



CyLaw-Report XXV: "IT-Sicherheit einer Homepage als Schutz vor Mitbewerbersurveillance?" (4/2009)

Entscheidung des OLG Hamm Urteil vom 10.06.2008 - Az.: 4 U 37/08 und des OLG Hamburg Urteil vom 18.04.2007 - Az.: 5 U 190/06

Die CyLaw-Reports I-XIX wurden im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts ([SICARI](#) (2003 – 2007)) erstellt. Mit CyLaw-Report XX folgende wird dieses Online-Legal-Casebook vom Fachgebiet Öffentliches Recht an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) fortgeführt. Die CyLaw-Reports sind keine „Living Documents“, die ständig aktualisiert werden. Zitierungen können deswegen veraltet sein. Die Rechtfertigung für diese klassische Perspektive ist, dass den in den CyLaw-Reports präsentierten Entscheidungen der Gerichte nur die jeweils geltende Rechtslage zu Grunde gelegt werden konnte. Der Aufgabe der Aktualisierung stellt sich der Lehrstuhl in der integrierten Veranstaltung „[Recht der Informationsgesellschaft](#)“. Hier wird das Methodenwissen von Studierenden der Technikwissenschaft so gefördert, dass sie in Übungen an der notwendigen Aktualisierung selbst mitwirken können.

Die Entscheidungen enthalten grundlegende Ausführungen zur wettbewerbsrechtlichen Prüfung von IT-Sicherheitsinstrumenten zum Schutz einer Homepage und zu Offenbarungspflichten der Funktionsweise dieser Sicherheitsmechanismen durch die Nutzer. Wirtschaftlicher Hintergrund der Entscheidungen ist der Wettbewerb zweier Anbieter im Druckerpatronenversandhandel und im Versandhandel für elektronische Geräte. Von essentieller Bedeutung für diese Geschäftsmodelle sind die Veröffentlichungen im Internet. Nicht nur die Qualität der Produkte und der Preis sind Instrumente des Wettbewerbs, sondern auch das Wettbewerbsrecht. Deshalb hat „Mitbewerber 1“ ein großes Interesse daran, dass er die Angebote von „Mitbewerber 2“ möglichst kostengünstig ermittelt und auf ihre Lauterkeit und das Fehlen irreführender geschäftlicher Handlungen (§ 4, 5 UWG) überprüft (Mitbewerbersurveillance). Als Testung der Preise und Verfügbarkeit des Gesamtangebots von „Mitbewerber 2“ wählt er folgende Informationstechnologie: Er greift auf die Seiten von „Mitbewerber 2“ zu, wobei der Aufruf der Seiten über einen Zeitraum von mindestens 2 Stunden mit teilweisen Abruffrequenzen von unter 2 Sekunden pro Seitenabruf, im Durchschnitt aber von höchstens 11 Sekunden, erfolgt. Die Seitenabrufe erfolgen innerhalb der Baumstruktur von unten nach oben und rufen nur Produktlisten ohne detaillierte Produktinformation mit Bildinformation ab. „Mitbewerber 2“ hat eine automatische Blacklist zum Schutz der Funktionsfähigkeit seiner Homepage installiert, die den power user „Mitbewerber 1“ von einem solchen Zugriff auf die Homepage ausschließt. „Mitbewerber 2“ argumentiert, dass sich „Mitbewerber 1“ nicht wie ein normaler Kunde verhalte und der Zugriff die Funktionsfähigkeit seiner Homepage gefährde. „Mitbewerber 1“ wehrt sich gegen die Sperre unter Berufung auf das Wettbewerbsrecht. Zwar könne „Mitbewerber 2“ seine Homepage mit einem IT-Sicherheitsinstrument schützen – er dürfe aber „Mitbewerber 1“ nicht von der Surveillance ausschließen. „Mitbewerber 1“ verlangt also einen exklusiven Zugang zum Internetangebot von „Mitbewerber 2“.

Teil 1: Sachverhalt.....	3
Teil 2: Anspruch auf Beseitigung der IP-Sperrung (§§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 10 UWG)	5
A. „Mitbewerber 1“ als Mitbewerber im Rechtssinne (§ 8 Abs. 3 Nr. 1 UWG)....	6
I. „Mitbewerber 1“ als Unternehmer.....	6
1. Geschäftliche Handlung (§ 2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG)	6
2. „Mit einem anderen Unternehmen“ (2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG) – „Mitbewerber 2“	7
a) Geschäftliche Handlung (§ 2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG)	7
b) In einem konkreten Wettbewerbsverhältnis (§ 2 Abs. 1 Nr. 3 UWG).....	7
3. Zwischenergebnis	7
B. „Eine nach § 3 Abs. 1 UWG unzulässige geschäftliche Handlung (§ 8 Abs. 1 S. 1 UWG).....	7
C. Unlauterkeit der geschäftlichen Handlung: Gezielte Handlung (§ 8 Abs. 1 S. 1 UWG)	8
D. Unlauterkeit der geschäftlichen Handlung: Behinderung (§ 8 Abs. 1 S. 1 UWG)	10
I. Rechtsprechung zur Mitbewerbersurveillance in der Realworld	10
II. Mitbewerbersurveillance im Cyberspace	13
1. Grundsätzliche Rechtmäßigkeit der Mitbewerbersurveillance auch im Cyberspace.....	13
2. „Normaler Kunde“.....	13
a) Öffnung der Homepage für möglichst viele Kunden.....	14
b) Verhinderung von Betriebsstörungen.....	14
aa) Es ist nicht erforderlich, dass bereits eine Betriebsstörung eingetreten ist.....	14
bb) Das OLG Hamm hat akzeptiert, dass das Sicherheitssystem des „Mitbewerbers 2“ technisch gerechtfertigt ist.	15
c) Exklusivzugang für den „Mitbewerber 1“?	16
E. Ergebnis	18
Teil 3: Anspruch auf Unterlassung der IP-Sperrung (§§ 8 Abs. 1 S.1 und 2, 3 Abs. 1, 4 Nr. 10 UWG)	19
Teil 4: Schlussfolgerungen	19

Teil 1: Sachverhalt

Die Parteien sind beide im Bereich des E-Commerce tätig. Es handelt sich um Konkurrenten im Bereich des Druckerpatronenversandhandels.¹ Am 10.8.2006 griff „Mitbewerber 1“ (eine Gesellschaft mit beschränkter Haftung (GmbH)) in kurzer Zeit insgesamt 652-mal auf die Internetseite des „Mitbewerber 2“ (ebenfalls eine GmbH) von seiner dynamischen IP-Adresse zu und durchsucht das gesamte Artikelsortiment, um nach eigenen Angaben zu überprüfen, ob tatsächlich – wie beworben – über 5000 lieferbare Artikel vorrätig seien. Er wählt dabei Seitenabrufe, die innerhalb der Baumstruktur von unten nach oben erfolgen und fordert dabei nur Produktlisten ohne detaillierte Produktinformation mit Bildinformation an. Daraufhin sperrte die automatisierte Sicherheitssoftware des „Mitbewerbers 2“² seine Seiten für die dynamischen IP-Adressen von „Mitbewerber 1“.

FÖR-Technik:

Die Effektivität von Filterungen und Sperrungen ist aus rechtswissenschaftlicher Sicht nicht einfach zu beurteilen. Ein Aspekt ist die Effektivität von Blacklisting etwa zum Schutz vor Spams. Der Online-Dienst heise.de (<http://www.heise.de/security/Blacklists-rennen-dem-Spam-hinterher--/news/meldung/102039>) (11.03.09) berichtet über eine Untersuchung des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen, wonach die von vielen Spamfiltern genutzte Methode des IP-Blacklisting keinen effektiven Schutz bieten kann. Rund 75 % der IP-Adressen hätten danach ohnehin nur eine Nutzungsdauer von einem Tag; nach drei Tagen wurden 92 % aller IP-Adressen nicht mehr genutzt. Die im Rahmen der Untersuchung vorgenommene Absenkung der Eintrags-Lebensdauer von vier auf drei Tage hätte die Ergebnisse der Spamerkennung daher auch kaum negativ beeinflusst. Jedenfalls wehrte sich ein Provider gegen das Blacklisting durch einen anderen Provider vor dem LG Lüneburg (MMR 2008, 61 - mit Anmerkung Heidrich (zu finden über beck-online) erfolgreich unter Berufung auf das Wettbewerbsrecht. **Die von FÖR hier ausgewählten Gerichtsentscheidungen zeigen, dass sich Mitbewerber von IT-Sperren in ihren Interessen an Mitbewerbersurveillance behindert fühlen.** Nicht nur beim Blacklisting stellt sich die Frage der Effektivität und Effizienz, sondern auch bei Internetsperren allgemein. Hierzu hat das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg ein Gutachten erstellt, das die unterschiedlichen Sperrtechnologien untersucht. [<http://www.iuscrim.mpg.de/ww/de/pub/forschung/publikationen/straf/s113.htm>] (18.03.2009)]. FÖR wird in einem späteren CyLAW-Report zu Internetsperren Stellung nehmen. Zur leichten Umgehbarkeit von bestimmten Sperrmaßnahmen führt etwa das LG Kiel aus:

LG Kiel:

„Nicht nur der Nutzer, sondern auch der Anbieter kann eine Sperrung über den DNS-Server ohne Weiteres umgehen. Er kann die Inhalte unter einer anderen Domain bereithalten, die dann auch wieder über den Server der Beklagten zu 1. (beim Beklagten zu 1. han-

¹ Es handelt sich um eine Vereinfachung der Verfahren, die OLG Hamm, Urt. v. 10.06.2008, Az. 4 U 37 / 08 zugrundeliegen.

² Die Verwendung männlicher Sprache ignoriert nicht die Existenz weiblicher Kompetenz.

delt es sich um einen Internetzugangsanbieter – Anm. d. Verf.) erreichbar wären. Vor diesem Hintergrund würde die Sperrung der Website über den DNS-Server dieses relativ kleinen Zugangsproviders nahezu wirkungslos bleiben und die Nutzung der rechtswidrigen Seiten nicht spürbar beeinträchtigen. Insofern hat die Beklagte zu 1. nicht nur vertraglich sondern auch tatsächlich nicht die Möglichkeit die Rechtsbeeinträchtigung über den DNS - Server zu verhindern.“³

Hierin sieht „Mitbewerber 1“ eine wettbewerbswidrige Behinderung und begehrt

- die Beseitigung der bestehenden IP-Sperre und
- die Unterlassung zukünftiger IP-Sperren.

Wenn „Mitbewerber 1“ Recht bekäme, wäre „Mitbewerber 2“ also gezwungen, seine Sicherheitssoftware zu verändern. Als rechtliches Argument gegen die virtuellen Hausverbote beruft sich „Mitbewerber 1“ auf §§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 10 UWG.

§ 8 Absatz 1 und 3 UWG Beseitigung und Unterlassung

(1) **Wer eine nach § 3 oder § 7 unzulässige geschäftliche Handlung vornimmt, kann auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden.** Der Anspruch auf Unterlassung besteht bereits dann, wenn eine derartige Zuwiderhandlung gegen § 3 oder § 7 droht.

(3) **Die Ansprüche aus Absatz 1 stehen zu:**

1. jedem Mitbewerber; [...].

§ 2 Abs. 1 Nr. 1-6 UWG Definitionen

(1) Im Sinne dieses Gesetzes bedeutet

1. „**geschäftliche Handlung**“ jedes Verhalten einer Person zugunsten des eigenen oder eines fremden Unternehmens vor, bei oder nach einem Geschäftsabschluss, das mit der Förderung des Absatzes oder des Bezugs von Waren oder Dienstleistungen oder mit dem Abschluss oder der Durchführung eines Vertrags über Waren oder Dienstleistungen objektiv zusammenhängt; als Waren gelten auch Grundstücke, als Dienstleistungen auch Rechte und Verpflichtungen; [...]

3. "**Mitbewerber**" jeder Unternehmer, der mit einem oder mehreren Unternehmern als Anbieter oder Nachfrager von Waren oder Dienstleistungen in einem konkreten Wettbewerbsverhältnis steht; [...]

6. „**Unternehmer**“ jede natürliche oder juristische Person, die geschäftliche Handlungen im Rahmen ihrer gewerblichen, handwerklichen oder beruflichen Tätigkeit vornimmt, und jede Person, die im Namen oder Auftrag einer solchen Person handelt; [...].

§ 3 Abs. 1 UWG Verbot unlauterer geschäftlicher Handlungen

(1) **Unlautere geschäftliche Handlungen sind unzulässig**, wenn sie geeignet sind, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen.

³ http://medien-internet-und-recht.de/pdf/VT_MIR_2007_413.pdf, S.7 (18.03.2009); LG Kiel Ur. v. 23.11.2007, Az. 14 O 125/07, Rn. 46.

§ 4 Nr. 10 UWG Beispiele unlauterer geschäftlicher Handlungen

Unlauter handelt insbesondere, wer

10. Mitbewerber gezielt behindert;

Die Surveillance des „Mitbewerbers 2“ sei Recht von „Mitbewerber 1“, das „Mitbewerber 2“ nicht durch eine automatische Sicherheitssoftware vereiteln dürfe. „Mitbewerber 2“ argumentiert, dass die Funktionsfähigkeit seiner Homepage essentieller Bestandteil seines Geschäftsmodells sei. „Mitbewerber 1“ habe sich nicht wie ein normaler Kunde verhalten, sondern durch die von ihm gewählte Informationstechnologie den Bestand der Homepage gefährdet. Eine Sicherheitssoftware – deren genaue Funktionsweise er aus Gründen seiner IT-Sicherheitspolicy nicht offenbare – müsse zum Schutz der Homepage einsetzbar sein. Mehrere Gerichte hatten in mehreren Verfahren zu entscheiden, welche rechtliche Argumentation sich durchsetzt.

Teil 2: Anspruch auf Beseitigung der IP-Sperrung (§§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 10 UWG)

„Mitbewerber 1“ könnte einen Anspruch auf Beseitigung der IP-Sperrung durch „Mitbewerber 2“ haben (§§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 10 UWG).

§ 8 Absatz 1 und 3 UWG Beseitigung und Unterlassung

(1) Wer eine nach § 3 oder § 7 unzulässige geschäftliche Handlung vornimmt, kann auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht bereits dann, wenn eine derartige Zuwiderhandlung gegen § 3 oder § 7 droht.

(3) Die Ansprüche aus Absatz 1 stehen zu:

1. **jedem Mitbewerber;**[...].

§ 2 Abs. 1 Nr. 1-6 UWG Definitionen

(1) Im Sinne dieses Gesetzes bedeutet

1. „**geschäftliche Handlung**“ jedes Verhalten einer Person zugunsten des eigenen oder eines fremden Unternehmens vor, bei oder nach einem Geschäftsabschluss, das mit der Förderung des Absatzes oder des Bezugs von Waren oder Dienstleistungen oder mit dem Abschluss oder der Durchführung eines Vertrags über Waren oder Dienstleistungen objektiv zusammenhängt; als Waren gelten auch Grundstücke, als Dienstleistungen auch Rechte und Verpflichtungen; [...]

3. "**Mitbewerber**" jeder Unternehmer, der mit einem oder mehreren Unternehmern als Anbieter oder Nachfrager von Waren oder Dienstleistungen in einem konkreten Wettbewerbsverhältnis steht; [...]

6 „**Unternehmer**“ jede natürliche oder juristische Person, die geschäftliche Handlungen im Rahmen ihrer gewerblichen, handwerklichen oder beruflichen Tätigkeit vornimmt, und jede Person, die im Namen oder Auftrag einer solchen Person handelt; [...].

§ 3 Abs. 1 UWG Verbot unlauterer geschäftlicher Handlungen

(1) **Unlautere geschäftliche Handlungen sind unzulässig**, wenn sie geeignet sind, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen.

§ 4 Nr. 10 UWG Beispiele unlauterer geschäftlicher Handlungen

Unlauter handelt insbesondere, wer

10. Mitbewerber gezielt behindert;

A. „Mitbewerber 1“ als Mitbewerber im Rechtssinne (§ 8 Abs. 3 Nr. 1 UWG)

Das Mitbewerberverhältnis ist legaldefiniert (§ 2 Abs. 1 Nr. 3 UWG).

§ 2 Abs. 1 Nr. 3 UWG Definitionen

3. **„Mitbewerber“** jeder **Unternehmer**, der mit einem oder mehreren **Unternehmern** als Anbieter oder Nachfrager von Waren oder Dienstleistungen **in einem konkreten Wettbewerbsverhältnis** steht;

I. „Mitbewerber 1“ als Unternehmer

1. Geschäftliche Handlung (§ 2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG)

§ 2 Abs. 1 Nr. 6 UWG Definitionen

6. **„Unternehmer“** jede natürliche oder juristische Person, die **geschäftliche Handlungen** im Rahmen ihrer **gewerblichen**, handwerklichen oder **beruflichen Tätigkeit** vornimmt, und jede Person, die im Namen oder Auftrag einer solchen Person handelt;

§ 2 Abs. 1 Nr. 1 UWG

(1) Im Sinne dieses Gesetzes bedeutet

1. **„geschäftliche Handlung“** jedes Verhalten einer Person **zugunsten des eigenen** oder eines fremden **Unternehmens** vor, bei oder nach einem Geschäftsabschluss, das mit **der Förderung des Absatzes** oder des Bezugs **von Waren** oder Dienstleistungen oder mit dem Abschluss oder der Durchführung eines Vertrags über Waren oder Dienstleistungen **objektiv zusammenhängt**; als Waren gelten auch Grundstücke, als Dienstleistungen auch Rechte und Verpflichtungen;

„Mitbewerber 1“ ist eine juristische Person, die Druckerpatronen vertreibt und damit zur Förderung des Absatzes von Waren tätig wird. Eine **geschäftliche Handlung** liegt damit vor (§ 2 Abs. 1 Nr. 1 UWG).

2. „Mit einem anderen Unternehmen“ (2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG) – „Mitbewerber 2“

Damit ein wettbewerbsrechtlicher Anspruch besteht, müsste auch „Mitbewerber 2“ ein Unternehmen sein.

a) Geschäftliche Handlung (§ 2 Abs. 1 Nr. 3 UWG i.V.m. § 2 Abs. 1 Nr. 6 i.V.m. § 2 Abs. 1 Nr. 1 UWG)

Auch „Mitbewerber 2“ ist eine juristische Person, die Druckerpatronen vertreibt und damit zur Förderung des Absatzes von Waren tätig wird. Eine **geschäftliche Handlung** liegt damit beim Warenabsatz vor (§ 2 Abs. 1 Nr. 1 UWG). Die Homepage von „Mitbewerber 2“ ist ein essentielles Vermarktungstool. Auch bei der Sperrung des „Mitbewerbers 1“ zur Sicherung dieses Internetauftritts handelt „Mitbewerber 2“ deshalb geschäftlich.

b) In einem konkreten Wettbewerbsverhältnis (§ 2 Abs. 1 Nr. 3 UWG)

Beide Parteien sind im Bereich des Internetversandhandels als Druckerpatronenverkäufer tätig, so dass sie sich an dieselbe Abnehmergruppe wenden und die Vorteile, die einer aus der Wettbewerbshandlung zieht, sind automatisch die Nachteile des Anderen.⁴ Sie stehen also in einem konkreten Wettbewerbsverhältnis zueinander.

3. Zwischenergebnis

Sowohl „Mitbewerber 1“ als auch „Mitbewerber 2“ erfüllen die Tatbestandsmerkmale der Mitbewerbereigenschaft.

B. „Eine nach § 3 Abs. 1 UWG unzulässige geschäftliche Handlung (§ 8 Abs. 1 S. 1 UWG)

Die Unlauterkeit der Wettbewerbshandlung im Sinne von § 3 Abs. 1 UWG wird durch die Regelbeispiele des § 4 UWG konkretisiert. Hier könnte mit der IP-Sperre „Mitbewerber 1“ in seinem Recht auf Mitbewerbersurveillance (von Mitbewerber 2) **gezielt behindert** worden sein (§ 3 Abs. 1, § 4 Nr. 10 UWG).

§ 8 Absatz 1 UWG Beseitigung und Unterlassung

(1) Wer eine nach § 3 oder § 7 unzulässige geschäftliche Handlung vornimmt, kann auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der

⁴ A. Ohly, Skript: „Unlauterer Wettbewerb“, http://www.zr8.uni-bayreuth.de/downloads/data0506/UWG_2.4.pdf (18.03.2009).

Anspruch auf Unterlassung besteht bereits dann, wenn eine derartige Zuwiderhandlung gegen § 3 oder § 7 droht.

§ 3 Abs. 1 UWG Verbot unlauterer geschäftlicher Handlungen

(1) **Unlautere geschäftliche Handlungen sind unzulässig**, wenn sie geeignet sind, die Interessen von Mitbewerbern, Verbrauchern oder sonstigen Marktteilnehmern spürbar zu beeinträchtigen.

§ 4 Nr. 10 UWG Beispiele unlauterer geschäftlicher Handlungen

Unlauter handelt insbesondere, wer

10. **Mitbewerber gezielt behindert.**

C. Unlauterkeit der geschäftlichen Handlung: Gezielte Handlung (§ 8 Abs. 1 S. 1 UWG)

Hier argumentiert „Mitbewerber 2“, dass er keine manuelle Filterung durchführe, sondern eine automatische. Darüberhinaus wisse das System nicht, dass sich hinter der gesperrten IP-Adresse „Mitbewerber 1“ verberge. Grund der Sperrung sei ein Zugriffsmuster, das zur Identifizierung der IP-Adresse und zur Sperrung führe. Grundsätzlich werde jeder power user mit diesem Zugriffsmuster gesperrt – also theoretisch auch andere. Es liege keine auf „Mitbewerber 1“ gezielte Handlung vor.

Argumentation von „Mitbewerber 2“:

„Sie (die Beklagten – Anm. d. Verf.) haben behauptet, die Sperrung sei schon mangels vorheriger Kenntnis der klägerischen IP-Adresse nicht gezielt erfolgt. Sie sei vielmehr automatisch durch ihre Sicherheitssoftware ausgelöst worden, die bei dem Zusammentreffen unterschiedlichster Auffälligkeiten (Zugriffszahlen, -seiten, etc.) einschreite, **deren exakte Funktionsweise sie jedoch aus Sicherheitsgründen nicht offen zu legen bereit seien**. Die Klägerin habe sich bei ihrem Vorgehen nicht wie ein normaler Kunde verhalten. Vielmehr deute ihr Aufrufverhalten auf den mit der Gefahr von Betriebsstörungen verbundenen Zugriff von Schwachstellenscannern und Spam-Systemen hin.“⁵

Das OLG Hamm hat es akzeptiert, dass der „Mitbewerber 2“ seine Sicherheitstechnologie nicht darlegt. Es hat die Feststellung des unterinstanzlichen Landgerichts akzeptiert (§ 529 Abs. 1 Nr. 1 ZPO), dass die von „Mitbewerber 2“ eingesetzte Technik den „Mitbewerber 1“ nicht kenne.

OLG Hamm:

„Bei der angegriffenen Sperrung der Beklagten handelt es sich zunächst nicht um ein zielgerichtetes manuelles virtuelles Hausverbot gegen die Klägerin, sondern um eine automatische IP-Sperre, die hier über das Schutzsystem der Beklagten ausgelöst wurde und die

⁵ OLG Hamm Urt. v. 10.06.2008, Az.: 4 U 37/08, Rn. 18.

unmittelbar mit der Klägerin auch nichts zu tun hat. Der Senat ist insoweit gem. § 529 I 1 Nr. 1 ZPO an die diesbezüglichen Feststellungen des Landgerichts gebunden, hinsichtlich derer in Bezug auf Richtigkeit und Vollständigkeit keine Zweifel bestehen. **Für eine individuelle und gezielte "Aussperrung" der Klägerin, um diese etwa an der Überprüfung der beanstandeten Werbeaussagen zu hindern, gibt es keinerlei Anhaltspunkte, zumal nicht ersichtlich ist, dass die Beklagten überhaupt eine konkrete Kenntnis davon hatten, dass die Klägerin auf ihre Seiten entsprechend Zugriff hat nehmen wollen**, so wie dies mit Schreiben der Beklagten vom 12.04.2007 zum Ausdruck gekommen ist, mit dem die IP-Nummer der Klägerin erst noch erfragt worden ist. Es ist in keiner Weise feststellbar, dass Sperrungen nur bestimmter IP-Nummern oder sonstige technische Zugangsbeschränkungen, die konkret gegen die Klägerin gerichtet waren, bewirkt worden sind.“⁶

FÖR-Technik:

Der rechtswissenschaftliche Lehrstuhl kann nicht abschließend beurteilen, welche Formen der Nachverfolgung von Zugriffsverhalten technisch möglich sind. Grundsätzlich wäre vorstellbar, dass B den „Mitbewerber 1“ als Konkurrenten sehr gut kennt und auch die Zugangsverbindungen filtert. Festzuhalten ist indes, dass das OLG Hamm den „Mitbewerber 2“ nicht gezwungen hat, die Funktionsweise seiner IT-Sicherheitstechnologie offenzulegen. Festzuhalten ist weiterhin, dass in der Entscheidung des OLG Hamburg die IP-Adressen des „Mitbewerbers 1“ bekannt waren.

OLG Hamburg:

„Die Antragsgegnerin habe zumindest nach ihrer Abmahnung gewusst, wem die IP-Nummern gehörten und gegen wen sich die Sperrung richte. Die IP-Nummern seien – unstreitig- zu jeder Zeit über die Seite www.nic.com (Anlage Ast 6) ermittelbar.“⁷

Kritisch anzumerken ist, dass das OLG Hamm bereits an diesem technischen Merkmal die rechtliche Prüfung hätte beenden müssen. Wenn die Zielgerichtetheit der geschäftlichen Handlung nicht nachzuweisen ist, fehlt es an einer unlauteren Behinderung im Sinne von § 4 Nr. 10 UWG. Weil das OLG Hamm sich hier offensichtlich wenig technischen Sachverstand zutraute, hat es das Tatbestandsmerkmal „gezielt“ nicht weiter geprüft und im Übrigen seine Entscheidung auf die Prüfung der „Behinderung“ fokussiert.

FÖR-Pragmatik:

Die Rechtssprechungspragmatik des OLG Hamm wird vielleicht durch ein Kostenargument unterstützt. Die Beiziehung eines IT-Sachverständigen, der die Sperrfunktionalität gutachterlich beurteilt, wäre kostspielig gewesen. Darüber hinaus hätte das OLG Hamm sich mit der auch im Kontext von Phishing höchst umstrittenen Frage auseinandersetzen müssen, inwieweit die Nutzer von IT-Sicherheitstechnologien zur Offenlegung der Funktionalitäten verpflichtet werden können (Vgl. Cylaw-Report V: „Sicherheit von EC-Karten“). Zusammenfassend folgt FÖR dieser Prüfungsreihenfolge des OLG Hamm und prüft im Folgenden die Behinderung.

⁶ OLG Hamm Ur. v. 10.06.2008, Az.: 4 U 37/08, Rn. 43.

⁷ OLG Hamburg Ur. v. 18.04.2007, Az.: 5 U 190/06, Rn. 5.

D. Unlauterkeit der geschäftlichen Handlung: Behinderung (§ 8 Abs. 1 S. 1 UWG)

§ 8 Absatz 1 UWG Beseitigung und Unterlassung

(1) Wer eine nach § 3 oder § 7 unzulässige geschäftliche Handlung vornimmt, kann auf Beseitigung und bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht bereits dann, wenn eine derartige Zuwiderhandlung gegen § 3 oder § 7 droht.

I. Rechtsprechung zur Mitbewerbersurveillance in der Realworld

Grundsätzlich bleibt festzuhalten, dass es ein „Mitbewerber 2“ dulden muss, dass ein „Mitbewerber 1“ in seine Geschäftsräume eintritt und das Angebot überprüft. Hierzu ist eine Rechtsprechung zur Rechtswidrigkeit von Hausverboten gegenüber Mitbewerbern ergangen.⁸ Von den vielen Entscheidungen zur Mitbewerbersurveillance sollen hier zunächst nur drei Bundesgerichtshof (BGH) Entscheidungen referiert werden. Dogmatisch legt der BGH eine „Normalkundenratio“ zugrunde, nach der maßgebend ist, ob sich der Mitbewerber „nicht anders als jeder andere Käufer“ verhält.

- Diese Formel findet sich bereits in einer Entscheidung des BGH (Hausverbot II) aus dem Jahr 1979, wo ein Apotheker sich unter Berufung auf sein Hausrecht gegen eine Surveillance (Testkäufe) wehrte, die dem Verbot von kostenlosen Zugaben diente.

BGH:

„Die Beklagte hat durch Eröffnung ihres Apothekenbetriebes für den allgemeinen Verkehr zu erkennen gegeben, daß sie zum Verkauf der angebotenen Arzneimittel und anderer Waren ohne Rücksicht darauf bereit ist, welche Zwecke der Käufer mit dem Erwerb der Ware verfolgt. **Verhält sich der Testkäufer nicht anders als jeder andere Käufer, der zur Deckung seines Bedarfs die Geschäftsräume betritt** - Umstände, die das Verhalten der Testkäufer im Streitfall als hiervon abweichend oder sittenwidrig erscheinen lassen könnten, sind weder dargetan noch festgestellt - so gilt der allgemeine Grundsatz, daß jeder Einzelhändler derartige Kontrollkäufe hinnehmen muß.“⁹

- Gegen dieses wettbewerbsrechtlich geschützte Recht auf Mitbewerbersurveillance darf sich ein Unternehmen auch nicht dadurch schützen, dass es Kundenausweise verteilt, die nur unter der vertragsstrafenbewehrten Verpflichtung erteilt werden, dass keine Testkäufe erfolgen (Metro-Entscheidung).

BGH:

„Der Zulässigkeit von Kontrollkäufen steht hier auch nicht entgegen, daß Testkäufer, um überhaupt Kontrollkäufe tätigen zu können, zunächst einen Kundenausweis erwerben und damit auch die vertragsstrafenbewehrte Verpflichtung übernehmen müssen, den Ausweis nicht zu einem Testkauf zu verwenden. **Denn wenn Kontrollkäufe zulässig und zur**

⁸ BGH GRUR 1991, 843, 844; Köhler in: Hefermehl/ Köhler/Bornkamm, Wettbewerbsrecht, 26. Auflage 2008, § 4, Rn. 10.161.

⁹ BGH Urt. v. 13.07.1979, Az.: I ZR 138/77, Rn. 18.

Überwachung des lautereren Wettbewerbs geboten und geeignet sind, darf sich ein Wettbewerber nicht durch eine solche Klausel der Überwachung seines Geschäftsbereichs entziehen.“¹⁰

- Die Grenze zur Duldungspflicht von Mitbewerbersurveillance hat der BGH in der Realworld bei der Anfertigung von Fotos in den Geschäftsräumen des Mitbewerbers zur Dokumentation von Rechtsverstößen gezogen.

BGH:

„Nach ständiger Rechtsprechung des Bundesgerichtshofs ist der Anbieter von Waren oder Dienstleistungen verpflichtet, Testkäufe oder die testweise Inanspruchnahme von Dienstleistungen zu dulden, sofern die den Test durchführenden Personen sich wie normale Nachfrager verhalten. (...) **Üblichem Käuferverhalten einer Testperson kann daher der Kaufmann ebensowenig entgegentreten wie der Anbieter von Dienstleistungen.** (...) Sie begehrt vielmehr das Recht, sich merkbar anders zu verhalten. Fotografieren in den Geschäftsräumen eines Kaufmanns durch Dritte bleibt dem Personal und der Kundschaft nicht verborgen **und begründet die Gefahr von Betriebsstörungen. Erfahrungsgemäß wird sich das Personal wegen der Ungewöhnlichkeit und Auffälligkeit eines solchen Verhaltens der Testperson besonders zuwenden, was Auseinandersetzungen über deren Vorgehen befürchten läßt. Es darf auch nicht vernachlässigt werden, daß mit einem derartigen Auftreten von Testpersonen die Gefahr der Rufschädigung des Kaufmanns verbunden ist,** weil etwa anwesende Kundschaft sich unzutreffende Vorstellungen über den Grund der Anfertigung von Fotografien machen kann. Außerdem ist auch die Möglichkeit der bewußten oder unbewußten Manipulation durch Anfertigung fotografischer Aufnahmen lediglich von einem Teilbereich des Geschäfts oder der sonst zu fotografierenden Objekte wie auch die Gefahr der Herstellung nur scheinbar beweiskräftiger Zufallsbeweise nicht von der Hand zu weisen.“¹¹

FÖR-Technik/Recht:

Diese Entscheidung stammt aus dem Jahr 1991 als der Einsatz von vergleichsweise großen Kameras noch relativ auffällig war. Zu hinterfragen ist 2009, ob das wesentlich weniger invasive Aufnahmen mit kleinen Webcams oder Digitalkameras oder Handys auch noch der Betriebsstörratio des BGH unterliegt. In einer Entscheidung aus dem Jahr 2007¹² lässt der BGH es rechtssprechungspragmatisch dahinstehen, ob **generell** von einer Rechtswidrigkeit von Testfotos weiter auszugehen ist. Er verlangt eine **Einzelfallabwägung**¹³ und hat bei der Anfertigung von Fotos zu Beweis Zwecken die Rechtmäßigkeit anerkannt.

¹⁰ BGH Urt. v. 26.06.1981, Az.: I ZR 71/79, Rn. 18.

¹¹ BGH Urt. v. 25.04.1991, Az.: I ZR 283/89, Rn. 13.

¹² BGH Urt. v. 25.01.2007, Az.: I ZR 133/04 (Testfotos III).

¹³ Hierzu M. Hagenkötter, Die Unlauterkeit von Testfotos, WRP 2008, 39-43, der zur Einzelfallabwägung folgende Kriterien vorschlägt: Gefahr einer Betriebsstörung im Einzelfall aufgrund der Art der verwendeten Kamera; Maß der Ungewöhnlichkeit der Anfertigung von Fotos nach Art des Geschäfts; Bedeutung des Zwecks der Aufnahmen.

BGH (Testfotos III):

„aa) **Schon aufgrund der geänderten Lebensverhältnisse** kann nicht mehr davon ausgegangen werden, dass mit ungenehmigtem Fotografieren in Geschäftsräumen generell die Gefahr einer erheblichen Störung des Betriebs des Geschäftsinhabers verbunden ist. Die **technische Entwicklung ermöglicht es inzwischen, mit Digitalkameras auch kleineren Formats, Kameras in Mobiltelefonen und sogar in Armbanduhren ohne größeren Aufwand jederzeit, an allen Orten und bei jeder Gelegenheit mehr oder weniger brauchbare Fotoaufnahmen herzustellen**. Von dieser Möglichkeit wird in zunehmendem Ausmaß Gebrauch gemacht, ohne dass damit generell eine erhebliche Behinderung oder unangemessene Belästigung Dritter verbunden sein muss. Zwar kann deshalb das Fotografieren in Geschäftsräumen noch nicht als ein normales Kundenverhalten angesehen werden. **Es ist jedoch auch nicht mehr wie früher generell als so ungewöhnlich anzusehen, dass grundsätzlich die Gefahr einer erheblichen Betriebsstörung zu befürchten ist. Jedermann kann heutzutage Fotoaufnahmen in Geschäftsräumen anfertigen, ohne Aufsehen zu erregen**. Auch wenn solche Aufnahmen im Einzelfall vom Publikum oder vom Personal bemerkt werden sollten, kann zudem nicht ohne weiteres davon ausgegangen werden, dass der betreffende Beobachter das Verhalten grundsätzlich als so ungewöhnlich ansehen wird, dass die Gefahr von Auseinandersetzungen und damit von Störungen des Betriebs ernsthaft zu befürchten ist. Angesichts des mittlerweile verbreiteten Einsatzes von Digitalkameras und Fotomobiltelefonen zu allen möglichen mehr oder weniger sinnvollen Zwecken kommt für den Beobachter auch in Betracht, dass das Fotografieren von Waren oder Warenpräsentationen durch Dritte aus anderen, nicht rufschädigenden Gründen erfolgt, etwa um vor dem Erwerb einer Ware die Meinung eines anderen hierzu einzuholen (vgl. Müller-Bidinger in Ullmann, jurisPK-UWG, § 4 Rdn. 106 Fn. 232).

bb) **Es kann im Streitfall dahinstehen**, ob unter diesen Umständen weiter daran festgehalten werden kann, dass Fotoaufnahmen in Geschäftslokalen zu Testzwecken grundsätzlich unabhängig davon unlauter sind, ob es im Einzelfall tatsächlich zu einer erheblichen Betriebsstörung kommt oder zumindest die (konkrete) Gefahr einer solchen besteht. Jedenfalls **kann bei der Interessenabwägung, die in Fällen wie dem vorliegenden vorzunehmen ist, in denen der Beweis eines Wettbewerbsverstoßes anders nicht zu führen ist, dem Interesse des Geschäftsinhabers, mögliche Betriebsstörungen zu verhindern, nur dann der Vorrang eingeräumt werden, wenn nach den Umständen des Einzelfalls die konkrete Gefahr einer erheblichen Betriebsstörung zu befürchten ist**. [...]Entgegen der Auffassung des Berufungsgerichts reicht die Feststellung, dass die Fotoaufnahmen mit Hilfe von Blitzlicht hergestellt worden sind, insoweit nicht aus. Auch solche Fotoaufnahmen führen nicht grundsätzlich zu einer erheblichen Belästigung [...].¹⁴

Das OLG Hamburg wollte nicht abschließend entscheiden, inwieweit im hier zu entscheidenden Cyberspace-Sachverhalt die gleichen Kriterien für Mitbewerbesurveillance bzw. Betriebsstörungen gelten:

¹⁴ BGH Urt. v. 25.01.2007, Az.: I ZR 133/04, Rn. 27 f..

OLG Hamburg:

„Ausgehend von diesen Grundsätzen braucht der Senat anlässlich des vorliegenden Sachverhaltes nicht die zwischen den Parteien streitige Rechtsfrage abschließend zu beantworten, ob die Rechtsprechung hinsichtlich von Zutrittsbeschränkungen zu Geschäftsräumen bzw. zur Zulässigkeit eines „Hausverbotes“ (BGH GRUR 1966, 564, 565 Hausverbot I; BGH GRUR 1979, 859, 860 -Hausverbot II; BGH GRUR 1981, 827, 828 -Vertragswidriger Testkauf) [...].“¹⁵

II. Mitbewerbersurveillance im Cyberspace

Zu prüfen ist, inwieweit diese Grundsätze der Realworld und des traditional law auf das virtuelle Hausverbot – die Sperrung des Zugangs zur Homepage – übertragen werden können. Das OLG Hamm und das OLG Hamburg verlangen eine Interessenabwägung zwischen dem Surveillanceinteresse des „Mitbewerbers 1“ und den Interessen des „Mitbewerbers 2“, der das Recht auf Vorbeugung von Betriebsstörungen beansprucht.

1. Grundsätzliche Rechtmäßigkeit der Mitbewerbersurveillance auch im Cyberspace

OLG Hamm:

„Dabei ist mit der Klägerin davon auszugehen, dass ein Gewerbetreibender, der sich mit seinem Angebot an die Öffentlichkeit wendet, Testmaßnahmen grundsätzlich im Interesse der Allgemeinheit sowie der betroffenen Mitbewerber dulden muss (MünchKomm.-Jänich, UWG, § 4 Nr. 10 Rn. 79 m.w.N.). Die Klägerin hatte von daher das Recht, sich wie ein **normaler Kunde** bei der Beklagten auf deren Internetpräsentation umzusehen und dabei Tests durchzuführen. Dies gilt allerdings nur, wenn sich der Tester wie ein normaler Nachfrager verhält (BGH GRUR 1991, 843, 844 - Testfotos I). Sofern sich der Tester merklich anders verhält als ein normaler Kunde und damit die Gefahr einer Betriebsstörung verbunden ist, darf sich der getestete Unternehmer hiergegen zur Wehr setzen (vgl. BGH GRUR 1979, 859, 860 - Hausverbot II; Hefermehl/Köhler/Bornkamm, 25.Aufl., § 4 Rn. 10.163). **Dabei gilt es indes abzuwägen zwischen dem Interesse des getesteten Unternehmers an der Vermeidung einer Betriebsstörung und dem Interesse des testenden Unternehmers, etwaige Wettbewerbsverstöße hinreichend darlegen und beweisen zu können** (BGH GRUR 2007, 802, 805 - Testfotos III).“¹⁶

Voraussetzung der Mitbewerbersurveillance ist danach, dass der „Mitbewerber 1“ sich wie ein „normaler Kunde“ verhält. Wie ein „normaler Kunde“ sich im Cyberspace verhält, war von den Gerichten in den vorliegenden Entscheidungen zu konturieren.

2. „Normaler Kunde“

Die Besonderheit beim OLG Hamm bestand darin, dass „Mitbewerber 2“ mit seiner Sicherheitssoftware informationstechnisch den „normalen Kunden“ konturierte. Das Gericht weist den Verdacht zurück, dass die Sicherheitssoftware gezielt so erstellt wurde, dass sie Surveillance der Konkurrenten ausschloss. Folgende Argumente sind zu belegen:

¹⁵ OLG Hamburg Urt. v. 18.04.2007, Az: 5 U 190/06, Rn. 15.

¹⁶ OLG Hamm Urt. v. 10.06.2008, Az.: 4 U 37/08, Rn. 45.

a) Öffnung der Homepage für möglichst viele Kunden

OLG Hamm:

„Bereits nach **allgemeiner Lebenserfahrung** und mit Rücksicht auf die kaufmännische Vernunft wird eine Sicherheitssoftware im allgemeinen nicht derart restriktiv programmiert, dass gegen einen Besucher einer Internetseite und damit gegen einen potentiellen Kunden eine IP-Sperre verhängt wird, ohne dass eine sicherheitsgefährdende Beeinträchtigung der Homepage ernsthaft zu befürchten steht. **Ein solches Vorgehen nämlich würde mit den ureigensten Interessen eines das Internet als zentrale Werbe- und Vertriebsplattform nutzenden Unternehmers kollidieren.**“¹⁷

Auch der Ausschluss eines Mitbewerbers von der Homepage ist nicht durchsetzbar:

OLG Hamburg:

„Einen vollständigen Ausschluss des Wettbewerbers im Sinne eines virtuellen Hausverbotes wird der einen Internetshop betreibende Unternehmer nicht bewirken und durchsetzen können. **Unter den Bedingungen des Internets ist grundsätzlich daher schon eine Erschwerung des Zuganges zu der Homepage des Internetshops als wettbewerbswidrig anzusehen, wenn dieses -wie hier- durch die Sperrung bestimmter IP-Nummern oder sonstige technische Zugangsbeschränkungen bewirkt wird.**“¹⁸

b) Verhinderung von Betriebsstörungen

aa) Es ist nicht erforderlich, dass bereits eine Betriebsstörung eingetreten ist.

OLG Hamm:

„Dieses Testverhalten hat auch die **Gefahr einer Betriebsstörung** verursacht. Insoweit ist nicht erforderlich, dass bereits eine Betriebsstörung eingetreten ist (vgl. BGH NJW-RR 1997, 104,105 - Testfotos II). Es reicht vielmehr aus, wenn aus der Sicht ex-ante eine Beeinträchtigung des ordnungsgemäßen betrieblichen Ablaufs zu befürchten ist. Von einer solchen Gefahr ist, wobei die Besonderheiten des Mediums Internet und die sich hieraus ergebenden besonderen Umstände zu beachten und die aufgezeigten Rechtsgedanken insofern nur sinngemäß übertragbar sind, vorliegend auszugehen. Der Seitenanbieter, hier die Beklagten, hat grundsätzlich ein berechtigtes Interesse an dem Schutz seiner Internetpräsenz vor sicherheitsrelevanten Störungen und Angriffen. Ihm kann es nicht verwehrt werden, geeignete Sicherheitssoftware hiergegen zu installieren. Dabei ist es ihm nicht zumutbar, es bei einem "verdächtigen" Zugriff erst zu einer tatsächlichen Störung kommen zu lassen. Dann wäre sein Sicherheitssystem obsolet. Es muss vielmehr ausreichen, dass sich für das System das Verhalten des Testers so darstellt wie ein Verhalten, das gerade zum Einsatz des Sicherheitssystems geführt hat.“¹⁹

¹⁷ OLG Hamm Ur. v. 10.06.2008, Az.: 4 U 37/08, Rn. 48.

¹⁸ OLG Hamm Ur. v. 10.06.2008, Az.: 4 U 37/08, Rn.15.

¹⁹ OLG Hamm Ur. v. 10.06.2008, Az.: 4 U 37/08, Rn. 48.

bb) Das OLG Hamm hat akzeptiert, dass das Sicherheitssystem des „Mitbewerbers 2“ technisch gerechtfertigt ist.

OLG Hamm:

„Die Beklagten [„Mitbewerber 2“ – Anm. d. Verf.] mussten die Gefahr einer Betriebsstörung im Rahmen einer Gesamtabwägung nicht hinnehmen. Ihr **legitimes Interesse, Gefahren für ihren Betrieb durch Vorhalten einer verdächtige Zugriffsversuche abblockenden Sicherheitssoftware abzuwenden** und es erst gar nicht zu einer Beeinträchtigung ihrer Internetseite kommen zu lassen, **überwiegt** gegenüber dem Interesse der sich nicht wie ein normaler Kunde verhaltenden und die Gefahr eines Angriffs auf die Homepage der Beklagten verursachenden Klägerin, eventuelle Wettbewerbsverstöße ihrer Konkurrenten darlegen und beweisen zu können. Zum einen ist wiederum die Widersprüchlichkeit der klägerischen Argumentation zu berücksichtigen. Diese konzediert den Beklagten zwar, ein Sicherheitssystem zu implementieren, verlangt dann aber für sich eine Abschaffung oder Öffnung dieses Systems und damit eine Privilegierung gegenüber dem normalen Kunden. Sie verhält sich eben auch nicht wie ein normaler Kunde, der die Seiten anders als sie nutzt. **Er ruft regelmäßig Einzelinformationen und auch Bilddateien auf, was im Regelfall auch länger dauert als das atypische Aufrufen der Seiten durch die Klägerin.**“

²⁰

Weil sich „Mitbewerber 2“ vor Gefahren durch den Internetzugriff des power users schützen darf, ist die Sperrpolicy grundsätzlich rechtmäßig. Ähnlich hat das OLG Hamburg entschieden:

OLG Hamburg:

„**Sie sind insbesondere aber dann verboten und Gegenmaßnahmen im angemessenen Rahmen ihrerseits gerechtfertigt, wenn sie zu einer Störung des zu kontrollierenden Betriebes führen können** (vgl. Harte/Henning/Omsels, UWG, § 4 Nr. 10 Rn. 49). Es ist insoweit bereits die Gefahr einer Betriebsstörung ausreichend, weil sich der Tester merklich anders verhält als ein normaler Nachfrager (vgl. Hefermehl/ Köhler /Bornkamm, Wettbewerbsrecht, 25. Aufl., § 4 Rn. 10.163). [...]

a. Die Antragsstellerin hat sich bereits nicht wie ein normaler Nachfrager bei dem Aufsuchen der Weiterleitungsseite www.e.de verhalten. **Denn sie hat unstreitig in 71 Fällen innerhalb kurzer Zeit am 10.8.2006 auf die Homepage zugegriffen. Es war auch in erster Instanz der Vortrag der Antragsgegnerin nicht substantiiert bestritten worden, dass übliche Kunden ohne Bestellung nur 1 bis 5mal pro Tag die Homepage der Antragsgegnerin aufsuchen. In diesem Größenbereich hat auch die Antragsstellerin in den Monaten Januar bis Juli 2006 trotz auch schon bestehender rechtlicher Auseinandersetzungen sich die Internetseite der Antragsgegnerin anzeigen lassen. Von diesem üblichen Verhalten weicht das Aufrufen der Homepage durch die Antragsstellerin am 10.8.2006 in 71 Fällen und dem Aufrufen von mindestens 346 Seiten deutlich ab. Dem Landgericht ist zuzustimmen, wenn es hierin ein unübliches Nachfrageverhalten sieht. Diese über bestimmte IP-Nummern der Antragsstellerin veranlassten Zugriffe waren derart auffällig und ungewöhnlich, dass die Sicherheitssoftware der Antragsgegnerin die Zugriffe unstreitig als Angriff definiert und zur Meldung gebracht hat.**

²⁰ OLG Hamm Urt. v. 10.06.2008, Az.: 4 U 37/08, Rn. 48.

b. Insbesondere hierdurch hat sich auch die Gefahr einer Betriebsstörung konkretisiert. Dieses wird dadurch hinreichend belegt, dass die Sicherheitssoftware der Antragsgegnerin Auffälligkeiten signalisierte und der Systemtechniker mit der Problematik befasst werden musste, um das Zugriffsverhalten analysieren und Abwehrmaßnahmen konzipieren zu können. **Durch das Verhalten der Antragsstellerin sind somit Veränderungen der Betriebsabläufe erforderlich geworden, die auch nach Auffassung des Senates als Betriebsstörung einzuordnen sind. Die von dem Systemtechniker bewirkte Sperrung der IP-Nummern der Antragsstellerin war damit als Abwehrmaßnahme gerechtfertigt.** Hierbei kommt es nicht darauf an, ob die Antragsgegnerin wusste, wer hinter den Zugriffen stand, oder ob dieses hätte ohne weiteres festgestellt werden können. Die Abwehrmaßnahmen waren auch nicht unverhältnismäßig, da die am Freitag, d. 11.8.2006 eingeführten Sperrmaßnahmen unstreitig bereits am Montag, dem 14.8.2006 von der Antragsgegnerin wieder aufgehoben worden sind.“²¹

c) Exklusivzugang für den „Mitbewerber 1“?

Das Gericht hat durchweg gesehen, dass das Surveillanceinteresse des „Mitbewerbers 1“ hohen rechtlichen Rang hat. Dennoch hat es den „Mitbewerber 2“ nicht verpflichtet gesehen, die Sperre für den „Mitbewerber 1“ zu durchbrechen. „Mitbewerber 1“ könne „Mitbewerber 2“ wie ein normaler Kunde (FÖR: **natürlich viel aufwendiger**) überwachen.

OLG Hamm:

„Denn es ist der **Klägerin unbenommen, das Internetangebot der Beklagten zu überprüfen**, indem sie sich dabei eines einem **normalen Kunden entsprechenden Zugriffsverhaltens** bedient, so dass weder der Anschein eines "Angriffs" auf die Seite der Beklagten entsteht noch damit auch die Sicherheitssoftware einschreitet. Dies wäre der Klägerin **auch zumutbar**, wenn sie etwa arbeitsteilig vorgeht und ihre Mitarbeiter, die sich **wie normale Kunden verhalten**, von verschiedenen Anschlüssen aus die unterschiedlichen Produktgruppen der Beklagten zu 1) zählen ließe.“

FEX: Ähnliches Urteil des OLG Hamburg²²:

Ein „Mitbewerber 1“ vermutete bei einem „Mitbewerber 2“, der einen Internetshop mit elektronischen Artikeln betreibt, die Angabe falscher Preise bei einer Preis-Suchmaschine („geizhals.de“). Um die Preisangaben mit den tatsächlich auf der Website des „Mitbewerbers 2“ verlangten zu überprüfen, wurden innerhalb kürzester Zeit die Preis-Suchmaschine und achtmal der Webshop angeklickt, wodurch die Sicherheitssoftware Alarm schlug. Der Systemadministrator schloss daher „Mitbewerber 1“ für zwei Tage vom Zugang auf die Shopseite aus. Auch hier beanstandete „Mitbewerber 1“ eine gezielte Behinderung seines wettbewerblichen Interesses an Mitbewerbersurveillance.

Das OLG Hamburg judizierte, dass wie ein Betreiber eines Geschäftslokals in der Realworld auch ein Internetshop-Unternehmer Surveillance hinnehmen müsse, damit Mitbewerber seine Wettbewerbs- oder Vertragsverstöße aufdecken können. Surveillancemaßnahmen seien aber dann rechtswidrig, wenn der „Mitbewerber 1“ sich nicht wie ein „normaler Kunde“ verhalte. Die Surveillancemaßnahmen von „Mitbewerber 2“ stellen eine Betriebsstörung dar, die

²¹ OLG Hamburg Urt. v. 18.04.2007 Az. 5 U 190/06, Rn. 16 ff..

²² OLG Hamburg Urt. v. 18.04.2007 Az. 5 U 190/06.

einen kurzzeitigen Zugangsausschluss von wenigen Tagen rechtfertigte. Das gelte insbesondere dann, wenn es sich um eine technische Abwehrmaßnahme handele, weil eine Sicherheitssoftware die Aufrufe der Internetseite als auffällig klassifiziert habe. Dem „Mitbewerber 1“ stand demnach kein Unterlassungs- bzw. Beseitigungsanspruch hinsichtlich der IP-Sperre zu. Somit bestätigt das OLG Hamburg im Wesentlichen die Rechtsprechung des OLG Hamm, auch wenn im Hamburger Fall zwei Unterschiede bestanden:

- die **IP-Adresse des „Mitbewerbers 1“ dem „Mitbewerber 2“ bekannt** war.

OLG Hamburg:

„Durch das Verhalten der Antragsstellerin sind somit Veränderungen der Betriebsabläufe erforderlich geworden, die auch nach Auffassung des Senates als Betriebsstörung einzuordnen sind. Die von dem Systemtechniker bewirkte Sperrung der IP-Nummern der Antragsstellerin war damit als Abwehrmaßnahme **gerechtfertigt. Hierbei kommt es nicht darauf an**, ob die Antragsgegnerin **wusste, wer** hinter den Zugriffen stand, oder ob dieses hätte ohne weiteres festgestellt werden können. Die Abwehrmaßnahmen waren auch nicht unverhältnismäßig, da die am Freitag, d. 11.8.2006 eingeführten Sperrmaßnahmen unstreitig bereits am Montag, dem 14.8.2006 von der Antragsgegnerin wieder aufgehoben worden sind.“²³

- und die Surveillance von „Mitbewerber 1“ eine **Kostenfolge** für den getesteten „Mitbewerber 2“ hatte.

OLG Hamburg:

„Die Tatsache, dass 63 der 71 Zugriffe der Antragsstellerin über einen - für die Antragsgegnerin zu vergütenden - Link des Portals (...) erfolgten, beinhalten zwar eine finanzielle Beanspruchung der Antragsgegnerin (üblicherweise € 0,10 je Zugriff). Der Senat ist aber nicht der Auffassung, dass hierdurch allein das Zugriffsverhalten der Antragsstellerin im Rahmen ihrer Testmaßnahmen unzulässig geworden ist, unabhängig von der zwischen den Parteien streitigen Frage, ob die Kosten im Hinblick auf Pauschalpreisvereinbarungen darunter liegen und keine Relevanz besitzen. **Denn das Aufsuchen ihrer Homepage über das für sie Kosten verursachende Preisvergleich-Portal entspricht gerade dem von der Antragsgegnerin vorgesehenen Zugangsweg. Das Zugriffsverhalten der Antragsstellerin hat auch noch nicht zu einem derartig hohen Kostenbetrag geführt, dass allein aus diesem Umstand sich die Unzulässigkeit des Testverhaltens der Antragsstellerin begründen lässt.**“²⁴

²³ OLG Hamburg Urt. v. 18.04.2007 Az. 5 U 190/06, Rn. 19.

²⁴ OLG Hamburg Urt. v. 18.04.2007 Az. 5 U 190/06, Rn. 20.

E. Ergebnis

Weil eine Behinderung nach der Interessenabwägung des OLG Hamm nicht vorliegt, hat „Mitbewerber 1“ keinen Anspruch auf Beseitigung der IP-Sperrung gegen „Mitbewerber 2“ (§§ 8 Abs. 1, 3 Abs. 1, 4 Nr. 10 UWG).

FEX: abweichendes Urteil des LG Lüneburg zur Rechtmäßigkeit von Blacklisting²⁵:

In diesem Urteil wurde ein Hosting-Provider („Mitbewerber 2“) dazu verurteilt, eine Sperre gegen „Mitbewerber 1“ aufzuheben, die verhindern sollte, dass seine Kunden Spam-E-mails von „Mitbewerber 1“ erhielten. Das LG Lüneburg hat also in der Blacklist eine gezielte Behinderung von „Mitbewerber 1“ gesehen. Nach einer Literatursicht wird die Entscheidung kritisiert, weil der per Blacklist gesperrte „Mitbewerber 1“ unstreitig unerwünschte E-mails versandt (§ 7 Abs. 1 UWG), das Email-System des Providers („Mitbewerber 2“) belastet und sich selbst wettbewerbswidrig verhalten hat.

§ 7 UWG Unzumutbare Belästigungen

(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht....

(2) Eine unzumutbare Belästigung ist stets anzunehmen

[...]

3.bei Werbung unter Verwendung [...] elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt, oder [...].

Wie auch vom OLG Hamm judiziert wurde, ist eine Sperrung durch eine Blacklist im Einzelfall gerechtfertigt, wenn das Verhalten des Dritten - wie im Fall des LG Lüneburg - mit einer Störung des Betriebsablaufs verbunden ist. Hierzu gehört nach **hier vertretener Ansicht**

- das Argument der Sicherung der technischen Betriebsabläufe von „Mitbewerber 2“ und
- das Argument der Verhinderung von Wettbewerbsverstößen (hier Zusendung rechtswidriger Spams)²⁶ von „Mitbewerber 1“.

Der Provider – „Mitbewerber 2“ - kann demzufolge unter Berufung auf das rechtswidrige und damit ungewöhnliche Nachfrageverhalten des „Mitbewerbers 1“ eine Domain Name System Blacklist verwenden.²⁷

²⁵ LG Lüneburg Urt. v. 27.09.2007 Az. 7 O 80/07 = MMR 2008, 61.

²⁶ FEX: Beim LG Lüneburg handelte es sich nicht um die Zusendung von Werbe-Spams im üblichen Sinne, sondern um die Zusendung unberechtigter Mahnungen.

²⁷ J. Heidrichs, Rechtliche Fragen bei der Verwendung von DNS-Blacklisting zur Spam-Filterung, CR 2009, 168, 170, der auch zu den unterschiedlichen Technologien (Online- und Offline-DNS-Blacklisting) Stellung nimmt; und derselbe in seiner Urteilsanmerkung, MMR 2008, 62, 63.

Teil 3: Anspruch auf Unterlassung der IP-Sperrung (§§ 8 Abs. 1 S.1 und 2, 3 Abs. 1, 4 Nr. 10 UWG)

Der Ablauf der Prüfung entspricht dem in Teil 2 geprüften Anspruch mit dem zusätzlich geforderten Merkmal der sog. Begehungsgefahr. Weil ein Beseitigungsanspruch nicht gegeben ist, sind auch die Voraussetzungen für einen Unterlassungsanspruch nicht gegeben – jedenfalls wenn man der Rechtsprechung des OLG Hamm folgt.

Teil 4: Schlussfolgerungen

- Die Sperrung von IP-Adressen eines Mitbewerbers ist grundsätzlich wettbewerbswidrig, da es dem Mitbewerber möglich sein muss, die Angebote seiner Konkurrenz auf ihre Rechtmäßigkeit zu überprüfen (Recht auf Mitbewerbersurveillance).
- Der Anbieter von Waren und Dienstleistungen ist also regelmäßig zur Duldung von Kontrollmaßnahmen verpflichtet, wenn die angewandten Informationstechnologien denen eines „normalen Kunden“ vergleichbar sind. Die Verhinderung dieser Surveillance wäre unlauter (§§ 3, 4 Nr. 10 UWG). Wer seine Geschäftsräume, seinen webspaces, für den allgemeinen Verkehr eröffnet, handelt wettbewerbswidrig, wenn er generell Kontrollmaßnahmen unter Berufung auf sein (virtuelles) Hausrecht untersagt.
- Nur in bestimmten Ausnahmefällen ist eine IP-Sperre rechtmäßig. Insbesondere dann, wenn ein Mitbewerber sich nicht wie ein „normaler Kunde“ verhält, sondern die Angebote der Konkurrenz in unverhältnismäßiger Weise in Anspruch nimmt oder vom Vorliegen besonderer Umstände auszugehen ist, die ausnahmsweise ein (virtuelles) Hausverbot rechtfertigen. Diese Umstände begründen dann die Konkretisierung eines wettbewerbsrechtlich tolerierten Rechts auf Vorbeugung von Betriebsstörungen – **wettbewerbsrechtliche Verankerung der IT-Sicherheit**.