BUNDESGERICHTSHOF

IM NAMEN DES VOLKES

URTEIL

X ZR 133/22

Verkündet am:
12. November 2024
Anderer
Justizangestellte
als Urkundsbeamtin
der Geschäftsstelle

in der Patentnichtigkeitssache

ECLI:DE:BGH:2024:121124UXZR133.22.0

Der X. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 12. November 2024 durch den Vorsitzenden Richter Dr. Bacher, den Richter Dr. Deichfuß und die Richterinnen Dr. Marx, Dr. Rombach und Dr. von Pückler

für Recht erkannt:

Die Berufung gegen das Urteil des 5. Senats (Nichtigkeitssenats) des Bundespatentgerichts vom 14. November 2022 wird auf Kosten der Beklagten zurückgewiesen.

Von Rechts wegen

Tatbestand:

1 Die Beklagte ist Inhaberin des mit Wirkung für die Bundesrepublik Deutschland erteilten europäischen Patents 3 257 202 (Streitpatents), das am 25. November 2015 unter Inanspruchnahme einer US-amerikanischen Priorität vom 10. Februar 2015 angemeldet wurde und die Korrelierung von Paketen in Kommunikationsnetzen betrifft.

2 Patentanspruch 1, auf den dreizehn Ansprüche zurückbezogen sind, lautet in der Verfahrenssprache:

> 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.

3 Patentanspruch 15 stellt eine Vorrichtung unter Schutz, die dazu konfiguriert ist, ein entsprechendes Verfahren durchzuführen.

4 Die Klägerinnen machen geltend, der Gegenstand des Streitpatents sei nicht patentfähig und gehe über den Inhalt der ursprünglichen Anmeldeunterlagen hinaus. Die Beklagte hat das Streitpatent in der erteilten Fassung und hilfsweise in neun geänderten Fassungen verteidigt.

5 Das Patentgericht hat das Streitpatent für nichtig erklärt. Dagegen richtet sich die Berufung der Beklagten, die das Streitpatent in erster Linie in der Fassung des erstinstanzlichen Hilfsantrags 1 und ergänzend mit fünf weiteren ihrer erstinstanzlichen Hilfsanträge sowie zehn neuen Hilfsanträgen in geänderten Fassungen verteidigt. Die Klägerinnen treten dem Rechtsmittel entgegen.

Entscheidungsgründe:

6 Die zulässige Berufung ist unbegründet.

7 I. Das Streitpatent betrifft die Korrelierung von Paketen in Kommunikationsnetzen.

8 1. Nach der Beschreibung des Streitpatents erfolgt die Kommunikation zwischen Endpunkten von paketvermittelten Netzwerken (packet-switched networks), beispielsweise von Hosts, in Form von Paketflüssen bzw. Datenströmen (flows). Pakete eines Datenstroms unterscheiden sich von Paketen, die einem anderen Datenstrom zugeordnet sind, beispielsweise durch Informationen in ihren Kopfzeilen (header).

9 Am Übergang zwischen zwei Netzwerken kann es zu Änderungen an den Paketen kommen (Abs. 2), zum Beispiel durch Übersetzung von Netzwerkadressen (network address translation, NAT), Proxy-Server oder Gateways (Abs. 18 ff.). Hierdurch kann der Datenstrom, dem das Paket zugeordnet ist, verschleiert werden (obfuscate), (Abs. 2). Dies kann von einer bösartigen Entität

(malicious entity) dazu genutzt werden, die Identität oder den Standort des entsendenden Hosts zu verschleiern oder zu verfälschen (Abs. 18 ff.).

10 2. Das Streitpatent betrifft vor diesem Hintergrund das technische Problem, die Zugehörigkeit von Paketen zu einem bestimmten Datenstrom auch dann bestimmen zu können, wenn die Pakete verändert worden sind.

11 3. Zur Lösung schlägt das Streitpatent in Patentanspruch 1 in der nunmehr in erster Linie verteidigten Fassung des erstinstanzlichen Hilfsantrags 1 ein Verfahren vor, dessen Merkmale sich wie folgt gliedern lassen (Änderungen gegenüber der erteilten Fassung sind hervorgehoben):

12

1	A method comprising:	Verfahren, umfassend:
2	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;
3	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 Logeinträgen (306, 308, 310), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden;
4	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;
5	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 Logeinträgen (312, 314, 316), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden;

6	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 Logeinträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden und der Vielzahl von Logeinträgen, 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
7	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:
7.1[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 to cause the first network to drop these 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 um das erste Netzwerk zu veranlassen, die vom Host, der sich im ersten Netzwerk befindet, empfangenen Pakete zu verwerfen; und
7.2	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.

13 4. Einige Merkmale bedürfen der näheren Erläuterung.

14 a) Eine Netzwerkvorrichtung (network device) im Sinne von Patentanspruch 1 muss nach den Merkmalen 2 und 4 dazu geeignet sein, (mindestens) von einem Host Datenpakete zu empfangen und diese (mindestens) an einen anderen Host zu übertragen, der sich in einem zweiten Netzwerk befindet.

15 aa) Patentanspruch 1 gibt nicht zwingend vor, dass die Netzwerkvorrichtung die Pakete vor der Weiterleitung verändert. Die in den Merkmalen 2 bis 5 vorgesehenen Verfahrensschritte zielen aber darauf ab, das in Merkmal 6 vorgesehene Korrelieren von Datenpaketen auch dann zu ermöglichen, wenn die Netzwerkvorrichtung diese verändert hat.

16 bb) Um das Korrelieren der Datenpakete zu ermöglichen, sehen die Merkmale 2 bis 5 vor, dass ein Rechensystem (computing system) die empfangenen und die übertragenen Pakete identifiziert und Logeinträge erzeugt, die diesen Paketen entsprechen.

17 cc) Auf der Grundlage dieser Logeinträge korreliert das Rechensystem gemäß Merkmal 6 die übertragenen mit den empfangenen Datenpaketen.

18 Wie das Patentgericht zutreffend und insoweit nicht angegriffen ausgeführt hat, ergibt sich aus dem Umstand, dass jeweils eine Vielzahl von Datenpaketen miteinander korreliert werden muss, dass es nicht genügt, empfangene und übertragene Datenpakete einander paarweise zuzuordnen. Vielmehr muss die Korrelation auch ermöglichen, das Verhältnis mehrerer empfangener bzw. übertragener Datenpakete zueinander zu bestimmen, etwa deren Zugehörigkeit zu einem bestimmten Datenstrom (flow).

19 Dieses Verständnis steht in Einklang mit den Ausführungen in der Beschreibung, wonach die Zugehörigkeit von Paketen zu einem Datenstrom durch Änderungen an der Netzwerkgrenze verschleiert werden (Abs. 2, Abs. 29,

Abs. 41) und das Korrelieren der Pakete die Bestimmung der zu einem Datenstrom gehörenden Pakete ermöglichen kann (Abs. 7, Abs. 52).

20 Merkmal 6 gibt zwar nicht zwingend vor, dass das Korrelieren die Zuordnung von Paketen zu einem Datenstrom ermöglichen muss. Die darin formulierte Vorgabe, dass eine Vielzahl von Paketen zu korrelieren ist, eröffnet aber die Möglichkeit, solche oder ähnliche Zuordnungen vorzunehmen.

21 dd) Merkmalsgruppe 7 gibt vor, dass das Korrelieren der Datenpakete zum Erzeugen von Regeln genutzt wird, anhand derer mit Hilfe einer Paketfiltervorrichtung Pakete identifiziert werden können, die die Netzwerkvorrichtung von dem im ersten Netzwerk angeordneten Host empfängt.

22 b) Der Aufbau der für das Verfahren eingesetzten Komponenten und Netzwerke ist in Patentanspruch 1 nicht näher vorgegeben.

23 aa) Die Hosts und die Netzwerkvorrichtung können nach der Beschreibung etwa als Server, Router, Gateway, Switch oder Access Point ausgebildet sein und jeweils auch mehrere Geräte umfassen (Abs. 12, Abs. 19 ff., Abs. 55).

24 bb) Die Funktionen des Rechensystems können nach der Beschreibung in Hard- oder Softwarevarianten oder einer Kombination ausgeführt werden (Abs. 54). Sie können auf einem Netzwerkgerät angeordnet oder auf mehrere Geräte und Netzwerke verteilt sein (Abs. 53, 55).

25 Bei dem in der Beschreibung geschilderten Ausführungsbeispiel, das in der nachfolgend wiedergegebenen Figur 1 schematisch dargestellt ist, umfasst das Rechensystem mehrere miteinander verbundene Komponenten.

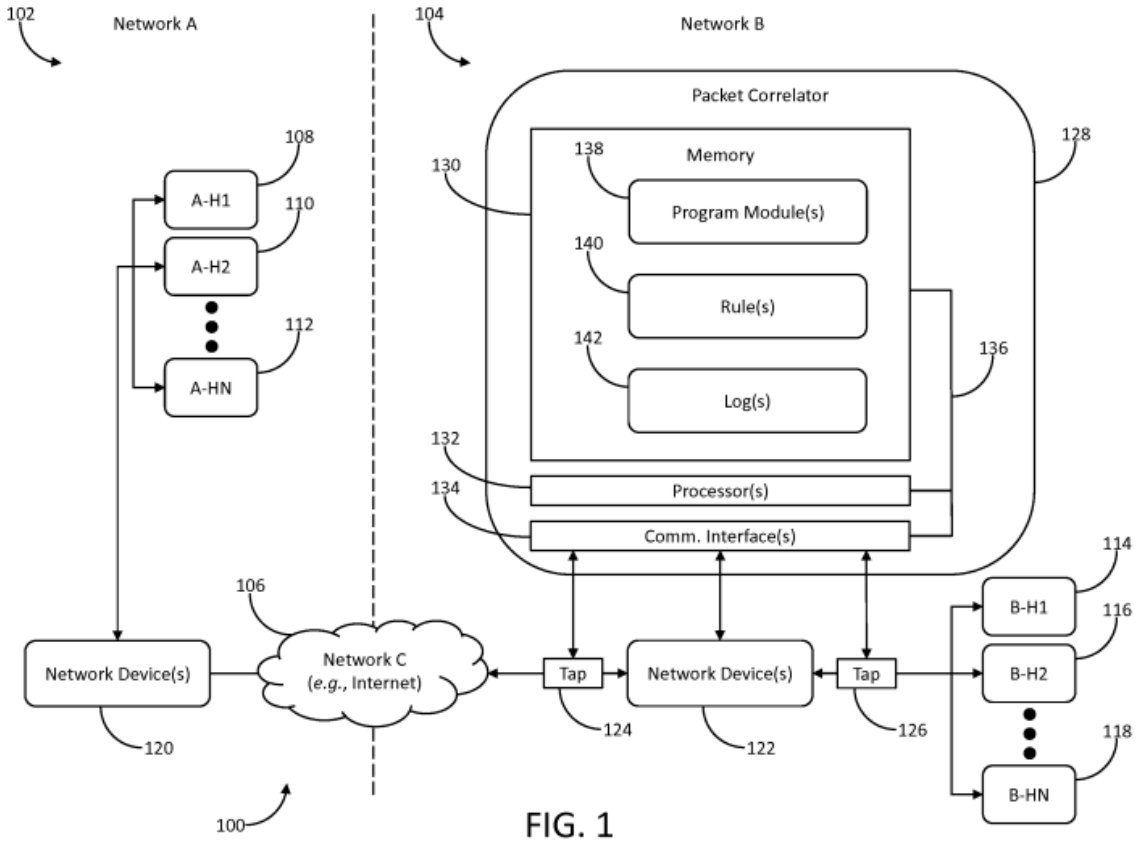


FIG. 1

26 Die Korreliervorrichtung (128) ist über Schnittstellen mit der Netzwerkvorrichtung (122) und zwei Abgreifvorrichtungen (tap devices 124, 126) verbunden. Letztere sind an den Übergängen in das erste bzw. zweite Netzwerk angeordnet. Sie können so ausgestaltet sein, dass sie Pakete, die bestimmten, in Regeln definierten Kriterien entsprechen, identifizieren und die identifizierten Pakete zum Beispiel weiterleiten, verwerfen, kopieren oder Loginformationen daraus ableiten. Hierzu können sie eine oder mehrere Vorrichtungen zur Paketfilterung umfassen (Abs. 13 Z. 12-33).

27 cc) Bei den Netzwerken kann es sich zum Beispiel um lokale Netzwerke (local area networks, LAN), Weitverkehrsnetze (wide area network, WAN), virtuelle private Netzwerke (VPN) oder Kombinationen davon handeln (Abs. 12).

28 c) Die in den Merkmalen 3 und 5 vorgesehenen Logeinträge enthalten Daten, die sich auf das jeweilige Datenpaket beziehen.

29 aa) Nach der Beschreibung kann es sich dabei um Informationen handeln, die aus den Paketen selbst stammen, zum Beispiel die Netzwerkebene, die Adressen oder Ports von Quelle oder Ziel, Signaturen, Schlüssel, Zeitstempel, Identifikatoren für Anwendungen, Sitzungen und Datenströme oder Authentifizierungsinformationen. Es kann sich aber auch um Umgebungsinformationen handeln, etwa den Zeitpunkt der Ankunft an der Netzwerkvorrichtung oder die Schnittstelle, über die das Paket angekommen ist (Abs. 16).

30 Welche Daten im Einzelnen im Logeintrag hinterlegt werden, ist in Patentanspruch 1 nicht näher festgelegt.

31 Dies lässt die Möglichkeit offen, den gesamten Inhalt eines Pakets zu hinterlegen. In Einklang damit sieht die Beschreibung vor, dass die zur Erzeugung der Logdaten eingesetzten Abgreifvorrichtungen so ausgestaltet sein können, dass sie identifizierte Pakete oder darin enthaltene Daten kopieren können (Abs. 13).

32 bb) Diese Logeinträge müssen nach den Merkmalen 3 und 5 für die empfangenen und für die übertragenen Pakete jeweils gesondert erstellt werden.

33 Aus der Vorgabe, dass die Vielzahl der Logeinträge der Vielzahl der Pakete entsprechen muss, ergibt sich ferner, dass eine klare Zuordnung zwischen einem Eintrag und einem Paket möglich sein muss.

34 cc) Entgegen der Auffassung des Patentgerichts ist Patentanspruch 1 hingegen nicht zu entnehmen, dass die Logeinträge zwingend einen Zeitstempel oder sonstige Daten enthalten müssen, anhand derer die zeitliche Reihenfolge der Pakete bestimmt werden kann.

35 Wie bereits oben dargelegt wurde, ist die Erfassung von Zeitstempeln in der Beschreibung nur als Beispiel aufgeführt. Auch Patentanspruch 1 enthält diesbezüglich keine zwingenden Vorgaben. Er gibt insbesondere nicht vor, dass

eine zeitliche Korrelation möglich sein muss. Merkmal 6 lässt vielmehr offen, anhand welcher Kriterien die Vielzahl von Datenpaketen miteinander in Beziehung gesetzt werden.

36 dd) Zu Recht und insoweit nicht angegriffen ist das Patentgericht davon ausgegangen, dass Patentanspruch 1 keine exakten Vorgaben dazu enthält, wie lange die Logeinträge vorgehalten werden müssen, dass diese Einträge aber jedenfalls so lange zur Verfügung stehen müssen, dass sie Eingang in den in Merkmal 6 vorgesehenen Korrelationsschritt finden können.

37 Da Patentanspruch 1 keine näheren Vorgaben dazu enthält, welche Daten erfasst und für das Korrelieren herangezogen werden, ist es allerdings unschädlich, wenn ein Teil der Logeinträge schon vor dem Korrelationsschritt verworfen wird. Ausreichend ist, wenn zumindest einzelne Logdaten für diesen Schritt zur Verfügung stehen.

38 ee) Entgegen der Auffassung des Patentgerichts kommen vor diesem Hintergrund auch so genannte Pointer, also Verweise auf die Speicheradressen von Paketen, die in einem Puffer vorgehalten werden, als Logeinträge im Sinne der Merkmale 3, 5 und 6 in Betracht.

39 Auch insoweit ist ausschlaggebend, dass Patentanspruch 1 keine näheren Anforderungen an den Inhalt der Logeinträge definiert. Die aus Merkmal 6 resultierende Anforderung, dass die Logeinträge geeignet sein müssen, um ein Korrelieren einer Vielzahl von Paketen zu ermöglichen, kann auch mit Hilfe von Pointern erfüllt werden, solange ein Zugriff auf die Pakete, auf die diese Pointer verweisen, noch möglich ist. Diese Voraussetzung kann erfüllt sein, wenn die in einem Puffer vorgehaltenen Pakete den Puffer erst verlassen, nachdem der in Merkmal 6 vorgesehene Korrelierschritt abgeschlossen ist.

40 d) Nach Merkmalsgruppe 7 muss das Rechensystem aufgrund des Korrelierens der Vielzahl von Paketen Regeln erzeugen und diese einer Paketfiltervorrichtung zur Verfügung zu stellen.

41 aa) Hinsichtlich des Inhalts der Regeln gibt Merkmal 7.1[1] vor, dass diese konfiguriert sind, um Pakete identifizieren zu können, die die Netzwerkvorrichtung von dem im ersten Netzwerk angeordneten Host empfängt. Anhand welcher Kriterien die Identifizierung erfolgen soll, ist nicht festgelegt.

42 bb) Die Regeln müssen zudem so konfiguriert sein, dass sie das erste Netzwerk veranlassen können, die von dem im ersten Netzwerk angeordneten Host empfangenen Pakete zu verwerfen.

43 cc) Das Erzeugen von Regeln kann nach der Beschreibung dadurch geschehen, dass das Rechensystem neue Regeln erzeugt oder bestehende Regeln aktualisiert (Abs. 49).

44 dd) Aus der in Merkmal 7.1[1] formulierten Vorgabe, dass die Regeln durch das Rechensystem erzeugt werden (generate), ergibt sich, dass das System in der Lage sein muss, die Regeln ohne Eingreifen eines Administrators oder Benutzers zu erstellen. Damit ist nicht ausgeschlossen, dass das Rechensystem einem Administrator oder Benutzer im Anschluss an das Erzeugen der Regeln die Möglichkeit bietet, zwischen unterschiedlichen Optionen auszuwählen.

45 5. Die in Patentanspruch 15 geschützte Vorrichtung wird durch ihre Eignung zur Durchführung des in Anspruch 1 geschützten Verfahrens geprägt. Beide Ansprüche unterliegen daher derselben Beurteilung.

46 II. Das Patentgericht hat seine Entscheidung, soweit für das Berufungsverfahren von Bedeutung, im Wesentlichen wie folgt begründet:

47 Der Gegenstand der erteilten Fassung des Streitpatents sei neu gegenüber der britischen Patentanmeldung 2 505 288 (NK2). NK2 offenbare die Erfassung von Paketdatenverkehr vor und hinter einem zwischen zwei Netzwerken angeordneten Netzwerkgerät. Einem Korrelator werde mittels Pointer-Listen ein Echtzeit-Zugriff auf die Pakete ermöglicht. Diese Listen seien jedoch keine Logeinträge im Sinne der Merkmale 3 und 5.

48 Der Gegenstand von Patentanspruch 1 in der erteilten Fassung und in der Fassung nach dem erstinstanzlichen Hilfsantrag 1 habe jedoch bei einer Zusammenschau der US-Patentanmeldung 2014/0280778 (NK12) und des US-Patents 8 413 238 (HLNK1) nahegelegen.

49 NK12 offenbare ein Verfahren für ein Rechensystem zur Identifikation von Paketen bzw. Paketquellen in einem Netzwerk mit einem einen Grenzübergang repräsentierenden Netzwerkgerät. Hierzu werde der Datenverkehr zwischen einem Client und einem Server vor und hinter dem Netzwerkgerät mit Sensoren abgegriffen. Dabei würden die Pakete auf der Applikationsschicht jeweils mit einem Zeitstempel versehen, für jedes Paket werde ein Hashwert für die Payload berechnet und die jeweiligen Paketinformationen würden in zwei FIFO-Queues abgespeichert. Anschließend würden die Pakete einander zugeordnet. Das Ergebnis werde in Form eines Logs ausgegeben. Diese Information werde einem Netzwerkadministrator zur Verfügung gestellt oder diene als Grundlage für eine Überwachung, um an der Netzwerkgrenze detektierte bösartige Netzaktivität ihrer originalen Paketquelle zuzuordnen. Die Einträge in die FIFO-Queues stellten Protokolleinträge dar. Das Matching komme einer Korrelation gleich. Nicht offenbart sei die Erzeugung und Bereitstellung von Regeln zur Identifikation der Pakete im Sinne von Merkmalsgruppe 7.

50 NK12 bilde einen geeigneten Ausgangspunkt, um die Aufgabe zu lösen, wie mit als infiziert identifizierten Hosts umzugehen sei. Hierfür hätte der Fachmann HLNK1 in Betracht gezogen. Diese betreffe ebenfalls die Identifizierung bösartiger Aktivitäten in Unternehmensnetzwerken. Wenn ein infiziertes oder bösartiges Gerät identifiziert worden sei, werde der Administrator informiert und/oder Spezialanwendungen zur Überprüfung der Gerätesoftware aktiviert. Zusätzlich könne der Datenverkehr automatisch durch die Verarbeitungsknoten gefiltert werden. Dazu gehöre ein automatisches Blockieren der Datenpakete basierend auf Regeln, was einem Verwerfen (drop) im Sinne des Streitpatents gleichkomme. Dem Fachmann stelle sich zwangsläufig das Problem, wie das Überwachungssystem der HLNK1, dessen Überwachungsfunktionalität von den

Verarbeitungsknoten eines externen Service Providers bereitgestellt werde, bei einer Adresstransformation an der Netzwerkgrenze des Unternehmensnetzes die private Adresse eines bösartigen Geräts innerhalb des Unternehmensnetzwerks eindeutig bestimme. Diesem Problem trage das mit der Lehre der NK12 erzielte Korrelationsergebnis Rechnung. Es könne daher unmittelbar durch die Ausführungsform gemäß HLNK1 verarbeitet werden.

51 Die mit den Hilfsanträgen 2b, 2c, 3, 4 und 5 verteidigten Gegenstände beruhten ausgehend von NK12 unter Berücksichtigung der HLNK1 nicht auf erfinderischer Tätigkeit. Der mit Hilfsantrag 3 verteidigte Gegenstand gehe zudem über den Inhalt der ursprünglichen Anmeldeunterlagen hinaus.

52 III. Diese Beurteilung hält der Überprüfung im Berufungsverfahren im Hinblick auf den jetzigen Hauptantrag (nachfolgend weiterhin - wie in erster Instanz - als Hilfsantrag 1 bezeichnet) im Ergebnis stand.

53 1. Entgegen der Auffassung der Berufungserwiderung geht der mit Hilfsantrag 1 verteidigte Gegenstand nicht über den Inhalt der ursprünglichen Anmeldung hinaus.

54 Die ursprünglich eingereichten Unterlagen offenbaren in Figur 2D und den darauf bezogenen Ausführungen in der Beschreibung, dass die Abgreifvorrichtung (126) durch die vom Rechensystem erzeugten Regeln dazu veranlasst werden kann, Pakete fallenzulassen (Abs. 51).

55 2. Der mit Hilfsantrag 1 verteidigte Gegenstand lag ausgehend von NK2 in Verbindung mit HLNK1 nahe.

56 a) NK2 nimmt diesen Gegenstand nicht vollständig vorweg.

57 aa) NK2 betrifft das Erfassen und Sammeln von Daten aus Netzwerkadressübersetzungen, insbesondere zum Zweck der Strafverfolgung.

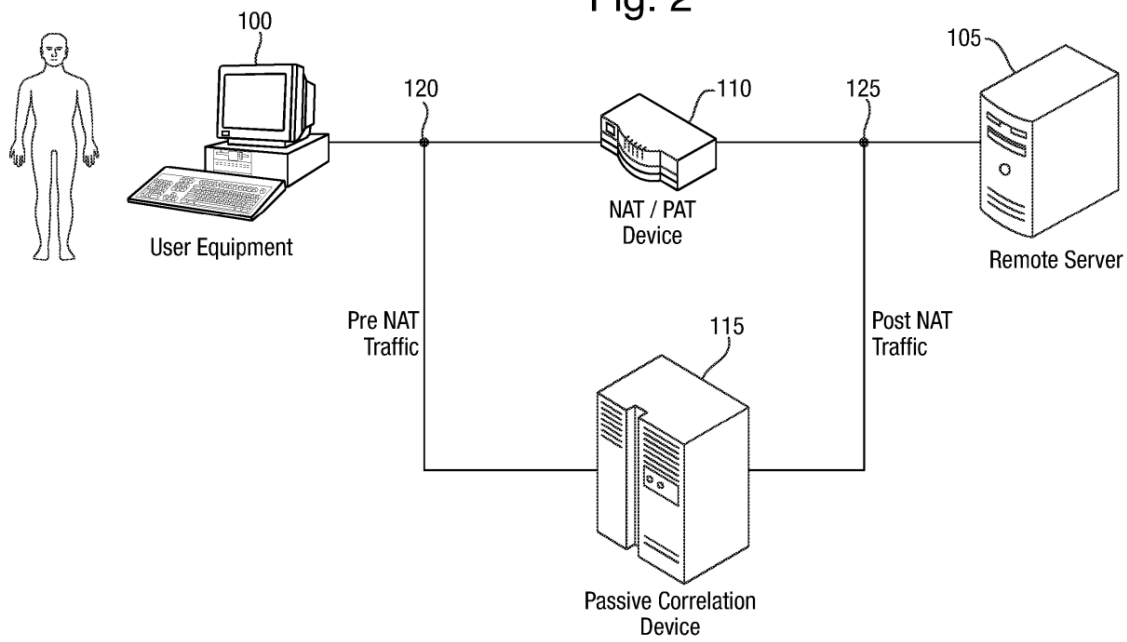
58 (1) NK2 führt aus, die Übersetzung von Netzwerkadressen und Ports (NAT, PAT) ermögliche es, ein privates Adressierungsschema hinter einer einzigen IP-Adresse oder einer kleinen Anzahl von IP-Adressen vor einem öffentlichen Netzwerk zu verbergen. Dies erfolge mittels eines Netzgeräts, das die Adressierungsinformationen in den Headern von aus dem privaten Netz ausgehenden Paketen verändere. Zugleich werde im Netz eine Übersetzungstabelle geführt, um innerhalb einer bestimmten Kommunikationssitzung zurückkehrende Pakete zurückzuübersetzen und an die ursprüngliche IP-Adresse zu routen (S. 1 Z. 7-20).

59 Die Verwendung von solchen Geräten könne Probleme verursachen, wenn die Überprüfung von Paketen keine eindeutige Kennung über ihren Absender liefere und diese mangels Speicherung entsprechender Daten auch nicht vom NAT/PAT-Gerät abgefragt werden könne (S. 1 Z. 21-31).

60 (2) NK2 schlägt deshalb vor, die Datenpakete vor und nach der Adressübersetzung zu erfassen und einander zuzuordnen (S. 2 Z. 1-11).

61 Ein Ausführungsbeispiel ist in der nachfolgend wiedergegebenen Figur 2 schematisch dargestellt.

Fig. 2



62 Bei diesem Beispiel kommuniziert ein Benutzerendgerät (100) mit einem Remote-Server (105) über einen Kommunikationspfad, der ein NAT/PAT-Gerät (110) umfasst.

63 Eine passive Korrelationsvorrichtung (115) überwacht Datenpakete auf diesem Pfad an zwei Abgreifpunkten (120, 125) (S. 5 Z. 20-28) und versucht, die Pakete einander zuzuordnen (S. 5 Z. 29 bis S. 6 Z. 3).

64 Für die Zuordnung werden in erster Linie fünf als IPQ bezeichnete Identifikationsfelder (Adresse und Port von Quelle und Ziel sowie das IP-Protokoll) herangezogen. Diese ermöglichen die Zuordnung zu einer TCP/UDP-Sitzung (session, S. 6 Z. 4-16). Wenn es vor der Adressübersetzung nur eine Sitzung mit derselben Zieladresse, demselben Zielport und demselben IP-Protokoll gibt, können die eingehenden und ausgehenden Pakete einander eindeutig zugeordnet werden (S. 6 Z. 20-32). Wenn diese drei Angaben in mehreren Sitzungen vor der Adressübersetzung vorkommen, müssen weitere Felder im IP-Header untersucht werden, die durch das NAT/PAT-Gerät nicht verändert werden. Um Rechenaufwand zu sparen, kann alternativ eine Liste mit in Frage kommenden Sitzungen erstellt werden (S. 7 Z. 1-9).

65 Um Pakete in verschiedenen Sitzungen zu identifizieren, führen die zur Korrelationsvorrichtung gehörenden Sitzungsfilter eine Hashfunktion an den IP-Identifikationsfeldern durch und führen Verzeichnisse (hash maps), in denen jeder einzelne Hashwert einem Identifikationswert für die Warteschlange einer Sitzung zugewiesen wird. Diese Warteschlangen können so ausgestaltet sein, dass sie lediglich eine Liste von Zeigern in den Hashmaps auf Pakete umfassen, die zu einer Sitzung gehören, während die Pakete selbst in einem gemeinsamen Puffer gehalten werden. Diese Anordnung ermöglicht es, alle zu einer Sitzung gehörenden Pakete durch denselben Ausführungsstrang (thread) zu verarbeiten, so dass keine Kommunikation zwischen den einzelnen Strängen erforderlich ist (S. 9 Z. 1-16).

66 Wird eine Übereinstimmung zwischen Identifikationsfeldern in Paketen vor und nach der Adressübersetzung festgestellt, signalisiert der Rechner den Sitzungsfiltern, dass sie keine weiteren Pakete der entsprechenden Sitzung mehr aufnehmen sollen. Die Sitzungsfilter löschen dann die entsprechenden Warteschlangen. Damit wird eine Belastung des Prozessors so weit wie möglich verhindert (S. 8 Z. 21- 29).

67 Festgestellte Übereinstimmungen werden in einem Log aufgezeichnet und regelmäßig an empfangende Anwendungen übermittelt (S. 7 Z. 10-14; S. 8 Z. 30-33). Dies kann auch ein Abhörsystem (Lawful Interception System) sein, in dem der überwachte Verkehr auf der öffentlichen Seite eines NAT-Geräts erfasst wird. Die protokollierten Zuordnungsinformationen können an ein solches Überwachungsgerät gesendet werden, damit dieses die richtigen Sitzungen identifizieren und Daten daraus sammeln kann (S. 5 Z. 9-14).

68 bb) Wie auch die Berufung nicht in Zweifel zieht, sind damit die Merkmale 1, 2 und 4 sowie ein Korrelieren im Sinne von Merkmal 6 offenbart.

69 cc) Entgegen der Auffassung des Patentgerichts und der Berufung offenbart NK2 auch Logeinträge im Sinne der Merkmale 3, 5 und 6.

70 (1) Wie bereits dargelegt wurde, stellen auch Einträge, die lediglich die Adresse eines an anderer Stelle vorgehaltenen Datenpakets wiedergeben, Logeinträge im Sinne der genannten Merkmale dar, weil Patentanspruch 1 Art und Umfang der gespeicherten Informationen nicht im Einzelnen vorgibt.

71 (2) Unabhängig davon wären die genannten Merkmale auch dann offenbart, wenn ein Logeintrag nicht den gesamten Inhalt eines Datenpakets umfassen dürfte.

72 Die in NK2 als besonders zweckmäßig offenbarten Verzeichnisse, in denen Hashwerte und Zeiger auf die zu einer Sitzung gehörenden Pakete abgelegt werden, enthalten Informationen, die aus dem Inhalt der einzelnen Pakete abgeleitet sind und deren Identifikation ermöglichen. Die Einträge in diesen Verzeichnissen sind damit ebenfalls Logeinträge im Sinne der Merkmale 3, 5 und 6.

73 (3) Entgegen der Auffassung des Patentgerichts erschöpft sich die in NK2 offenbarte Vorgehensweise nach dem Vorstehenden nicht in einer unspezifischen Speicherung von Paketen in einem gemeinsamen Puffer.

74 Durch die Zuordnung zu einzelnen Sitzungen mit Hilfe von Hashwerten und Zeigern wird eine Strukturierung erreicht, die das in Merkmal 6 vorgesehene Korrelieren erleichtert. Ob anhand der vorgehaltenen Daten die Reihenfolge der Pakete festgestellt oder ein Zeitstempel angebracht werden kann, ist unerheblich, weil Patentanspruch 1 eine solche Ausgestaltung nicht zwingend vorsieht.

75 dd) Merkmalsgruppe 7 ist demgegenüber nicht vollständig offenbart.

76 (1) Wie das Patentgericht zu Recht angenommen hat, offenbart NK2 das Erzeugen von Regeln im Sinne von Merkmal 7.1 gemäß der erteilten Fassung.

77 Solche Regeln werden in NK2 erzeugt, wenn eine Übereinstimmung zwischen Identifikationsfeldern vor und nach der Adressübersetzung festgestellt wird. Sie signalisieren den Sitzungsfiltern, keine weiteren Pakete der entsprechenden Sitzung in den Korrelierungsvorgang mehr aufzunehmen und die entsprechenden Warteschlangen zu löschen.

78 (2) Die Sitzungsfilter, die diese Anweisung ausführen, sind Paketfilter im Sinne von Merkmal 7.2, weil sie Pakete anhand von bestimmten Kriterien identifizieren und in Abhängigkeit von den ermittelten Werten einer unterschiedlichen Behandlung zuführen.

79 (3) Die in NK2 erzeugten Regeln verwirklichen Merkmal 7.1[1] jedoch deshalb nicht, weil sie das erste Netzwerk nicht veranlassen, die von einem darin angeordneten Host empfangenen Pakete zu verwerfen.

80 Die in NK2 vorgesehenen Regeln führen lediglich dazu, dass die so identifizierten Datenpakete nicht mehr für die Korrelation verwendet werden. Sie haben aber keinen Einfluss auf die Weiterleitung des Pakets aus dem ersten in das zweite Netzwerk.

81 b) Der mit Hilfsantrag 1 verteidigte Gegenstand war ausgehend von NK2 durch HLNK1 nahegelegt.

82 aa) In NK2 steht zwar die Zuordnung der Pakete zueinander und zu einzelnen Sitzungen im Mittelpunkt. Gleichwohl ergeben sich bereits aus NK2 selbst Hinweise darauf, dass die gewonnenen Informationen auch für weitere Anwendungen eingesetzt werden können.

83 NK2 führt aus, Einzelheiten der abgeglichenen pre-NAT- und post-NAT-IPQs würden an ein Protokoll ausgegeben. Dieses sei für andere Prozesse zugänglich, um abgeglichene pre-NAT- und post-NAT-IPQs an externe Systeme zu berichten (S. 8 Z. 30).

84 Als konkrete Möglichkeit zur Verwendung dieser Daten führt NK2 das rechtmäßige Abhören zum Zweck der Strafverfolgung an. Dabei könnten die durch die Korrelation erfassten Echtzeit-Zuordnungsinformationen bestimmter Zielsitzungen an ein Überwachungsgerät gesendet werden, damit dieses die richtigen Sitzungen identifizieren und deren Daten sammeln könne. Diese Art der Datenverwertung wird aber lediglich als Beispiel angeführt (S. 10 Z. 9 ff.: "would also be of use").

85 Daraus ergab sich die Veranlassung, nach weiteren Möglichkeiten zur Nutzung der gewonnenen und für andere Prozesse zugänglichen Daten zu suchen.

86 bb) Bei der Suche nach solchen Möglichkeiten bot sich HLNK1 an, weil es dort ebenfalls um die Identifizierung von möglicherweise bösartigen Aktivitäten und um mögliche Abwehrmaßnahmen geht.

87 (1) HLNK1 schlägt ein verteiltes Sicherheitssystem vor, das beispielsweise als Overlay-Netzwerk in einem Weitverkehrsnetz (WAN) implementiert werden kann (Sp. 2 Z. 41-44).

88 Ein Ausführungsbeispiel ist in der nachfolgend wiedergegebenen Figur 1 schematisch dargestellt.

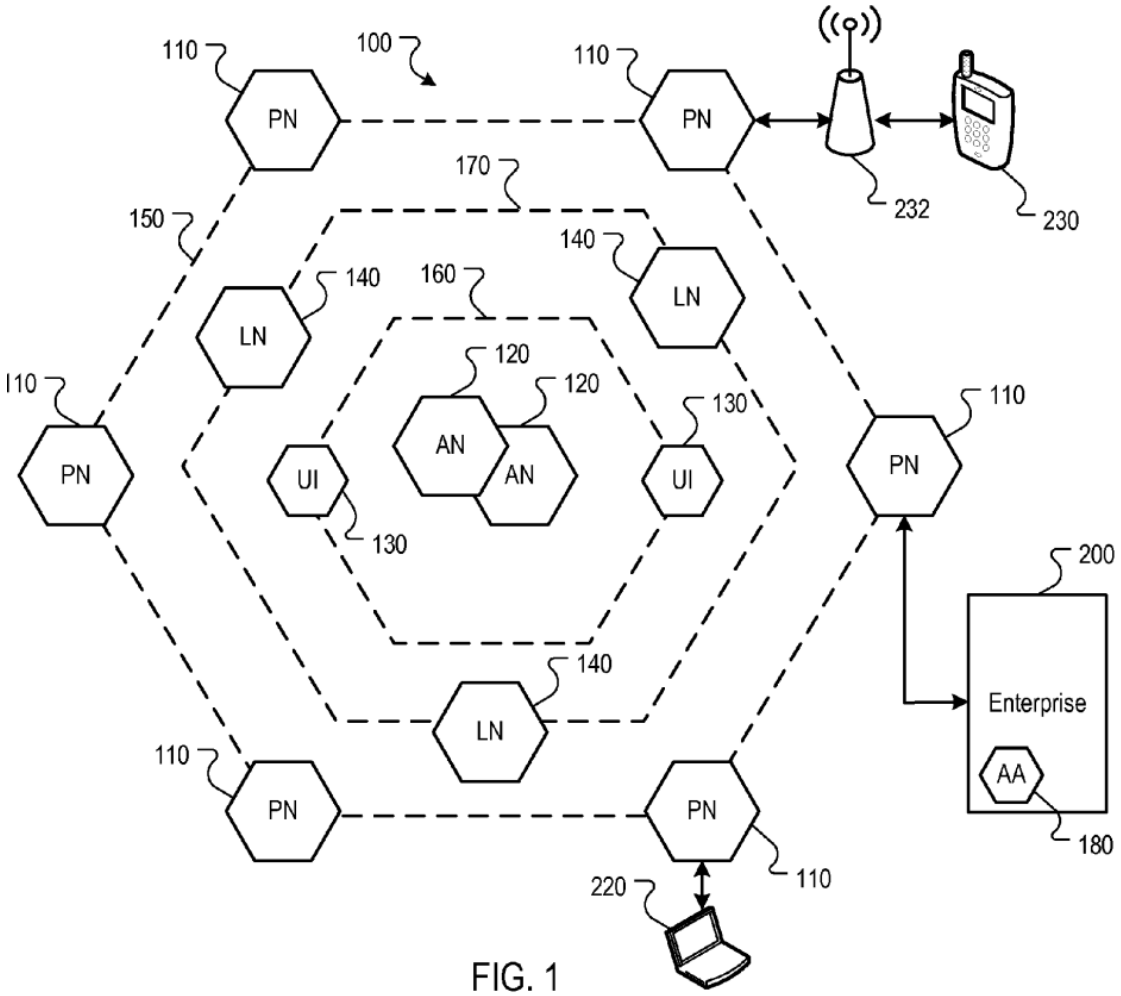


FIG. 1

89 Das Überwachungssystem (100) besteht aus Verarbeitungsknoten (110), Autoritätsknoten (120) und einem externen System (200), beispielsweise einem Unternehmen. Die Verarbeitungsknoten (110) können durch die Verarbeitung der von allen oder einem Teil der externen Systeme (200, 220, 230) gesendeten und empfangenen Daten die Verbreitung von Sicherheitsbedrohungen, beispielsweise Malware, erkennen und verhindern (Sp. 2 Z. 44-50).

90 (2) Eine als bevorzugt bezeichnete Ausführungsform ist in der nachfolgend wiedergegebenen Figur 2 dargestellt.

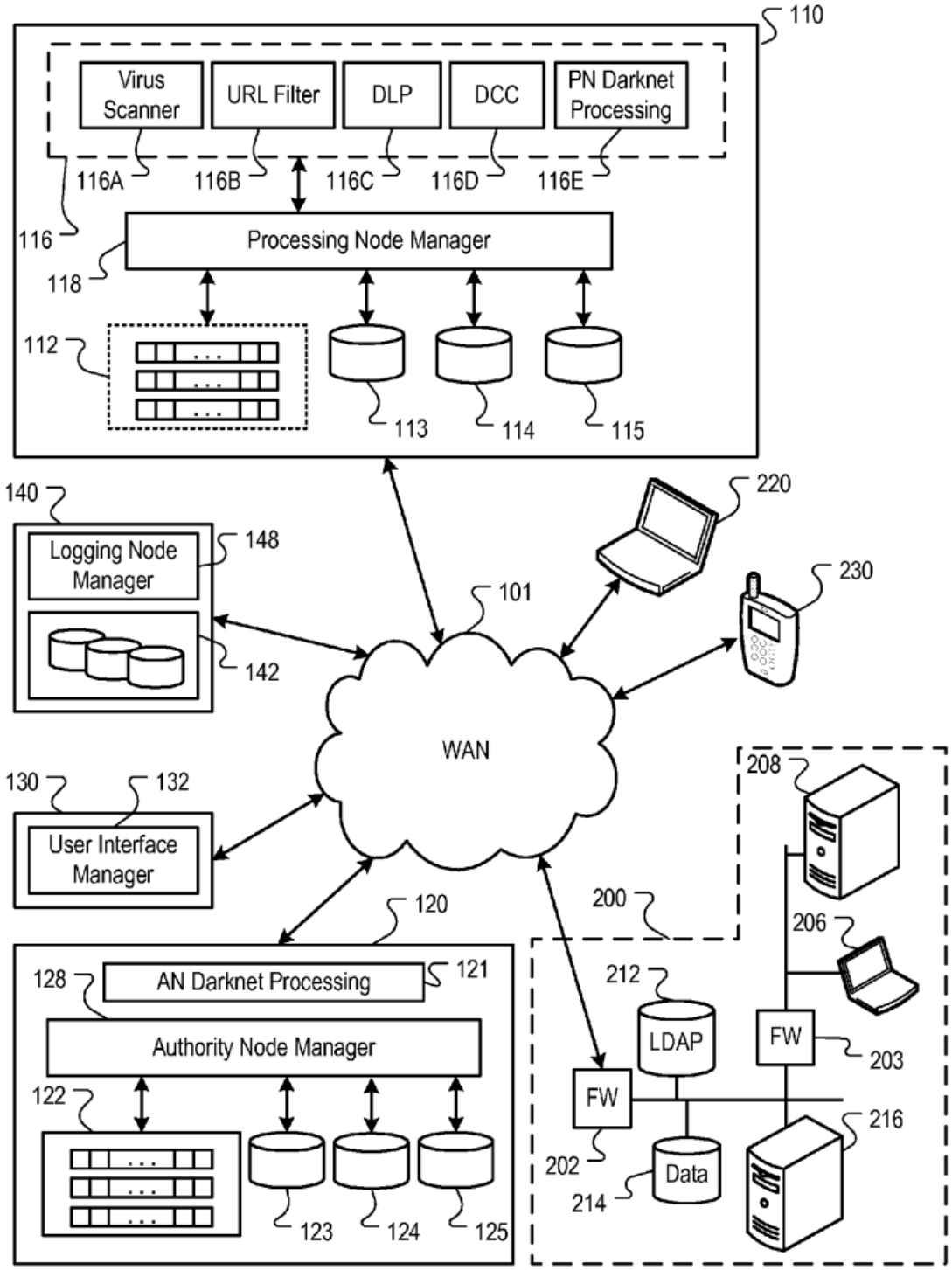


FIG. 2

91 Die Verarbeitungsknoten (110) können beispielsweise durch die Verarbeitung der von dem externen System (200) über die Benutzerendgeräte (206, 208) über Firewalls (202, 203) an das Weitverkehrsnetz (WAN) gesendeten und empfangenen Daten die Verbreitung von Sicherheitsbedrohungen wie etwa Malware erkennen und verhindern (Sp. 2 Z. 44-50).

92 Dafür enthält der Verarbeitungsknoten Datenprüfmaschinen (116), die einen Bedrohungserkennungsprozess durchführen, um Inhaltselemente für eine entsprechende Bedrohung zu klassifizieren (z.B. sauber, Spyware, Malware, unerwünschte Inhalte, unbekannt). Für die Klassifizierung greifen sie auf eine in Autoritätsknoten (120) enthaltene Bedrohungsklassifizierung oder dort gespeicherte Sicherheitsrichtlinien des zu schützenden Netzwerks zurück (Sp. 3 Z. 54 ff.; Sp. 6 Z. 3 ff.).

93 Bei den Datenprüfmaschinen handelt es sich beispielsweise um einen Virenscanner (116A), der ein Inhaltselement als infiziert oder sauber klassifizieren kann, einen Netzwerk-URL-Filter (116B), der eine Netzwerkadresse (Uniform Resource Locator, URL) als erlaubt oder eingeschränkt klassifizieren kann, eine Data Leakage Protection (DLP)-Engine (116C), die ein Inhaltselement als sicher oder undicht identifizieren kann, eine Dynamic Content Categorization (DCC)-Engine (116D), die ein Inhaltselement als bestanden oder nicht bestanden klassifizieren kann, oder um eine PN-Darknet-Verarbeitung (116E), die Darknet-Adressen identifizieren und in einer Darknet-Adressdatenbank (115) speichern kann (Sp. 6 Z. 7-17).

94 Die Feststellung, dass es sich bei einer Ziel- oder Absenderadresse um eine Darknet-Adresse handelt, kann beispielsweise durch einen Vergleich mit einer Liste von Darknet-Adressen getroffen werden (Sp. 10 Z. 53-59).

95 Auf der Grundlage der Bedrohungsklassifizierung kann der Verarbeitungsknoten die Verbreitung des Inhaltselements unmittelbar oder nach einem Reinigungsprozess zulassen, die Verbreitung des Inhaltselements ausschließen oder eine Bedrohungserkennung für das Inhaltselement durchführen (Sp. 3 Z. 10-14).

96 In den Implementierungen, in denen die gesamte Kommunikation untersucht wird, können Vorrichtungen identifiziert werden, die wahrscheinlich mit bösartigen Aktivitäten in Verbindung stehen. Befinden sich solche Vorrichtungen innerhalb des Unternehmensnetzwerks, kann eine Benachrichtigung an das Unternehmensnetzwerk gesendet werden, die auf den möglichen bösartigen Softwarecode hinweist. Befinden sich solche Vorrichtungen außerhalb des Unternehmensnetzes, können die Daten der Autoritätsknoten-Richtlinie verwendet werden, um eine Regel zu implementieren, die verhindert, dass solche Vorrichtungen mit Vorrichtungen innerhalb des geschützten Unternehmensnetzes kommunizieren (Sp. 10 Z. 60 ff.).

97 Bei Implementierungen, bei denen nur die von Vorrichtungen innerhalb eines geschützten Unternehmensnetzwerks stammende Kommunikation untersucht wird, gilt entsprechendes. Zusätzlich können Verarbeitungsknoten versuchen, den bösartigen Programmcode von der Vorrichtung zu entfernen, oder die von der Vorrichtung stammende Kommunikation kann aktiv gefiltert werden (Sp. 11 Z. 4-18).

98 In einem Ausführungsbeispiel, dem zufolge schädliche Aktivitäten aufgrund des Darknets identifiziert werden, wird zunächst eine Bestätigung ausgegeben, dass es sich bei einer identifizierten Zieladresse um eine Darknet-Adresse handelt. Darauf folgt eine Benachrichtigung an das Unternehmensnetzwerk oder eine Spezialanwendung, die den bösartigen Programmcode von der Vorrichtung entfernen kann. Die Benachrichtigung kann auch an andere Verarbeitungsknoten mit Anweisungen zur Filterung oder detaillierten Prüfung von als ähnlich identifizierten Kommunikationen (etwa aufgrund der Herkunftsadresse) weitergeleitetet werden. Zusätzlich kann der Datenverkehr auf der Grundlage von vordefinierten Regeln automatisch blockiert, umgeleitet oder gefiltert werden (Sp. 12 Z. 57 bis Sp. 13 Z. 9; Figur 4 Schritt 450).

99 (3) HLNK1 offenbart damit, dass auf eine Vielzahl von festgestellten Bedrohungen mit einer Vielzahl von Maßnahmen reagiert werden kann, und dass zu diesen Maßnahmen insbesondere das Scannen der Daten sowie die Unterbindung der Weiterleitung von Informationen über möglicherweise bösartige Verbindungen gehört (Sp. 6 Z. 8).

100 Diese Vorgehensweise ist ausgehend von NK2 von Interesse, weil auch dort Informationen über zumindest potenziell schädliche Aktivitäten gewonnen werden und für eine Weiterverarbeitung zur Verfügung stehen.

101 (4) Entgegen der Auffassung der Berufung stand einer Kombination von NK2 und HLNK1 nicht entgegen, dass die Übersetzung von Netzwerkadressen (NAT) in HLNK1 nicht erwähnt wird.

102 Wie die Klägerinnen zu Recht geltend machen, zeigt HLNK1 eine Vielzahl von Übergängen zwischen unterschiedlichen Netzwerken auf. Auch wenn hierbei die Nutzung virtueller Tunnel im Vordergrund steht, ist zu erwarten, dass es beim Übergang von einem Netzwerk in ein anderes zur Änderung von Adressdaten in Paketen kommt.

103 Zudem geht aus den Ausführungen in NK2 hervor, dass es nicht nur bei der Übersetzung von Netzwerkadressen oder Ports (NAT/PAT) zu Änderungen des Paketinhalts kommen kann, sondern grundsätzlich an jedem Übergang zwischen zwei Netzwerken (S. 1 Z. 3-6).

104 Vor diesem Hintergrund bot es sich an, Informationen über die Zuordnung von Paketen, die mit dem in NK2 offenbarten Verfahren gewonnen worden sind, auch in einem Umfeld auszuwerten, wie es HLNK1 offenbart. Dies gilt insbesondere auch deshalb, weil HLNK1 einen modularen Aufbau zeigt, bei dem zahlreiche unterschiedlichen Komponenten miteinander agieren können. Die in NK2 offenbarten Möglichkeiten zur Korrelation zwischen Paketen stellten sich vor diesem Hintergrund als weiterer modularer Baustein dar, auf den bei Bedarf zurückgegriffen werden kann.

105 cc) Bei einer Berücksichtigung von HLNK1 lag es nahe, die mit Hilfe des Verfahrens aus NK2 gewonnenen Informationen automatisch zu Regeln weiterzuverarbeiten, wie dies in Merkmalsgruppe 7 vorgesehen ist.

106 (1) Eine Anregung dazu ergab sich bereits aus NK2, weil die mit Hilfe der Korrelation gewonnenen Erkenntnisse zur Erzeugung von automatischen Regeln zum Löschen von Warteschlangen genutzt werden.

107 (2) Entgegen der Auffassung der Berufung sieht HLNK1 ebenfalls eine automatisierte Erstellung von Regeln vor.

108 HLNK1 schildert zwar die Möglichkeit, Benachrichtigungen über bösartige Aktivitäten an einen Administrator zu senden (Sp. 10 Z. 60; Sp. 12 Z. 64). Als Alternative wird aber beschrieben, dass bestimmte Kommunikationsvorgänge als potenziell bösartig gekennzeichnet werden oder dass eine Nachricht an eine für spezielle Zwecke vorgesehene Anwendung (special purpose application) übermittelt wird, die ein Gerät auf bösartigen Programmcode untersuchen und diesen gegebenenfalls entfernen kann (Sp. 12 Z. 65 bis Sp. 13 Z. 3).

109 dd) Wie oben dargelegt wurde, gehört zu den in HLNK1 geschilderten Maßnahmen auch das Blockieren von verdächtigem Datenverkehr. Dies entspricht der in Merkmal 7.1^1 vorgesehenen Vorgehensweise.

110 Dass das in NK2 eingesetzte passive Korrelationsgerät nicht dazu vorgesehen ist, Pakete zu verwerfen, führt entgegen der Auffassung der Berufung nicht zu einer abweichenden Beurteilung. Aus dem bereits erwähnten Hinweis in NK2, dass die gewonnenen Informationen an eine andere Anwendung weitergegeben werden können, ergab sich die Anregung, bei Bedarf einen zusätzlichen Paketfilter vorzusehen, der diese Aktion ausführen kann, oder das passive Korrelationsgerät um solche aktiven Funktionen zu erweitern.

111 IV. Die mit den Hilfsanträgen verteidigten Gegenstände sind ebenfalls nicht patentfähig.

112 1. Die erstmals in zweiter Instanz gestellten Hilfsanträge sind allerdings zulässig, § 117 PatG und § 531 Abs. 2 ZPO.

113 a) Nach der Rechtsprechung des Senats kann die hilfsweise Verteidigung des Streitpatents mit geänderten Ansprüchen in der Berufungsinstanz regelmäßig nicht mehr als sachdienlich im Sinne von § 116 Abs. 2 Nr. 1 PatG angesehen werden, wenn der Nichtigkeitsbeklagte hierzu bereits in erster Instanz Veranlassung hatte. Ein solcher Anlass zur zumindest hilfsweisen beschränkten Verteidigung kann sich daraus ergeben, dass das Patentgericht in seinem nach § 83 Abs. 1 PatG erteilten Hinweis mitgeteilt hat, dass nach seiner vorläufigen Auffassung der Gegenstand des Streitpatents nicht patentfähig sein dürfte (BGH, Urteil vom 15. März 2022 - X ZR 18/20, GRUR 2022, 1049 Rn. 67 - Fahrerlose Transporteinrichtung). Dagegen hat ein Nichtigkeitsbeklagter grundsätzlich keinen Anlass zur Stellung von Hilfsanträgen, wenn er dem gemäß § 83 Abs. 1 PatG erteilten Hinweis entnehmen darf, dass das Streitpatent voraussichtlich in der erteilten Fassung Bestand haben wird (vgl. nur BGH, Urteil vom 15. März 2022 - X ZR 18/20, GRUR 2022, 1049 Rn. 67 ff. - Fahrerlose Transporteinrichtung).

114 b) Im Streitfall hat das Patentgericht in seinem nach § 83 Abs. 1 PatG erteilten Hinweis die vorläufige Auffassung geäußert, der Gegenstand von Patentanspruch 1 in der erteilten Fassung sei patentfähig. Bei dieser Ausgangslage hatte die Beklagte keinen Anlass, im Vorfeld der mündlichen Verhandlung erster Instanz weitere Hilfsanträge zu stellen.

115 In ihren Stellungnahmen zum Hinweis des Patentgerichts haben die Klägerinnen zwar zahlreiche neue Gesichtspunkte vorgetragen und die Klägerin zu 2 hat ergänzend die Entgegenhaltungen HLNK1 bis HLNK3 vorgelegt. Daraus ergab sich für die Beklagte aber keine zusätzliche Veranlassung, sich vorsorglich von der bereits zuvor vorgelegten Entgegenhaltung NK2 weiter abzugrenzen.

116 c) Der Beklagten kann auch nicht angelastet werden, dass sie die in zweiter Instanz zusätzlich gestellten Hilfsanträge 1c, 1d und 3a sowie 2d, 2e, 2f, 2g, 6 und 6a nicht schon in der mündlichen Verhandlung vor dem Patentgericht gestellt hat. In dieser Situation war nicht zu erwarten, dass die Beklagte vollständig überblicken konnte, welche zusätzlichen Verteidigungsmöglichkeiten angesichts der geänderten Einschätzung des Patentgerichts sachdienlich waren.

117 2. Die erst nach Ablauf der Frist für die Berufungsbegründung gestellten Hilfsanträge 2d, 2e, 2f, 2g, 6 und 6a unterliegen auch nicht der Zurückweisung nach § 117 und § 112 Abs. 2 PatG in Verbindung mit § 530 und § 296 Abs. 1 ZPO.

118 Dabei kann dahingestellt bleiben, ob bereits das angefochtene Urteil Anlass gab, diese Hilfsanträge zu stellen. Selbst wenn dies zu bejahen wäre, sind diese Anträge jedenfalls deshalb zu berücksichtigen, weil der Senat über sie abschließend entscheiden kann und damit keine Verzögerung des Rechtsstreits eintritt.

119 3. Der mit Hilfsantrag 1c verteidigte Gegenstand ist nicht patentfähig.

120 a) Gemäß Hilfsantrag 1c soll die erteilte Fassung von Patentanspruch 1 wie folgt modifiziert werden:

121

7.1^{1c}	generating (30), by the computing system, one or more rules (140) configured to identify <u>and drop</u> packets received from the host located in the first network <u>destined for the host in the second network (102)</u>; and	Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren <u>und zu verwerfen</u>, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet<u>,</u> <u>und die für den Host in dem zweiten Netzwerk (102) bestimmt sind</u>; und

7.2[1c]	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 destined for the host in the second network (102).	Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet, und die für den Host in dem zweiten Netzwerk (102) bestimmt sind.

122 b) Diese Ausgestaltung war aus denselben Gründen nahegelegt wie der mit Hilfsantrag 1 verteidigte Gegenstand.

123 4. Für Hilfsantrag 1d gilt Entsprechendes.

124 a) Gemäß Hilfsantrag 1d soll die erteilte Fassung von Patentanspruch 1 in der Fassung des Hilfsantrags 1c wie folgt modifiziert werden:

125

7.1[1d]	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 destined for the host in the second network (102) and preventing the packets from reaching the host in the second network (102); and	Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet, und die für den Host in dem zweiten Netzwerk (102) bestimmt sind, und um zu verhindern, dass die Pakete den Host in dem zweiten Netzwerk (102) erreichen; und

7.2[1d]	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 destined for the host in the second network (102), and preventing the packets from reaching the host in the second network (102).	Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet, und die für den Host in dem zweiten Netzwerk (102) bestimmt sind, und um zu verhindern, dass die Pakete den Host in dem zweiten Netzwerk (102) erreichen.

126 b) Der damit verteidigte Gegenstand unterscheidet sich in der Sache nicht von dem mit Hilfsantrag 1c verteidigten Gegenstand.

127 5. Zu Recht hat das Patentgericht den mit Hilfsantrag 2b verteidigten Gegenstand ebenfalls als nicht patentfähig angesehen.

128 a) Nach Hilfsantrag 2b soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

129

4[2b]	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);	Identifizieren (8, 406), durch das Rechensystem, einer Vielzahl von Paketen (P1', P2', P3'), die durch die Netzwerkvorrichtung an einen bösartigen Host (108) übertragen werden, der sich in einem zweiten Netzwerk (102) befindet;
7.1[2b]	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	Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet; und
7.2[2b]	provisioning (31, 32) a packet-filtering device (124, 126) with	Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen

	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).	oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet, um die Verbreitung von Malware zu verhindern, die von einem bösartigen Host (108), der in dem zweiten Netzwerk (102) verortet ist, auf dem Host (114) in dem ersten Netzwerk (104) installiert wurde.

130 b) Im Vergleich zum Hauptantrag (erstinstanzlich: Hilfsantrag 1) sowie zu den Hilfsanträgen 1c und 1d ist damit lediglich eine Motivation angegeben, weshalb einzelne Datenpakete identifiziert und verworfen werden sollen.

131 Dass es sinnvoll ist, Datenverkehr insbesondere dann zu unterbinden, wenn er durch ein bösartiges System verursacht wird, bedurfte ausgehend von NK2 und HLNK1 keines besonderen Hinweises.

132 6. Für Hilfsantrag 2c gilt nichts anderes.

133 a) Nach Hilfsantrag 2c soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

134

4^{2c}	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);	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, wobei die Kommunikation hinsichtlich der Pakete (P1', P2', P3') auf Malware hinweist, die von dem Host (108), der in dem zweiten Netzwerk (102) verortet ist, auf dem Host (114) im ersten Netzwerk (104) installiert wurde;

7.1[2c]	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	Erzeugen (30), durch das Rechensystem, von einer oder mehreren Regeln (140), die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet; und
7.2[2c]	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).	Bereitstellen (31, 32) einer Paketfiltervorrichtung (124, 126) mit der einen oder den mehreren Regeln, die konfiguriert sind, um Pakete zu identifizieren und zu verwerfen, die von dem Host empfangen werden, der sich in dem ersten Netzwerk befindet, um die Verbreitung von Malware zu verhindern, die von einem bösartigen Host (108), der in dem zweiten Netzwerk (102) verortet ist, auf dem Host (114) in dem ersten Netzwerk (104) installiert wurde.

135 b) Auch damit ist nur ein naheliegender Anwendungsfall angegeben, in dem sich das Verwerfen von Paketen aufgrund von Hinweisen auf die Installation von Malware anbietet.

136 7. Der mit Hilfsantrag 2d verteidigte Gegenstand ist nicht patentfähig.

137 a) Nach Hilfsantrag 2d soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 2c dahin ergänzt werden, dass am Anfang von Merkmal 7.1[2c] das Wort "automatically" eingefügt wird.

138 b) Dass ausgehend von NK2 eine automatische Erstellung von Filterregeln nahelag, wurde bereits oben dargelegt.

139 8. Der mit Hilfsantrag 2e verteidigte Gegenstand ist ebenfalls nicht patentfähig.

140 a) Nach Hilfsantrag 2e soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 2c um folgendes Merkmal ergänzt werden:

141

7.0^{2e}	determining (26), by the computing system and based on the correlating, that the host (108) located in the second network (102) has communicated with the host (114) located in the first network (104);	Ermitteln (26) durch das Rechensystem und basierend auf der Korrelation, dass der Host (108), der sich im zweiten Netzwerk (102) befindet, mit dem Host (114) kommuniziert hat, der sich im ersten Netzwerk (104) befindet;

142 b) Damit ist ebenfalls nur ein naheliegender Anwendungsfall beschrieben.

143 9. Für Hilfsantrag 2f gilt nichts anderes.

144 a) Nach Hilfsantrag 2f soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 2e wie folgt modifiziert werden:

145

7.0^{2f}	determining (26), by the computing system and based on ~~the correlating~~ data in the log entries corresponding to the correlated plurality of packets, that the host (108) located in the second network (102) has communicated with the host (114) located in the first network (104);	Bestimmen (26) durch das Rechensystem und basierend auf ~~der Korrelation~~ Daten in den Logeinträgen, die der Vielzahl der korrelierten Pakete entsprechen, dass der Host (108), der sich im zweiten Netzwerk (102) befindet, mit dem Host (114) kommuniziert hat, der sich im ersten Netzwerk (104) befindet;

146 b) Daten in den Logeinträgen bilden auch in NK2 die Grundlage für weitere Aktionen mit den identifizierten Paketen.

147 10. Der mit Hilfsantrag 2g verteidigte Gegenstand ist ebenfalls nicht patentfähig.

148 a) Gemäß Hilfsantrag 2g soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 2f wie folgt ergänzt werden:

149

7.0[2f]	determining (26), by the computing system and based on ~~on data in~~ the log entries corresponding to the correlated plurality of packets, a network address associated with the host (114) located in the first network and determining, based on the network address, that the host (108) located in the second network (102) has communicated with the host (114) located in the first network (104);	Bestimmen (26) durch das Rechensystem und basierend auf ~~Daten in~~ den Logeinträgen, die der Vielzahl der korrelierten Pakete entsprechen, einer Netzwerkadresse, die dem Host (114) zugeordnet ist, der sich im ersten Netzwerk befindet, und Bestimmen, basierend auf der Netzwerkadresse, dass der Host (108), der sich im zweiten Netzwerk (102) befindet, mit dem Host (114) kommuniziert hat, der sich im ersten Netzwerk (104) befindet;

150 b) Die Bestimmung der Netzwerkadresse des im ersten Netzwerk angeordneten Hosts steht im Mittelpunkt von NK2.

151 NK2 schlägt hierzu vor, die Datenpakete vor und nach einer Adressübersetzung zu erfassen und einander zuzuordnen (S. 2 Z. 1-11).

152 11. Zu Recht hat das Patentgericht den mit Hilfsantrag 3 verteidigten Gegenstand als nicht patentfähig angesehen.

153 a) Nach Hilfsantrag 3 soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

154

6^3	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	Korrelieren (16, 410), durch das Rechensystem und auf Grundlage der Vielzahl von Logeinträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden und der Vielzahl von Logeinträgen, 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, um zu bestimmen, dass mindestens ein Paket aus der Vielzahl von Paketen, die von der Netzwerkvorrichtung empfangen wurden, mit mindestens einem Paket aus der Vielzahl von Paketen, die von der Netzwerkvorrichtung gesendet wurden, korreliert; und

155 b) Die Zuordnung von empfangenen und gesendeten Paketen zum Zweck der Zuordnung der Pakete zu einem bestimmten Datenstrom ist in NK2 offenbart.

156 12. Für Hilfsantrag 3a gilt nichts anderes.

157 a) Nach Hilfsantrag 3a soll die erteilte Fassung von Patentanspruch 1 in der Fassung des Hilfsantrags 3 wie folgt modifiziert werden:

158

6[3a]	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~~ transmitted by the network device is correlated with at least one packet of the plurality of packets ~~transmitted~~ received by the network device; and	Korrelieren (16, 410), durch das Rechensystem und auf Grundlage der Vielzahl von Logeinträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden und der Vielzahl von Logeinträgen, 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, um zu bestimmen, dass mindestens ein Paket aus der Vielzahl von Paketen, die von der Netzwerkvorrichtung ~~empfangen~~ gesendet wurden, mit mindestens einem Paket aus der Vielzahl von Paketen, die von der Netzwerkvorrichtung ~~gesendet~~ empfangen wurden, korreliert; und

159 b) Wie die Berufung im Ansatz zu Recht geltend macht, begründet es keinen wesentlichen Unterschied, ob gesendete mit empfangenen Paketen korreliert werden oder umgekehrt. Hilfsantrag 3a kann deshalb ebenso wenig Erfolg haben wie Hilfsantrag 3.

160 13. Zu Recht ist das Patentgericht davon ausgegangen, dass der mit Hilfsantrag 4 verteidigte Gegenstand nicht patentfähig ist.

161 a) Nach Hilfsantrag 4 soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

162

6.1[4]	wherein correlating the plurality of packets transmitted by the network device with the plurality of packets received	wobei das Korrelieren der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden, mit der Vielzahl von Paketen, die durch die

	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	Netzwerkvorrichtung empfangen werden, zumindest das Vergleichen umfasst von einer oder mehreren Zeiten, die durch die Vielzahl von Logeinträgen angegeben werden, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden, mit einer oder mehreren Zeiten, die durch die Vielzahl von Logeinträgen angegeben werden, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden; und

163 b) Die Erfassung von zeitbezogenen Informationen ist in NK2 offenbart, und zwar für den Fall, dass mehrere Nutzer im Wesentlichen gleichzeitig Sitzungen mit derselben Website unterhalten (S. 9 Z. 25 bis S. 10 Z. 2).

164 14. Ebenfalls zu Recht hat das Patentgericht den mit Hilfsantrag 5 verteidigten Gegenstand als nicht patentfähig angesehen.

165 a) Nach Hilfsantrag 5 soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 4 wie folgt ergänzt werden:

166

3.1^5	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;	das Erzeugen der Vielzahl von Logeinträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden, umfasst das Erzeugen einer Vielzahl von Zeitstempeln, die Zeiten angeben, die dem Empfang der Vielzahl der von der Netzwerkvorrichtung empfangenen Paketen entsprechen;
5.1^5	generating the plurality of log entries corresponding to the plurality of packets transmitted	das Erzeugen der Vielzahl von Logeinträgen, die der Vielzahl von Paketen entsprechen, die durch die Netzwerk-

	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;	vorrichtung übertragen werden, umfasst das Erzeugen einer Vielzahl von Zeitstempeln, die Zeiten angeben, die der Übertragung der Vielzahl von Paketen, die durch die Netzwerkvorrichtung übertragen werden, durch die Netzwerkvorrichtung entsprechen;
6.2[5]	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.	das Vergleichen der einen oder mehreren Zeiten, die durch die Vielzahl von Logeinträgen angegeben werden, umfasst das Vergleichen von einer oder mehreren Zeiten, die durch die Vielzahl von Zeitstempeln angegeben werden, die Zeiten angeben, die dem Empfang entsprechen, mit einer oder mehreren Zeiten, die durch die Vielzahl von Zeitstempeln angegeben werden, die Zeiten angeben, die der Übertragung entsprechen.

167 b) Damit wird der mit Hilfsantrag 4 verteidigte Gegenstand im Hinblick darauf klargestellt, dass die Logeinträge Zeitstempel umfassen. Dies ergibt sich bereits aus Merkmal 6.1[4] nach Hilfsantrag 4 und ist in NK2 offenbart.

168 15. Hilfsantrag 6 ist ebenfalls nicht patentfähig.

169 a) Gemäß Hilfsantrag 6 soll die erteilte Fassung von Patentanspruch 1 wie folgt ergänzt werden:

170

3[6]	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, wherein the log entry is information associated with or contained in the packets;	Erzeugen (6, 404), durch das Rechensystem, einer Vielzahl von Logeinträgen (306, 308, 310), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden, wobei der Logeintrag aus Informationen besteht, die den Paketen zugeordnet oder in ihnen enthalten sind;

5^6	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, wherein the log entry is information associated with or contained in the packets;	Erzeugen (9, 408), durch das Rechensystem, einer Vielzahl von Logeinträgen (312, 314, 316), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden, wobei der Logeintrag aus Informationen besteht, die den Paketen zugeordnet oder in ihnen enthalten sind;

171 b) Entgegen der Auffassung der Berufung enthalten die in NK2 offenbarten Logeinträge Informationen, die den Paketen zugeordnet sind.

172 Selbst wenn der Logeintrag in den Hashmaps nur aus einer Liste von Zeigern auf Pakete besteht, sind diese Zeiger den Paketen zugeordnet, weil der ihnen zugeordnete Hashwert aus Informationen des einzelnen Pakets erzeugt worden ist.

173 c) Unabhängig davon war die Hinterlegung anderer Informationen in den Logeinträgen ausgehend von NK2 nahegelegt.

174 Die in NK2 beschriebenen Hashwerte und Zeiger werden dort lediglich als besonders effizientes Mittel zur Verwaltung der benötigten Informationen beschrieben. Schon daraus ergab sich, dass je nach Bedarf auch andere Arten der Informationserfassung in Betracht kommen. Dazu gehört das Speichern von Informationen, die in den Paketen enthalten oder diesen zugeordnet sind.

175 16. Für Hilfsantrag 6a gilt nichts anderes.

176 a) Nach Hilfsantrag 6a soll die erteilte Fassung von Patentanspruch 1 in der Fassung von Hilfsantrag 6 wie folgt ergänzt werden:

177

3^{6a}	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, wherein the log entry is a subset of the information contained in the packets and/or information associated with or the packets;	Erzeugen (6, 404), durch das Rechensystem, einer Vielzahl von Logeinträgen (306, 308, 310), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung empfangen werden, wobei der Logeintrag aus einer Teilmenge der in den Paketen enthaltenen Informationen und/oder aus den Paketen zugeordneten Informationen besteht;
5^{6a}	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, wherein the log entry is a subset of the information contained in the packets and/or information associated with or the packets;	Erzeugen (9, 408), durch das Rechensystem, einer Vielzahl von Logeinträgen (312, 314, 316), die der Vielzahl von Paketen entsprechen, die durch die Netzwerkvorrichtung übertragen werden, wobei der Logeintrag aus einer Teilmenge der in den Paketen enthaltenen Informationen und/oder aus den Paketen zugeordneten Informationen besteht;

178 b) Diese Ausgestaltung war aus den oben dargelegten Gründen ausgehend von NK2 zumindest nahegelegt.

179 NK2 schlägt vor, für die Zuordnung in erster Linie die als IPQ bezeichneten Identifikationsfelder (Adresse und Port von Quelle und Ziel sowie das IP-Protokoll) heranzuziehen. Wenn danach eine Zuordnung nicht möglich ist, können aber weitere Felder im IP-Header untersucht werden, die durch das NAT/PAT-Gerät nicht verändert werden (S. 7 Z. 1-9).

180 17. Hilfsantrag 6b unterliegt keiner abweichenden Beurteilung.

181 a) Nach Hilfsantrag 6b sollen die zusätzlichen Merkmale aus den Hilfsanträgen 2g und 6 kombiniert werden.

182 b) Diese Merkmale sind auch in ihrer Kombination aus den oben dargelegten Gründen naheliegend.

183 V. Die Kostenentscheidung beruht auf § 121 Abs. 2 PatG und § 97 Abs. 1 ZPO.

Bacher Deichfuß Marx

Rombach von Pückler

Vorinstanzen:
Bundespatentgericht, Entscheidung vom 14.11.2022 - 5 Ni 50/20 (EP) und 5 Ni 57/21 (EP) -