TE OGH 2020/7/7 33R37/20h

JUSLINE Entscheidung

Veröffentlicht am 07.07.2020

Kopf

Das Oberlandesgericht Wien hat als Rekursgericht durch den Senatspräsidenten Dr. Hinger als Vorsitzenden sowie den Richter Dr. Schober und den Patentanwalt DI Dr. Poth in der Rechtssache der klagenden Partei T*****, vertreten durch die Kletzer Messner Mosing Schnider Schultes Rechtsanwälte OG in Wien und Patentanwalt Mag. DI Dr. Andreas Gehring, Puchberger & Partner Patentanwälte in Wien, gegen die beklagte Partei A*****, vertreten durch die Schwarz Schönherr Rechtsanwälte KG in Wien und Weiser und Voith Patentanwälte Partnerschaft in Wien, wegen Unterlassung, Vernichtung, Rechnungslegung, Schadenersatz sowie Veröffentlichung, Sicherungsinteresse EUR 31.000, über den Rekurs der klagenden Partei gegen den Beschluss des Handelsgerichts Wien vom 26.2.2020, 58 Cg 37/19b-11, in nichtöffentlicher Sitzung den

Beschluss

gefasst:

Spruch

Dem Rekurs wird nicht Folge gegeben.

Die klagende Partei ist schuldig, der beklagten Partei die Kosten der Rekursbeantwortung von EUR 3.256,20 (darin EUR 544,20 USt) zu ersetzen.

Der Wert des Entscheidungsgegenstands übersteigt EUR 30.000.

Der ordentliche Revisionsrekurs ist nicht zulässig.

Begründung

Text

1 . Die Klägerin stützt ihr Begehren auf die Verletzung ihres Patents EP 1259046 B1, „Anlage für die sichere Durchführung von Transaktionen mittels mehrerer Authentifizierungscodes“ („Streitpatent“), dessen Ansprüche lauten wie folgt (Hervorhebungen nicht im Original):

1. Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen mit einem Terminal (102), das zur Eingabe einer Benutzerkennung dient, mit einer Auswerteeinheit (106), die mit dem Terminal (102) über ein primäres Netz (101) verbunden ist, und im wesentlichen aus einer Speicher- und Prozessoreinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, mit einem Codegenerator, der einen Sicherheitscode erzeugt, mit einer Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108) sendet, und mit einer Eingabemöglichkeit für den Sicherheitscode am Terminal und einer Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit (106), dadurch gekennzeichnet, dass die Auswerteeinheit (106) einen zusätzlichen Codegenerator zur Erstellung eine[s] Zusatzcodes aufweist und eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über

das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes aufweist, wobei das Terminal neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist und die Auswerteeinheit (106) derart ausgestaltet ist, dass diese den eingegebenen Zusatzcode überprüft und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert.

2. Anlage nach Anspruch 1, dadurch gekennzeichnet, dass die Auswerteeinheit (106) eine Einheit (106a) zur Entschlüsselung der vom Terminal (102) gesendeten Anmeldedaten und eine an diese Einheit (106a) angeschlossene Einheit (106b) zur Durchführung der Transaktion aufweist.

3. Anlage nach Anspruch 2, dadurch gekennzeichnet, dass die Auswerteeinheit (106) aus einer oder mehreren Einheit/en (106a) zur Vermittlung der Anmeldedaten und eine oder mehrere Einheit/en (106b) zur Durchführung der Transaktion besteht.

4. Anlage nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Terminal (102) zusätzliche Eingabemöglichkeiten für weitere Identifizierungsmerkmale aufweist.

5. Anlage nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Auswerteeinheit (106) einen weiteren Generator beinhaltet, der eine Eingabereihenfolge des Sicherheitscode, des Zusatzcode und gegebenenfalls von weiteren Identifizierungsmerkmalen für die Eingabe in das Terminal generiert und dass die Auswerteeinheit (106) eine Sendeeinrichtung zur Übermittlung der Eingabereihenfolge an das Terminal (102) aufweist.

6. Anlage nach Anspruch 5, dadurch gekennzeichnet, dass das Terminal (102) eine Eingabemöglichkeit für den Sicherheitscode, den Zusatzcode und gegebenenfalls weitere Identifizierungsmerkmale in der vom Generator generierten Reihenfolge durch den Benutzer aufweist.

Die Klägerin gliedert die Merkmale des Anspruchs 1 wie folgt auf (Hervorhebungen nicht im Original):

Oberbegriff

M1.A Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen

M1.B Die Anlage hat ein Terminal (102), das zur Eingabe einer Benutzerkennung dient.

M1.C Die Anlage hat eine Auswerteeinheit (106).

M1.D Die Auswerteeinheit ist mit dem Terminal (102) über ein primäres Netz (101) verbunden.

M1.E Die Auswerteeinheit besteht und im wesentlichen aus einer Speicher- und Prozessoreinheit, die zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient.

M1.F Die Anlage hat einen Codegenerator, der einen Sicherheitscode erzeugt.

M1.G Die Anlage hat eine Sendeeinrichtung, die den Sicherheitscode über ein sekundäres Netz (107) an ein Empfangsgerät (108) sendet.

M1.H Die Anlage hat eine Eingabemöglichkeit für den Sicherheitscode am Terminal.

M1.I Die Anlage hat die Möglichkeit zur Überprüfung des eingegebenen Sicherheitscodes auf Gültigkeit durch die Auswerteeinheit (106).

Kennzeichnender Teil

M1.J Die Auswerteeinheit (106) weist einen zusätzlichen Codegenerator zur Erstellung eines Zusatzcodes auf.

M1.K Die Auswerteeinheit weist eine zusätzliche Sendeeinrichtung zur Übermittlung des Zusatzcodes über das primäre Netz (101) an das Terminal (102) und zur Ausgabe des Zusatzcodes auf.

M1.L Das Terminal weist neben der Eingabemöglichkeit des Sicherheitscodes eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode auf.

M1.M Die Auswerteeinheit (106) ist derart ausgestaltet, dass diese den eingegebenen Zusatzcode überprüft.

M1.N Die Auswerteeinheit (106) autorisiert bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion.

Die Klägerin gliedert die Merkmale des Anspruchs 2 wie folgt auf:

M2.A Die Auswerteeinheit (106) weist eine Entschlüsselungseinheit (106a) der vom Terminal (102) gesendeten Anmeldedaten auf.

M2.B Die Auswerteeinheit (106) weist eine an die Entschlüsselungseinheit (106a) angeschlossene Einheit (106b) zur Durchführung der Transaktion auf.

Die Klägerin gliedert die Merkmale des Anspruchs 3 wie folgt auf:

M3.A Die Auswerteeinheit (106) besteht aus einer oder mehreren Einheiten (106a) zur Vermittlung der Anmeldedaten.

M3.B Die Auswerteeinheit (106) besteht aus einer oder mehreren Einheiten (106b) zur Durchführung der Transaktion.

2.1 Die Klägerin stützt ihre Ansprüche auf das Vorbringen, die Beklagte habe Handlungen gesetzt, die das Patent verletzten, und begehrt, die Beklagte zur Unterlassung zu verpflichten; sie zur Vernichtung aller Eingriffsgegenstände zu verurteilen, soferne sie darüber die Verfügungsgewalt habe; sie zur Rechnungslegung gegenüber der Klägerin zu verpflichten, ihr sodann nach der Wahl der Klägerin den Ersatz des materiellen und immateriellen Schadens einschließlich des entgangenen Gewinns oder eines angemessenen Entgelts oder die Herausgabe des Gewinns aufzutragen; überdies begehrt die Klägerin, die Beklagte zur Veröffentlichung des stattgebenden Teils des Urteils zu verpflichten; weiters begehrt sie die Ermächtigung, den stattgebenden Teil des Urteils in einer bestimmten Ausformung zu veröffentlichen.

2.2 Zur Sicherung des Unterlassungsanspruchs begehrt sie, der Beklagten zu verbieten, im Gebiet der Republik Österreich eine Anlage für die sichere Durchführung von Transaktionen zwischen informationsverarbeitenden Systemen zu verwenden oder zur Verfügung zu stellen,

1. bestehend aus einem Terminal, das zur Eingabe einer Benutzerkennung dient, aus einer Auswerteeinheit, die mit dem Terminal über eine primäre Verbindung verbunden ist, und im Wesentlichen aus einer Speicher- und Prozessoreinheit besteht, welche zur Speicherung von Benutzerstammdaten und laufenden Transaktionsdaten dient, aus einem Codegenerator, der einen Sicherheitscode erzeugt, aus einer Sendeeinrichtung, die den Sicherheitscode über eine sekundäre Verbindung an ein Empfangsgerät sendet, aus einer Eingabemöglichkeit für den Sicherheitscode am Terminal und einer Überprüfung des eingegebenen Sicherheitscode auf Gültigkeit durch die Auswerteeinheit, dadurch gekennzeichnet, dass die Auswerteeinheit einen zusätzlichen Codegenerator aufweist, die einen Zusatzcode erstellt und die Auswerteeinheit aus einer zusätzlichen Sendeeinrichtung besteht, die den Zusatzcode über die primäre Verbindung an das Terminal, welches neben der Eingabemöglichkeit des Sicherheitscode, eine Ausgabe- und Eingabemöglichkeit für den Zusatzcode aufweist, übermittelt und zur Ausgabe bringt und nach Eingabe der eingegebene Zusatzcode durch die auswertete Einheit überprüft wird und bei Gültigkeit von eingegebenem Sicherheitscode und Zusatzcode die Transaktion autorisiert wird;

2. insbesondere wenn eine vermittelnde Auswerteeinheit die vom Terminal übermittelten Anmeldedaten entschlüsselt und auf Grund der ermittelten Informationen die Transaktion an die durchführende Auswerteeinheit übergibt;

3. insbesondere wenn die Auswerteeinheit aus einer oder mehreren vermittelnden und einer oder mehreren durchführenden Auswerteeinheiten besteht; und/oder

insbesondere die Passwortrücksetzung für das Log-in im Kundenbereich auf der Website www.A1.net zu betreiben.

2.3 Die Klägerin sieht das Patent durch die von der Beklagten ihren Kunden angebotene Methode zur Zurücksetzung eines vergessenen Passworts als verletzt an.

3. Die Beklagte verneint die Patentverletzung und trägt – kurz zusammengefasst (§ 500a ZPO) – vor, bei der Passwortzurücksetzung werde insbesondere kein Zusatzcode im Sinn des Streitpatents verwendet.

4. Das Erstgericht wies den Sicherungsantrag mit der angefochtenen Entscheidung ab und ging dabei vom bescheinigten Sachverhalt aus, den es auf den Seiten 2 bis 4 und 5/6 der Entscheidungsausfertigung festhielt, auf den verwiesen und aus dem hervorgehoben wird:

4.1 Das Passwortrücksetzungsverfahren der Beklagten wird mittels mehrerer Server betrieben, die zu Frontend- und Backend-Serversystemen zusammengefasst sind.

Das Frontend-System dient der Kommunikation mit den Benutzern über das Internet. Für die Implementierung des

Frontend wird die Software „Spring-WebFlow-Framework“ verwendet. Diese dient üblicherweise der Steuerung der Präsentation einer Abfolge von Webseiten an den Benutzer, der mit den Vorwärts- und Zurück-Buttons hin- und herspringen kann, ohne dass der Programmlauf (Flow) am Frontend durcheinander kommt. Dazu erstellt das Spring-WebFlow-Framework einen Flowsteuerungsparamenter („FlowExecutionKey“, in der Folge: „Execution Parameter“ [strittig: von der Klägerin als Zusatzcode im Sinn des Streitpatents angesehen; nicht so von der Beklagten], der sich zusammensetzt aus einer Execution-ID („e1“), die den gerade laufenden logischen Flow kennzeichnet, und eine Snapshot-ID („s1“), die einen restorebaren Zustand (Snapshot) des Flows kennzeichnet. Das Passwortrücksetzungsverfahren verwendet stets die Snapshot-ID „s1“, weil ein Hin- und Herspringen zwischen den Webseiten nicht vorgesehen ist.

Bei jedem Neustart des Verfahrens innerhalb der gleichen Session, wird mit der ersten Eingabemaske (Website 1) begonnen und die Execution-ID hochgezählt („e1s1“, „e2s1“, „e3s1“).

Der Backend-System dient hingegen der Erzeugung des Sicherheitscodes und der Durchführung der Transaktion. Dazu werden im Backend-System die Benutzerdaten und die Transaktionsdaten gespeichert. Der Execution Parameter wird nicht an das Backend-System durchgereicht.

Nach der Eingabe der E-Mail-Adresse in der Maske 1 und der Bestätigung wird auf Maske 2 die Mobiltelefonnummer abgefragt, an die die TAN („Transaktionsnummer“) [unstrittig: Sicherheitscode im Sinn des Streitpatents] per SMS versandt werden soll. Nach der Eingabe und der Bestätigung der Daten durch den Nutzer wird über ein Gateway vom Backend zum A1-Mobilfunknetz die TAN [Sicherheitscode] an das Empfangsgerät übersandt.

Gleichzeitig wechselt der Nutzer zur Maske 3, in der er die empfangene TAN eingeben kann. Bestätigt der Nutzer die Eingabe, wird die TAN zusammen mit dem Execution Parameter („e1s1“) mittels der Methode „POST“ an das Frontend versandt.

Die Passwortänderung wird durchgeführt, wenn das Frontend den erwarteten Execution Parameter erhält und das Backend die TAN auf Gültigkeit geprüft hat. Das Backend-System wartet für die Durchführung der Transaktion nur auf die Übermittlung einer TAN zur Überprüfung. Der Wert des Execution Parameter ist für die Durchführung der Transaktion hingegen nicht relevant. Der Execution Parameter und der Sicherheitscode (TAN) werden entkoppelt voneinander verwendet.

4.2 Disloziert auf Seite 7 sieht das Erstgericht den folgenden Ablauf als bescheinigt an(unbekämpft):

Wenn in einem ersten Flow mit Execution Parameter „e1s1“ eine erste Transaktion gestartet wird und am Mobiltelefon eine erste TAN erhalten wird, der Execution Parameter aber auf „e2s1“ verändert wird, führt die Transaktion mit der erhaltenen TAN nicht zum Ergebnis, sondern es kann eine weitere Transaktion gestartet und am Mobiltelefon eine zweite TAN erhalten werden. Wenn dann die zweite TAN mit dem ersten Execution Parameter „e1s1“ an den Frontend-Server retourniert wird, wird die Passwortänderung durchgeführt.

4.3 Rechtlich kam das Erstgericht zum Ergebnis, das inkriminierte Vorgehen der Beklagten verletze das Patent nicht. Das Bescheinigungsverfahren habe ergeben, dass der bei der Passwortänderung benutzte Execution Parameter nicht eine bestimmte Transaktion absichere und auch nicht als transaktionsbezogen angesehen werden könne. Er könne daher nicht als Zusatzcode im Sinne des Streitpatents angesehen werden. Die Merkmale M1.J bis M1.N des Streitpatents seien daher nicht verletzt.

5 . Dagegen richtet sich der Rekurs der Klägerin, die unrichtige Tatsachenfeststellung sowie unrichtige rechtliche Beurteilung geltend macht und beantragt, die Entscheidung zu ändern und die beantragte einstweilige Verfügung zu erlassen.

Die Beklagte beantragt, dem Rekurs nicht Folge zu geben.

Rechtliche Beurteilung

Der Rekurs ist nicht berechtigt.

6.1 In der Feststellungsrüge bekämpft die Klägerin die Feststellung des Erstgerichts, dass der Wert des Execution Parameter für die Durchführung der Transaktion nicht relevant sei und dass er nur zur Steuerung der Webseiten genützt werde. Stattdessen begehrt die Klägerin die Feststellung, dass der Wert des Execution Parameter für die

Durchführung der Transaktion (sehr wohl) relevant sei. Die beiden Daten würden zwar entkoppelt voneinander auf die Gültigkeit geprüft, der Execution Parameter sichere jedoch eine bestimmte Transaktion ab, sodass diese Transaktion nur bei der Gültigkeit des Sicherheitscodes (TAN) und des Zusatzcodes (Exekution Parameter) autorisiert werde.

Damit trägt die Klägerin aber in Wahrheit eine Kritik an der rechtlichen Beurteilung vor, sodass das Rekursgericht insgesamt die rechtliche Beurteilung des Erstgerichts zu überprüfen hat.

6.2 Dazu hat der Senat erwogen:

Der Begriff der „Transaktion" ist auslegungsbedürftig. Dabei muss nicht nur auf die Patentansprüche, sondern auf die Patentschrift insgesamt geblickt werden. Dort werden als Anwendungsbeispiele das Online Banking, Bezahlvorgänge im Online-Handel etc genannt. All diese Dinge sind sicherheitsrelevant und dadurch gekennzeichnet, dass Missbrauch verhindert werden soll. Bei der Kommunikation zwischen informationsverarbeitenden Systemen kommt es auf eine besondere Autorisierung oder Authentifizierung an. Schließlich sind die Interessen der beteiligten Personen massiv betroffen, zum Beispiel weil vermögensrelevante Änderungen vorgenommen werden sollen (vgl dazu BGH X ZR 139/17, Rn 12 ff; den Parteien bekannt).

Diese Sicherheitsüberlegungen gebieten es, bei der Auslegung der Patentansprüche speziell die Verwendung des jeweiligen Singular bei „Sicherheitscode", „Zusatzcode" und „Transaktion" zu berücksichtigen: vgl oben die von der Klägerin präsentierten und formulierten Merkmale M1.F – „einen Sicherheitscode"; M1.J – „eines Zusatzcodes"; und M1.N – „die Transaktion". Daraus ist abzuleiten, dass eine einzelne Transaktion nur dann sicher ist, wenn ein einziger Sicherheitscode mit einem einzigen Zusatzcode korrespondiert und nur bei einer wechselseitig eindeutigen Übereinstimmung diese einzelne Transaktion durchgeführt wird. Jede Möglichkeit des „Experimentierens" und jede Doppel- oder Mehrdeutigkeit sollen verhindert werden und führen aus dem Schutzbereich des Streitpatents hinaus.

Beim inkriminierten Verhalten der Beklagten ist diese Eindeutigkeit nicht gegeben, weil es möglich ist, den Benutzer in die Lage zu versetzen, zwischen (mindestens) zwei TAN zu wählen und genauso einen von (mindestens) zwei Executive Parameter zu verwenden, um das eine angestrebte Ziel zu erreichen, nämlich die Gewinnung eines neuen Passworts anstelle jenes, das vergessen (oder – im Fall eines Missbrauchs – als „vergessen" präsentiert) wurde.

Auf dieses Ziel ist somit beim Begriff „transaktionsbezogen" bei der Patentauslegung abzustellen. Daraus folgt, dass der von der Beklagten verwendete Modus für die Transaktion „Erzeugung eines neuen Passworts" nicht zwingend nur einen einzigen Zusatzcode erstellt (wie in M1.J gefordert) und daher das Streitpatent in keinem Anspruch verletzt.

Die Entscheidung des Erstgerichts bedarf daher keiner Korrektur.

7. Die Kostenentscheidung beruht auf § 393 Abs 1 EO iVm §§ 41, 52 Abs 1 ZPO. Soweit dem Gegner der gefährdeten Partei die Abwehr des Sicherungsantrags gelingt, ist die Entscheidung über seine Kosten des Provisorialverfahrens nicht vorzubehalten (RIS-Justiz RS0005667 [T4]). Da die Gegnerin der gefährdeten Parteien im Rechtsmittelverfahren zur Gänze obsiegte, hat sie Anspruch auf Ersatz der Kosten der

Rekursbeantwortung. Der

Zuschlag für die Beiziehung eines

Patentanwalts steht zu, weil nicht nur prozessual-juristische Fragen Gegenstand des Rechtsmittelverfahrens waren (4 Ob 71/19y).

8. Der Ausspruch über den Wert des Entscheidungsgegenstandes stützt sich auf §§ 78, 402 Abs 4 EO iVm § 500 Abs 2 Z 1 lit b ZPO.

Der ordentliche Revisionsrekurs ist unzulässig, weil die Auslegung der Patentansprüche im konkreten Fall keine darüber hinauswirkenden erheblichen Rechtsfragen aufwirft.

Schlagworte

Gewerblicher Rechtsschutz – Patentrecht; Anlage für die sichere Durchführung von Transaktionen mittels mehrerer Authentifizierungscodes,

Textnummer

EW0001052

European Case Law Identifier (ECLI)

ECLI:AT:OLG0009:2020:03300R00037.20H.0707.000

Im RIS seit

29.09.2020

Zuletzt aktualisiert am

30.09.2020