BUNDESPATENTGERICHT

IM NAMEN DES VOLKES

URTEIL

Zugestellt an
Verkündungs Statt am

14.11.2022
…

5 Ni 50/20 (EP)
hinzuverb.
5 Ni 57/21 (EP)

(Aktenzeichen)

In der Patentnichtigkeitssache

…

ECLI:DE:BPatG:2022:141122U5Ni50.20EP.0

betreffend das europäische Patent EP 3 257 202
(DE 60 2015 026 499)

hat der 5. Senat (Nichtigkeitssenat) des Bundespatentgerichts auf Grund der mündlichen Verhandlung vom 1. August 2022 durch den Vorsitzenden Richter Voit und die Richter Dipl.-Geophys. Univ. Dr. Wollny, Dipl.-Phys. Univ. Bieringer, Dr. Meiser und Dr.-Ing. Ball

für Recht erkannt:

I. Das europäische Patent 3 257 202 wird mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland für nichtig erklärt.

II. Die Beklagte trägt die Kosten des Rechtsstreits.

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

T a t b e s t a n d

Die Beklagte ist eingetragene Inhaberin des auch mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland erteilten europäischen Patents 3 257 202 (Streitpatent), das am 25. November 2015 angemeldet wurde und die Priorität einer US-Anmeldung vom 10. Februar 2015 (US 2015 14618967) in Anspruch nimmt. Das Streitpatent wird beim Deutschen Patent- und Markenamt unter dem Aktenzeichen DE 60 2015 026 499.1 geführt und trägt in der Verfahrenssprache die Bezeichnung „Correlating Packets in Communications Networks“ (Deutsch: Korrelierung von Paketen in Kommunikationsnetzen). Es umfasst 15 Patentansprüche, die alle mit den Nichtigkeitsklagen angegriffen sind.

Patentanspruch 1 lautet in der erteilten Fassung in der Verfahrenssprache Englisch wie folgt:

1. A method comprising:

identifying (5, 402), by a computing system, a plurality of packets (P1, P2, P3) received by a network device (122) from a host (114) located in a first network (104);
generating (6, 404), by the computing system, a plurality of log entries (306, 308, 310) corresponding to the plurality of packets received by the network device;
identifying (8, 406), by the computing system, a plurality of packets (P1', P2', P3') transmitted by the network device to a host (108) located in a second network (102);
generating (9, 408), by the computing system, a plurality of log entries (312, 314, 316) corresponding to the plurality of packets transmitted by the network device;
correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and
responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:

generating (30), by the computing system, one or more rules (140) configured to identify packets received from the host located in the first network; and
provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify packets received from the host located in the first network.

In der deutschen Übersetzung gemäß Streitpatentschrift lautet Anspruch 1:

1. Verfahren, umfassend:

Identifizieren (5, 402), durch ein Rechensystem, einer Vielzahl von Paketen (P1, P2, P3), die durch eine Netzwerkvorrichtung (122) von einem Host (114) empfangen werden, der sich in einem ersten Netzwerk (104) befindet;
Erzeugen (6, 404), durch das Rechensystem, einer Vielzahl von Log-Einträgen (306, 308, 310), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden;
Identifizieren (8, 406), durch das Rechensystem, einer Vielzahl von Paketen (P1', P2', P3'), die durch die Netzwerkvorrichtung an einen Host (108) übertragen werden, der sich in einem zweiten Netzwerk (102) befindet;
Erzeugen (9, 408), durch das Rechensystem, einer Vielzahl von Log-Einträgen (312, 314, 316), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden;
Korrelieren (16, 410), durch das Rechensystem und auf Grundlage der Vielzahl von Log-Einträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden und der Vielzahl von Log-Einträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden, der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden mit der Vielzahl von Paketen, die durch die Netzwerkvorrichtung empfangen werden; und
als Reaktion auf das Korrelieren der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden, mit der Vielzahl von Paketen, die durch die Netzwerkvorrichtung empfangen werden:

Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren, die von dem Host empfangen werden,

der sich in dem ersten Netzwerk befindet; und
Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet.

Wegen des Wortlauts des nebengeordneten Patentanspruchs 15 sowie der Unteransprüche 2 bis 14 wird auf die Streitpatentschrift Bezug genommen.

Die Klägerinnen, die wegen Verletzung des Streitpatents in Anspruch genommen werden, machen in ihren Klagen vom 26. November 2020 und vom 29. Oktober 2021 geltend, das Streitpatent sei wegen fehlender Patentfähigkeit in vollem Umfang für nichtig zu erklären. Darüber hinaus sei sein Gegenstand unzulässig erweitert.

Zur unzulässigen Erweiterung des erteilten Anspruchs 1 tragen die Klägerinnen insbesondere vor, der im Prüfungsverfahren vor dem Europäischen Patentamt geänderte Anspruch 1 umfasse Paketfiltervorrichtungen, die mit einer Regel zum Identifizieren von einem Host in einem ersten Netzwerk stammenden Datenpaketen konfiguriert werde, wobei diese Regel auch zu anderen Zwecken verwendet werden könne als zur bloßen Identifikation und ggf. zum Eliminieren von Datenpaketen, weshalb eine in den Ursprungsunterlagen so nicht offenbarte Erweiterung vorliege. Zudem beanspruche Anspruch 1 der erteilten Fassung ein Rechensystem, das in Reaktion auf das Korrelieren von Datenpaketen eine Paketfilterfunktion mit einer Regel zum Identifizieren von Datenpaketen umfasse, wobei die ursprüngliche Offenbarung nur eine Regel zum Identifizieren und Fallenlassen von Datenpaketen in Reaktion auf die Bestimmung bösartiger, von einem Host gesendeter Datenpakete offenbare, nicht aber eine Reaktion auf das Korrelieren.
Zur fehlenden Patentfähigkeit tragen die Klägerinnen insbesondere vor, die Gegenstände der Ansprüche 1 und 15 seien durch die Entgegenhaltungen NK2 und NK 3 neuheitsschädlich vorweggenommen, zudem beruhe Anspruch 1 der erteilten Fassung nicht auf erfinderischer Tätigkeit.
Hierzu stützen sich die Klägerinnen auf folgende Dokumente:

NK2 GB 2 505 288 A
NK3 US 7 995 584 B2
NK4 US 2014 / 0 280 825 A1

NK5 Ingham, K. und Forrest, S.: „A History and Survey of Network Firewalls“, in: The University of New Mexico Computer Science Department Technical Review, 2002-37

NK6 US 2013 / 0 081 102 A1

NK7 US 2012 / 0 218 999 A1

NK8 US 8 219 675 B2

NK9 US 2006 / 0 159 028 A1

NK10 US 2003 / 0 223 367 A1

NK11 US 8 934 487 B2

NK12 US 2014 / 0 280 778 A1

NK13 US 2012 / 0 030 750 A1

NK14 US 8 204 984 B1

NK15 US 2013 / 0 262 655 A1

NK16 WO 2012 / 146 265 A1

NK17 US 2004 / 0 073 655 A1

NK18 US 2014 /0 281 030 A1

Als Reaktion auf den gerichtlichen Hinweis legte die Klägerin zu 2 noch folgende Dokumente zur Stützung des klägerischen Vorbringens vor:

HLNK1 US 8 413 238 B1

HLNK2 Zwicky, E.D., Cooper, S. und Chapman, B.: „Building Internet Firewalls“, 2. Aufl., Juni 2000.

HLNK3-1 „Wireshark“, in: Wikipedia, Fassung vom 18. Dezember 2014

HLNK3-2 YouTube-Video, „Wireshark Tutorial – ACL Generator“, veröffentlicht am 5. Mai 2012

HLNK3-2a Bildschirmfotos der HLNK3-2 zu verschiedenen Zeitpunkten

HLNK3-3 Blogeintrag „NAT Packet Analysis Using Wireshark“, veröffentlicht am 3. Februar 2013

HLNK3-4 YouTube-Video „Multitrace NAT Analysis Using Wireshark“, veröffentlicht am 1. Januar 2013

HLNK3-4a Bildschirmfoto der HLNK3-4 zu dem Zeitindex 2:10

HLNK3-5 Videos gemäß Anlagen HLNK3-2 und HLNK3-4 auf CD

Die Klägerinnen beantragen,

> das europäische Patent 3 257 202 mit Wirkung für das Hoheitsgebiet der Bundesrepublik Deutschland in vollem Umfang für nichtig zu erklären.

Die Beklagte beantragt, die Klage abzuweisen,

> hilfsweise nach Maßgabe der Hilfsanträge 0, 1, 1b, 2, 2b, 2c, 3, 4 und 5.

Wegen des Wortlauts der Hilfsanträge wird auf die Akte verwiesen.

Die Beklagte tritt dem Vorbringen der Klägerinnen in allen Punkten entgegen, hält das Streitpatent in der erteilten Fassung nicht für unzulässig erweitert und den Gegenstand des Streitpatents in der erteilten Fassung, jedenfalls aber in der Fassung eines der Hilfsanträge, für schutzfähig.

Der Senat hat den Parteien einen qualifizierten Hinweis mit Fristen zur Stellungnahme auf den Hinweis und etwaiges Vorbringen der Gegenseite am 25. April 2022 zukommen lassen.

Im Übrigen nehmen die Parteien u. a. noch auf folgende weitere Dokumente Bezug:

NK21 Offenlegungsschrift der PCT-Anmeldung WO 2016/130196 A1

NK25 Wikipedia „Packet analyzer“, Version vom 01.11.2014

NK26 Wikipedia „Intrusion detection system“, Version vom 03.02.2015

MFG1 Security Encyclopedia „Lawful Interception (LI)“, Version vom 07.02.2022

MFG11 Wikipedia „X-Forward-For“, Version vom 08.01.2015

MFG12 Zscaler, „Configuring Proxy Chaining“

Wegen der weiteren Einzelheiten des Sach- und Streitstands wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen, auf das Protokoll der mündlichen Verhandlung sowie den weiteren Akteninhalt Bezug genommen.

E n t s c h e i d u n g s g r ü n d e

A.

Die zulässige Klage ist begründet und hat in der Sache Erfolg, da das Streitpatent mangels Patentfähigkeit für nichtig zu erklären ist.
Denn dem Gegenstand des Streitpatents in der erteilten Fassung – wie auch nach den Hilfsanträgen 1, 1b, 2, 2b, 2c, 3, 4 sowie 5 – steht jeweils der Nichtigkeitsgrund der mangelnden Patentfähigkeit entgegen, Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 Buchst. a) EPÜ i. V. m. Art. 52, 54, 56 EPÜ.
Der Hilfsantrag 0 war nach § 83 Abs. 4 PatG als verspätet zurückzuweisen und deshalb keiner Sachprüfung zu unterziehen.
Darüber hinaus geht der Gegenstand des Streitpatents nach den Hilfsanträgen 2 und 3 über den Inhalt der ursprünglichen Anmeldungsunterlagen in ihrer Fassung hinaus, wie sie bei der zuständigen Behörde ursprünglich eingereicht worden sind, Art. II § 6 Abs. 1 Nr. 3 IntPatÜG i. V. m. Art. 138 Abs. 1 Buchst. c), Art. 123 Abs. 2 EPÜ.

I. Zu Gegenstand und Auslegung des Streitpatents sowie zum Fachmann

1. Das Streitpatent (EP 3 257 202 B1) mit dem Titel „Korrelierung von Paketen in Kommunikationsnetzen“ betrifft die Kommunikation zwischen Endpunkten in

paketvermittelnden Netzwerken, wobei die Kommunikation aus Flüssen bzw. Datenströmen („flows“) zusammengehöriger Pakete bestehe, wobei die Zuordnung eines Pakets zu einem bestimmten Fluss beispielsweise durch die Paket-Header-Informationen bestimmt sei (vgl. Streitpatent, Titel und Abs. [0002]).

In den Kommunikationsnetzwerken zwischen den Endpunkten angeordnete Netzwerk-Geräte bzw. Netzwerkvorrichtungen („network devices“) könnten jedoch möglicherweise die Pakete verändern und so die Zugehörigkeit eines Pakets zu einem bestimmten Fluss verschleiern (vgl. Streitpatent, Abs. [0002], dort: „obfuscate“). Als Beispiele beschreibt das Streitpatent in den Absätzen [0018] bis [0022] flusstransformierende Geräte, NATs („network address translation“), Web-/DNS-/SIP-Proxies, Gateways und bösartige Entitäten („malicious entities“), welche u.a. Teil eines „man-in-the-middle“ Angriffs sein könnten. Darüber hinaus nennt das Streitpatent in den Absätzen [0003] bis [0004] mit den Druckschriften US 2004/0073655 A1 und US 2014/0281030 A1 (ebenfalls als Anlagen NK17 und NK18 von der Klägerin zu 1) eingereicht) einen Stand der Technik zur Netzwerk-Überwachung („network flow monitoring“, „network monitoring“).

In diesem technischen Kontext – Netzwerk-Überwachung bzw. Netzwerk-Sicherheit - bestehe ein Bedarf bzw. stelle sich das Streitpatent die Aufgabe, Datenpakete in Kommunikationsnetzwerken zu korrelieren (vgl. Streitpatent, Abs. [0002]).

Die Offenbarung des Streitpatents zeigt, dass an einem Netzwerk-Gerät die von einem ersten Host in einem ersten Netzwerk empfangenen Pakete mit den an einen zweiten Host in einem zweiten Netzwerk gesendeten Paketen korreliert werden, um so zusammengehörige Datenpakete zu identifizieren und diese - trotz vorhandener Änderungen - einem entsprechenden Fluss zuzuordnen (vgl. Streitpatent, Abs. [0006] - [0007]).

2. Die erteilten Patentansprüche 1 und 15 lassen sich in der maßgeblichen englischen Verfahrenssprache und der deutschen Übersetzung wie folgt gliedern:

Merkmal	Patentanspruch 1 lt. **Streitpatent** in englischer Verfahrenssprache	Deutsche Übersetzung lt. **Streitpatent**
M1	A method comprising:	Verfahren, umfassend:
M2	identifying (5, 402), by a computing system, a plurality of packets (P1, P2, P3) received by a network device (122) from a host (114) located in a first network (104);	Identifizieren (5, 402), durch ein Rechensystem, einer Vielzahl von Paketen (P1, P2, P3), die durch eine Netzwerkvorrichtung (122) von einem Host (114) empfangen werden, der sich in einem ersten Netzwerk (104) befindet;
M3	generating (6, 404), by the computing system, a plurality of log entries (306, 308, 310) corresponding to the plurality of packets received by the network device;	Erzeugen (6, 404), durch das Rechensystem, einer Vielzahl von Log-Einträgen (306, 308, 310), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden;
M4	identifying (8, 406), by the computing system, a plurality of packets (P1’, P2’, P3’) transmitted by the network device to a host (108) located in a second network (102);	Identifizieren (8, 406), durch das Rechensystem, einer Vielzahl von Paketen (P1', P2', P3'), die durch die Netzwerkvorrichtung an einen Host (108) übertragen werden, der sich in einem zweiten Netzwerk (102) befindet;
M5	generating (9, 408), by the computing system, a plurality of log entries (312, 314, 316) corresponding to the plurality of packets transmitted by the network device;	Erzeugen (9, 408), durch das Rechensystem, einer Vielzahl von Log-Einträgen (312, 314, 316), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden;

M6	correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device; and	Korrelieren (16, 410), durch das Rechensystem und auf Grundlage der Vielzahl von Log-Einträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden und der Vielzahl von Log-Einträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden, der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden mit der Vielzahl von Paketen, die durch die Netzwerk-vorrichtung empfangen werden; und
M7	responsive to correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device:	als Reaktion auf das Korrelieren der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden, mit der Vielzahl von Paketen, die durch die Netzwerkvorrichtung empfangen werden:
M7.1	generating (30), by the computing system, one or more rules (140) configured to identify packets received from the host located in the first network; and	Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet; und
M7.2	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify packets received from the host located in the first network.	Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet.

Merkmal	Patentanspruch 15 lt. **Streitpatent** in englischer Verfahrenssprache	Deutsche Übersetzung lt. **Streitpatent**
15 M1	An apparatus configured to	Vorrichtung, die konfiguriert ist,
15 M2	perform each step of the method of any one of claims 1-14.	um jeden Schritt des Verfahrens nach einem der Ansprüche 1-14 durchzuführen.

3. Das Streitpatent richtet sich als zuständigen Fachmann an einen Ingenieur der Elektrotechnik bzw. Nachrichtentechnik / Informationstechnik mit abgeschlossenem Universitätsstudium und mit mehrjähriger Berufserfahrung in der Entwicklung vernetzter, paketvermittelnder Datenübertragungs- und Kommunikationssysteme, wobei dieser insbesondere detaillierte Kenntnisse hinsichtlich der einschlägigen Netzwerkprotokolle sowie Netzwerk-Sicherheit aufweist.

Insoweit die Beklagte darauf abstellt, dass der Fachmann durchaus versiert wäre, jedoch ihrer Meinung nach definitiv keinen Source-Code entwickeln, sondern lediglich kommerziell verfügbare Rack-Lösungen erwerben und kombinieren würde, vermag diese Auffassung nicht zu überzeugen. Denn um eine Lehre, wie sie das Streitpatent vermittelt, zu verstehen und anzuwenden (d.h. die Entwicklung eines Kommunikationssystems) muss der Fachmann aus Sicht des Senates ein Konstrukteur mit Erfahrungen auf dem Gebiet der Entwicklung derartiger Systeme sein und kein Anwender bzw. Integrator bereits kommerziell erhältlicher Systeme aus diesem Bereich (vgl. BGH, Urteil vom 18.06.2009, X ZR 138/05 - Fischbissanzeiger), wofür dieser über eine entsprechende akademische, d.h. auch mathematische und informationstechnische, Vorbildung verfügt.

4. Dieser Fachmann versteht die Lehre des Streitpatents und die in den angegriffenen Ansprüchen verwendete Begriffe bzw. Merkmale vor deren technischem Hintergrund wie folgt:

Zum Patentanspruch 1

Mit dem Merkmal M1 ist ein Verfahren beansprucht, welches gemäß den Merkmalen M2 und M4 das Identifizieren einer Vielzahl von Paketen mittels eines Rechensystems umfasst, welche einerseits an einem Netzwerk-Gerät von einem ersten Host in einem ersten Netzwerk empfangen und andererseits an einen zweiten Host in einem zweiten Netzwerk gesendet werden. Der Netzwerk-Typ bleibt offen, das Streitpatent spricht in Absatz [0012] sogar nur von einem einzigen Netzwerk oder aber auch von mehreren Netzwerken umfassend LAN, WAN, VPNs, Regierungsnetze, Unternehmensnetze, Service Provider Netzwerke, Internet oder entsprechende Kombinationen. Die Hosts umfassen u. a. Server, Desktops, Laptops, Handys/Smartphones, Router, Switches, Gateways oder Access Points. Das Identifizieren der Pakete kann im Netzwerk-Gerät selbst oder mittels geeigneter Abgriffe („taps“) an den beiden Schnittstellen des Netzwerk-Geräts zum ersten/zweiten Netzwerk bzw. im Prinzip sogar an zwei beliebigen Positionen im Übertragungsweg der Pakete im ersten/zweiten Netzwerk erfolgen.

Die Merkmale M3 und M5 betreffen das Generieren einer Vielzahl von „Log entries“ entsprechend der Vielzahl von Paketen jeweils für gesendete bzw. empfangene Pakete. Darunter versteht der Fachmann jeweils ein getrenntes Protokollieren der Pakete für die Empfangsseite und die Sendeseite des Netzwerk-Geräts mit einer Datenstruktur mit einer Vielzahl von Einträgen, wobei eine Vielzahl eine Anzahl größer oder gleich zwei bedeutet (also nicht unbedingt sämtliche Pakete betrifft). Ein Protokollieren umfasst ebenfalls zumindest ein Einhalten einer zeitlichen Reihenfolge der Pakete, wobei der üblicherweise in Logs vorhandene Zeitstempel hinreichend aber nicht notwendig ist. Der „Log entry“ für ein einzelnes Paket betrifft Klartext oder kodierte Paket-Informationen, welche zumindest aus Teilen des Pakets, bspw. Header oder Payload, gewonnen werden. Vorzugsweise sollte der „Log entry“ Rückschlüsse auf das Paket und/oder den/die Host(s) erlauben, um so

bspw. eine Identifizierung bzw. Zuordnung mittels Adressen, (Fluss-)IDs etc. zu ermöglichen.

Der Fachmann geht davon aus, dass die Protokolleinträge („Log entries“) zumindest so lange in einem Speicher gehalten werden, wie es beabsichtigt ist, sie zu verwenden, d.h. hier im Wirkzusammenhang mit dem Merkmal M6 zumindest so lange, wie die Durchführung der Korrelationsfunktion dafür benötigt. Insofern müssen die Protokolleinträge für eine gewisse Zeit vorgehalten werden, wozu allerdings auch ein flüchtiger (temporärer) Speicher ausreicht. Soweit nämlich die Vielzahl der Protokolleinträge zur Korrelation verwendet werden soll (vgl. Merkmal M6), muss das Rechensystem (d.h. ein im Patentanspruch gegenständlich nicht beanspruchter Korrelator) auf eine Vielzahl von Protokolleinträgen gemäß Merkmal M3 und auf eine Vielzahl von Protokolleinträgen gemäß Merkmal M5 zurückgreifen können. Somit ist aber weder das Schreiben von Log-Dateien in einen persistenten Speicher noch die Anzahl von Dateien spezifiziert.
Eine Liste von Pointern (Speicheradressen) erfüllt diese genannten Kriterien für ein Log bzw. für „Log entries“ jedoch nicht. Das Streitpatent offenbart „Log entries“ bspw. in Figur 3 i. V. m. Absätzen [0016] – [0017].

Das Merkmal M6 betrifft ein Korrelieren der Pakete basierend auf einem Korrelieren bzw. einem Vergleichen einer Vielzahl von „Log entries“ der Sendeseite mit der Vielzahl von „Log entries“ der Empfangsseite (vgl. Streitpatent, Abs. [0034] – [0035], Ansprüche 4 und 6), wobei der Fachmann unter einer Korrelation ein Ermitteln einer Wechsel-Beziehung aufgrund von Inhalten, Merkmalen, Zuständen oder Funktionen der Vielzahl von Paketen versteht. Das Korrelieren multipler Pakete der Sendeseite mit multiplen Paketen der Empfangsseite stellt eine Kreuzkorrelation dar. Ein einfacher 1:1 Vergleich von zwei Paketen, d.h. jeweils einem Sendepaket mit jeweils einem Empfangspaket, ist nach fachmännischem Verständnis keine Korrelation und genügt somit nicht dem Merkmal M6.

Die Merkmalsgruppe M7, M7.1 und M7.2 fordert, dass in Ansprechen („responsive“) auf das Korrelieren, d.h. sozusagen im Nachgang als Konsequenz der Korrelation, durch das Rechensystem mindestens eine Regel zum Identifizieren von Paketen, welche vom ersten Host im ersten Netzwerk empfangen werden, generiert wird. Diese Regelgenerierung erfolgt definitiv nicht manuell sondern anspruchsgemäß durch das Rechensystem; das Streitpatent schweigt jedoch darüber, ob die Regelgenerierung „halb-automatisch“ (bspw. unter Einbeziehung des Systemadministrators) oder „voll-automatisch“ durchgeführt wird. Ein Identifizieren des ersten Hosts ist in einem Paketdatennetzwerk ggf. anhand der Source-Adresse oder einer entsprechenden ID in den Paket-Headern leicht möglich. Die Regel soll einem Paketfilter („packet-filtering device“) zugeführt werden, welcher dann die Aufgabe der Paket-Identifizierung übernimmt.

Der Patentanspruch 1 lässt offen, wo der Paketfilter im Netzwerk implementiert ist, d.h. der Paketfilter könnte sich in einem Abgriff/Tap oder im Netzwerk-Gerät oder im Korrelator oder an einer anderen Stelle im Netzwerk befinden, wo Pakete des ersten Hosts auftreten und dem Paketfilter zugeführt werden könnten. Die Position des Paketfilters spielt keine Rolle, so lange der Filter („packet-filtering device“) geeignet ist, die vom Host empfangenen Pakete zu identifizieren (vgl. Streitpatent, Sp. 4, Z. 25 ff.: „… tap devices 124 and 126 may comprise one or more packet-filtering devices and may be provisioned with rule(s) 140, which may configure tap device(s) 124 and 126 to identify packets meeting criteria specified by rule(s) 140 …“) und die erwähnten Regel(n) aufweist, d. h. sie auch anwendet. Dazu muss er sich örtlich nur an einem beliebigen Ort in, auf oder an dem Pfad bzw. Übertragungsweg zwischen ersten Host, Netzwerk-Gerät und zweitem Host befinden bzw. zumindest mittelbar mit diesem Pfad verbunden sein. Das Streitpatent zeigt im Ausführungsbeispiel gemäß Figur 1 i. V. m. Absatz [0013] zwei in den beiden „tap devices“ integrierte Paketfilter, wobei die jeweiligen Filter in den Pfad vor und hinter dem Netzwerk-Gerät eingefügt sind bzw. zumindest eine Verbindung zum Pfad aufweisen (ebenda: „Tap device 124 may be located on or have access to a communication path that interfaces network device(s) 122 and

network 106. Tap device 126 may be located on or have access to a communication path that interfaces network device(s) 122 and network 104 (e.g., one or more of hosts 114, 116, and 118).“). Zudem soll gemäß Streitpatent, Absatz [0055] die dort offenbarte Funktionalität zentral in einem Gerät konzentriert oder auch beliebig im Netzwerk verteilbar sein (dort: „… operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device …“).

Darüber hinaus bleibt im Patentanspruch 1 unbestimmt, was mit einem vom Paketfilter identifizierten Paket bzw. nach der erfolgreichen Identifizierung eines Pakets geschehen soll. Bei einer mit der Identifizierung verknüpften Handlung/Aktion könnte es sich ggf. um ein Speichern, Kopieren/Duplizieren, Loggen, Verwerfen, Modifizieren, Routen/Umrouten, Weiterleiten/Forward oder ähnlichem handeln. Genauso gut wäre ebenfalls eine Signalisierung bzw. Alarmierung denkbar.

Das Streitpatent beschreibt die Regeln sowie die daraus abgeleiteten bzw. resultierenden Handlungen/Aktionen in den Absätzen [0013] bis [0014] und [0048] bis [0049].

Zum nebengeordneten Patentanspruch 15

Der nebengeordnete Patentanspruch 15 betrifft eine entsprechende Vorrichtung zur Durchführung des Verfahrens u. a. gemäß Patentanspruch 1. Der Fachmann versteht den nebengeordneten Patentanspruch 15 daher entsprechend seinem Verständnis zu diesem.

II. Zur erteilten Fassung

Das Streitpatent ist in seiner erteilten Fassung für nichtig zu erklären, weil dem Gegenstand des Streitpatents in erteilter Fassung der Nichtigkeitsgrund der mangelnden Patentfähigkeit entgegensteht (Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 Buchst. a) EPÜ i. V. m. Art. 52, 56 EPÜ). Denn die Gegenstände der nebengeordneten Patentansprüche 1 und 15 in der erteilten Fassung erfüllen zwar das Kriterium der Neuheit (Art. 54 EPÜ), beruhen jedoch nicht auf einer erfinderischen Tätigkeit, da sich für den Fachmann die Erfindung in naheliegender Weise aus dem Stand der Technik, und zwar aus einer Zusammenschau der Druckschriften NK2 und NK7/NK12 bzw. NK12 und HLNK1, ergibt (Art. 56 EPÜ).

1. Die nebengeordneten Patentansprüche 1 und 15 in der erteilten Fassung sind zulässig, da ihre Gegenstände nicht über den Inhalt der ursprünglichen Anmeldungsunterlagen hinausgehen (Art. II § 6 Abs. 1 Nr. 3 IntPatÜG i. V. m. Art. 138 Abs. 1 Buchst. c), Art. 123 Abs. 2 EPÜ).

Entgegen der Auffassung der Klägerinnen kommt es im Hinblick auf die Zulässigkeit des erteilten Patentanspruchs 1 auf die gesamte ursprünglich offenbarte Lehre an (so schon BGH, Urteil vom 22. Februar 2000, X ZR 111/98 – Positionierungsverfahren, juris Rn. 70; BGH, Urteil vom 17. Februar 2015, X ZR 162/12 – Wundbehandlungsvorrichtung, Rn 21) und nicht allein darauf, welche Merkmale des ursprünglichen Unteranspruchs 22 in den erteilten Patentanspruch 1 aufgenommen sein könnten.

Die Auffassung der Klägerinnen (vgl. Nichtigkeitsklage vom 26.11.2020, S. 17), der im europäischen Prüfungsverfahren geänderte Anspruch 1 umfasse Paketfiltervorrichtungen, die gemäß Merkmalsgruppe 7 mit einer Regel zum Identifizieren von einem Host in einem ersten Netzwerk kommenden Datenpaketen konfiguriert werden, wobei diese Regel auch zu anderen Handlungen verwendet

werden könne als zum Identifizieren und Fallenlassen von Datenpaketen, so dass eine Verallgemeinerung des Schutzbereichs vorläge, überzeugt den Senat nicht. Auch die Ansicht der Klägerinnen, das Ausführungsbeispiel gemäß den Figuren 2C und 2D würde nur eine Regel zum Identifizieren und Fallenlassen offenbaren, wobei die Regel ggf. auch nicht in Reaktion auf das Korrelieren sondern vielmehr in Reaktion auf das Bestimmen von einem bösartigen Host gesendeter Datenpakete erfolge, greift nicht durch.

Denn die ursprüngliche Anmeldung offenbart (vgl. NK21, Offenlegungsschrift, Abs. [15]) einen Korrelator, welcher die Taps/Paketfilter mit Regeln versieht, welche die Taps/Paketfilter zum Identifizieren von Paketen sowie zum Durchführen von auch anderweitig spezifizierten Handlungen veranlassen, welche sich nicht nur auf das Fallenlassen von Paketen (vgl. NK21, Ausführungsbeispiel gemäß Figur 2D, Schritt 34 i. V. m. den Absätzen [51] – [52]) beschränken, sondern welche neben dem Fallenlassen/Drop beispielhaft ebenso ein Routen, Weiterleiten/Forward, Logging und Kopieren oder ähnliches umfassen (vgl. Offenlegungsschrift, NK21, Abs. [15], dort: „Rule(s) 140 may be generated by packet correlator 128 and may be configured to cause tap device(s) 124 and 126 to identify packets meeting criteria specified by rule(s) 140 and to perform one or more functions specified by rule(s) 140 on the identified packets (e.g., forward (or route) the packets toward their respective destinations, drop the packets, log information associated with or contained in the packets, copy the packets (or data contained therein), or the like) … tap devices 124 and 126 may comprise one or more packet-filtering devices and may be provisioned with rule(s) 140, which may configure tap device(s) 124 and 126 ...“).

Entgegen der Auffassung der Klägerinnen muss der Paketfilter nicht zwingend zwischen dem ersten Host und dem Netzwerk-Gerät angeordnet sein. Die ursprüngliche Anmeldung NK21 zeigt in Figur 1 i. V. m. Absatz [15] sowie Figur 2D i. V. m. Absatz [51] vielmehr bereits zwei „tap devices“ 124 und 126, welche vor und hinter dem Netzwerk-Gerät 122 angeordnet sind, welche beide jeweils einen

Paketfilter umfassen, und welche beide jeweils mit Regeln bzw. Regel-Updates beaufschlagt werden, um Pakete zu identifizieren und entsprechende Funktionen wie bspw. ein Fallenlassen/Verwerfen von Paketen auszuüben (vgl. NK21, Abs. [51]: „to configure tap devices 124 and 126 to identify and drop packets received from host 114.“; vgl. NK21, Abs. [15]: „Tap device 124 may be located on or have access to a communication path that interfaces network device(s) 122 and network 106. Tap device 126 may be located on or have access to a communication path that interfaces network device(s) 122 and network 104 (e.g., one or more of hosts 114, 116, and 118).“). Zudem können gemäß NK21, Absätze [12] bis [13], die in der Beschreibung bzw. den Ausführungsbeispielen angegebenen Verbindungen direkt oder auch indirekt sein, sowie soll gemäß den Absätzen [55] bis [57] die erfindungsgemäße Funktionalität zentral in einem Gerät konzentriert oder auch beliebig im Netzwerk verteilbar sein (dort: „… operative across one or more computing devices and networks. The functionality may be distributed in any manner or may be located in a single computing device …“).

Somit entnimmt der Fachmann die Gegenstände der Ansprüche 1 und 15 den ursprünglichen Anmeldeunterlagen unmittelbar und eindeutig.

2. Der Gegenstand des erteilten Patentanspruchs 1 ist gegenüber der Lehre der Druckschriften **NK2** (GB 2 505 288 A) sowie der **NK3** (US 7 995 584 B2) neu, da er nicht mit sämtlichen Merkmalen aus jeweils einer dieser Druckschriften bekannt ist (Art. 54 EPÜ).

2.1 Die **NK2** (GB 2 505 288 A) betrifft – im Gegensatz zum Streitpatent - kein Verfahren bzw. System für die Netzwerk-Überwachung bzw. Netzwerk-Sicherheit, sondern für ein „Law Enforcement“ (LE) bzw. „Lawful Intercept“ in Netzwerken mit Adress-Änderungen, welche bspw. durch Proxies oder NATs („network address translation“) hervorgerufen wurden, um dort entsprechende Hosts oder den

Datenverkehr krimineller Teilnehmer zu erfassen (vgl. NK2, S. 4, Z. 32 – S. 5, Z. 14, S. 13, Z. 23; **Merkmal M1**).

Dazu wird gemäß NK2 der Paketdatenverkehr jeweils vor und hinter dem Netzwerk-Gerät (Proxy, NAT) mit einem passiven Korrelationsgerät („Passive Correlation Device“) erfasst, wobei Paketfilter („Pre-NAT Session Filter 150“ und „Post-NAT Session Filter 155“, vgl. NK2, Fig. 3) die Pakete einzelnen Sessions zuordnen und in entsprechende Session-Queues einsortieren (vgl. NK2, Fig. 2 und 3). Der NAT ist hierbei an der Grenze zwischen zwei Netzwerken, bspw. einem GPRS-Mobilfunknetz und dem Internet angeordnet, so dass die Pakete der Session-Queues verschiedenen Hosts in einem ersten/zweiten Netzwerk zugeordnet sind (vgl. NK2, Fig. 1; **Merkmale M2, M4**).

Einem Korrelator wird mittels Pointer-Listen („a list of pointers“, vgl. NK2, S. 9, Z. 7) auf die Pakete in den Session-Queues bzw. Speicherstellen der Pakete in einem gemeinsamen Buffer ein Echtzeit-Zugriff bzw. eine Echtzeit-Verarbeitung ermöglicht (vgl. NK2, S. 5, Z. 11 - 12, S. 5, Z. 32, S. 9, Z. 1 - 16, S. 13, Z. 8).
Entgegen der Auffassung der Klägerinnen handelt es sich bei der unspezifischen Abspeicherung von Paketen in einem gemeinsamen Buffer nicht um einen Log i.S. des Streitpatents, da jegliche Eigenschaften einer Protokollierung, bspw. ein Einhalten einer festen Paketreihenfolge bzw. eine (optionale) Beaufschlagung der Pakete mit einem Zeitstempel, fehlen (vgl. NK2, S. 9, Z. 6 – 9, „… the packets being otherwise held in a common buffer.“). Die in der NK2 genannte, aufgezeichnete Zeitinformation bezieht sich offensichtlich nicht auf die Pakete sondern ausschließlich auf die jeweiligen Sessions (vgl. NK2, S. 9, Z. 29 – S. 10, Z. 4, „The session filters 150, 155 are arranged to record timing information to a high level of accuracy for each observed session, …“). Im Übrigen wird die Argumentation, dass gemäß NK2 die Pakete mit einem Log-typischen Zeitstempel markiert würden, von den Klägerinnen in der mündlichen Verhandlung nicht mehr weiterverfolgt.

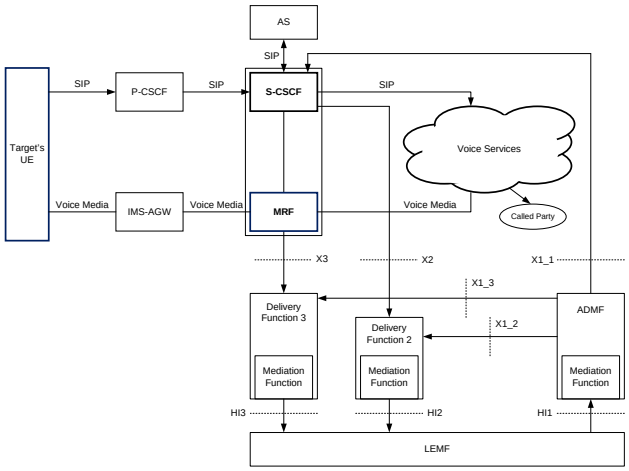
Der Korrelator gemäß NK2 umfasst einen Prozessor mit vier Kernen zur Parallelverarbeitung (vgl. NK2, Fig. 3, S. 8, Z. 10 – 17, „… the processor 170

comprises four processor cores with each processor core arranged to execute, in a separate processing thread, an instance of the correlation functionality. Each of the executing correlation threads is arranged to receive queued IP packets from a different post-NAT session queue 165, in parallel, and to look for a matching session from amongst the queued IP packets in the pre-NAT session queues 160.“). Der Korrelator korreliert die Pakete der Post-NAT-Sessions mit denjenigen der Pre-NAT-Sessions, wobei der Korrelator **über die Pointer** auf die Header-Informationen der Pakete zugreift, insbesondere auf die IPQuint, d. h. die fünf Datenfelder im TCP/UDP Paketheader umfassend Quell-IP-Adresse und Portnummer, Ziel-IP-Adresse und Portnummer sowie das IP-Protokoll, und weitere IP Identifikations-Felder, um über die Zusammengehörigkeit von Pre-NAT und Post-NAT Paketen auf das Adress-/Port-Mapping des Proxies/NATs zu schließen, wobei bei Mehrdeutigkeiten auch noch auf weitere Paketinformation zurückgegriffen wird (vgl. NK2, S. 9, Z. 17 – S. 10, Z. 11; **Merkmal M6 teilweise**).

Das Adress- /Port-Mapping von vom Korrelator erfolgreich zugeordneten / „gematchten“ Sessions wird in einem Log abgespeichert, der einer Vielzahl von Anwendungen (NK2, S. 5, Umbruch zu S. 6, „for use in numerous applications“) und/oder externen Systemen (NK2, S. 8, Z. 33, „external systems“) zur Verfügung gestellt wird (vgl. NK2, Fig. 4, S. 6, Z. 1, S. 7, Z. 12, S. 8, Z. 33, S. 11, Z. 14 – S. 12, Z. 2; **Merkmal M7**).

Das vom Korrelator generierte Mapping von privaten / öffentlichen Teilnehmeradressen kann beispielsweise einer/-m „Lawful Intercept“ Applikation/System zur Verfügung gestellt werden, wobei diese/-s dann Regeln für das Identifizieren von Paketen eines kriminellen Teilnehmers generiert, mit diesen Regeln einen Paketfilter konfiguriert und mittels Paketfilter die Pakete des kriminellen Teilnehmers aus dem Netzwerkverkehr filtert und für die Strafverfolgung abspeichert (vgl. NK2, S. 4, Z. 32 – S. 5, Z. 14, insb. Z. 11 ff.: „Realtime mapping information of particular target sessions, captured by the present invention, may be sent to a respective monitoring device so that it may identify and collect data for the correct sessions“). Die NK2 zeigt in der Figur 1 i. V. m. Seite 3, Zeilen 22 bis 32

bereits ein GPRS-Mobilfunknetz. „Lawful Intercept“ Systeme sind im Allgemeinen standardisiert. Der Fachmann liest somit aufgrund des GPRS Mobilfunknetzes in der NK2, Figur 1 ein „Lawful Intercept“ System gemäß dem zum Prioritätsdatum des Streitpatents relevanten 3GPP-Standard TS 33.107 V12.9.0 (2014-12) mit, welches im Fall eines NAT eine Architektur gemäß dortiger Figur E 3.1 auf Seite 196 aufweist:



Das Abhören eines Teilnehmers wird von einem ADMF unter Zuhilfenahme der Zielidentität initiiert, wobei der ADMF über den S-CSCF letztendlich den MRF (Paketfilter im „Lawful Intercept“ System) instruiert, einen Call der Zielperson aufzunehmen, wobei dann dem S-CSCF und dem MRF gemäß NK2 die IP-/Port-Adressen zur Verfügung gestellt werden (**Merkmale M7, M7.1, M7.2**).

Soweit die Beklagte in der Verhandlung vorträgt, dass die GPRS-Architektur der NK2 mit der UMTS-Architektur des 3GPP-Standards TS 33.107 V12.9.0 umfassend ein IP Multimedia Subsystem (IMS) mit einem SIP-basierten Session-Aufbau inkompatibel sei, greift dies nicht durch. Denn der Fachmann weiss, dass „Lawful Intercept“ ebenfalls bereits früher für GPRS standardisiert wurde, wobei dort der ADMF unter Zuhilfenahme der Zielidentität des Teilnehmers den GPRS Support Node (GSN) zum Herausfiltern der Paketdaten dieses Teilnehmers aussteuert (vgl. 3GPP TS 03.33 V8.1.0 (2000-12), S. 40 ff., „Annex B (normative): Interception for GPRS“).

Darüber hinaus lehrt die NK2 in Ansprechen auf ein erfolgreiches Matching zwischen einer Eingangs- sowie einer Ausgangs-Session-Queue durch den Korrelator, dass die entsprechenden Session-Queues in den Paketfiltern (des passiven Korrelationsgeräts / „Passive Correlation Device“) gelöscht werden sollen, und dass die Paketfilter keine weiteren Pakete dieser Sessions aufnehmen sollen, um multiples Matching für die gleiche Session zu verhindern, wobei es sich dabei ebenfalls um Regeln handelt, welche über die Steuerleitungen gemäß NK2, Figur 3, Bezugszeichen 175, 180 vom Korrelator an die Paketfilter 150, 155 übermittelt werden (vgl. NK2, Fig.3, Bezugszeichen 175, 180 i. V. m. S. 8, Z. 21 - 29, dort: „the processor signals to the post-NAT session filter 165 to cease capture of IP packets in the matched session (post-NAT IPQ + IP Identification field). Similarly, the processor 170 signals to the pre-NAT session filter to cease capture of IP packets relating to the matched pre-NAT session. Each session filter 150, 155 responds by clearing the respective queues 160, 165 of packets and begins to queue IP packets with a newly identified IPQ + IP Identification field, captured at the respective tap points 120, 125. In this way, the loading on the processor's correlation functionality is reduced as far as possible.“; ebenfalls **Merkmale M7, M7.1, M7.2**).

In der NK2 fehlt ein Generieren von „Log entries“ für die vom Netzwerk-Gerät – d. h. in diesem Fall dem NAT/Proxy - gesendeten bzw. empfangenen Pakete, wobei jedoch gemäß NK2 dem Korrelator über die Pointer-Listen für die im Speicher / Buffer befindlichen Pre-/Post-NAT Pakete sämtliche notwendigen Informationen mittels Speicherzugriff bereitgestellt werden. In Folge basiert die Korrelation gemäß Merkmal M6 ebenfalls nicht auf den „Log entries“. Daher **fehlen** in der NK2 die **Merkmale M3, M5 teilweise** sowie ebenfalls das **Merkmal M6 teilweise**.

Der Gegenstand des erteilten Patentanspruchs 1 ist somit neu gegenüber der Lehre der Druckschrift **NK2.**

2.2 Die **NK3** (US 7,995,584 B2) betrifft ein Detektieren eines bösartigen Routers in einem Netzwerk („for detecting malicious routers“) bzw. ein Detektieren von TCP-

SYN- oder DoS-Attacken eines in der Nähe des Routers befindlichen Hosts (vgl. NK3, Sp. 1, Z. 7 - 10, Sp. 6, Z. 27 - 60).

Hierzu wird fortlaufend für jedes nicht für den Router selbst bestimmte Paket am Eingang („ingress“) sowie am Ausgang („egress“) des Routers ein jeweiliger Hash-Wert oder alternativ bei Verwendung von Bloom-Filtern multiple Werte für Sub-Pakete bzw. Paket-Header bestimmt, in einem Hash-Buffer abgespeichert und miteinander verglichen (vgl. NK3, Fig. 1 - 3, Sp. 2, Z. 50 – Sp. 3, Z. 31 und Sp. 4, Z. 10 - 16).

Wird ein Router als bösartig erkannt, erfährt das aktuelle Egress-Paket am Router-Ausgang eine Spezialbehandlung („appropriate action“), wobei das Paket verworfen, weitergeleitet oder geloggt wird (vgl. NK3, Sp. 3, Z. 32 - 43).

In der NK3 **fehlt** das **Merkmal M6** umfassend ein Korrelieren multipler gesendeter und multipler empfangener Pakete, da gemäß dortiger Lehre jeweils sequentiell Paket für Paket behandelt wird, wobei ein Vergleich von Informationen von jeweils nur einem Paket auf der Ingress- sowie einem auf der Egress-Seite nach fachmännischem Verständnis keine Korrelation im streitpatentgemäßen Sinne darstellt. Die NK3 schweigt zudem hinsichtlich einer Regelgenerierung für einen Paketfilter, so dass dort ebenfalls die **Merkmalsgruppe M7 fehlt**.

Der Gegenstand des erteilten Patentanspruchs 1 ist somit neu gegenüber der Lehre der Druckschrift **NK3.**

2.3 Gleiches gilt für den nebengeordneten Patentanspruch 15, der eine entsprechende Vorrichtung zur Durchführung des Verfahrens u.a. gemäß Patentanspruch 1 betrifft.

3. Der Gegenstand des erteilten Patentanspruchs 1 beruht nicht auf einer erfinderischen Tätigkeit, da sich für den Fachmann die Erfindung in naheliegender Weise aus dem Stand der Technik aus einer Zusammenschau der Druckschriften **NK2 und NK7** (US 2012/0218999 A1), **NK2 und NK12** (US 2014/0280778 A1) oder **NK12 und HLNK1** (US 8413238 B1) ergibt (Art. 56 EPÜ).

3.1 Zur Zusammenschau von NK12 und HLNK1

Die **NK12** (US 2014 / 0 280 778 A1) betrifft ein Verfahren für ein Rechensystem („a computer implemented method is described“) zum Identifizieren von Paketen bzw. Paketquellen in einem Netzwerk („tracking the identity of a network packet“) mit einem einen Grenzübergang („boundary“) repräsentierendem Netzwerk-Gerät, welches ein Router, ein Proxy, ein Gateway, eine Firewall oder ein NAT sein kann (vgl. NK12, Abs. [0003] – [0006]; **Merkmal M1**).

Hierzu wird gemäß NK12 der Datenverkehr zwischen einem Client und einem Server vor und hinter dem Netzwerk-Gerät mit Sensoren („inside sensor 120“, „outside sensor 125“) abgegriffen, wobei jeweils die Pakete auf der Applikations-Schicht mit einem Zeitstempel versehen werden, für jedes Paket ein Hash-Wert für die Payload berechnet wird, und die jeweiligen Paketinformationen wie Zeitstempel, IP-Adresse(n) und Hash-Wert in zwei FIFO-Queues einsortiert bzw. abgespeichert werden, wobei die Pakete aus den FIFO-Queues anschließend einander zugeordnet („match“) werden (vgl. NK12, Fig. 1 - 3, Abs. [0003], [0006], [0018], [0021]). Die durch die Sensoren erfassten bzw. aufgenommenen (vgl. NK12, Abs. [0018] - [0020], „passively record traffic“) Einträge in den beiden FIFO-Queues sind „Log entries“ i.S. des Streitpatents für eine Vielzahl von Paketen jeweils auf der Empfangs- sowie auf der Sendeseite des Netzwerk-Geräts (**Merkmale M2 bis M5**).

Das anschließende Matching der Pakete basierend auf den „Log entries“ erfolgt anhand der Kriterien Zeitstempel, IP-Adresse und Hash-Wert, wobei ggf. der Einsatz von Fuzzy-Logik nicht nur ein Matching aufgrund identischer Einträge

sondern auch ein Matching anhand von Ähnlichkeiten erlaubt (vgl. NK12, Abs. [0021], [0029]). Das Matching berücksichtigt eine unterschiedliche Paketreihenfolge, so dass eine Korrelation multipler Eingangs- und multipler Ausgangspakete vorliegt (vgl. NK12, Fig. 2 - 3, Abs. [0024] - [0025]). Die NK12 benennt das Matching gemäß Figur 2 auch explizit als „Correlation“ (**Merkmal M6**), wobei die Paketverarbeitung und Korrelation gemäß NK12 nahezu in Echtzeit erfolgen soll (vgl. NK12, Abs. [0027], „live packet capture mode“, „near real time“).

Die NK12, Figur 2 i. V. m. Absatz [0023] zeigt exemplarisch für ein Paket die Ausgabe des Korrelations- bzw. Matching-Ergebnisses in Form eines Logs umfassend die Header-Daten, insbesondere die IP-Adressen, sowie den MD5-Hash, wobei beim Vergleich vom Egress-Paket des Routers bzw. Gateways an der Netzwerkgrenze („Outpacket“) und dem Ingress-Paket („Inpacket“) die durch die NAT verursachte Änderung der Ursprungsadresse („SrcAddr“) der Paketquelle ersichtlich ist. Der Log umfasst selbstverständlich eine Vielzahl von Paketen und beschreibt somit vollständig das NAT-Mapping zwischen privaten und öffentlichen Adressen an der Netzwerk-Grenze.

Gemäß NK12, Absatz [0030] soll das Identifizieren der wahren Paketquelle („identify the true source of packet transmission“) einen signifikanten Beitrag für die Netzwerk-Sicherheit bspw. in Unternehmensnetzen leisten, indem infizierte, bösartige Netzknoten im Firmennetz durch das Inspizieren der Pakete an der Netzwerkgrenze erkannt werden („provide a way to quickly identify nodes that are infected with malicious content“). Diese Information wird entweder einem Netzwerkadministrator zur Verfügung gestellt, oder kann als Grundlage für eine Unternehmensnetzwerk-Architektur mit signifikanten Investitionen in die Überwachung („monitoring“) dienen, welche diese Technik nutzt, um an der Netzwerkgrenze detektierte bösartige Netzaktivität ihrer originalen Paketquelle zuzuordnen (vgl. NK12, Abs. [0030], „Enterprises with significant visibility and monitoring investments into the network backbone can utilize this technique to

attribute malicious activity sensed at the edge of a network back to its original source.“).

Wird bspw. von einem Überwachungssystem ein bösartiges Egress-Paket detektiert, kann das Überwachungssystem unter Heranziehen des o.g. Logs, welcher das Korrelations- bzw. Matching-Ergebnis für das Paket umfasst, auf das zugehörige Ingress-Paket rückschließen und somit die Ursprungsadresse („SrcAddr“) der Paketquelle ermitteln.

Von der streitpatentgemäßen Lehre unterscheidet sich die NK12 lediglich dadurch, dass gemäß NK12 keine Regeln zur Identifikation der (bösartigen) Host-Pakete bzw. des (bösartigen) Hosts generiert werden und solche auch nicht für einen Paketfilter bereitgestellt werden. Somit zeigt die NK12 die Merkmale M7.1 und M7.2 nicht. Diese Auffassung des Senats wurde den Parteien im Übrigen mit dem gerichtlichen Hinweis vom 25. April 2022 mitgeteilt.

Da die NK12 im Kontext der Netzwerk-Sicherheit von Unternehmensnetzwerken eine Lösung für das technische Problem des Identifizierens und Trackens von Paketen infizierter, bösartiger Netzknoten bzw. Hosts an Netzwerkgrenzen eines Unternehmensnetzwerks, an denen eine Verschleierung bedingt durch eine NAT-Funktionalität eines Gateways bzw. Routers auftritt, sowie der entsprechenden Zuordnung der Pakete zu einer wahren Ursprungsquelle des Paketdatenflusses, d.h. zu dem infizierten, bösartigen Netzknoten, anbietet, war sie ein geeigneter Ausgangspunkt, um Maßnahmen gegen infizierte bzw. bösartige Netzknoten in Unternehmensnetzwerken bereitzustellen.

Soweit die Klägerinnen in der mündlichen Verhandlung vorgetragen haben, dass sich dem Fachmann die Frage stelle, was mit dem als infiziert erkannten Netzknoten bzw. Host zu machen sei, hatte der Fachmann ausgehend von der NK12 die Aufgabe zu lösen, wie mit den nach der Lehre der NK12 als infiziert identifizierten

Hosts umzugehen ist, um das in Absatz [0030] der NK12 angesprochene Unternehmensnetzwerk zu schützen.

Entgegen der Auffassung der Beklagten, wonach der Fachmann keinen Anlass gehabt hätte, die Lehre der NK12 zu verlassen, da diese eine Vorratsdatenspeicherung betreffe, offenbart die Lehre der NK12 explizit, diese in Unternehmensnetzwerken zu verwenden (vgl. NK12, Abs. [0030]: „… it can provide a stable foundation for building tiered enterprise network architectures with an inherent capability for attribution of malicious activity. Enterprises with significant visibility and monitoring investments into the network backbone … “, Unterstreichungen hinzugefügt). Darüber hinaus hatte der Fachmann die Lehre der NK12 nicht zu verlassen, sondern diese infolge der impliziten Fragestellung im Absatz [0030] - wie oben beschrieben - fortzuführen.

Der Fachmann würde auch die **HLNK1** (US 8413238 B1) in Betracht ziehen. Denn diese betrifft ebenfalls die Netzwerk-Sicherheit in Unternehmensnetzwerken, wobei von einem Überwachungssystem („monitoring systems and/or methods“, „Monitor communications“) bösartige Aktivitäten („malicious activity“), Attacken („attacks such as a denial of service“) sowie Zugriffe ins Dark-Net auch bei verschleierten („spoofed“, „faked“) IP-Adressen abgewehrt werden sollen (vgl. HLNK1, Fig. 4 Bezugszeichen 420, Sp. 1 Z. 36 - 51, Sp. 2, Z. 6 - 19, Sp. 3 Z. 24 – 53, Sp. 10, Z. 52 – 53, Sp. 11, Z. 43 - 46). Insbesondere betrifft die HLNK1 dabei – genauso wie die NK12 - ein Identifizieren von Geräten mit bösartiger Aktivität (vgl. HLNK1, Sp. 10, Z. 60 – 63: „In those implementations where all communications 350 are inspected, the communications 350 can be processed to identify devices which are likely associated with malicious activity.“).

Die HLNK1 Figuren 1 und 2 zeigen die Systemarchitektur des Überwachungssystems 100 für ein Unternehmensnetz 200, wobei die Benutzer-Endgeräte 206, 208 („user computers“) über die Firewalls 202, 203 sowie einen

(nicht gezeigten) Enterprise-Gateway / Router an ein Weitverkehrsnetz / WAN 101 sowie das Internet, angeschlossen sind (vgl. HLNK1, Sp. 5, Z. 12 - 31).

Die eigentliche Überwachungsfunktionalität für den Datenverkehr des Unternehmens wird von den „processing nodes 110“ eines Service Providers bereitgestellt, welche sich außerhalb des Unternehmensnetzwerks befinden (vgl. HLNK1, Sp. 4, Z. 59 – 60, „In another example, the processing nodes 110 can be deployed at Internet service provider (ISP) nodes.“). Die HLNK1 offenbart „security policies“, welche den „processing nodes“ – wie bspw. Server, Gateways und Switches – von „authority nodes 120“ zur Verfügung gestellt werden (vgl. HLNK1, Sp. 3, Z. 1 - 63, Sp. 6, Z. 3 - 4, Sp. 10, Z. 39 – 59). Das Enterprise-Gateway an der Grenze zwischen Unternehmensnetz und Providernetz routet den ganzen (externen) Datenverkehr des Unternehmens zum Zweck der Dateninspektion über die „processing nodes“ des Service Providers, welche eine Proxy-Funktionalität („forward proxy“) umfassen und welche dann als „next hop router“ den Datenverkehr letztendlich an die externen Server, d.h. die Zieladressen im Internet, weiterleiten (vgl. HLNK1, Sp. 3, Z. 38 – 53, Sp. 4, Z. 45 – Sp. 5, Z. 4).

Für die Untersuchung des hinein- und/oder herausgehenden Datenverkehrs des Unternehmensnetzes umfassen die „processing nodes“ Dateninspektionsmaschinen („data inspection engines“), welche den Inhalt der Kommunikation überprüfen, Bedrohungen hinsichtlich „spyware“, „malware“, Viren und ungewünschte Inhalte, wie bspw. pornographische Inhalte, erkennen sowie darüber hinaus eine Bedrohungsklassifikation („threat classification“) bereitstellen (vgl. HLNK1, Sp. 3, Z. 1 – 14, Sp. 7, Z. 4 – 17, Sp. 7, Z. 56 - 67). Darüber hinaus wird der Zugriff auf das „Darknet“ überwacht (vgl. HLNK1, Sp.8, Z. 18 – 19, „… monitoring darknet access.“)

Im Fall eines identifizierten infizierten bzw. bösartigen Geräts - bspw. innerhalb des Unternehmensnetzes - wird gemäß der technischen Lehre der HLNK1 der

Administrator informiert, Spezialanwendungen werden zur Überprüfung der Gerätesoftware aktiviert und/oder die „processing nodes“ filtern automatisch dessen Datenverkehr, wozu ein automatisches Blockieren der Datenpakete basierend auf Regeln gehört (vgl. HLNK1, Sp. 10, Z. 60 – Sp. 11, Z. 3, „ … implement a rule preventing such devices from communicating with devices within the protected enterprise network.“ und Sp. 12, Z. 57 – Sp. 13, Z.14, insb. Sp. 13, Z. 3 - 8: „ … the notification can be provided to other processing nodes with instructions to provide filtering or detailed inspection of communications identified as similar (e.g., **based upon an origination address**). Additionally, traffic may be automatically blocked, redirected or filtered based on predefined rules.“; Hervorhebung hinzugefügt; **Merkmale 7.1 und 7.2**).

Dem Fachmann stellt sich zwangsläufig das Problem, wie das Überwachungssystem der HLNK1, dessen eigentliche Überwachungsfunktionalität für den Datenverkehr des Unternehmens von den „processing nodes 110“ eines (externen) Service Providers bereitgestellt wird, beim Vorliegen einer Adressen-Transformation (NAT) an der Netzwerk-Grenze des Unternehmensnetzes, bspw. hervorgerufen durch das o.g. Enterprise-Gateway, das infizierte bzw. bösartige Gerät innerhalb des Unternehmensnetzes identifiziert, d.h. dessen (private) „origination address“ ein-eindeutig bestimmt. Denn obwohl das bösartige Gerät den „processing node“ direkt adressiert (vgl. HLNK1, Sp.4, Z. 45 – 47, „the processing node 110 may act as a forward proxy that receives user requests to external servers addressed directly to the processing node 110.“), tauscht beim Vorliegen einer Adressen-Transformation (NAT) der Enterprise-Gateway die im Datenpaket mitübertragene private Ursprungs-IP-Adresse in eine öffentliche IP-Adresse um, wobei die Adressen-Transformation im Allgemeinen eine surjektive Abbildung darstellt, wobei der komplette private Adressraum auf signifikant weniger öffentliche Adressen transformiert wird. Ein Blockieren des Datenverkehrs im „processing node“ anhand der öffentlichen IP-Adresse würde somit nicht nur das infizierte bzw. bösartige Gerät dediziert treffen, sondern ggf. auch weitere Geräte anderer Benutzer im Unternehmensnetz.

Das ausgehend von der Lehre der NK12 bereits vorliegende Korrelationsergebnis wird nun unmittelbar durch die Ausführungsform gemäß HLNK1 verarbeitet, denn da der „processing node“ der „next hop“ des Enterprise-Gateways ist und die vom „processing node“ empfangenen Pakete die Egress-Pakete des Enterprise-Gateways sind, muss er nur für das von ihm identifizierte, verdächtige Paket (vgl. NK12, Fig. 2, „Outpacket“) im vorliegenden Korrelationsergebnis gemäß NK12 nachschlagen und dem dazugehörigen Ingress-Paket des Enterprise-Gateways die (private) „origination address“ (vgl. NK12, Fig. 2, „Inpacket“, „SrcAddr“) des bösartigen Hosts im Unternehmensnetzwerk entnehmen. Dem „processing node“ steht nämlich das Korrelationsergebnis gemäß NK12 zur Verfügung, da dieses gemäß NK12, Absatz [0030] als Grundlage für das Überwachungssystem vorgesehen ist und das gesuchte NAT-Mapping zwischen privaten und öffentlichen Adressen an der Netzwerk-Grenze nahezu in Echtzeit auf Paketbasis zum Zweck der Identifizierung eines bösartigen Geräts bzw. der wahren Paketquelle im Unternehmensnetz bereitstellt (vgl. NK12, Abs. [0030], „The ability to identify the true source of packet transmission through a boundary can provide significant benefits to network security.“, „Furthermore, it can provide a stable foundation for building tiered enterprise network architectures with an inherent capability for attribution of malicious activity. Enterprises with significant visibility and monitoring investments into the network backbone can utilize this technique to attribute malicious activity sensed at the edge of a network back to its original source.“).

Diese Identifizierung des infizierten bzw. bösartigen Geräts als Reaktion auf das Korrelieren (**Merkmal M7**) erfolgt noch vor den Verfahrensschritten gemäß den Merkmalen M7.1 und M7.2, welche die anschließend durchzuführende Regelgenerierung für die Behandlung des Datenverkehrs bzw. der Pakete des identifizierten Geräts betreffen.

Die Beklagte verneint in der Verhandlung, dass der Fachmann die Druckschriften NK12 und HLNK1 überhaupt kombinieren würde, und argumentiert damit, dass die

Anmelderin der NK12 die US Navy und die Anmelderin der HLNK1 die Firma Zscaler seien, wobei beide Anmelderinnen ihrer Auffassung nach „Zero Trust Architekturen“ bereitstellen würden und keinerlei Zugang zu irgendeinem Source-Code gewährten. Diese Argumentation der Beklagten ist in der Sache nicht zutreffend, denn für den Offenbarungsgehalt einer Vorveröffentlichung ist ausschließlich maßgeblich, welche technische Information dem Fachmann dort offenbart bzw. ggf. vom Fachmann mitgelesen wird (BGH, Urteil vom 16.12.2008, X ZR 89/07 - Olanzapin). Der Offenbarungsbegriff ist dabei kein anderer, als er auch sonst im Patentrecht zugrunde gelegt wird. Die Benennung eines bestimmten Erfinders bzw. Anmelders auf der Titelseite eines Patentdokuments bzw. sonstige bibliographische Informationen spielen daher bei der Bestimmung des Offenbarungsgehalts einer Entgegenhaltung keine Rolle.

Übrigens schlägt die NK12 selbst in Absatz [0030] keine (geheimhaltungsbedürftige) militärische, sondern sogar explizit eine zivile Anwendung in Überwachungssystemen für Unternehmensnetzwerke vor, wobei das Verfahren mittels „open source technology“ auf gängiger Hardware („commodity hardware“) zu implementieren sei.
Darüber hinaus vertreibt die Firma Zscaler zwar zum Prioritätstag (10.02.2015) des Streitpatents Cloud-basierte „Zero Trust“ Sicherheitslösungen, der Fachmann kann der ca. sieben Jahre früher (21.07.2008) angemeldeten HLNK1 darüber jedoch (noch) Nichts entnehmen.

Gleiches gilt für die Auffassung der Beklagten, dass in der HLNK1 die Benutzer und deren IP-Adressen in den „processing nodes“ bekannt seien, da in Zscaler Systemen das Benutzergerät seine eigene IP-Adresse an den „3rd Party processing node“ mittels XFF-Protokoll („X-Forward-For“) mitschicken würde (vgl. MFG11, MFG12). Denn die HLNK1 beschreibt in Figur 2 i. V. m. Spalte 4, Zeilen 13 bis 44 ausschließlich eine Benutzerschnittstelle 130 („user interface front-end 130“), welche den Benutzern („users“) einen Account für das Überwachungssystem beim Internet Service Provider zur Verfügung stellt, womit die Benutzer „security policies“

bspw. für ihren E-Mail-Verkehr definieren können. Die HLNK1 schweigt aber sowohl hinsichtlich eines potentiellen Hinterlegens der aktuellen IP-Adresse des gerade vom Benutzer verwendeten Geräts im genannten Account, welche ggf. dynamisch dem Benutzerlaptop 206 oder dem Benutzerdesktop 208 vom Router im Unternehmensnetz beim Einschalten des jeweiligen Geräts zugewiesen wird, als auch hinsichtlich einer XFF-Signalisierung der ursprünglichen IP-Adresse im http-Header, falls der Benutzer bspw. mit einem Browser im Internet surft.

Die Argumentation der Beklagten, dass ein „Monitoring System“ gemäß NK12, Absatz [0030] nur den Datenverkehr überwachen und selbstverständlich keine Pakete blockieren/droppen würde, vermag den Senat nicht zu überzeugen. Denn die HLNK1 beschreibt offensichtlich ein solches „Monitoring System“ (vgl. HLNK1, Sp. 11, Z. 45, „monitoring systems and/or methods“), welches eben gerade Pakete von infizierten bzw. bösartigen Geräten mittels den „processing nodes“ automatisch blockiert.

Auch die Argumentation der Beklagten, die NK12 wäre mit Verweis auf die SQL-Datenbank in Absatz [0026] nur auf eine reine Vorratsdatenspeicherung gerichtet, greift nicht durch. Denn zum einen ist die in der NK12, Absatz [0026] erwähnte SQL-Datenbank offensichtlich optional („can be stored“) und zum anderen kann der Fachmann der NK12 auch nirgends eine Umschreibung einer Vorratsdatenspeicherung entnehmen. Vielmehr befasst sich die Druckschrift NK12 gemäß Absätzen [0002] bis [0004] ganz allgemein mit einem Identifizieren und Tracking von Paketen, insbesondere beim Vorliegen eines NATs, Proxies oder Gateways an der Netzwerkgrenze, und gemäß Absatz [0030] im Speziellen mit der Netzwerk-Sicherheit in Unternehmensnetzen.

Der Gegenstand des Patentanspruchs 1 ist somit dem Fachmann ausgehend von der Druckschrift NK12 in Kombination mit der HLNK1 in sämtlichen Merkmalen nahegelegt.

Soweit die Klägerinnen vorgetragen und überzeugend begründet haben, dass der Fachmann ausgehend von der NK12 in Zusammenschau mit der HLNK1 in naheliegender Weise zum Gegenstand des Patentanspruchs 1 gelangt, und der Vortrag der Beklagten dies nicht entkräften konnte, kann somit dahingestellt bleiben, ob die umgekehrte Kombination ausgehend von der HLNK1 in Zusammenschau mit der NK12 den Gegenstand des Patentanspruchs 1 ebenfalls nahegelegt hätte.

Denn die Beklagte vertritt die Auffassung, dass der Fachmann als Ausgangspunkt nicht die NK12 sondern die HLNK1 gewählt hätte, was ihrer Meinung nach aber nicht zum Gegenstand des erteilten Patentanspruchs 1 führen würde.

Für den Fachmann ist es zunächst grundsätzlich ohne Bedeutung, ob andere Ausgangspunkte möglicherweise als noch näherliegend in Betracht kommen, die Wahl einer bestimmten Entgegenhaltung oder Vorbenutzung als Ausgangspunkt für die Lösung eines technischen Problems bedarf jedoch grundsätzlich der Rechtfertigung (vgl. BGH, Urteil vom 05.10.2016, X ZR 78/14 – Opto-Bauelement).

Auch wenn die HLNK1 die NAT-Problematik nicht unmittelbar anspricht und gänzlich hinsichtlich einer Korrelation von Paketen schweigt, betrifft sie - wie das Streitpatent - den Kontext der Netzwerk-Sicherheit und dort im Speziellen das Identifizieren von Paketen über die Netzwerkgrenze zwischen einem ersten Netzwerk (Unternehmensnetz) sowie einem zweiten Netzwerk (Providernetz) sowie die entsprechende Zuordnung der Pakete zu einem Paketdatenfluss bzw. einer Ursprungsquelle des Paketdatenflusses. Darüber hinaus ist dem Fachmann zum Anmeldetag bekannt, dass Enterprise-Gateways in Unternehmensnetzen eine NAT-Funktionalität umfassen und somit paketverändernd wirken, so dass die Identifizierung der Ursprungsadresse eines infizierten bzw. bösartigen Geräts im Unternehmensnetz und das automatische Blockieren des Datenverkehrs dieses Geräts durch den „processing node“ im Providernetz Kenntnisse über Paketveränderungen, insbesondere Adressenänderungen, erfordern. Schließlich beschreibt die HLNK1 in Spalte 4, Zeile 52 bis Zeile 67 sogar einen Tunnel zwischen

dem Enterprise-Gateway und dem „processing node“ sowie „MPLS labelling“, welche beide ggf. paketverändernd wirken (vgl. auch Streitpatent, Abs. [0021], „tunneling gateway“).

Dem Fachmann ist am Anmeldetag zur Umgehung bzw. zur Lösung der NAT-Problematik neben der paketbasierten und protokollunabhängigen Korrelationsmethode gemäß NK12 als weitere Alternative die von der Beklagten genannte XFF-Protokoll-Ergänzung bekannt. Der Fachmann weiß auch, dass XFF jedoch nur mit HTTP/HTTPS Verkehr funktioniert, andere Protokolle wie SNMP, FTP, Telnet, VoIP, Video, SMTP/POP/IMAP (Mail) etc. profitieren von XFF hingegen nicht. Der X-Forwarded-For (XFF) ist ein De-facto-Standard-HTTP-Header-Eintrag im Internet, wobei der Header dazu dient, die IP-Adresse des Benutzers zu übermitteln, wenn dieser durch einen Proxy auf einen Webserver zugreift (vgl. MFG11, MFG12).

Ausgehend von der HLNK1 überträgt die XFF-Protokoll-Ergänzung bei einem Internet-Zugriff, bspw. beim Browsen oder bei einem Zugriff auf einen Webserver, die (private) Ursprungsadresse des Benutzergeräts im Unternehmensnetz in dem zusätzlichen Header-Feld jedes HTTP/HTTPS-Requests im „Klartext“ an den „processing node“, der gemäß HLNK1 einen Proxy darstellt, so dass dieser auch beim Vorliegen einer Adressänderung hervorgerufen durch eine NAT im Enterprise-Gateway ein bösartiges Benutzergerät bzw. die wahre Paketquelle im Unternehmensnetz sofort identifizieren kann, ohne dass er auf eine NAT-Mapping-Tabelle des Enterprise-Gateways zugreifen muss.

Kommen für den Fachmann aber mehrere solche gangbaren Alternativen in Betracht, können folglich mehrere von ihnen naheliegend sein, wobei es grundsätzlich ohne Bedeutung ist, welche der Lösungsalternativen der Fachmann als erste in Betracht zöge (vgl. BGH, Urteil vom 16.02.2016, X ZR 5/14 – Anrufroutingverfahren; vgl. BGH, Urteil vom 06.03.2012, X ZR 50/09, juris Rn. 19; vgl. BGH, Urteil vom 06.05.2003, X ZR 113/00 - Flachantenne).

Nach Auffassung des Senats würde sich somit auch beim Wechsel des Ausgangspunkts von der NK12 zur HLNK1 die Bewertung der erfinderischen Tätigkeit nicht ändern. Der Gegenstand des Patentanspruchs 1 wäre dem Fachmann ebenfalls ausgehend von der Druckschrift HLNK1 in Kombination mit der NK12 nahegelegt.

3.2 Zur Zusammenschau von NK2 und NK12 bzw. NK2 und NK7

Der NK2 (GB 2 505 288 A), welche keine Netzsicherheit, sondern ein Abhören zum Zweck der Strafverfolgung betrifft, fehlen ausschließlich die die Protokollierung mittels Logs / „Log entries“ betreffenden Merkmale (d.h. Merkmale M3, M5, M6 jeweils teilweise). Zwar zeigt auch die NK2 eine Protokollierung mittels Log, wobei jedoch erst beim Auffinden einer Übereinstimmung/Match die Ergebnisse der Korrelation im Prozessor 170 in eine (ggf. externe) Protokolldatei geschrieben werden (vgl. NK2, Fig. 4 i. V. m. S. 11, Z. 14 – S. 12, Z. 2).

Nach Auffassung der Klägerinnen würde der Fachmann die auf Pointern zu in Session-Queues organisierte IPQuint-Paketinformation basierende Hochgeschwindigkeits-Korrelation in dem vorliegenden externen passiven Korrelationsgerät angepasst an 10 Gbit/s NAT-Geräte gemäß NK2 zugunsten einer Protokollierung mittels Logs und einer Korrelation bzw. Vergleichen von „Log entries“ modifizieren, um die Technik zu verbessern bzw. zu optimieren.

Insbesondere würde der Fachmann die NK12 heranziehen, da diese ebenfalls nahezu in Echtzeit mittels Korrelation von passiv aufgenommenen Logs eine von einem NAT an der Netzwerkgrenze veränderte Paketidentität tracken kann, wobei mittels der Verwendung von MD5-Hashes Speicherplatz eingespart werden könne (vgl. NK12, Fig. 1 – 3 i. V. m. Abs. [0003], [0006], [0018]). Gleiches würde ausgehend von der NK2 für die NK7 gelten, welche zudem zum Zwecke des „Law

enforcements“ eingesetzt werden könne, und welche vorab nur Pakete mit einer hohen Identifikationswahrscheinlicheit selektieren und die Korrelation nur mit Paketen innerhalb eines gewissen Zeitfensters effizient und speicherplatzsparend durchführen würde (vgl. NK7, Fig. 1 und Fig. 7 i. V. m. Abs. [0004], [0006], [0020], [0028] – [0029]).

Gemäß NK2 werden die Daten mit Vorliegen des Korrelationsergebnisses jedoch bereits nach ca. 100 ms aus dem Speicher gelöscht (vgl. NK2, S. 9, Z. 22 - 24). Bei dem Datendurchsatz des NAT-Geräts von 10 Gbit/s (vgl. NK2, S. 13, Z. 7 ff.) ergibt sich daher eine maximal mögliche Optimierung des Speicherplatzes von 100 ms * 10 Gbit/s = 125 MByte. Bei dem in der NK2 angesprochenen HP DL830 G7 Server mit einem großen Arbeitsspeicher von 10 GByte RAM ist dieses geringe Einsparpotential an Speicherplatz von nur 1¼ Prozent unerheblich und – nach Auffassung des Senats - nicht relevant genug, um dem Fachmann hinreichend Motivation und Veranlassung zur Modifikation des Verfahrens bzw. der Vorrichtung gemäß NK2 zu geben (vgl. NK2, S. 13, Z. 10 - 13).

Soweit diese Argumentation der Klägerinnen nicht durchgreift, haben diese ihr schriftsätzliches Vorbringen in der mündlichen Verhandlung dahingehend ergänzt, dass die Paket-Logs gemäß NK7 / NK12 letztlich nichts anderes als eine von mehreren Implementierungs-Alternativen wären, welche zum Standardrepertoire des Fachmanns zählten. Dies ist für die Beurteilung der erfinderischen Tätigkeit entscheidend.

Denn kommen für den Fachmann verschiedene Alternativen in Betracht, können mehrere von ihnen naheliegend sein, wobei es grundsätzlich ohne Bedeutung ist, welche der Lösungsalternativen der Fachmann als erste in Betracht zöge (vgl. BGH, Urteil vom 16.02.2016, X ZR 5/14 – Anrufroutingverfahren). Darüber hinaus besteht Veranlassung zum Heranziehen einer generellen Lösung, solange deren Nutzung sich dem Fachmann im Rahmen seines Standardrepertoire-Fachwissens als objektiv zweckmäßig darstellt und keine besonderen Umstände dagegen sprechen

(vgl. BGH, Urteil vom 11.03.2014, X ZR 139/10 – Farbversorgungssystem; BGH, Urteil vom 27.03.2018, X ZR 59/16 – Kinderbett; BGH, Urteil vom 26.09.2017, X ZR 109/15 - Spinfrequenz).

Damit stellt die Erzeugung von Logs und deren Verwendung bei einer Korrelation (vgl. NK12 bzw. NK7) eine gängige Lösung dar, die beim „Lawful Intercept“ System der NK2 fachmännisch ohne besondere Schwierigkeiten implementiert werden kann.

Der Gegenstand des erteilten Patentanspruchs 1 ist somit aus der Kombination der Druckschrift NK2 mit einer der Druckschriften NK7 bzw. NK12 jeweils nahegelegt und beruht somit nicht auf einer erfinderischen Tätigkeit.

3.3 Gleiches gilt für den nebengeordneten Patentanspruch 15, der eine entsprechende Vorrichtung zur Durchführung des Verfahrens u.a. gemäß Patentanspruch 1 betrifft.

4. Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 nach erteilter Fassung des Streitpatents sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 14 der erteilten Fassung des Streitpatents für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

III. Zu den Hilfsanträgen 0, 1, 1b, 2, 2b, 2c, 3, 4 und 5

Der erst in der mündlichen Verhandlung eingereichte Hilfsantrag 0 war nach § 83 Abs. 4 PatG als verspätet zurückzuweisen und deshalb keiner Sachprüfung zu unterziehen.

In keiner der Fassungen nach den Hilfsanträgen 1, 1b, 2, 2b, 2c, 3, 4 und 5 kann das Streitpatent Bestand haben, da der Gegenstand des Streitpatents mit der verteidigten Fassung nach den Hilfsanträgen 2 und 3 jeweils über den Inhalt der ursprünglichen Anmeldungsunterlagen hinausgeht, Art. II § 6 Abs. 1 Nr. 3 IntPatÜG, Art. 138 Abs. 1 Buchst. c) EPÜ i. V. m. Art. 123 Abs. 2 EPÜ, und weil dem Gegenstand des Patentanspruchs 1 der mit den Hilfsanträgen 1, 1b, 2, 2b, 2c, 3, 4 und 5 verteidigten Anspruchsfassungen des Streitpatents jeweils der Nichtigkeitsgrund der mangelnden Patentfähigkeit entgegensteht, Art. II § 6 Abs. 1 Nr. 1 IntPatÜG, Art. 138 Abs. 1 Buchst. a) EPÜ i. V. m. Art. 52, 56 EPÜ.

1. Zu Hilfsantrag 0

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 0 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1	„…“
M2_Hi0	identifying (5, 402), by a computing system, a plurality of packets (P1, P2, P3) received by a network device (122) from a host (114) located in a first network (104), **the network device not performing network address translation;**
M3 – M7.2	„…“

Das Merkmal M2 des Patentanspruchs 1 der erteilten Fassung wurde durch das Merkmal M2_Hi0 dahingehend modifiziert, dass das Netzwerk-Gerät nunmehr keine NAT-Funktionalität ausführen soll. Das Merkmal M2_Hi0 ist – analog zu einem Disclaimer - negativ formuliert, wobei die Beklagte auf die paketverändernden alternativen Netzwerk-Geräte ohne NAT-Funktionalität gemäß Streitpatent, Absätze [0020] und [0021], verweist. Dort werden bspw. Proxies und Gateways mit VPN und Tunnel genannt („VPN or tunnelling gateway“).

Der erst in der mündlichen Verhandlung formulierte und gestellte Hilfsantrag 0 war als verspätet zurückzuweisen und bleibt deshalb unberücksichtigt.

Die Voraussetzungen für eine Zurückweisung sind vorliegend gegeben, nachdem die Klägerinnen sich mit dem Gegenstand dieses Hilfsantrags bisher nicht befassen konnten und daher eine Vertagung erforderlich gewesen wäre.

Die Beschränkung mit einem negativen Merkmal ist keine geringfügige Änderung eines verteidigten Patentanspruchs. Der Hilfsantrag 0 stellt vielmehr eine neue Verteidigungslinie der Beklagten i. S. d. § 83 Abs. 4 Satz 1 PatG dar und konfrontiert die Klägerinnen mit neuen Tatsachen. Es war ihnen daher nicht zuzumuten, sich hiermit kurzfristig auseinanderzusetzen, ohne nach einschlägigem Stand der Technik bezüglich der geänderten Antragstellung zu recherchieren.

2. Zu Hilfsantrag 1

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 1 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M7	„…“

M7.1_Hi1.	generating (30), by the computing system, one or more rules (140) configured to identify packets received from the host located in the first network **and to cause the first network to drop these packets received from the host located in the first network**; and
M7.2.	„…“

Gegenüber dem Merkmal M7.1 des Patentanspruchs 1 der erteilten Fassung ist das Merkmal M7.1_Hi1 dahingehend modifiziert, dass das Rechensystem die generierte(n) Regel(n) hinsichtlich eines Fallenlassens („drop“) identifizierter Pakete durch das erste Netzwerk konfiguriert.

2.1 Der Patentanspruch 1 gemäß Hilfsantrag 1 ist zulässig. Die Änderung hinsichtlich eines „packet droppings“ ist beispielsweise dem Streitpatent, Absätze [0013] und [0049] sowie Patentanspruch 12 bzw. der Offenlegungsschrift, Absätze [15] und [51] sowie Patentanspruch 21 zu entnehmen.

2.2 Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 1 ist jedoch nicht patentfähig, da er gegenüber der Lehre der Druckschriften **NK12 und HLNK1** nicht auf einer erfinderischen Tätigkeit beruht (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Den neuen technischen Sachgehalt gemäß dem modifizierten Merkmal M7.1_Hi1 entnimmt der Fachmann ebenfalls der HLNK1; im Einzelnen:

Die HLNK1 beschreibt eine Überwachung von bidirektionalem Datenverkehr, wobei infizierte Hosts bzw. Geräte mit bösartigen Aktivitäten sowohl innerhalb des Unternehmensnetzwerks als auch außerhalb, bspw. im Internet, identifiziert und isoliert werden, indem deren Datenverkehr automatisch blockiert bzw. gefiltert wird (vgl. HLNK1, Sp. 10, Z. 60 – Sp. 11, Z. 18, Sp. 12, Z. 57 – Sp. 13, Z. 9). Das

Blockieren und Filtern gemäß HLNK1 entspricht dem, was gemäß Streipatent unter „drop“ zu verstehen ist, denn gemäß der Lehre der HLNK1 erfolgt das Blockieren/Filtern der Pakete infizierter Hosts stets im „processing node“, der sich im Providernetz außerhalb des Unternehmensnetzes befindet, d.h. Pakete bspw. von einem infizierten Host im Internet werden auf der Empfangsseite der Netzwerkvorrichtung („enterprise gateway“) im ersten Netzwerk blockiert, wohingegen Pakete eines infizierten Hosts im Unternehmensnetz auf der Sendeseite der Netzwerkvorrichtung im zweiten Netzwerk blockiert werden.

Allerdings ist im letzteren Fall eines infizierten Hosts im Unternehmensnetz der „processing node“ der „next hop router“ der Netzwerkvorrichtung bzw. des „enterprise gateways“ (vgl. HLNK1, Sp. 5, Z. 1 - 4), so dass es technisch keine Rolle spielt, ob das Paket am Eingang der Netzwerkvorrichtung im ersten Netzwerk oder am Ausgang der Netzwerkvorrichtung im zweiten Netzwerk fallengelassen wird.

Darüber hinaus zeigt die HLNK1, Figur 2 noch eine Firewall FW 202 an der Grenze zwischen Unternehmensnetz und Providernetz, so dass es für den Fachmann naheliegt, auch diesen bei Bedarf zur Isolation des infizierten Hosts im Unternehmensnetz heranzuziehen. Zum Beleg dieses Fachwissens wird bspw. auf die Druckschrift **HLNK2**, Figur 5.1 i. V. m. Absatz 5.1 verwiesen.

Damit sind sämtliche Merkmale des Patentanspruchs 1 gemäß Hilfsantrag 1 aus der Zusammenschau der Druckschriften **NK12 und HLNK1** nahegelegt.

Gleiches gilt für den nebengeordneten Patentanspruch 15 in der Fassung gemäß Hilfsantrag 1.

2.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 1 sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 14 für nichtig zu erklären, da die

Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

3. Zu Hilfsantrag 1b

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 1b wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M7	„…“
M7.1_Hi1b	generating (30), by the computing system, one or more rules (140) configured to identify **and drop** packets received from the host located in the first network; and
M7.2_Hi1b	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify **and drop** packets received from the host located in the first network.

Die Merkmale M7.1_Hi1b und M7.2_Hi1b sind gegenüber der erteilten Fassung so geändert, dass das Rechensystem die generierte(n) Regel(n) hinsichtlich eines Fallenlassens („drop“) identifizierter Pakete konfiguriert und damit den Paketfilter versorgt. Im Gegensatz zum Hilfsantrag 1 bleibt aber offen, ob die Filterung im ersten oder zweiten Netzwerk erfolgen soll.

3.1 Der Hilfsantrag 1b ist zulässig. Zur Begründung wird entsprechend auf die Ausführungen des entsprechenden Abschnitts III.2.1 zum Hilfsantrag 1 verwiesen.

3.2 Die Merkmale M7.1_Hi1b und M7.2_Hi1b können keine erfinderische Tätigkeit begründen.

Die HLNK1 umfasst ein automatisches Blockieren bzw. Filtern des Datenverkehrs von identifizierten bösartigen/infizierten Hosts, welche sich bspw im Unternehmensnetz befinden, wobei das Blockieren/Filtern mittels Regeln stets im „processing node“ im Providernetz erfolgt (vgl. HLNK1, Sp. 10, Z. 60 – Sp. 11, Z. 18, Sp. 12, Z. 57 – Sp. 13, Z. 9). Hierzu gelten auch die Ausführungen zum Hilfsantrag 1 entsprechend (siehe dazu Abschnitt III.2.2).

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Damit beruht der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 1b ebenfalls nicht auf einer erfinderischen Tätigkeit.

Gleiches gilt für den nebengeordneten Patentanspruch 13 in der Fassung gemäß Hilfsantrag 1b.

3.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 1b sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 12 für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

4. Zu Hilfsantrag 2

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 2 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M5	„…“
M6_Hi2	correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device **to determine that the host located in the second network is associated with a malicious entity**; and
M7	„…“
M7.1_Hi1	generating (30), by the computing system, one or more rules (140) configured to identify packets received from the host located in the first network **and to cause the first network to drop these packets received from the host located in the first network**; and
M7.2_Hi1b	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify **and drop** packets received from the host located in the first network.

Merkmal M6_Hi2 wurde dahingehend geändert, dass beim Korrelieren ein Host im zweiten Netzwerk als mit einer bösartigen Einheit assoziiert bestimmt wird.
Die modifizierten Merkmale M7.1_Hi1 und M7.2_Hi1b lauten analog zu den entsprechenden Merkmalen in den vorangegangenen Hilfsanträgen 1 bzw. 1b.

4.1 Die Änderung gemäß Merkmal M6_Hi2 hinsichtlich eines Bestimmens eines „malicious hosts“ im zweiten Netzwerk im Verfahrensschritt des Korrelierens ist unzulässig, da der Gegenstand des Patentanspruchs 1 in der verteidigten Fassung nach Hilfsantrag 2 über den Inhalt der ursprünglichen Anmeldungsunterlagen (vgl.

NK21) hinausgeht (Art. II § 6 Abs. 1 Nr. 3 IntPatÜG i.V.m. Art. 138 Abs. 1 Buchst. c), Art. 123 Abs. 2 EPÜ).

Zwar offenbart die ursprüngliche Anmeldung eine Bestimmung eines Hosts 108, welcher mit einer bösartigen Einheit assoziiert ist (vgl. Offenlegungsschrift, Abs. [50] - [51], Anspruch 21), diese Bestimmung erfolgt jedoch nicht mittels Korrelieren, sondern vielmehr bei einer nicht näher beschriebenen Untersuchung des Datenverkehrs („For example, **one or more of the communications between host 108 and 114** (e.g., P1 and P1', P2 and P2', P3 and P3', P10 and P10', or P11 and P11') **may be indicative of malware** installed by a computing device associated with host 108 (e.g., the malicious entity) on a computing device associated with host 114, and rule(s) 140 may be configured to prevent the spread of the malware."; Hervorhebung hinzugefügt).
Darüber hinaus offenbart die Offenlegungsschrift, Absatz [24] zwar eine Detektion einer Verschleierung durch eine bösartige Einheit mittels Korrelation, dabei handelt es sich jedoch nicht um einen Host sondern um die Netzwerkvorrichtung selbst (dort: „For example, network device(s) 122 may be employed by a malicious entity to attempt to obfuscate, spoof, or proxy for the identity or location of host 114 (e.g., network device(s) 122 may be employed as part of a man-in-the-middle attack).").

4.2 Ließe man die Unzulässigkeit der Anspruchsfassung dahinstehen, würde das hier hinzugefügte Merkmal **M6_Hi2** vor dem Hintergrund der Druckschriften **NK12 und HLNK1** keine erfinderische Tätigkeit begründen (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die HLNK1 lehrt ebenfalls eine Detektion einer bösartigen Einheit im zweiten Netzwerk (vgl. HLNK1, Sp. 10, Z. 60 – Sp. 11, Z. 3, „In those implementations where all communications 350 are inspected, the communications 350 can be processed to identify devices which are likely associated with malicious activity…. If such devices are outside of the enterprise network, the authority node policy data can be

used to implement a rule preventing such devices from communicating with devices within the protected enterprise network.“).

Zu den modifizierten Merkmalen M7.1_Hi1 und M7.2_Hi1b wird zur Begründung jeweils auf die entsprechenden Ausführungen zum Hilfsantrag 1 (siehe dazu Abschnitt III.2.2) bzw. Hilfsantrag 1b (siehe dazu Abschnitt III.3.2) verwiesen.
Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Gleiches gilt für den nebengeordneten Patentanspruch 14 in der Fassung gemäß Hilfsantrag 2.

5. Zu Hilfsantrag 2b

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 2b wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M3	„…“
M4_Hi2b	identifying (8, 406), by the computing system, a plurality of packets (P1', P2', P3') transmitted by the network device to a **malicious** host (108) located in a second network (102);
M5 - M7	„…“
M7.1_Hi1b	generating (30), by the computing system, one or more rules (140) configured to identify **and drop** packets received from the host located in the first network; and
M7.2_Hi2b	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify **and drop** packets received from the host located in the first network **in order to prevent the spread of malware installed by the malicious host (108) located in the second network (102) on the host (114) located in the first network (104).**

Merkmal M4_Hi2b umfasst ein Senden von Paketen an ein bösartiges Gerät im zweiten Netzwerk und Merkmal M7.2_Hi2b betrifft das Zweckmerkmal, ein (Weiter-)Verbreiten der Malware durch einen infizierten Host im ersten Netzwerk zu unterbinden.
Das modifizierte Merkmal M7.1_Hi1b lautet analog zu dem gemäß Hilfsantrag 1b.

5.1 Die Anspruchsfassung gemäß Hilfsantrag 2b ist zulässig. Die Änderungen gemäß den Merkmalen M4_Hi2b und M7.2_Hi2b hinsichtlich eines Identifizierens von Paketen an ein bösartiges Gerät im zweiten Netzwerk sowie eines Verhinderns einer Malware-Verbreitung durch den Host im ersten Netzwerk ergeben sich aus dem Streitpatent, Absatz [0049] bzw. der Offenlegungsschrift, Absatz [51] („For example, one or more of the communications between host 108 and 114 (e.g., P1 and P1', P2 and P2', P3 and P3', P10 and P10', or P11 and P11') may be indicative of malware installed by a computing device associated with host 108 (e.g., the malicious entity) on a computing device associated with host 1 14, and rule(s) 140 may be configured to prevent the spread of the malware.“)

5.2 Dennoch können die hier neu hinzufügten Merkmale **M4_Hi2b und M7_Hi2b** vor dem Hintergrund der Druckschriften **NK12 und HLNK1** ebenfalls keine erfinderische Tätigkeit begründen (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die HLNK1 offenbart eine Überwachung von bidirektionalem Datenverkehr, wobei infizierte Hosts bzw. Geräte mit bösartigen Aktivitäten sowohl innerhalb des Unternehmensnetzwerks als auch außerhalb, bspw. im Internet, identifiziert und isoliert werden, indem deren Datenverkehr automatisch blockiert bzw. gefiltert wird (vgl. HLNK1, Sp. 10, Z. 60 – Sp. 11, Z. 18, Sp. 12, Z. 57 – Sp. 13, Z. 9).

Zum modifizierten Merkmal M7.1_Hi1b wird zur Begründung auf die entsprechenden Ausführungen zum Hilfsantrag 1b (siehe dazu Abschnitt III.3.2) verwiesen.

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Damit beruht der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 2b nicht auf einer erfinderischen Tätigkeit.

Gleiches gilt für den nebengeordneten Patentanspruch 13 in der Fassung gemäß Hilfsantrag 2b.

5.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 2b sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 12 für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

6. Zu Hilfsantrag 2c

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 2c wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M3	„…“
M4_Hi2c	identifying (8, 406), by the computing system, a plurality of packets (P1', P2', P3') transmitted by the network device to a host (108) located in a

	second network (102), **the communication related to the packets (P1', P2', P3') being indicative of malware installed by the host (108) located in the second network (102) on the host (114) located in the first network (104);**
M5 - M7	„…“
M7.1_Hi1b	generating (30), by the computing system, one or more rules (140) configured to identify **and drop** packets received from the host located in the first network; and
M7.2_Hi2b	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify **and drop** packets received from the host located in the first network **in order to prevent the spread of malware installed by the malicious host (108) located in the second network (102) on the host (114) located in the first network (104).**

Merkmal M4_Hi2c betrifft das Identifizieren einer Kommunikation mit Malware anzeigenden Paketen, wobei ein Host im ersten Netzwerk von einem Host aus dem zweiten Netzwerk mit Malware infiziert wurde.
Die modifizierten Merkmale M7.1_Hi1b und M7.2_Hi2b lauten analog zu den entsprechenden Merkmalen in den Hilfsanträgen 1b bzw. 2b.

6.1 Die Anspruchsfassung gemäß Hilfsantrag 2c ist zulässig. Die Änderungen gemäß Merkmal M4_Hi2c hinsichtlich eines Identifizierens von Paketen eines von einem Host im zweiten Netzwerk infizierten Hosts im ersten Netzwerk ergeben sich aus dem Streitpatent, Absatz [0049] bzw. der Offenlegungsschrift, Absatz [51] („For example, one or more of the communications between host 108 and 114 (e.g., P1 and P1', P2 and P2', P3 and P3', P10 and P10', or P11 and P11') may be indicative of malware installed by a computing device associated with host 108 (e.g., the malicious entity) on a computing device associated with host 1 14, and rule(s) 140 may be configured to prevent the spread of the malware.“)

6.2 Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 2c umfassend das neu hinzugetretene Merkmal **M4_Hi2c** beruht vor dem Hintergrund der Druckschriften **NK12 und HLNK1** ebenfalls nicht auf erfinderischer Tätigkeit (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die HLNK1 offenbart eine Überwachung von bidirektionalem Datenverkehr, wobei infizierte Hosts bzw. Geräte mit bösartigen Aktivitäten sowohl innerhalb des Unternehmensnetzwerks als auch außerhalb, bspw. im Internet, identifiziert und isoliert werden, indem deren Datenverkehr automatisch blockiert bzw. gefiltert wird (vgl. HLNK1, Sp.10, Z. 60 – Sp.11, Z.18, Sp. 12, Z. 57 – Sp. 13, Z. 9).

Zu den modifizierten Merkmalen M7.1_Hi1b und M7.2_Hi2b wird zur Begründung jeweils auf die entsprechenden Ausführungen zum Hilfsantrag 1b (siehe dazu Abschnitt III.3.2) bzw. Hilfsantrag 2b (siehe dazu Abschnitt III.5.2) verwiesen.

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Damit beruht der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 2c ebenfalls nicht auf einer erfinderischen Tätigkeit.

Gleiches gilt für den nebengeordneten Patentanspruch 13 in der Fassung gemäß Hilfsantrag 2c.

6.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 2c sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 12 für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

7. Zu Hilfsantrag 3

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 3 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M5	„…“
M6_Hi3	correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device **to determine that at least one packet of the plurality of packets received by the network device is correlated with at least one packet of the plurality of packets transmitted by the network device**; and
M7 – M7.2	„…“

Merkmal M6_Hi3 umfasst die Zweckangabe, dass der Zweck der Korrelation der multiplen Eingangs- und Ausgangspakete die Bestimmung einer Korrelation zwischen zumindest einem Eingangs- sowie einem Ausgangspaket ist.

7.1 Die Änderung gemäß Merkmal M6_Hi3 hinsichtlich eines Korrelierens von empfangenen mit gesendeten Paketen ist unzulässig. Der Gegenstand des Patentanspruchs 1 in der verteidigten Fassung nach Hilfsantrag 3 geht über den Inhalt der ursprünglichen Anmeldungsunterlagen (vgl. NK21) hinaus (Art. II § 6 Abs. 1 Nr. 3 IntPatÜG i.V.m. Art. 138 Abs. 1 Buchst. c), Art. 123 Abs. 2 EPÜ), da gemäß Offenlegungsschrift, Absätze [36] bis [38] am Netzwerkgerät die gesendeten mit den empfangen Paketen korreliert werden sowie eine Übereinstimmung zwischen einem gesendeten und einem empfangenen Paket festgestellt wird und nicht umgekehrt.

Darüber hinaus sind nach Auffassung des Senats die Erfordernisse für eine Beschränkung nicht erfüllt. Der ureigenste Zweck einer (Kreuz-)Korrelation zwischen multiplen eingangsseitigen und ausgangsseitigen Datenpaketen ist stets die Bestimmung von Korrelationskoeffizienten, welche die „Ähnlichkeit“ zwischen den Eingangs- und den Ausgangs-Daten spezifizieren. Die Offenlegungsschrift beschreibt in den Absätzen [36] - [37], dass mittels der Korrelation ein Bestimmen von Übereinstimmungen zumindest von Teilen der Datenpakete festgestellt werden soll und dass ggf. Punktzahlen („scores“) hinsichtlich der Übereinstimmungen vergeben werden sollen.
Es handelt sich bei den Änderungen im Merkmal M4_Hi3 somit offensichtlich um ein „Nullmerkmal“, denn beim Zugrundelegen der Definition aus dem Streitpatent wird dem ursprünglichen Merkmal M6 nichts hinzugefügt, was zu einer Beschränkung führen würde.

7.2 Ließe man die Unzulässigkeit der Anspruchsfassung dahinstehen, würde der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 3 umfassend das neu hinzugetretene Merkmale **M6_Hi3** vor dem Hintergrund der Druckschriften **NK12 und HLNK1** ebenfalls nicht auf erfinderischer Tätigkeit beruhen (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die NK12 lehrt eine Korrelation multipler Eingangs- sowie Ausgangs-Pakete, wobei eine Übereinstimmung („match“) zwischen jeweils einem Ausgangs- sowie einem Eingangs-Paket bestimmt wird (vgl. NK12, Fig. 2 – 3, Abs. [0006] – [0008], [0021] – [0025]).

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Gleiches gilt für den nebengeordneten Patentanspruch 15 in der Fassung gemäß Hilfsantrag 3.

8. Zu Hilfsantrag 4

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 4 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M5	„…“
M6_Hi4	correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device, **wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more times indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device; and**
M7 – M7.2	„…“

Merkmal M6_Hi4 betrifft nunmehr ein Korrelieren der sendeseitigen mit den empfangsseitigen Paketen, umfassend ein Vergleichen von Zeiten, welche von den jeweiligen „Log entries“ angezeigt werden.

8.1 Patentanspruch 1 gemäß Hilfsantrag 4 ist zulässig, da sowohl im Streitpatent als auch in der Offenlegungsschrift eine Korrelation mit einem Vergleichen von Zeiten bzw. Zeitstempeln in den „Log entries“ offenbart wird (vgl. Streitpatent, Abs. [0033], [0036], [0047] und Ansprüche 7 - 9; vgl. Offenlegungsschrift, Abs. [36], [38], [49] und Ansprüche 15 - 18).

8.2 Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 4 umfassend das im Vergleich zur erteilten Fassung einzig neu hinzugetretene Merkmal **M6_Hi4** beruht vor dem Hintergrund der Druckschriften **NK12 und HLNK1** ebenfalls nicht auf erfinderischer Tätigkeit (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die NK12 lehrt eine Korrelation multipler Ausgangs-/Eingangs-Pakete unter Berücksichtigung von Zeitstempeln, welche jeweils in den „Log entries“ für die Eingangs- sowie die Ausgangs-Pakete hinterlegt sind (vgl. NK12, Fig. 2, „Correlation by time“, Abs. [0006], [0008], [0022] – [0023], Anspruch 19).

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Damit beruht der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 4 ebenfalls nicht auf einer erfinderischen Tätigkeit.

Gleiches gilt für den nebengeordneten Patentanspruch 14 in der Fassung gemäß Hilfsantrag 4.

8.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 4 sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 13 für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

9. Zu Hilfsantrag 5

Auf der Grundlage der Gliederung gemäß erteilter Fassung aufbauend, kann der Patentanspruch 1 gemäß Hilfsantrag 5 wie folgt gegliedert werden (Änderungen im Vergleich zur erteilten Fassung fett hervorgehoben):

M	**Merkmalstext in Englisch**
M1 – M5	„…“
M6_Hi4	correlating (16, 410), by the computing system and based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device, the plurality of packets transmitted by the network device with the plurality of packets received by the network device, **wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received by the network device comprises comparing one or more times indicated by the plurality of log entries corresponding to the plurality of packets received by the network device with one or more times indicated by the plurality of log entries corresponding to the plurality of packets transmitted by the network device; and**
M7 – M7.1	„…“
M7.2_Hi5	provisioning (31, 32) a packet-filtering device (124, 126) with the one or more rules configured to identify packets received from the host located in the first network; **wherein: generating the plurality of log entries corresponding to the plurality of packets received by the network device comprises generating a plurality of timestamps indicating times corresponding to receipt, by the network device, of the plurality of packets received by the network device; generating the plurality of log entries corresponding to the plurality of packets transmitted by the network device comprises generating a plurality of timestamps indicating times corresponding to transmission, by the network device, of the plurality of packets transmitted by the network device; and comparing the one or more times indicated by the plurality of log entries comprises comparing one or more times indicated by the plurality of timestamps indicating times corresponding to receipt with one or more times indicated by the**

	plurality of timestamps indicating times corresponding to transmission.

Merkmal M7.2_Hi5 betrifft nunmehr ein Korrelieren der Pakete umfassend ein Vergleichen von Zeitstempeln („timestamps“), welche den „Log entries“ der gesendeten und der empfangenen Pakete jeweils hinzugefügt werden. Das modifizierte Merkmal M6_Hi4 lautet analog wie in Hilfsantrag 4.

9.1 Patentanspruch 1 gemäß Hilfsantrag 5 ist zulässig, da sowohl im Streitpatent als auch in der Offenlegungsschrift ein Vergleichen von Zeitstempeln in den „Log entries“ offenbart wird (vgl. Streitpatent, Abs. [0033], [0036], [0047] und Ansprüche 7 - 9; vgl. Offenlegungsschrift, Abs. [35], [38], [49] und Ansprüche 15 - 18).

9.2 Der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 5 umfassend das im Vergleich zum Hilfsantrag 4 einzig neu hinzugetretene Merkmal **M7.2_Hi5** beruht vor dem Hintergrund der Druckschriften **NK12 und HLNK1** ebenfalls nicht auf erfinderischer Tätigkeit (vgl. Art. II § 6 Abs. 1 Nr. 1 IntPatÜG i. V. m. Art. 138 Abs. 1 Nr. 1, Art. 52, 56 EPÜ).

Denn die NK12 lehrt eine Korrelation multipler Eingangs- sowie Ausgangs-Pakete unter Berücksichtigung von Zeitstempeln („timestamps“), wobei diese jeweils in den „Log entries“ für die Eingangs- sowie die Ausgangs-Pakete enthalten sind (vgl. NK12, Fig. 2, „Correlation by time“, Abs. [0006], [0008], [0022] – [0023], Ansprüche 4, 5, 16, 17, 19).

Insbesondere beschreibt die NK12 ein Vergleichen der Zeitstempel für die Empfangszeiten mit denjenigen der Sendezeiten, um so eine konsistente Entscheidung hinsichtlich einer Paketidentität treffen zu können (vgl. NK12, Abs. [0023], „Furthermore, it is also observed that the time in TimeSecs (seconds) are equal, but the time in TimeMSecs (milliseconds) differ by 814 milliseconds. In other words, the inside packet arrived 814 milliseconds before the outside packet, which

is consistent with the inside packet sensing the packet first. In this case, the identity of the packet is the SrcAddr (source address) of the packet sensed from each side, which is 132.xxx.xxx.102/172.xxx.xxx.240.“).

Zu dem modifizierten Merkmal M6_Hi4 wird zur Begründung auf die entsprechenden Ausführungen zum Hilfsantrag 4 (siehe dazu Abschnitt III.8.2) verwiesen.

Zu den im Vergleich zur erteilten Fassung unveränderten Merkmalen wird auf die entsprechenden Ausführungen in Abschnitt II.3.1 verwiesen.

Damit beruht der Gegenstand des Patentanspruchs 1 gemäß Hilfsantrag 5 ebenfalls nicht auf einer erfinderischen Tätigkeit.

Gleiches gilt für den nebengeordneten Patentanspruch 13 in der Fassung gemäß Hilfsantrag 5.

9.3 Da die Beklagte die abhängigen Unteransprüche nicht isoliert verteidigt, bedürfen diese keiner gesonderten Prüfung. Mit dem sich als nicht patentfähig erweisenden Patentanspruch 1 gemäß Hilfsantrag 5 sind auch die darauf direkt oder indirekt rückbezogenen Unteransprüche 2 bis 12 für nichtig zu erklären, da die Beklagte weder geltend gemacht hat noch sonst ersichtlich ist, dass die zusätzlichen Merkmale dieser Ansprüche zu einer anderen Beurteilung der Patentfähigkeit führen (vgl. BGH, Beschluss vom 27. Juni 2007 – X ZB 6/05, GRUR 2007, 862 Leitsatz – Informationsübermittlungsverfahren II; BGH, Urteil vom 29. September 2011 - X ZR 109/08 1. Leitsatz – Sensoranordnung).

B.

N e b e n e n t s c h e i d u n g e n

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.

R e c h t s m i t t e l b e l e h r u n g

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 der Verkündung (§ 110 Abs. 3 PatG).

Die Berufung wird nach § 110 Abs. 2 PatG durch Einreichung der Berufungsschrift beim Bundesgerichtshof, Herrenstr. 45a, 76133 Karlsruhe eingelegt.

Voit Dr. Wollny Bieringer Dr. Meiser Dr. Ball