(1) Asymmetrische Verteilung der Informationskosten

Die erste Voraussetzungen ist eine asymmetrische Verteilung der Informa- 639
tionskosten. Wenn beide Seiten vergleichbare Informationskosten haben, dann ist keine der beiden Seiten der *Cheapest Cost Avoider*. Wenn der Vertrauende niedrige Kosten zur Informationsbeschaffung hat, der Geschäftsgegner hingegen hohe, ist es wirtschaftlich sinnvoll, dem Vertrauenden den Anreiz zur Informationsbeschaffung in Form der Versagung einer Haftung zu schaffen. Nur wenn der Vertrauende hohe Informationskosten und der Geschäftsgegner niedrige Informationskosten hat, kann unter den weiteren Umständen ein Vertrauensschutz geboten sein.[650]

Um zu prüfen, ob die erste Voraussetzung bei dem Missbrauch von Zu- 640
gangsdaten im Internet vorliegt, müssen zunächst die Informationskosten des Vertrauenden und des Account-Inhabers gegenüber gestellt werden. Dabei stellt sich zunächst die Frage, welche Information beschafft werden soll. Die relevante Information für den Empfänger einer Willenserklärung im Internet ist, ob der Account-Inhaber die Willenserklärung selbst oder ein Dritter mit Vertretungsmacht abgegeben hat. Beim Abstellen auf diese Information hat der Account-Inhaber keine Kosten bei der Informationsbeschaffung, weil er derjenige ist, von dem die Information stammt.

Die Informationskosten beziehen sich jedoch ebenfalls darauf, dass der 641
Account-Inhaber verhindert, dass Willenserklärungen in seinem Namen ohne Vertretungsmacht abgegeben werden oder dass er den darauf potentiell Vertrauenden über die fehlende Vertretungsmacht aufklärt. Die Kosten einer solchen Aufklärung sind nicht gering. Der Account-Inhaber muss die Existenz einer durch einen Dritten in seinem Namen abgegebenen Willenserklärung erst in Erfahrung bringen. Regelmäßig hinterlassen online abgegebene Willenserklärungen Spuren in Form von gespeicherten E-Mails bei den gesendeten Objekten oder Benachrichtigungs-E-Mails über den Kauf einer Ware oder das Bieten bei einer Online-Auktion. Diese Spuren können jedoch verwischt werden, beispielsweise durch das Löschen der entsprechenden E-Mails. Einen effektiven Schutz dagegen, dass ein Dritter auf eine Erklärung des Account-Inhabers vertraut, kann nur erreicht werden, wenn der Account-Inhaber den Vertrauenden zeitnah informiert. Die dafür

650 *Schäfer/C. Ott*[5], S. 558. Dazu auch *Fleischer*, S. 306 f.; *Kötz/Schäfer*, S. 173; *C. Ott*, in: Ökonomische Probleme, 142, 157 ff.; *Schepple*, S. 121 f.; vgl. auch *Posner*[8], S. 139 f.

erforderlichen regelmäßigen und zeitnahen Kontrollen stellen mittelhohe Informationskosten dar.

642 Der Account-Inhaber kann jedoch ebenfalls auf der Stufe davor ansetzen. Durch eine sichere Verwahrung der Zugangsdaten kann er dazu beitragen, dass diese nicht missbraucht werden können.[651] Durch einen aktuellen Virenschutz,[652] eine generelle Vorsicht, eine Geheimhaltung seines Passworts und einer sorgfältigen Verwahrung einer Chip-Karte kann der Account-Inhaber das Missbrauchsrisiko vermindern. Dieser Vermeidungsaufwand stellt einen niedrigen bis mittleren Kostenaufwand für den Account-Inhaber dar. Es gibt jedoch Angriffe, gegen die sich der Account-Inhaber auch mit diesen Methoden nicht sichern kann, beispielsweise Man-in-the-Middle-Angriffen mittels Pharming in Form des DNS-Cache-Poisoning.[653] Ein Missbrauch der Zugangsdaten kann auch durch Schwachstellen in der Sicherheitsinfrastruktur des Kommunikationsübermittlers, beispielsweise im SMTP-Server oder dem Webserver eines Internetauktionshauses, ermöglicht werden.[654] Auch mit sehr hohen Informationsbeschaffungskosten kann der Account-Inhaber solche Fälle des Missbrauchs nicht verhindern. Er kann lediglich versuchen, Spuren missbräuchlich darüber abgegebener Willenserklärungen zu entdecken und ein eventuelles Vertrauen des Geschäftsgegners durch eine Aufklärung verhindern.

643 In Konstellationen, in denen die Kommunikation von einem Diensteanbieter kontrolliert wird, wie bei Internet-Auktionsplattformen, kann dieser Diensteanbieter durch Vorsorgeaufwand ebenfalls einen Missbrauch der Zugangsdaten verhindern. Er kann beispielsweise die eigene IT-Infrastruktur so absichern, dass ein Missbrauch ohne die Zugangsdaten verhindert wird.[655] Die Internet-Auktionsplattform wird vereinzelt als *Cheapest Cost Avoider* beim Missbrauch von Zugangsdaten im Internet identifiziert.[656] Diese habe es in der Hand durch die Vorgabe eines sicheren Authentisierungsverfahrens Missbrauch zu verhindern. Die Marktmacht der Online-Handelsplattformen könnte zwar ausreichend sein, um eine sicherere Authentisierungsmethode durchzusetzen. Eine effiziente Lösung muss dies dennoch nicht sein. Sicherere Authentisierungsmethoden, beispielsweise

651 Zur sicheren Verwahrung oben Rn. 558.
652 Oben Rn. 202.
653 Dazu oben Rn. 153.
654 Oben Rn. 211 ff.
655 Zu möglichen Schwachstellen oben Rn. 215.
656 *Wiebe*, MMR 2002, 257, 258; *ders.*, in: Internet-Auktionen[2], Kap. 4 Rn. 68.