BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Verkündet am
11. Mai 2016
…

5 Ni 29/13 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

betreffend das europäische Patent 1 464 150

(DE 501 08 695)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 11. Mai 2016 durch den Vorsitzenden Richter Voit, die Richterin Martens sowie die Richter Dipl.-Ing. Gottstein, Dipl.-Ing. Univ. Albertshofer und Dipl.-Phys. Univ. Bieringer,

für Recht erkannt:

I. Die Klage wird abgewiesen.

II. Die Klägerin trägt die Kosten des Rechtsstreits.

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

Tatbestand

Die Beklagte ist eingetragene Inhaberin des auch mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland erteilten europäischen Patents 1 464 150 (Streitpatent), das am 13. August 2001 als internationale Anmeldung mit dem Aktenzeichen PCT/EP2001/009328 angemeldet worden ist. Das Streitpatent wird beim Deutschen Patent- und Markenamt unter dem Aktenzeichen 501 08 695.1 geführt. Es trägt die Bezeichnung: „Verfahren, Datenträger, Computersystem und Computerprogrammprodukt zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und –Betreibern“ und umfasst 10 Ansprüche, die alle mit der Nichtigkeitsklage angegriffen sind.

Die erteilten Patentansprüche 1, 7, 9 und 10 sind nebengeordnet, die übrigen Patentansprüche mittelbar oder unmittelbar auf die jeweiligen nebengeordneten Patentansprüche rückbezogen.

Die nebengeordneten Patentansprüche in der erteilten Fassung lauten in der Verfahrenssprache wie folgt:

„1. Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme (2) von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerätes (4), dass ein Computerprogramm enthält, **gekennzeichnet durch** die Verfahrensschritte

- Schutz vor DoS- und DDos-Attacken (Flood-Attacken), wobei,

  - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
  - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und

- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und Benutzer und Umlenkung von Diensteanfragen auf andere Server (2).“

„7. Datenträger, enthaltend ein Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern zum Einsatz in einem in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerät (4), das Computerprogramm **gekennzeichnet durch** die Programmschritte

- Schutz vor DoS- und DDos-Attacken (Flood-Attacken), wobei,

    - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
    - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abge-

schlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und Benutzer und Umlenkung von Diensteanfragen auf andere Server (2).“

„9. Computersystem, dass mit einem Netzwerk, wie Internet (6), Intranet und dergleichen, verbindbar ist, aufweisend einen oder mehrere Computer, die als Server-Computer (2) oder als Client-Computer konfiguriert sind, das Computersystem **dadurch gekennzeichnet**, dass es ein in eine zu schützende Datenleitung (5, 7, 8) zwischen das Netzwerk (6) und den Server- (2) oder Client-Computer enthält geschaltetes elektronisches Gerät (4) enthält, welches mit einem Datenträger versehen ist, der ein Computerprogramm aufweist, das die Programmschritte enthält:

- Schutz vor DoS- und DDos-Attacken (Flood-Attacken), wobei,

    - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und
    - der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden

Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und

- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und
- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und Benutzer und Umlenkung von Diensteanfragen auf andere Server.“

„10. Computerprogrammprodukt, aufweisend Computerproramm-Codes zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerätes (4), dass dieses Computerprogrammprodukt enthält, **gekennzeichnet durch** die Programmschritte

- Schutz vor DoS- und DDos-Attacken (Flood-Attacken), wobei,

    - jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem Syn Ack beantwortet wird, während das registrierte Syn-Paket auf Gültigkeit und die im Zielssystem verfügbaren Dienste geprüft wird und

- der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum von dem von außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und

- Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird, und
- Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und
- Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und
- TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und
- Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und
- Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und
- Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und
- Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und

- Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und Benutzer und Umlenkung von Diensteanfragen auf andere Server.“

Wegen des Wortlauts der Unteransprüche 2 bis 6 und 8 wird auf die Streitpatentschrift (EP 1 464 150 B1) Bezug genommen.

Die Klägerin ist der Ansicht, das Streitpatent sei schon deshalb für nichtig zu erklären, weil es die vermeintliche Erfindung nicht so deutlich und vollständig offenbare, dass ein Fachmann sie ausführen könne (Art. II § 6 Abs. 1 Nr. 2 IntPatÜG i. V. m. Art. 138 Abs. 1 b) EPÜ). Die Gegenstände der nebengeordneten Ansprüche 1, 7, 9 und 10 sowie der Unteransprüche beruhten im Übrigen nicht auf erfinderischer Tätigkeit, da der Fachmann am Anmeldetag ausgehend von der Entgegenhaltung **NK8** (GONCALVES, Marcus und BROWN, Steven A.: Check Point FireWall-1 Administration Guide, New York, McGraw-Hill, 2000 - Part of ISBN 0-07-134229-X) auf naheliegende Weise zu den Gegenständen der Ansprüche gelangen konnte (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 a) EPÜ).

Als weiteren Stand der Technik nennt die Klägerin die Dokumente:

NK5: HUNT, Ray: Internet/Intranet firewall security-policy, architecture and transaction services. In: Computer Communications, Band 21, 1998, Heft 13, S. 1107 bis 1123.

NK6: WO 99/48303 A2

NK9: KENNEY, Malachi: Ping of Death, veröffentlicht am 21. Oktober 1996 online unter http://insecure.org/sploits/ping-o-death.html

NK9a: Ausdruck der Website http://insecure.org/sploits/ping-o-death.html aus dem Internet-Archive (http://web.archive.org) vom 5. Dezember 1998

NK10: McIntyre, Jim: Using PAM to restrict access based on time, veröffentlicht am 12. Oktober 2000 online unter

http://www.techrepublic.com/article/using-pam-to-restrict-access-based-on-time/

NK14: Baker, F.: Request for Comments (RFC) 1812, June 1995

NK15: Ptacek, Thomas H. and Newsham, Timothy N.: Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection, January 1998

NK16: Smart, Matthew et al.: Defeating TCP/IP Stack Fingerprinting, Proceedings of the 9th USENIX Security Symposium, August 14-17, 2000, Denver, Colorado, USA

Die Klägerin überreicht als **NK13** eine Kopie des Urteils vom 29. April 2014 (Landgericht Mannheim Az. 2 O 98/13) aus dem Verletzungsverfahren betreffend das Streitpatent, das die Beklagte gegen ein konzernverbundenes Unternehmen der Klägerin führt.

Die Klägerin beantragt,

> das europäische Patent 1 464 150 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nicht zu erklären.

Die Beklagte beantragt,

> die Klage abzuweisen.

Hilfsweise verteidigt sie das Streitpatent in der Fassung eines Hilfsantrags, vorgelegt als Anlage W&C 18 zum Schriftsatz vom 14. April 2016.

Die Beklagte tritt der Argumentation der Klägerin in allen Punkten entgegen. Sie hält die Erfindung für ausführbar sowie die Gegenstände des Streitpatents für patentfähig, da durch den im Verfahren befindlichen Stand der Technik nicht nahegelegt.

Ihr Vorbringen stützt sie auf die folgenden Dokumente:

W&C1: Presseveröffentlichungen zu DDoS-Angriffen

W&C2: SCHÄFER, G: Sabotageangriffe auf Kommunikationsstrukturen: Angriffstechniken und Abwehrmaßnahmen

W&C3: SPECHT, Stephan M; LEE, Ruby B.: Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures.

W&C4: GOLDFARB, Avi: Why do denial of service attacks reduce future visits? Switching costs vs. changing preference, Februar 2005

W&C5: BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: Empfehlungen zum Schutz vor verteilten Denial of Service-Angriffen im Internet, 2000.

W&C6: RAZMOV, Valentin: Denial of Service Attacks and How to Defend Against Them, Mai 2000

W&C7: LAN, Felix [et al.]: Distributed Denial of Service Attacks

W&C8: KESSLER, Gary C.: Defenses Against Distributed Denial of Service Attacks, November 2000

W&C9: PUPPE, Christph; MAIER, Jörn: Von allen Seiten - Maßnahmen gegen Distributed-Denial-of-Service-Angriffe

W&C10: PENG, Tao [et al.]: Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring

W&C11: BRUTSCHKY, Arne; PROF. DR. IRMSCHER, K.: Intrusion Detection Systems - Problemseminar Mobilität und Sicherheit im Internet. Universität Leipzig, 2003

W&C12: HAGEDORN, Axel: Distributed Denial of Service - Angriffswerkzeuge und Abwehrmöglichkeiten, Fachgebiet Sicherheit in der Informationstechnik - TU Darmstadt, Wintersemester 2002/2003

W&C13: [genannt, aber nicht eingereicht:] Möller/Kelm,: Distributed Denial of Service Angriffe, aus der Zeitschrift „Datenschutz und Datensicherheit“, 2000

W&C14: GRIMMER, Jürgen: "Black Boxes" sollen die Attacken aus dem Netz stoppen, Spiegel Online, 01. August 2001

W&C15: iSecure gegen DDOS-Angriffe: In Computerwelt, 10.08.2001

W&C16: Grundfunktionen iSecure - iSecure-Funktionsweise, Version 0.2 vom 13.02.2014

Zum Wortlaut der hilfsweise verteidigten Anspruchsfassung sowie des Hinweises des Senats nach § 83 PatG vom 25. Januar 2016 wird auf die Gerichtsakte verwiesen.

Entscheidungsgründe

A.

Die zulässige Klage, mit der die Nichtigkeitsgründe der unzureichenden Offenbarung sowie der fehlenden Patentfähigkeit geltend gemacht werden (Art. II § 6 Abs. 1 Nr. 1 und 2 IntPatÜG i. V. m. Art. 138 Abs. 1 a) und 1b) EPÜ), ist nicht begründet und war daher abzuweisen.

I. Zum Gegenstand des Streitpatents

1. Das Streitpatent betrifft ein Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Dienstanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, das ein Computerprogramm aufweist, sowie einen Datenträger, der ein Computerprogramm zur Durchführung dieses Verfahrens enthält. (vgl. Streitpatentschrift, NK2, Abs. [0001]).

In der Streitpatentschrift wird ausgeführt, dass der Anstieg im Bereich des Online-Marketing und eBusiness im gleichen Maße zur Gefahr führe, dass diese Server aus dem Internet angegriffen werden, insbesondere im Wege von durch DoS- und DDoS-Attacken (Denial of Service und Distributed Denial of Service = Verhindern eines Zugriffes oder Nutzens eines Computers bzw. des darauf befindlichen Serviceprozesses). Um die damit verbundenen Schäden zu verhindern, nennt das

Streitpatent zum Stand der Technik einen Artikel von Ray Hunt (NK5), der einen Überblick über bekannte Firewall-Architekturen gebe und die WO 99/48303 (NK6), die ein Verfahren zum Blockieren von unerwünschten Zugriffsattacken auf private Computer-Netzwerke offenbare [vgl. NK2, Abs. [0019] und [0020]).

Vor diesem Hintergrund benennt das Streitpatent es als eine Aufgabe, Mittel zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Dienstanbietern und -betreibern zu schaffen, mit denen DoS- und DDoS-Attacken gezielt erkannt und abgewehrt werden können, um dadurch ein möglichst hohes Maß an Sicherheit und Schutz vor DoS- und DDoS-Attacken zu erzielen und den Computer bzw. das Computersystem dauerhaft stabil und leistungsfähig zu erhalten (vgl. NK2, Abs. [0021] und insbesondere die Ansprüche 1, 7, 9 und 10).

2. Zur Lösung der genannten Aufgabenstellung werden mit den einander nebengeordneten Patentansprüchen 1, 7, 9 und 10 in der erteilten Fassung Gegenstände vorgeschlagen, die sich in folgende Merkmale gliedern lassen:

Patentanspruch 1:

M1	Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme (2) von Netzwerk-Diensteanbietern und –betreibern mittels eines in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerätes (4), dass ein Computerprogramm enthält
	gekennzeichnet durch die Verfahrensschritte
a	Schutz vor DoS- und DDoS-Attacken (Flood-Attacken), wobei
aa-i	jeder IP Syn (IP-Verbindungsaufbauwunsch) registriert und
aa-ii	zur Bewahrung im IP-Protokoll festgelegten Zeitbeschränkung mit einem SynAck beantwortet wird,
aa-iii	während das registrierte Syn-Paket auf Gültigkeit und auf die im Zielsystem verfügbaren Dienste geprüft wird und

bb der Verbindungsaufbau mit dem Zielsystem initialisiert und das empfangene Datenpaket an das Zielsystem zur weiteren Bearbeitung übergeben wird, wenn die Prüfung erfolgreich abgeschlossen ist und zwischenzeitlich der wiederum außen anfragenden System auszusendende Ack sowie ein darauf folgendes gültiges Datenpaket empfangen wurde, und

b Link Level Sicherheit, wobei die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 (Link Level) übernommen wird[sic!], und

c Untersuchung gültiger IP-Header, wobei der Aufbau jedes IP-Paketes vor dessen Weiterleitung auf das Zielsystem auf Gültigkeit überprüft und jedes ungültige IP-Paket verworfen wird, und

d Untersuchung des IP-Paketes durch Überprüfung insbesondere der Länge und der Prüfsumme des IP-Paketes auf Übereinstimmung der Angaben im TCP- oder IP-Header mit dem Aufbau des IP-Paketes, und,

e TCP/IP Fingerprint-Schutz, wobei der als Antwort ausgehende Datenverkehr von den geschützten Systemen zu den von außen anfragenden Systemen neutralisiert wird, indem musterhafte Protokoll-Identifizierer verwendet werden, und

f Sperrung aller UDP-Netzwerkpakete zur Verhinderung von Angriffen auf die geschützten Systeme über das Netzwerkprotokoll UDP, indem über UDP erreichbare benötigte Dienste gezielt registriert und freigegeben werden, wobei Nachrichten explizit für diese UDP-Ports zugelassen werden, die übrigen Ports jedoch geschlossen bleiben, und

g Längenbeschränkungen von ICMP-Paketen, wobei ICMP_Nachrichten nur in einer vorgegebenen Maximallänge als gültige Datenpakete erkannt und hiervon abweichende ICMP-Pakete verworfen werden, und

h Ausschließen bestimmter externer IP-Adressen von der Kommunikation mit dem Zielsystem, und

i Paket-Level-Firewall-Funktion, wobei ein- und ausgehende IP-Pakete mittels frei definierbarer Regeln untersucht und auf Grund dieser Regeln abgelehnt oder an das Zielsystem weitergeleitet werden, und

j Schutz von erreichbaren Diensten des Zielsystems durch Ausschluss bestimmter Dienste und Benutzer und Umlenkung von Diensteanfragen auf andere Server (2).

Patentanspruch 7:

M7 Datenträger, enthaltend ein Computerprogramm zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern zum Einsatz in einem in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerät (4),

das Computerprogramm gekennzeichnet durch die Programmschritte

[a] bis [j] gemäß Patenanspruch 1

Patentanspruch 9:

M9 Computersystem, dass mit einem Netzwerk, wie Internet (6), Intranet und dergleichen, verbindbar ist, aufweisend einen oder mehrere Computer, die als Server-Computer (2) oder als Client-Computer konfiguriert sind, das Computersystem dadurch gekennzeichnet, dass es ein in eine zu schützende Datenleitung (5, 7, 8) zwischen das Netzwerk (6) und den Server- (2) oder Client-Computer enthält geschaltetes elektronisches Gerät (4) enthält, welches mit einem Datenträger ver-

sehen ist, der ein Computerprogramm aufweist, das die Programmschritte enthält:

[a] bis [j] gemäß Patenanspruch 1

Patentanspruch 10:

M10 Computerprogrammprodukt, aufweisend Computerproramm-Codes[sic!] zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Dienste-anbietern und -betreibern mittels eines in ein Computer-Netzwerk (1) einzubindenden elektronischen Gerätes (4), dass dieses Computerprogrammprodukt enthält, gekennzeichnet durch die Programmschritte

[a] bis [j] gemäß Patenanspruch 1

3. Das Streitpatent wendet sich an einen Diplom-Informatiker oder Diplom-Ingenieur der Informationstechnik mit Hochschulabschluss, der auf die Entwicklung von Sicherheitsprodukten im Netzwerkumfeld spezialisiert ist und einschlägige Erfahrung in diesem Bereich aufweist. Diesem Fachmann sind die zum Anmeldezeitpunkt einschlägigen Standards der verwendeten Übertragungsprotokolle bekannt.

Nachdem der Vorsitzende zu Beginn der mündlichen Verhandlung in seiner Einführung in den Sach- und Streitstand die vorläufige Meinung des Senats bekannt gegeben hatte, wonach das Merkmal b die Patentfähigkeit der Gegenstände der erteilten Fassung begründen könne, da weder die NK8 noch der übrige Stand der Technik dieses Merkmal zeigten, beschränkten sich die Erörterungen zwischen und mit den Parteien auf diesen Gesichtspunkt.

Die Verfahrensmerkmale a) bis j) dienen der Erkennung und Abwehr von Angriffen auf Serversysteme. Bei Merkmal b) handelt es sich um ein in sich geschlossenes Merkmal, dessen Auslegung daher unabhängig von den übrigen Merkmalen a) und c) bis j) erfolgen kann.

In seinem Hinweis vom 25. Januar 2016 hatte der Senat bereits ausgeführt, dass unter „Link Level Sicherheit“ gemäß Merkmal b) zu verstehen ist, dass für das Gerät 4 keine eigene IP-Adresse erforderlich ist und deshalb weder ein gezielter Angriff noch ein Ausspähen möglich ist (vgl. Streitpatentschrift Abs. [0029]).

Der Meinung der Klägerin im Schriftsatz vom 14. März 2016 und auch vorgetragen in der mündlichen Verhandlung, dass mit „Link Level Sicherheit“ anspruchsgemäß nur gefordert sei, dass die Daten direkt von der OSI-Schicht-2 entnommen würden und sowohl der Anspruchswortlaut wie auch die Beschreibung eine Auslegung, wie der Senat sie vorgenommen habe, nicht zulasse, kann sich der Senat nicht anschließen.

Bei dem Begriff „Link Level Sicherheit“ handelt es sich – wie beide Parteien in der mündlichen Verhandlung bestätigten – nicht um einen gängigen Fachbegriff, so dass für sein Verständnis auf die Beschreibung des Streitpatents zurückzugreifen ist. Aus Absatz [0029] der Streitpatentschrift ist zwar zunächst zu entnehmen, dass die zu prüfenden Datenpakete direkt von der OSI-Schicht 2 übernommen würden und daher eine eigene IP-Adresse nicht notwendig sei. Soweit die Klägerin ausführt, dass das Entscheidende für die „Link Level Sicherheit“ deshalb die Entnahme der Daten aus der OSI-Schicht 2 sei und sich daraus lediglich die Wirkung ergäbe, dass keine IP-Adresse notwendig sei, so ist dem entgegenzuhalten, dass die Streitpatentschrift im Absatz [0029] weiter ausführt, dass es nicht notwendig sei, aufwändige Umkonfigurationen der bestehenden Netzwerkumgebung bezüglich der logischen Adressierung (IP-Routing) durchzuführen und dass die mit dem Verfahren betriebene Hardware keine adressierbare Netzwerkkomponente bilde, so dass weder ein gezielter Angriff aus dem Netzwerk noch ein Ausspähen möglich sei (vgl. NK2, Abs. [0029]). Dem Streitpatent ist in Absatz [0041] des Weiteren als Besonderheit des geschützten Gegenstandes zu entnehmen, dass das Schutzsystem selbst nicht auf IP-Ebene angegriffen werden könne, da dieses System keine über das IP-Protokoll adressierbare Komponente darstelle und sich damit für aktive Netzwerkkomponenten als völlig unsichtbar darstelle (vgl. NK2, Abs. [0041], Sp. 12, Z. 22 bis 27). Für den Fachmann bedeutet „Link Level Sicherheit“ gemäß Merkmal b) mithin nicht nur, dass für das Gerät 4 keine eigene IP-Ad-

resse erforderlich sei, sondern vielmehr, dass das elektronische Gerät 4 keine eigene IP-Adresse besitzt und mithin nicht adressierbar ist.

Auch der Meinung der Klägerin, wonach das elektronische Gerät 4 unter Verweis auf die Ausführungsbeispiele in Absatz [0046] und [0047] des Streitpatents eine IP-Adresse aufweisen müsse, da es als Router für den Zugriff auf Dienste des Internets verwendet wird (vgl. Abs. [0046], Sp. 14, Z. 2 bis 12) bzw. als integrierter Firewall-Router eingesetzt wird (vgl. Abs. [0047], Sp. 14, Z. 21 bis 27), und obiges Verständnis daher nicht zutreffen könne, kann sich der Senat nicht anschließen.
Gemäß der Figur 1 des Streitpatents ist das elektronische Gerät 4 über eine ISDN-Datenleitung 5 mit dem Internet verbunden und dient dem Schutz vor DoS- und DDoS-Attacken. Es besitzt eine erweiterte Funktionalität als Internet-Gateway über ISDN und ist mit einem Ethernet- und einem ISDN-Adapter ausgestattet (vgl. NK2, Abs. [0046], Sp. 14, Z. 2 bis 8). Jeder der mehreren Server-Computer 2, die durch nicht dargestellte Datenleitungen miteinander vernetzt sein können, ist über eine Datenleitung 3 mit dem elektronischen Gerät 4 verbunden (vgl. NK2, Abs. [0045], Sp 13, Z. 49 bis 54). Soweit nun weiter ausgeführt wird, dass das elektronische Gerät als Router für den Zugriff auf Dienste des Internets verwendet wird, so bedeutet dies aus fachmännischer Sicht, dass, falls von einem der Server-Computer 2 eine Kommunikationsanbindung an das externe Netzwerk gewünscht wird, in dem elektronischen Gerät 4 zusätzlich eine Umsetzung eines für die Ethernet-Technologie ausgelegten Netzwerkprotokolls auf das leitungsvermittelte ISDN-Protokoll (z. B. DSS1) durchgeführt wird. Damit handelt es sich für den Fachmann um ein Gateway (in der Telekommunikation auch als Netzübergang bezeichnet), wofür eine IP-Adresse nicht erforderlich ist.

Gleiches gilt für das Ausführungsbeispiel in Absatz [0047], bei dem das elektronische Gerät 4 ebenfalls über eine ISDN/Ethernet-Datenleitung mit dem Internet verbunden ist und in dem Gerät ein nicht sichtbares Firewall-Funktionsmodul integriert ist. Bereits aus der Formulierung „nicht sichtbar“ schließt der Fachmann, dass dieses Gerät keine IP-Adresse aufweist (vgl. NK2, Abs. [0047], Sp. 14, Z. 21 bis 27). Wird im Folgenden in Absatz [0047] von einem Einsatz des Geräts als integrierter Firewall-Router gesprochen, so bedeutet dies aus fachmännischer

Sicht lediglich, dass das Gerät neben der Funktionalität zur Abwehr von Angriffen zusätzlich sowohl die Funktionalität einer Firewall als auch – analog dem Ausführungsbeispiel in Absatz [0046] – die Funktionalität eines Gateways (Netzübergang) aufweist, wofür keine IP-Adresse erforderlich ist. Das elektronische Gerät 4 bildet daher keinen adressierbaren Router.

II. Zu den geltend gemachten Nichtigkeitsgründen

1. Zum Nichtigkeitsgrund der unzureichenden Offenbarung (Art. II § 6 Abs. 1 Nr. 2 IntPatÜG i. V. m. Art. 138 Abs. 1 b) EPÜ).

Die Klägerin hat in der mündlichen Verhandlung vorgetragenen, dass unter der vom Senat vorgenommen Auslegung des Begriffs der „Link Level Sicherheit“ das Streitpatent den Fachmann im Unklaren lasse, wie das „unsichtbare“ elektronische Gerät 4 ohne IP-Adresse

a) Daten bekommen und
b) gesteuert bzw. konfiguriert werden könne.

Aus diesem Grund sei die Erfindung nicht so deutlich und vollständig offenbart sei, dass ein Fachmann sie ausführen könne. Sie ist der Meinung, dass im Hinblick auf eine ausführbare Lehre das elektronische Gerät 4 unter Verweis auf die Ausführungsbeispiele in Absatz [0046] und [0047] des Streitpatents eine IP-Adresse aufweisen müsse. Dieser Meinung kann sich der Senat nicht anschließen.

a) Entsprechend den Figuren 1 bis 3 der Streitpatentschrift ist das elektronische Gerät 4 in die Leitung (5, 7 bzw. 8) zum Internet geschaltet. Es weist hierzu Anschlüsse für Ethernet und ISDN (vgl. NK2, Fig. 1 und 2, Sp. 14, Z. 7 bis 8 , „ […] mit einem Ethernet- und einem ISDN-Adapter ausgestattet“) bzw. zwei Ethernet-Anschlüsse auf (vgl. NK2, Fig. 3, Sp. 14, Z. 57 bis 58, „ist über eine Ethernet-Datenleitung 8 mit dem Internet 6 verbunden […]“). Das Gerät wird dabei aus fachmännischer Sicht über die MAC-Adresse angesprochen und arbeitet wie eine

„Bridge“ oder ein „Switch“ auf der OSI-Schicht 2. Eine IP-Adresse ist bei derartigen Geräten nicht erforderlich.

b) Wie dem Streitpatent in Patentanspruch 5 zu entnehmen ist, können administrative Eingriffe zur Konfiguration und Sicherstellung der uneingeschränkten Funktion des Verfahrens von einer Konsole oder über gesicherte Netzwerk-Verbindungen erfolgen (vgl. NK2, Patentanspruch 5). Neben der direkten Konfiguration über eine Konsole kennt der Fachmann als gesicherte Verbindungen beispielsweise eine serielle Schnittstelle oder Netzwerkprotokolle, die unabhängig von IP-gestützten Netzwerkanschlüssen an dem elektronischen Gerät vorgesehen werden können.

Auch der Meinung der Klägerin in ihrer Klagebegründung, dem Fachmann sei nicht klar, was unter einer „Prüfung des „Syn-Paket[es] auf Gültigkeit und die im Zielsystem verfügbaren Dienste" gemäß Merkmal aa-iii zu verstehen sei, kann der Senat nicht folgen. Der Fachmann versteht hierunter eine Prüfung dahingehend, ob es sich bei dem empfangenen Paket um ein Paket handelt, bei dem tatsächlich ein Syn-Flag gesetzt ist, das nicht bereits Teil einer existierenden Verbindung ist und bei dem es sich daher tatsächlich um eine neue Verbindungsanfrage handelt. Zudem entnimmt er den Figuren 4 bis 8 des Streitpatents, dass dort eine Prüfung erfolgt, ob es sich um ein gültiges IP-Daten-Paket entsprechend dem Standard handelt. Diese Prüfungen werden bei allen eingehenden Datenpaketen bzw. Nachrichten und nicht nur bei der ersten Anfrage mit dem Syn-Befehl durchgeführt (vgl. Fig. 4 bis 8 des Streitpatents und Abs. [0035]). Bei der Prüfung auf die im Zielsystem verfügbaren Dienste wird überprüft, ob ein angefragter Dienst im Zielsystem zur Verfügung steht oder nicht. Diese Prüfung kann aus fachmännischer Sicht entweder durch eine Anfrage an das Zielsystem oder an Hand von im Gerät 4 vorhandenen Informationen erfolgen.

Soweit in der Klageschrift gerügt wird, die Beschreibung enthalte keine Information darüber, was unter einem „musterhaften" Protokoll-Identifizierer zu verstehen sei und wie ein solcher realisiert werden könne, sieht der Senat darin keine Stütze für den angeführten Nichtigkeitsgrund. Dem Fachmann ist bekannt, dass mittels eines

TCP/IP Fingerprints eine Erkennung von Betriebssystemen im Netzwerk aus der Ferne möglich ist und dabei die Eigenschaft genutzt wird, dass jedes Betriebssystem seine eigene TCP/IP-Protokollstapel-Implementierung hat, dessen Einstellungen sich im Header von Netzwerkpaketen wiederfinden und die sich von denen anderer Betriebssysteme unterscheiden. Damit ist ihm bekannt, welche Felder im Header der übertragenen Datenpakete Aufschluss auf das verwendete Betriebssystem geben und mittels musterhaften Protokoll-Identifizierer neutralisiert werden müssen (Zum Fachwissen siehe auch NK16, „Defeating TCP/IP Stack Fingerprinting“).

Auch der Auffassung der Klägerin in der Klageschrift, wonach Anspruch 2 im Widerspruch zu Merkmal g des Anspruchs 1 stehe und das Verfahren deshalb nicht ausführbar sei, kann der Senat nicht folgen. Merkmal g des erteilten Patenanspruchs 1 ist unmittelbar und eindeutig zu entnehmen, was unter einer Längenbeschränkung zu verstehen ist. Demnach werden alle ICMP_Nachrichten verworfen, deren Paket-Länge eine vorgegebene Maximallänge übersteigt. Patentanspruch 2 bildet dieses Merkmal derart weiter, dass bei der Längenbegrenzung die ungültige Länge des ICMP-Paketes auf eine zulässige Länge reduziert wird. Danach weist das Daten-Paket eine gültige Länge auf. Dies widerspricht somit auch nicht Patentanspruch 1, da ja jetzt das Daten-Paket eine gültige Länge hat. Insgesamt entnimmt der Fachmann die Lehre, entweder das ungekürzte Paket zu verwerfen (Anspruch 1, Merkmal g), oder das Paket auf eine zulässige Länge zu kürzen und nicht zu verwerfen (Anspruch 2). Es werden mithin nur ICMP_Nachrichten mit einer vorgegebenen maximalen Länge an den Server weitergeleitet.

Aus alledem ergibt sich, dass die Erfindung so deutlich und vollständig offenbart ist, dass ein Fachmann sie ausführen kann.

2. Zum Nichtigkeitsgrund der mangelnden Patentfähigkeit (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 a) EPÜ).

Die von der Klägerin eingeführten Druckschriften sind nicht geeignet, die Patentfähigkeit des Gegenstandes des Streitpatents in Frage zu stellen. Denn ausge-

hend von der jeweiligen Lehre der vorgelegten Druckschriften hat der Fachmann keine Veranlassung oder Anregung, bei einem der dort beschriebenen Gegenstände eine „Link Level Sicherheit“ vorzusehen und somit das Merkmal b) in Verbindung mit den übrigen Merkmalen für die Erkennung und Abwehr von Angriffen auf Serversysteme (2) von Netzwerk-Diensteanbietern und –betreibern zu realisieren.

a) Bei der Druckschrift **NK8** handelt es sich um ein Administrationshandbuch für eine Firewall („Check Point Firewall-1“), welche für den Schutz eines Netzwerkes gegen Angriffe von außen dient. Unter einer Firewall versteht der einschlägige Fachmann ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Sie basiert auf einer Softwarekomponente. Diese überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden, vgl. NK8, Seite 2:

> *„This special technology is a firewall, which protects an internal network from the outside world and only permits those protocols and services allowed in through a corporate security policy.“*

Bei der Firewall gemäß der Druckschrift NK8 handelt es sich mithin um ein Verfahren zur Erkennung und Abwehr von Angriffen auf Serversysteme von Netzwerk-Diensteanbietern und -betreibern mittels eines in ein Computer-Netzwerk einzubindenden elektronischen Gerätes, dass ein Computerprogramm enthält (vgl. NK8, Seite 3, Fig. 1.1). Das **Merkmal M1** geht somit unstrittig aus der Druckschrift NK8 hervor.

Diese aus der Druckschrift NK8 bekannte Firewall-1 kontrolliert den Datenverkehr zwischen Netzwerken und ist zwischen der Schicht 2 und Schicht 3 des OSI-Referenzmodells angeordnet. Durch diese Anordnung werden alle ein- und ausgehenden Datenpakte aller Schnittstellen abgehört und inspiziert. Das Firewall-Modul hat Zugriff auf die „Roh-Daten“ („raw messages“) und kann alle enthaltenen Informationen, insbesondere die Informationen höherer Layer und die Nachrichtentexte

(die Anwendungsdaten) überprüfen. Es überprüft IP-Adressen (IP-Layer), port numbers (TCP-Layer), und alle anderen erforderlichen Informationen, um zu entscheiden, ob ein Datenpaket – entsprechend den Regeln der Regeldatenbank - akzeptiert wird (vgl. NK8, S. 26, zweiter Absatz bis Seite 27, erster Absatz in Verbindung mit Fig. 2.4). Die zu prüfenden Datenpakete werden mithin aus der OSI-Schicht 2 (Link Level) entnommen **(Merkmal b_{teilw})**.

Wie dem Handbuch (NK8) in Kapitel 3 („Installing Firewall-1“) zu entnehmen ist, müssen - bevor die Firewall auf einem Gateway-Computer installiert wird - einige Voraussetzungen sichergestellt werden, beispielsweise dass das Routing und DNS (Domain Name System) korrekt konfiguriert werden (vgl. NK8, S. 54, Unterstreichung hinzugefügt):

> *„Before installing FireWall-1 on a gateway computer, first ensure that a number of preconditions exist (for example, that routing and DNS are correctly configured). Perform the procedures below before beginning the installation process.“*

Weiter ist dem Handbuch zu entnehmen, dass Namen und IP-Adressen des Gateways notiert werden sollen, da diese Informationen für die spätere Sicherheitsstrategie benötigt werden (vgl. NK8, S. 55, zweiter Absatz),

> *„Make a note of the names and IP addresses of all the gateway's interfaces. This information will be required later in defining security policy.“*

und anschließend bestätigt werden soll, dass der Name des Gateways in der Datei „hosts“ (UNIX) bzw. „lmhosts“ (Windows) mit der IP-Adresse des externen Interface des Gateways übereinstimmt (vgl. NK8, S. 55, vierter Absatz):

> *„Confirm that the gateway's name, as given in the hosts (UNIX) and Imhosts (Windows) files, corresponds to the IP address of the gateway's external interface.“*

Gemäß diesen Offenbarungsstellen muss der Gateway-Computer (anders als das elektronische Gerät 4 aus Merkmal 1 des Patentanspruch 1), auf dem die Firewall installiert wird, eine IP-Adresse besitzen. Mithin weist das in der Druckschrift NK8 beschriebene Gerät keine patentgemäße „Link Level-Sicherheit“ auf, und kann somit selbst Ziel eines Angriffes werden (**nicht Merkmal b_{Rest}**).

Der Fachmann kann der Druckschrift NK8 auch keinen Hinweis und keine Anregung entnehmen, das Gateway so zu betreiben, dass es auf die IP-Adresse verzichten könnte. Ganz im Gegenteil wird gezielt darauf hingewiesen, dass das IP-Routing korrekt konfiguriert sein muss (siehe obige Ausführungen). Er würde deshalb - entgegen der Auffassung der Klägerin in der mündlichen Verhandlung - auch die Hinweise aus dem von der Beklagten genannten Stand der Technik, wonach zusätzliche IP-Adressen bei bestimmten Produkten zur Abwehr von Distributed-Denial-of-Service (DDoS) Attacken nicht benötigt würden (vgl. W&C14, S. 1, letzter Absatz, W&C15), bei der Firewall-Lösung nach NK8 gar nicht in Betracht ziehen, da die Druckschrift NK8 den Fachmann durch die geforderte Routing-Eigenschaft des Gateways explizit weg von der Realisierung der „Link Level Sicherheit“ gemäß dem Gegenstand des Streitpatents führt.

Somit ist der Gegenstand des erteilten Patentanspruchs 1 neu gegenüber der Druckschrift NK8 und beruht auch auf einer erfinderischen Tätigkeit.

b) Die übrigen von der Klägerin im Verfahren genannten Druckschriften NK5, NK6, NK9, NK10, NK14, NK15, NK16 liegen weiter ab.

Keine dieser Druckschriften geht auf das Problem der „Link Level Sicherheit“ gemäß Merkmal b) ein und kann daher die Patenfähigkeit der Gegenstände des Streitpatents aus Sicht des Senats auch nicht in Frage stellen. Gegenteiliges hat die Klägerin zu diesen Druckschriften in Bezug auf das Merkmal b) auch nicht vorgetragen.

3. Die nebengeordneten Patentansprüche 7, 9 und 10 weisen ebenfalls das Merkmal b) auf. Es gelten daher für diese Ansprüche die obigen Ausführungen

zum Patentanspruch 1 entsprechend. Auch diese Gegenstände sind somit patentfähig.

4. Da die behaupteten Nichtigkeitsgründe bezüglich der nebengeordneten Ansprüche nicht vorliegen, hat das Streitpatent in seiner erteilten Fassung mitsamt den Unteransprüchen Bestand und die Klage war abzuweisen.

B.

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

C. Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung gegeben.

Die Berufung ist innerhalb eines Monats nach Zustellung des Urteils, spätestens aber mit Ablauf von fünf Monaten nach der Verkündung, durch einen Rechts- oder Patentanwalt als Bevollmächtigten schriftlich beim Bundesgerichtshof, Herrenstr. 45a, 76133 Karlsruhe, einzulegen.

Voit Martens Gottstein Albertshofer Bieringer

Hu