbart.

54 cc) Ebenfalls zu Recht hat das Patentgericht angenommen, dass ein Sicherheitsprofil im Sinne der Merkmale 4b und 4c in K9 nicht offenbart ist.

55 Der in K9 vorgesehene Vergleich von CRC-Prüfsummen ermöglicht zwar die Feststellung, ob das untersuchte Programm verdächtige Operationen durchgeführt hat. Die als Beispiel angeführten Änderungen an IRQ table, FAT und Dateien sind auch auf einer vergleichbaren Programmierebene angeordnet wie die in der Beschreibung des Streitpatents angeführten Operationen. Solche Operationen können in K9 jedoch nur dadurch festgestellt werden, dass das zu untersuchende Programm in der geschützten Umgebung gestartet wird. Eine Analyse ohne das zu untersuchende Programm auf dem Sicherheitssystem oder dem Zielrechner auszuführen, findet damit nicht statt. Dies ist aus den oben genannten Gründen zur Verwirklichung von Merkmal 4b nicht ausreichend.

56 b) In K4 sind die Merkmale von Patentanspruch 1 ebenfalls nicht vollständig offenbart. Deshalb kann offenbleiben, ob das Handbuch zum Stand der Technik gehört.

57 aa) K4 beschreibt verschiedene Module einer Virenschutzsoftware für Computer mit dem Betriebssystem DOS.

58 (1) Ein als TbScan bezeichnetes Modul dient der Überprüfung von ausführbaren Programmdateien, die auf einem Datenträger gespeichert sind. Hierbei wird ein Signaturscanner eingesetzt, der anhand einer regelmäßig aktualisierten Liste von Signaturen nach bekannten Viren sucht (S. 1).

59 Ergänzend erfolgt eine heuristische Analyse, um auch neue und unbekannte Viren erkennen zu können. Hierzu wird die zu untersuchende Datei disassembliert und auf verdächtige Befehlssequenzen untersucht (S. 154). Das Ergebnis dieser Untersuchung wird mit besonderen Markierungen (heuristic flags)

kenntlich gemacht, die aus einzelnen Buchstaben bestehen. Kleinbuchstaben deuten auf Besonderheiten hin, denen Informationswert zukommt, Großbuchstaben zeigen ernsthaftere Gefahren an (S. 76 unter 3.2.5). Dazu gehören zum Beispiel verdächtige Speicherzuweisungen (S. 181 unter A), direkte Zugriffe auf einen Datenträger (S. 182 unter D) und die Suche nach Dateien mit den Endungen .com oder .exe (S. 184 unter S). Jeder Kennzeichnung ist eine Punktzahl zugeordnet. Übersteigt die Summe der Punktzahlen einen vordefinierten Grenzwert, wird die Datei als virusbehaftet betrachtet (S. 155 unter 4.3.2). Die zugewiesenen Kennzeichnungen können während der Überprüfung am Bildschirm ausgegeben oder in eine Logdatei geschrieben werden (S. 73 f.).

60 (2) Ein Modul namens TbScanX wird als speicherresidente Version von TbScan bezeichnet. Dieser Signaturscanner verbleibe dauerhaft im Speicher und scanne Dateien, die ausgeführt, kopiert, einem Archiv entnommen, heruntergeladen oder in ähnlicher Weise aufgerufen würden (S. 2 Mitte).

61 Damit soll die Sicherheitslücke geschlossen werden, die verbleibt, weil TbScan nur diejenigen Dateien untersuchen kann, die bei der Ausführung dieses Moduls bereits auf der Festplatte gespeichert sind (S. 84 unter 3.4.1). Wenn TbScanX eine verdächtige Signatur entdeckt, gibt das Modul eine Meldung aus (S. 90 unten). Mittels eines beim Aufruf des Moduls einstellbaren Startparameters kann festgelegt werden, dass verdächtige Operationen stattdessen ungefragt unterbunden werden (S. 89: secure). Um den Namen eines Virus auszugeben, benötigt das Modul Zugriff auf die Datei mit den Virensignaturen. Es entdeckt Viren auch dann, wenn diese Datei nicht zugänglich ist; dann zeigt es diese mit dem Zusatz "(Name unknown)" an (S. 91).

62 Der Speicherbedarf von TbScanX wird für den Fall, dass alle Funktionen aktiviert sind und das Modul nach 1.400 Familiensignaturen sucht, mit 30 Kilobyte angegeben (S. 148 oben). Mit Hilfe der Optionen EMS und XMS kann das Modul in den nicht von DOS genutzten Speicherbereich verlagert werden. Dann verbleibt nur ein Kilobyte im DOS-Speicher (S. 148 unten).

63 bb) Damit sind, wie auch die Berufung nicht in Zweifel zieht, die Merkmale 1, 3b, 3c, 4a und 4d offenbart.

64 cc) Entgegen der Auffassung des Patentgerichts ist Merkmal 4b nur für das Modul TbScan offenbart, nicht aber für TbScanX.

65 (1) Entgegen der Auffassung der Klägerin verwirklicht der in K4 für beide Module vorgesehene Signaturscanner das Merkmal 4b nicht.

66 Dabei kann dahingestellt bleiben, ob und unter welchen Voraussetzungen ein Vergleich mit der vom Europäischen Institut für Computer-Antiviren-Forschung (EICAR) entwickelten Testdatei das Merkmal 4b verwirklicht. Aus K4 geht nicht hervor, dass diese Datei herangezogen wird.

67 Eine Suche anhand von vorgegebenen Signaturen, wie sie in K4 offenbart ist, reicht zur Verwirklichung von Merkmal 4b nicht aus, weil der Inhalt der Signatur allein von der in der Datei enthaltenen Zeichenfolge abhängt, nicht aber zwingend davon, welche Befehle oder Operationen diese Zeichenfolge repräsentiert.

68 (2) Demgegenüber ist Merkmal 4b bei der in K4 für das Modul TbScan beschriebenen heuristischen Suche verwirklicht.

69 (a) Auch in diesem Zusammenhang kann offenbleiben, ob als Computeroperationen im Sinne von Merkmal 4b nur solche Befehle angesehen werden können, die auf einer höheren Ebene angeordnet sind. Zumindest die oben beispielhaft angeführten Befehlssequenzen, für die K4 eine Markierung mit einem Großbuchstaben vorsieht, gehören zu einer solchen Ebene.

70 Dem steht nicht entgegen, dass TbScan die zu untersuchende Datei disassembliert, also auf einer vergleichsweise niedrigen Ebene analysiert. Die auf einen Verdacht hinweisenden Kennzeichnungen beziehen sich nicht auf einzelne Befehle auf dieser Ebene, sondern auf Befehlssequenzen, die auf ungewöhnliche Aktivitäten hindeuten. Die hierbei beispielhaft aufgeführten Aktivitäten wie verdächtige Speicherzuweisungen, direkte Zugriffe auf einen Datenträger

oder Suchvorgänge im Hinblick auf Dateien mit den Endungen .com oder .exe sind hinsichtlich ihres Abstraktionsgrads vergleichbar mit den in der Beschreibung des Streitpatents beispielhaft angeführten Operationen wie etwa Read a file, Listen on a Socket, Read a registry item oder Exit Windows.

71 (b) Die in K4 offenbarte Zuordnung von Zahlenwerten und der Vergleich mit einem Höchstwert ist ein Test im Sinne von Merkmal 4b.

72 Diese Maßnahmen führen dazu, dass die vom Modul TbScan ermittelten verdächtigen Operationen zu einer Einordnung als Virus und - bei Aufruf des entsprechenden Startparameters - zum automatischen Blockieren des Programms führen. Dass K4 nicht näher aufzeigt, welche Zahlenwerte den einzelnen Kennzeichnungen zugeordnet sind und welche Schwellenwerte verwendet werden, ist unerheblich, weil auch Patentanspruch 1 insoweit keine näheren Vorgaben enthält.

73 Zutreffend hat das Patentgericht ferner angenommen, dass die in K4 vorgesehene Auswertung und Anzeige der Kennzeichnungen voraussetzt, dass diese zumindest temporär zwischengespeichert werden.

74 (3) Entgegen der Auffassung des Patentgerichts ergibt sich aus K4 jedoch nicht unmittelbar und eindeutig, dass die für TbScan beschriebene heuristische Suche auch bei TbScanX zum Einsatz kommt.

75 Für das vom Patentgericht zugrunde gelegte Verständnis spricht allerdings der in der Einleitung von K4 enthaltene Hinweis, TbScanX sei die speicherresidente Variante von TbScan. Schon im nachfolgenden Satz ist aber von "diesem Signaturenscanner" (this signature scanner) die Rede. Vor diesem Hintergrund lässt sich der Bezeichnung als Variante nicht eindeutig entnehmen, dass der Funktionsumfang der beiden Module identisch ist.

76 Gegen einen identischen Funktionsumfang spricht der von der Berufung angeführte Umstand, dass sich die Listen der Startparameter der beiden Module

unterscheiden und dass in der Liste der Parameter für TbScanX (S. 86 ff. unter 3.4.3) insbesondere diejenigen Parameter aus der Liste für TbScan (S. 62 ff. unter 3.2.3: heuristic, noautohr, expertlog) nicht vorgesehen sind, mit denen bei TbScan das Verhalten der heuristischen Suche beeinflusst werden kann. Damit steht in Einklang, dass bei der Beschreibung der Anzeige eines Prüfergebnisses für TbScan Beispiele mit heuristic flags angeführt werden (S. 155 oben), während für TbScanX nur Meldungen gezeigt werden, aus denen sich ergibt, dass ein bestimmter Virus gefunden wurde (S. 90 f. unter 3.4.4).

77 Bei dieser Ausgangslage lassen sich auch aus den Angaben zum Speicherbedarf keine eindeutigen Schlussfolgerungen ziehen. Zwar mag der geringere Speicherbedarf von TbScanX auch darauf zurückzuführen sein, dass die Benutzeroberfläche weniger umfangreich ist. Diese Schlussfolgerung ist aber nicht zwingend. Ergänzende Angaben, die eine zusätzliche Stütze dafür bilden könnten, sind nicht ersichtlich. Der Umstand, dass als für den Speicherbedarf von TbScan maßgeblicher Faktor nur die Anzahl der eingesetzten Familiensignaturen ausdrücklich angeführt wird, spricht sogar eher gegen diese Deutung.

78 Ebenfalls keine eindeutigen Schlussfolgerungen ergeben sich aus dem Umstand, dass die Erkennung von Viren auch ohne Zugriff auf die Signaturdatei möglich bleibt. Wie die Berufung zu Recht geltend macht, kann diese Funktionalität auch darauf beruhen, dass das Modul die Virensignaturen selbst im Speicher hält und nur die Namen aufgefundener Viren bei Bedarf aus der Datei ausliest. Für diese Deutung zudem spricht der bereits erwähnte Umstand, dass die Zahl der eingesetzten Familiensignaturen ausdrücklich als maßgeblicher Faktor für den Speicherbedarf benannt wird.

79 (4) Für eine Vernehmung des Zeugen Z. besteht kein Anlass.

80 Die in das Wissen des Zeugen gestellte Behauptung, das Modul TbScanX habe am Prioritätstag eine heuristische Suche umfasst, wie sie K4 für das Modul TbScan beschreibt, ist für die Ermittlung des Offenbarungsgehalts von K4 nicht

von Bedeutung. Welcher Offenbarungsgehalt K4 zukommt, hängt nicht davon ab, welche Funktionen die darin beschriebene Software tatsächlich aufgewiesen hat, sondern allein davon, was den schriftlichen Ausführungen in der Entgegenhaltung zu entnehmen ist.

81 Dass die behauptete Funktionalität von TbScanX am Prioritätstag unabhängig von K4 öffentlich bekannt oder durch Benutzung der Software erkennbar war, ergibt sich aus dem Vorbringen der Klägerin nicht.

82 dd) Entgegen der Auffassung der Klägerin ist auch Merkmal 2 nicht offenbart.

83 Die in K4 beschriebene Software läuft auf dem Zielrechner, der vor den gesuchten Viren geschützt werden soll. Wie bereits oben ausgeführt wurde, reicht dies zur Verwirklichung von Merkmal 2 nicht aus.

84 Unabhängig davon ist aus K4 nicht ersichtlich, dass die Module TbScan und TbScanX in einer von den übrigen Programmen isolierten Betriebssystemumgebung laufen, wie dies das Patentgericht für die Verwirklichung von Merkmal 2 als ausreichend angesehen hat.

85 c) In der Veröffentlichung von Swimmer et al. (Dynamic detection and classification of computer viruses using general behaviour patterns, Virus Bulletin Conference 1995, 75, K8) ist der Gegenstand von Patentanspruch 1 ebenfalls nicht vollständig offenbart.

86 aa) K8 offenbart ein Verfahren zur Entdeckung von Computerviren.

87 Als gebräuchlichste Methode zum Erkennen von Viren wird in K8 das Suchen nach bestimmten Mustern bezeichnet. Diese Vorgehensweise werde durch verschlüsselte und polymorphe Viren erschwert. Als neuer Ansatz habe sich die heuristische Suche entwickelt. Diese führe aber zu einer relativ hohen Rate an falsch-positiven Ergebnissen (S. 77 unter 2.2).

88 Als weitere Möglichkeit wird das Beobachten von für Viren typischen Replikationsvorgängen angeführt. Unter dem Betriebssystem DOS sei dies aber nur eingeschränkt möglich, weil DOS keine Prozessisolation zulasse und Viren deshalb die Überwachungsprozesse umgehen könnten. Als Alternative komme die Überprüfung von Dateien mittels Prüfsummen in Betracht. Damit könne aber nicht beurteilt werden, ob eine festgestellte Veränderung durch einen Virus verursacht worden sei (S. 77 f. unter 2.3).

89 Als Alternative schlägt K8 den Einsatz eines Expertensystems vor, mit dem auf der Grundlage von vordefinierten Regeln das Verhalten des zu untersuchenden Programms beurteilt wird (S. 78 ff. unter 3). Hierzu werde ein Überwachungssystem benötigt, das den Virus zuverlässig daran hindere, das System zu kompromittieren. DOS wird hierfür als ungeeignet eingestuft (S. 81 unter 4). Auch ein DOS-Fenster in OS/2 biete keine ausreichende Sicherheit (S. 82 unter 4.2). Deshalb sei ein 8086-Prozessor mit Software emuliert worden. Dies sei sicher, weil der Virus keinen Zugang zum Hostcomputer habe (S. 82 f. unter 4.4). In diese Umgebung sei ein Überwachungssystem integriert worden.

90 Die Aktivitäten des zu untersuchenden Programms in der geschützten Umgebung werden mit Hilfe einer hierfür geeigneten Sprache in Datensätzen (audit records) aufgezeichnet (S. 83 unter 4.5) und anschließend mit Hilfe des Expertensystems ASAX (advanced security audit trail analysis on Unix) analysiert (S. 85 f. unter 5). Die hierzu eingesetzten Regeln betreffen unter anderem die Art und Weise, in der das Programm auf vorhandene Dateien zugreift (S. 79 f. unter 3.2).

91 Als mögliche Anwendungsbereiche des vorgestellten Systems werden der Einsatz als Firewall für Programme, die in ein geschütztes Netzwerk Eingang finden, und die Erkennung von Viren in den DOS-Sitzungen eines künftigen 32-bit-Betriebssystems angeführt (S. 87 unter 6).

92 bb) Damit sind, wie auch die Beklagte nicht in Zweifel zieht, die Merkmale 1 bis 4a sowie die Merkmale 4c und 4d offenbart.

93 cc) Nicht offenbart ist Merkmal 4b.

94 Dabei kann dahingestellt bleiben, ob den Ausführungen in K8, wonach die Aktivitätsdatensätze mit geeigneten Attributen befüllt werden (S. 83 unter 4.5), eindeutig und unmittelbar zu entnehmen ist, dass nur potentiell verdächtigte Operationen aufgezeichnet werden. Wie in K9 wird die Liste der vom Programm ausgeführten Operationen jedenfalls nicht durch Analyse des Programmcodes erstellt, sondern durch Ausführen des Programms in einer geschützten Umgebung.

95 d) Die internationale Anmeldung WO 97/12321 (K7) nimmt den Gegenstand von Patentanspruch 1 ebenfalls nicht vollständig vorweg.

96 aa) Die vor dem Prioritätstag des Streitpatents eingereichte und in dessen Prioritätsintervall veröffentlichte Anmeldung K7 ist gemäß Art. 54 Abs. 3 EPÜ nur für die Neuheitsprüfung relevant.

97 Entgegen der Auffassung der Klägerin, der das Patentgericht in seinem gemäß § 83 Abs. 1 PatG erteilten Hinweis beigetreten ist, nimmt das Streitpatent die Priorität der US-Anmeldung 60/030.639 (K3b) zu Recht in Anspruch.

98 (1) In K3b sind auch solche Systeme als zur Erfindung gehörend offenbart, bei denen nur ein Test anhand eines Sicherheitsprofils zwingend ist und weitere Tests optional sind.

99 Bei dem in K3b geschilderten bevorzugten Ausführungsbeispiel werden zwar zwei Komparatoren eingesetzt, von denen der erste überprüft, ob das zu untersuchende Programm bereits bekannt ist, und der zweite ein Sicherheitsprofil mit einer Richtlinie abgleicht (S. 9 Z. 20 bis S. 11 Z. 5).

100 Wie auch die Klägerin im Ansatz nicht verkennt, betrifft der in K3b formulierte Anspruch 1 aber ein System, bei dem nur der zweite Test durchgeführt wird, während Anspruch 2 beide Tests vorsieht. Daraus wird hinreichend deutlich, dass die einzelnen Tests grundsätzlich beliebig kombinierbar sind.

101 (2) In K3b ist ferner bereits offenbart, dass das Sicherheitsprofil nur dann durch Untersuchung des Programmcodes mittels des Codescanners (325) erstellt wird, wenn das Programm noch nicht bekannt ist, während Programme, die als nicht feindlich erkannt worden sind, zusammen mit dem zugehörigen Sicherheitsprofil direkt an den zweiten Komparator (330) weitergereicht werden (S. 10 Z. 5-13).

102 Dies entspricht den in der Beschreibung des Streitpatents aufgezeigten Möglichkeiten zur Bereitstellung des Sicherheitsprofils.

103 bb) K7 offenbart ein System und ein Verfahren zum Entdecken und Entfernen von Computerviren.

104 Als im Stand der Technik bekannte Methoden zum Entdecken von Viren benennt K7 die Überwachung des Computers auf ungewöhnliche Aktivitäten, das Scannen anhand von Signaturen und das Vergleichen von Prüfsummen (S. 2 Z. 10-24). Als ein Nachteil dieser Methoden wird angeführt, diese könnten nicht auf Dateien angewendet werden, die über ein Gateway in ein Netzwerk eingebracht würden (S. 2 Z. 29-33).

105 Zur Verbesserung wird ein Gateway vorgeschlagen, der Viren entdeckt, bevor sie in das Netzwerk oder aus diesem heraus übermittelt werden (S. 3 Z. 11-29; S. 5 Z. 6-10). Wenn ein Client eine Datei mittels des Protokolls ftp herunterladen will, wird diese Anfrage an einen auf dem Gateway laufenden ftp-Proxy übermittelt. Wenn die Datei ihrem Typ nach Viren enthalten kann, wird sie zunächst zum Proxy übertragen, auf dem Gateway zwischengespeichert und dort auf Viren untersucht (S. 9 Z. 15 bis S. 10 Z. 32). Hierzu können ein üblicher Signaturscanner oder beliebige andere Verfahren eingesetzt werden (S. 10 Z. 32 bis S. 11 Z. 3). Wenn keine Viren erkannt wurden, wird die Datei an den Client weitergeleitet; anderenfalls kann der Proxy auf verschiedene Arten reagieren, zum Beispiel durch Löschen der Datei oder durch Speichern derselben in einem hierfür vorgesehenen Verzeichnis (S. 11 Z. 5-17). Entsprechende Schritte können

auch mit ausgehenden Dateien (S. 12 Z. 1 bis S. 13 Z. 6) und mit E-Mails (S. 13 Z. 7 bis S. 16 Z. 12) ausgeführt werden.

106 cc) Damit sind, wie auch die Beklagte nicht in Zweifel zieht, die Merkmale 1 bis 4a sowie die Merkmale 4c und 4d offenbart.

107 dd) Hingegen ist Merkmal 4b nicht vorweggenommen.

108 (1) Wie auch die Klägerin im Ansatz nicht verkennt, führt K7 als konkretes Beispiel für die Untersuchung auf Viren lediglich einen Signaturenscan an.

109 Wie bereits oben dargelegt wurde, ist dieses Verfahren zur Verwirklichung von Merkmal 4b nicht ausreichend.

110 (2) Aus den ergänzenden Ausführungen in K7, wonach auch jedes beliebige andere Verfahren zum Einsatz gelangen kann, ergibt sich kein unmittelbarer Hinweis auf den Vergleich mit einer Liste von verdächtigen Computeroperationen.

111 Diesen Ausführungen ist zwar zu entnehmen, dass auch eines der anderen im Stand der Technik bekannten Verfahren in Betracht kommt. Wie bereits oben dargelegt wurde, führt K7 insoweit aber nur die Überwachung der Computeraktivitäten und den Vergleich von Prüfsummen an. Um stattdessen oder zusätzlich einen Test anhand einer Liste von verdächtigen Operationen in Betracht zu ziehen, war ein ergänzender Rückgriff auf konkretes Fachwissen erforderlich. Dies reicht für eine unmittelbare Offenbarung nicht aus.

112 2. Entgegen der Auffassung des Patentgerichts war der Gegenstand von Patentanspruch 1 durch den Stand der Technik nicht nahegelegt.

113 a) Aus K4 ergab sich keine Anregung, das in K9 offenbarte Verfahren um die Merkmale 4b und 4c zu ergänzen.

114 aa) Entgegen der Auffassung der Berufung stehen einer diesbezüglichen Anregung allerdings nicht schon die in K4 enthaltenen Erläuterungen zum Startparameter "secure" entgegen.

115 Wie bereits oben dargelegt wurde, bewirkt dieser Parameter beim Modul TbScanX, dass die Entdeckung eines Virus abweichend vom Standardverhalten des Moduls nicht zum Anlass genommen wird, bei Benutzer rückzufragen, ob der Vorgang fortgesetzt oder abgebrochen wird; stattdessen werden verdächtige Operationen unterbunden (S. 89). Eine Übertragung dieses Mechanismus auf das in K9 offenbarte Verfahren führt dazu, dass die untersuchte Datei nicht für den Zielcomputer freigegeben wird. Damit wird die Datei im Sinne von Merkmal 4d verworfen.

116 Dass der gleichnamige Parameter beim Modul TbScan lediglich verhindert, dass die Ausführung des Moduls durch die Tastenkombination Strg-Pause verhindert werden kann (S. 66), führt entgegen der Auffassung der Berufung nicht zu einer abweichenden Beurteilung. Beim Modul TbScan stehen - anders als bei TbScanX - ergänzend die Startparameter "delete" und "kill" zur Verfügung, die zur automatischen Löschung einer als Virus erkannten Datei führen (S. 69). Auch damit wird die Datei im Sinne von Merkmal 4d verworfen.

117 bb) An einer Anregung zur Ergänzung um Merkmal 4b fehlt es indes, weil K4 dieses Merkmal nur für die Untersuchung von Dateien offenbart, die bereits auf einem Datenträger gespeichert sind, nicht aber für die Untersuchung von Dateien, die neu in das System eingespielt werden.

118 Die in K4 nur für das Modul TbScan offenbarte Methode mag aus objektiver Sicht zwar auch für das Einsatzszenario des Moduls TbScanX geeignet sein. Aus K4 ergibt sich aber keine Anregung, von dieser Möglichkeit Gebrauch zu machen. Der Umstand, dass K4 beim Modul TbScanX keine heuristische Suche

erkennen lässt, obwohl dieses Modul als Variante von TbScan bezeichnet wird, spricht eher gegen eine solche Übertragung.

119 cc) Unabhängig davon - und damit auch unabhängig von der Frage, ob K4 für TbScanX eine heuristische Suche offenbart - bestand auch deshalb keine Veranlassung, das in K9 offenbarte Verfahren um eine Prüfung gemäß Merkmal 4b zu ergänzen, weil dies mit einer Abkehr von zentralen Elementen des in K9 gewählten Ansatzes verbunden gewesen wäre.

120 Das in K9 offenbarte Verfahren dient einem ähnlichen Zweck wie die vom Streitpatent vorgeschlagene Untersuchung des Programmcodes. Beide Verfahren geben Aufschluss darüber, welche Operationen das zu untersuchende Programm nach Aufruf voraussichtlich durchführt. K9 sieht als zentrales Mittel zur Erreichung dieses Ziels einen Weg vor, der nach den Feststellungen des Patentgerichts ressourcenintensiv und wenig performant ist. Vor diesem Hintergrund bestand kein Anlass, diese Vorgehensweise durch weitere, auf dasselbe Ziel gerichtete Verfahren zu ergänzen, die ein weiteres Ansteigen des Ressourcenbedarfs und ein weiteres Absinken der Geschwindigkeit erwarten lassen. Eine Ersetzung der in K9 vorgesehenen Emulation durch die in K4 offenbarte Analyse des Programmcodes hätte der Sache nach eine vollständige Abkehr von K9 bedeutet und war ausgehend von dieser Entgegenhaltung erst recht nicht naheliegend.

121 b) Eine weitergehende Anregung ergab sich auch nicht ausgehend von K4.

122 K4 offenbart ein System, das die Untersuchung von im Dateisystem abgelegten und von heruntergeladenen Programmen auf dem Zielrechner ermöglicht, ohne eine isolierte Umgebung einzusetzen. Bei dieser Ausgangslage mag eine vorgelagerte Prüfung vor der Weiterleitung an den Zielrechner, wie sie K9 offenbart, zwar objektiv gesehen zusätzliche Vorteile bieten. Aus K9 ergaben sich aber keine diesbezüglichen Anregungen. Dort wird das vorgelagerte System nicht zur

Analyse des Programmcodes eingesetzt, sondern zur Ausführung des zu untersuchenden Programms in einer gesicherten Umgebung. Um zur Erfindung zu gelangen, hätte der Fachmann mithin gezielt einzelne Aspekte aus K9 übernehmen und diese in einen anderen Funktionszusammenhang übertragen müssen. Hierzu ergibt sich weder aus K4 noch aus K9 eine hinreichende Anregung.

123 c) Aus K8 ergaben sich keine weitergehenden Anregungen.

124 Wie K9 sieht auch diese Entgegenhaltung nicht einen Test anhand einer vor Ausführung des Programms erzeugten Liste mit verdächtigen Operationen vor, sondern eine Ausführung des zu untersuchenden Programms in einer isolierten Umgebung.

125 d) K7 ist aus den bereits oben angeführten Gründen für die Beurteilung der erfinderischen Tätigkeit nicht relevant.

126 IV. Die angefochtene Entscheidung erweist sich nicht aus anderen Gründen als im Ergebnis zutreffend (§ 119 Abs. 1 PatG).

127 1. Aus den sonstigen Entgegenhaltungen ergeben sich keine weitergehenden Anregungen.

128 2. Entgegen der Auffassung der Klägerin geht der Gegenstand von Patentanspruch 1 über den Inhalt der ursprünglich eingereichten Unterlagen, die unter WO 98/21683 A2 (K3a) veröffentlicht sind, nicht hinaus.

129 a) Dass die in K3a in Anspruch 1 verwendete Formulierung "A computer-based method" ersetzt wurde durch die Merkmale 1 und 2, führt nicht zu einer relevanten Abweichung.

130 aa) Schon der ursprünglichen Formulierung ist zu entnehmen, dass es sich um ein Verfahren zum Betreiben eines Computersystems handelt, wie dies Merkmal 1 vorsieht.

131

bb) Dass das Verfahren ein System umfasst, das einen Client-Computer mit einem externen Netz koppelt, ergibt sich, wie die Beklagte zu Recht geltend macht, aus den auf Figur 1 bezogenen Ausführungen in der Beschreibung der Anmeldung (S. 4 Z. 13-20).

132 An dieser Stelle ist zwar nur von einem internen Computer-Netzwerk die Rede. Dass dieses Clients umfasst und das System deren Schutz dient, ergibt sich aber schon aus der Zusammenfassung (S. 2 Z. 12-15). Dass der Client ein Computer sein kann, ergibt sich jedenfalls daraus, dass er in der Lage ist, Java Applets und ähnliche Programme auszuführen.

133 b) Die gegenüber dem in der Anmeldung formulierten Anspruch 1 vorgenommenen Änderungen bezüglich der Merkmale 3 bis 4d sind, wie die Beklagte zutreffend darlegt, ebenfalls ursprünglich offenbart.

134 V. Der Rechtsstreit ist zur Endentscheidung reif (§ 119 Abs. 5 Satz 2 PatG).

135 Das Streitpatent erweist sich aus den oben dargelegten Gründen als rechtsbeständig.

136 VI. Die Kostenentscheidung beruht auf § 121 Abs. 2 Satz 2 PatG und § 91 Abs. 1 ZPO.

Bacher Grabinski Hoffmann

Deichfuß Marx

Vorinstanz:
Bundespatentgericht, Entscheidung vom 29.11.2018 - 2 Ni 53/16 (EP) -