# § 9 Haftung der anderen Beteiligten

## *I. Haftung des Handelnden*

Die Haftung des handelnden Dritten kommt gegenüber dem Geschäftsgegner sowie dem Account-Inhaber in Betracht. **762**

### *1. Haftung gegenüber dem Geschäftsgegner*

Bei der Haftung gegenüber dem Geschäftsgegner sind zwei Fälle zu unterscheiden. Zunächst wird der Fall betrachtet, in dem der Account-Inhaber dem Geschäftsgegner nicht nach Rechtsscheingrundsätzen auf das positive Interesse haftet. Weil die Regeln über die Stellvertretung (§§ 164 ff. BGB) auf das Handeln unter fremdem Namen entsprechend angewendet werden,[1] werden konsequenterweise die §§ 177 ff. BGB ebenfalls analog angewendet.[2] Bei mangelnder Genehmigung haftet der Handelnde also dem Geschäftsgegner analog zu § 179 BGB. Dabei wird regelmäßig § 179 Abs. 1 BGB einschlägig sein.[3] **763**

Problematisch an dem Anspruch ist für den Geschäftsgegner, dass der Handelnde nur schwer zu ermitteln ist.[4] Der Geschäftsgegner sieht nur, von welchem Account eine Erklärung stammt. Eventuell kann er mittels der IP-Adresse den Anschlussinhaber ermitteln. Über diese kann jedoch nicht bestimmt werden, wer im konkreten Fall gehandelt hat.[5] Die Behauptung, dass nur mit Hilfe des Account-Inhabers der Handelnde identifiziert werden kann,[6] darf nicht dahingehend verstanden werden, dass er stets helfen kann. Zwar kann der Account-Inhaber die Identität des Dritten offenbaren, **764**

---

1 Oben Rn. 283 ff.

2 *OLG Köln*, Urteil v. 13. 1. 2006, 19 U 120/05 – NJW 2006, 1676; *Faust*, JuS 2011, 1027, 1029; *Herresthal*, JZ 2011, 1171, 1172; *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13.

3 *Hauck*, JuS 2011, 967, 970.

4 *Süßenberger*, S. 124; *Herresthal*, JZ 2011, 1171, 1172; *ders.*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 24; *Kuhn*, S. 206.

5 Oben Rn. 47.

6 *Herresthal*, K&R 2008, 705, 706; *ders.*, in: *Taeger/Wiebe*, 21, 26; *ders.*, JZ 2011, 1171, 1172.

wenn er die Zugangsdaten in einer Schlüsselbund-Verwaltung gespeichert hat oder er einen Klebezettels mit dem Passwort auf seinem Monitor angebracht hat[7] und einen Dritter seinen Rechner benutzten lässt, sofern der Missbrauch im zeitlichen Zusammenhang damit auftritt. In vielen Fällen kennt der Account-Inhaber eventuell nur Umstände, die auf einen Dritten hindeuten, wie der Befall seines Rechners mit einem Trojaner.[8] Diese Information deutet jedoch nur auf einen Missbrauchsweg hin und nicht auf den handelnden Dritten. Darüber hinaus kann der Account-Inhaber bei Brute-Force-Angriffen[9] oder bei unbefugter Weitergabe der Zugangsdaten durch den Authentisierungsnehmer[10] noch nicht einmal Hinweise auf den Missbrauchsweg geben, weil diese Missbrauchswege nicht aus seiner Sphäre stammen. Ein Anspruch analog zu § 179 Abs. 1 BGB gegen den Handelnden ist somit regelmäßig schwer bis nicht durchsetzbar.[11]

765 Der zweite Fall ist, dass der Account-Inhaber dem Geschäftsgegner nach Rechtsscheingrundsätzen haftet. Dabei hat der Geschäftsgegner bereits einen Anspruchsgegner. Wenn dem Geschäftsgegner entgegen der herrschenden Meinung ein Wahlrecht zwischen wahrer und scheinbarer Rechtslage zusteht,[12] kommt in diesem Fall eine Haftung des Handelnden analog zu § 179 Abs. 1 BGB in Betracht. Darüber hinaus kann eine Haftung des Handelnden wegen einer vorsätzlichen sittenwidrigen Schädigung (§ 826 BGB) des Geschäftsgegners nach den Umständen des Einzelfalls in Betracht kommen. Ebenso kann eine Haftung des Handeln nach § 823 Abs. 2 BGB i.V.m. § 263 Abs. 1 StGB bestehen, weil ein sog. Eingehungsbetrug mit dem Erlangen einer Verpflichtung bei einer nur minderwertigen, da vom Account-Inhaber nicht gewollten, Gegenleistung vorliegen kann.[13] Bei dem hier abgelehnten Lösungsweg über die *culpa in contrahendo* mit einer Haftung des Accounts-Inhabers auf das negative Interesse,[14] kann daneben der Handelnde analog zu § 179 Abs. 1 BGB in Anspruch genommen werden.[15]

---

7 Siehe oben Rn. 132 ff.
8 Oben Rn. 193.
9 Oben Rn. 181.
10 Oben Rn. 221.
11 *Herresthal*, JZ 2011, 1171, 1172.
12 Oben Rn. 714.
13 Zum Eingehungsbetrug *T. Fischer*, in: StGB-Kommentar[60], § 263 Rn. 176 m.w.N.
14 Dazu oben Rn. 428 ff.
15 *Spindler/Anton*, in: *Spindler/F. Schuster*[2], § 164 BGB Rn. 13.

### 2. Haftung gegenüber dem Account-Inhaber

Eine Haftung des Handelnden gegenüber dem Account-Inhaber kommt ebenso in Betracht. Hat der Account-Inhaber dem Dritten die Zugangsdaten weitergegeben und missbraucht dieser sie, so kommt eine Haftung aufgrund des Innenverhältnisses zwischen den beiden in Betracht. Eine solche Haftung besteht insbesondere dann, wenn der Account-Inhaber wirksam verpflichtet wird oder er dem Geschäftsgegner anderweitig schadensersatzpflichtig ist. Darüber hinaus können dem Account-Inhaber Kosten durch die unberechtigte Inanspruchnahme durch den Geschäftsgegner entstehen, die er vom Handelnden ersetzt verlangen kann. **766**

Fehlt es an einem Vertragsverhältnis, kommt eine deliktische Haftung in Betracht. Bei reinen Vermögensschäden scheidet eine solche Haftung nach § 823 Abs. 1 BGB jedoch aus. Der Dritte haftet nach § 823 Abs. 1 BGB nur, wenn er durch den Missbrauch des Accounts das absolut geschützte Rechte des Account-Inhabers verletzt. Das wird regelmäßig nicht der Fall sein. In Betracht kommt jedoch, die §§ 202a, 202b StGB sowie § 263 Abs. 1 StGB als Schutzgesetze im Rahmen des § 823 Abs. 2 BGB anzuerkennen. Bei denjenigen Missbrauchswegen, die unter diese Strafgesetze fallen, könnte demnach eine Haftung in Betracht kommen. Beim Betrug nach § 263 Abs. 1 StGB kommt ein solcher Anspruch nur in Betracht, sofern der Betrug zu Lasten des Account-Inhabers geschah. Hat der Dritte die Zugangsdaten mit der Absicht missbraucht, den Account-Inhaber beispielsweise aus Mutwillen zu schädigen,[16] kommt eine Haftung aus § 826 BGB in Betracht. **767**

## II. Haftung des Authentisierungsnehmers

Die Haftung des Authentisierungsnehmers kommt gegenüber zwei anderen Beteiligten, dem Account-Inhaber und dem Geschäftsgegner, in Betracht. Mit dem Account-Inhaber hat der Authentisierungsnehmer ein Vertragsverhältnis, aus dem sich die Pflicht ergibt, auf die Interessen des Account-Inhabers Rücksicht zu nehmen (§ 241 Abs. 2 BGB). Teilweise ergeben sich aus den Verträgen oder aus dem Gesetz spezifische Leistungspflichten. Bei Verletzung dieser Pflichten haftet der Authentisierungsnehmer dem Account- **768**

16 Siehe dazu oben Rn. 634.

Inhaber nach §§ 280 Abs. 1, 241 Abs. 2 BGB bzw. nach §§ 280 Abs. 1, Abs. 3, 283 S. 1 BGB.

769 Eine mögliche Pflichtverletzung besteht darin, dass der Authentisierungsnehmer seine Pflicht zur Sicherung der Zugangsdaten, insbesondere deren Geheimhaltung, verletzt. Denkbar ist dabei die unbefugte Offenbarung der Zugangsdaten an einen Unberechtigten.[17] Ebenso stellt es eine Pflichtverletzung dar, wenn der Authentisierungsnehmer seine IT-Infrastruktur nicht ausreichend sichert.[18]

770 Die mangelnde Information des Account-Inhabers über grundsätzliche oder aktuelle Risiken kann ebenfalls eine Pflichtverletzung des Authentisierungsnehmers darstellen. Insbesondere im Rahmen des Online-Bankings werden Aufklärungspflichten der Bank gegenüber ihrem Kunden angenommen, weil diese einen überlegenen Sachverstand besitzt und aktuelle Entwicklungen besser nachverfolgen kann.[19] Ebenso muss der Authentisierungsnehmer sicherstellen, dass ausreichend sichere Authentisierungsmethoden verwendet werden. Bei Banken wird beispielsweise angenommen, dass diese eine Pflicht trifft, Authentisierungsmethoden zu verwenden, die ein angemessenen Schutz gegen Missbrauch bieten.[20]

771 Mit dem Geschäftsgegner hat der Authentisierungsnehmer häufig keine vertragliche Verbindung, auf die eine Haftung gestützt werden könnte. Man könnte erwägen, das Verhältnis des Account-Inhabers mit dem Authentisierungsnehmer, als Schuldverhältnis mit Schutzwirkungen zu Gunsten des Geschäftsgegners anzusehen.[21] Dies wird jedoch regelmäßig an der Erkennbarkeit der einbezogenen Personen für den Authentisierungsnehmer scheitern.[22] Für qualifizierte elektronische Signaturen besteht eine spezialgesetzliche Haftungspflicht des Zertifizierungsdiensteanbieters nach § 11 Abs. 1 S. 1 SigG.[23] Im Rahmen des DeMailG gibt es eine solche Haftung nicht, sodass nur die Anerkennung der Pflichten der Diensteanbieter als Schutzge-

17 Oben Rn. 221.

18 *Borges*, Elektronischer Identitätsnachweis, S. 195; *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 294; *Spindler*, CR 2011, 309, 317; *Bergfelder*, S. 397.

19 *Borges*/*Schwenk*/*Stuckenberg*/*Wegener*, S. 295; *Borges*, Elektronischer Identitätsnachweis, S. 198 ff.; *ders.*, NJW 2012, 2385, 2388; *Hanau*, Handeln unter fremder Nummer, S. 70; *Kind*/*Dennis Werner*, CR 2006, 353, 356.

20 *Hanau*, Handeln unter fremder Nummer, S. 71 f.; *Kind*/*Dennis Werner*, CR 2006, 353, 359; *Schulte am Hülse*/*Klabunde*, MMR 2010, 84, 88.

21 Ebenso wie bei der Haftung des Account-Inhabers oben Rn. 403 ff.

22 *Spindler*, CR 2011, 309, 317.

23 Dazu *Bergfelder*, S. 395.

setz zu einer Haftung nach § 823 Abs. 2 BGB führen kann.[24] Fehlen gesetzliche Haftungstatbestände oder Pflichten für den Authentisierungsnehmer, kommt eine Haftung von ihm gegenüber dem Geschäftsgegner nicht in Betracht.

24 Diese befürwortend *Spindler*, CR 2011, 309, 317.