

Sicherheit am virtuellen Marktplatz:
Zivilrechtliche und technische
Anforderungen

IT-Law-Symposium 2009

19.10.2009

RA Dr. Ralf Blaha LL.M.

Inhalt



1. IT-Sicherheit in den Medien
2. Technische und wirtschaftliche Aspekte
3. Judikatur

1. IT-Sicherheit in den Medien

Heise Online 6.2.2009

- > Am 8.11.2008 wurden in einer koordinierten Aktion von 130 Geldautomaten in 49 Städten weltweit unter Verwendung geklonter Karten 9 Mio USD abgehoben. Die zum Erstellen der Karten erforderlichen Daten stammen offenbar aus einem Angriff auf den Finanzdienstleister RBS World Pay, bei denen die Daten von **100 Karten ausgespäht** wurden

Heise Online 6.2.2009

- > Eine **Spionagesoftware** soll über mehrere Wochen hinweg Kreditkartendaten bei einem der größten Kreditkarten-Transaktionsdienstleister der USA, Heartland Payment Systems, der **Kartenzahlungen für insgesamt 250.000 Dienstleister** abwickelt, ausgespäht haben. HPS rechnet mit einer Sammelklage wegen Schadenersatzansprüchen seitens seiner Kunden

Heise Online 27.7.2009

- > Beim Registrar und Hosting-Provider Network Solutions haben Unbekannte über **500.000 Datensätze mit Kreditkartennummern gestohlen**, indem sie in Shop-Systeme Code einschleusten, der die Transaktionsdaten klappte

Heise Online 18.8.2009

- > In den USA verantwortet sich ein Cracker vor Gericht, der über mehrere Jahre **130 Mio Kreditkartendatensätze** unter anderem bei einem Unternehmen für Zahlungsabwicklungen, einer Supermarktkette und Einzelhändlern **ausgespäht** hat

Trend Micro Inc. August 2009



- > Estnischer Internetdienstleister als **Drehscheibe für Cyberkriminalität**
 - Betreibt DNS-Server, welche die Domains nicht zu den legitimen, sondern zu falschen IP-Adressen auflösen
 - Betreibt Infrastruktur, die für Trojaner-infizierte User falsche Werbung einblendet (zB Werbung für Medikamente auf der www.cnn.com) und Google-Suchanfragen „entführt“ und die Ergebnisse manipuliert

(Trend Micro Inc., Whitepaper „A Cybercrime Hub“)

Kurier 6.10. und 8.10.2009

Hotmail: Tausende Passwörter gestohlen

Der populäre Online-eMail-Dienst „Windows Live Hotmail“ wurde Opfer einer Hackerattacke. Laut Technologie-Blog *Neowin.com* waren Passwörter von mehr als 10.000 eMail-Konten im Internet veröffentlicht. Auf einer Online-Liste sollen eMail-Adressen mit den Endungen hotmail.com, msn.com und live.com angeführt gewesen sein. Die Daten dürften vorwiegend von Anwendern aus Europa stammen. Microsoft hat laut BBC sofortige Gegenmaßnahmen angekündigt.

Phishing: Auch Googles eMail-Konten geknackt

Anfang der Woche ist im Netz eine Liste mit über 10.000 Passwörtern für Hotmail-eMail-Adressen aufgetaucht (der KURIER berichtete). Jetzt wurde bekannt, dass auch Nutzer der eMail-Dienste von Google, Yahoo! und AOL Opfer der groß angelegten Phishing-Attacke wurden. Insgesamt sollen über 20.000 eMail-Konten betroffen sein. Bei Phishing-Attacken werden die Benutzer auf Webseiten gelockt, die jenen der Betreiber täuschend ähnlich sehen. Geben sie dort Name und Passwort ein, werden die Daten direkt an Cyberkriminelle weitergeleitet, die das Konto etwa zum Versenden von Spam nutzen.

Wind große

Micros
mer be
Europa
chen d
tungen
darauf
von „W
tober d
fe nach
Ballme
Windo

LOGITECH

Kinder-

Kleine Zeitung 7.10.2009

KREDITKARTEN

U2-Hysterie für Daten-Diebstahl missbraucht

Mehrere Websites stahlen Daten von Kreditkarten.

WIEN. Am Samstag wollten zehntausende Fans der irischen Rockband U2 gleichzeitig Karten für das nächstjährige Konzert in Wien kaufen. Online ging bald nichts mehr, die Server von Ö-Ticket & Co. brachen zusammen. Zumindest zwei Dienste aber waren bestens erreichbar: *WorldWideTickets.com* und *u2010tickets.com*.

Wer dort kaufte, könnte dies bald bereuen, handelt es sich dabei doch um kriminelle Angebote mit nur einem Zweck: Beschaffung von Kreditkartendaten. Die Seite *u2010tickets* etwa gibt es erst am 24. September in Mexiko registriert. In der Bestätigungs-Mail hieß es: „Wenn die

Viele s

H

2. Technische und wirtschaftliche Aspekte



Die vier Aspekte der IT-Sicherheit

	Authentizität	Integrität	Vertraulichkeit	Verfügbarkeit
Defini- tion	Sicherheit über den Abgeber einer Willenserklärung	Unversehrtheit der Daten	Nur Berechtigte können auf Daten zugreifen	Informationen und Dienste sind abrufbar
Bei- spiele	Bieter ist der, für den er sich ausgibt	Gebot wird korrekt gespeichert	Mitbieter kennt mein höchstes Gebot nicht	Website ist erreichbar
Bedroh- ungen	Phishing, Angabe falscher Identitätsdaten	Destruktiver Virus, fehlerhafte Schnittstelle	Phishing, Man-in-the-middle-Attack	Denial of Service-Attacken, HW/SW-Ausfälle
Abwehr	Digitale Signaturen, Passwörter, PIN/TANs, Trusted Computing	Spiegelung, Backups, Prüfsummen	Verschlüsselung (zB SSL), Trusted Computing	Backup-Infrastruktur, Spiegelung
Recht- lich	SigG; §§ 5, 18 ECG; § 3 E-GovG; § 148a StGB	§ 14 DSGVO; § 7 GTelG; § 126a StGB; SLAs	§§ 3 ff ZuKG; §§ 14 f DSGVO; §§ 93 ff TKG, § 6 GTelG; § 12 E-GovG; §§ 118a ff StGB	§ 126b StGB; SLAs

Begriffe

- > **Phishing**: Über gefälschte WWW-Adressen an Daten eines Internet-Benutzers gelangen
- > **Pharming**: Manipulation der DNS-Anfragen von Webbrowsern, um den Benutzer auf gefälschte Webseiten umzuleiten
- > **Keylogging**: Mitprotokollieren der Eingaben des Benutzers

Anzahl der Sicherheitslücken

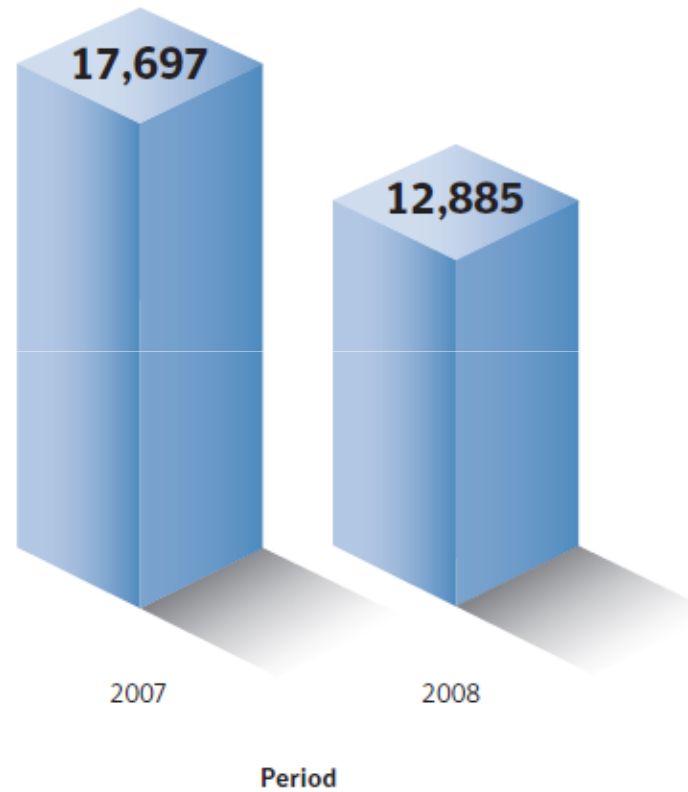


Figure 1. Site-specific vulnerabilities
Source: Based on data provided by the XSSed Project⁵

Bedrohungen durch böartigen Code

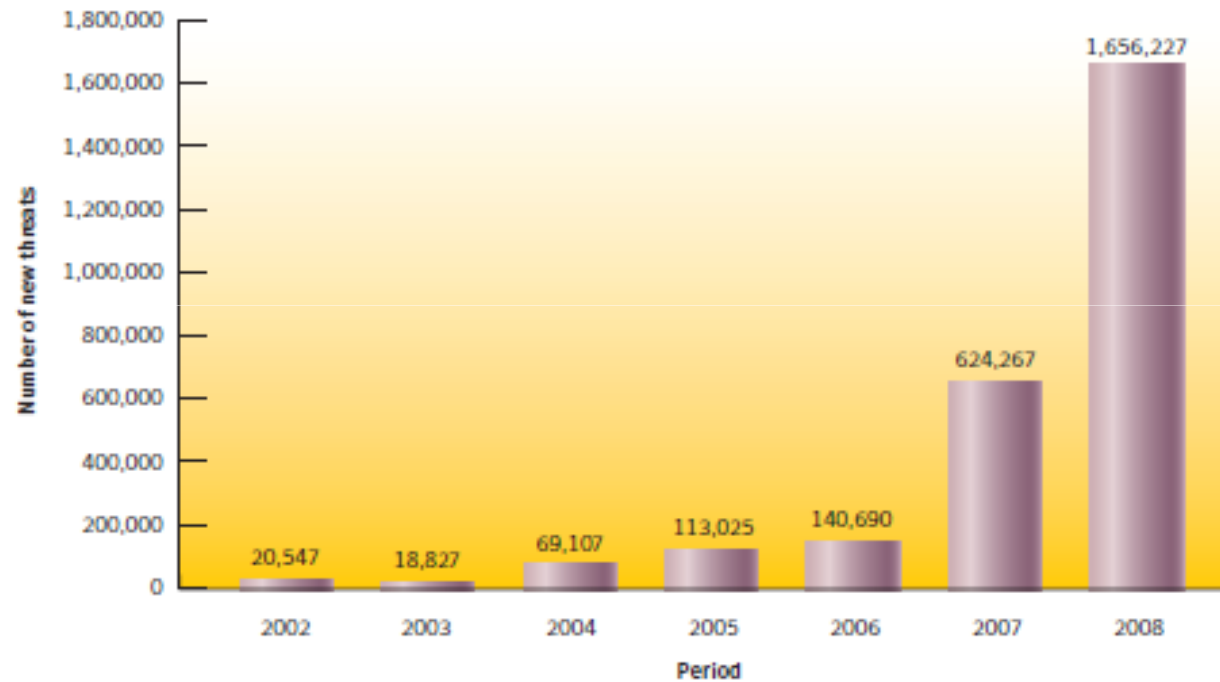
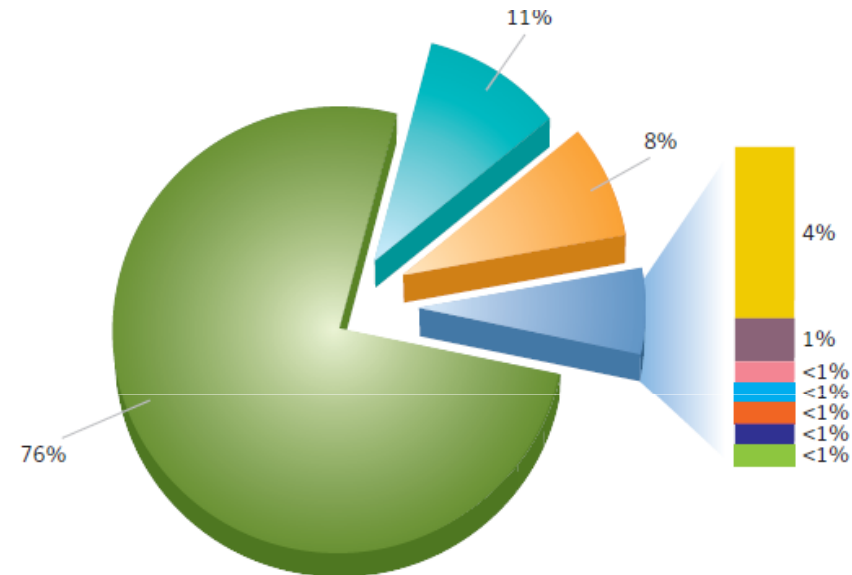


Figure 3. New malicious code threats
Source: Symantec


Ziele des Phishing



- Financial
- ISP
- Retail
- Internet community
- Government
- Online gaming
- Computer hardware
- Insurance
- Telecom
- Computer software

Figure 2. Phished sectors by volume of phishing lures
Source: Symantec Corporation

Quellen der Angriffe



2008 EMEA Rank	2007 EMEA Rank	Country	2008 EMEA Percentage	2007 EMEA Percentage	2008 Global Percentage
1	1	United States	28%	22%	25%
2	2	China	14%	16%	13%
3	3	United Kingdom	10%	11%	6%
4	8	France	4%	3%	4%
5	7	Italy	4%	3%	3%
6	6	Germany	3%	4%	6%
7	14	Russia	3%	1%	2%
8	10	Canada	3%	2%	3%
9	15	Netherlands	2%	1%	1%
10	43	United Arab Emirates	2%	<1%	<1%

Table 2. Top countries of attack origin, EMEA

Source: Symantec

Wirtschaftliche Bedeutung der IT-Sicherheit



- > Sicherheitsbedenken sind der Hauptgrund dafür, dass sich E-Commerce-Nutzer **Limits für ihre Einkaufsvolumina** im Netz setzen
- > Um **attraktiv** zu sein, müssen Online-Shops Sicherheitsmechanismen bieten. Dies ist noch wichtiger als der Preis

(eBay/TNS Infratest-Studie: Sicherheit im Online-Handel 2006)

Wirtschaftliche Bedeutung der IT-Unsicherheit



2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	\$0.06–\$30
2	2	Bank account credentials	19%	17%	\$10–\$1000
3	9	Email accounts	5%	4%	\$0.10–\$100
4	3	Email addresses	5%	6%	\$0.33/MB–\$100/MB
5	12	Proxies	4%	3%	\$0.16–\$20
6	4	Full identities	4%	6%	\$0.70–\$60
7	6	Mailers	3%	5%	\$2–\$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of \$200–\$2000 per item
9	17	Shell scripts	3%	2%	\$2–\$20
10	8	Scams	3%	5%	\$3–\$40/week for hosting, \$2–\$20 design


Table 1. Goods and services available for sale on underground economy servers

Source: Symantec

Verhaltensempfehlungen für Unternehmen (1)

- > Verteidigung in der Tiefe, die auch den Ausfall einer Verteidigungslinie verkraftet, mittels Antivirenprogrammen, Firewalls, Intrusion Detection Systems und Intrusion Protection Systems auf den Client-Systemen
- > Nicht benötigte Dienste deaktivieren
- > Netzwerkdienste, für die Exploits existieren, deaktivieren, bis ein Patch verfügbar und installiert ist
- > Patch Levels **aktuell** halten
- > Lösungen einsetzen, die infizierte **mobile User** aus dem Netzwerk draußen halten bzw sie desinfizieren
- > Effektive **Password-Policy** durchsetzen

Verhaltensempfehlungen für Unternehmen (2)



- > Mailserver so konfigurieren, dass Anhänge, die für Viren verwendet werden (vbs, bat, exe, pif, scr) geblockt werden
- > Infizierte Computer rasch isolieren
- > Mitarbeiter schulen, Anhänge nur zu öffnen, wenn sie von einem bekannten Absender kommen und erwartet werden und Software aus dem Internet nur nach Virenskan auszuführen
- > Notfallpläne zB zur Wiederherstellung nach einem erfolgreichen Angriff oder Datenverlust vorsehen
- > Sicherheitssysteme testen
- > Nur bestimmte Anwendungen auf den Desktops zulassen

(Symantec EMEA Internet Security Threat Report 2008 Vol XIV April 2009, 42 f)

Verhaltensempfehlungen für Verbraucher



- > Internet-Sicherheitslösung mit Antivirus, Firewall, IDS und Antiphishinglösung einsetzen
- > Patch Levels und Virendefinitionsdateien **aktuell halten**
- > Nur **Passworte** verwenden, die aus Buchstaben und Ziffern bestehen und diese oft wechseln; keine Passworte verwenden, die im Wörterbuch zu finden sind
- > Anhänge nur öffnen, wenn sie von einem bekannten Absender kommen und erwartet werden
- > **EULAs lesen**, weil infolge der Akzeptanz Sicherheitsrisiken installiert werden können
- > Vorsichtig mit Programmen sein, die Werbung einblenden, da sie oft mit Spyware zusammenhängen

(Symantec EMEA Internet Security Threat Report 2008 Vol XIV April 2009, 42 f)

3. Judikatur





OGH 27.5.2003, 1 Ob 244/02t
(Telefonsex)

Sachverhalt

- > Anschlussinhaberin besucht Krankenpflegeschule und wohnt im Schwesternheim, Freund ruft inzwischen bei Telefonsex-Hotline an
- > Anschlussinhaberin verweigert Zahlung der Telefonrechnung, Telekom klagt

OGH dazu



- > Dritter nur dann im Vertrauen auf den äußeren Tatbestand zu schützen, wenn der rechtfertigende Tatbestand **mit Zutun** desjenigen zustande gekommen ist, dem der Schutz zum Nachteil gereicht
- > Anscheinsvollmacht setzt voraus, dass das Vertrauen seine **Grundlage im Verhalten des Vollmachtsgebers** hat
- > Voraussetzungen in aller Strenge zu prüfen
- > Die bloße Tatsache, dass der Kunde der Klägerin über einen Telefonanschluss verfügt, den möglicherweise - aber keinesfalls stets typischerweise - **auch andere Personen benützen können**, kann **nicht den Anschein der Bevollmächtigung** erwecken

Schlüsse für Verbraucher



- > OGH lehnt weitgehende Risikozurechnung ab
- > Technische Möglichkeit des Telefonierens begründet keine Rechtsscheinhaftung
- > Keine Verpflichtung des Verbrauchers zu technischen Maßnahmen (zB Nummern zu sperren)



OGH 19.2.2009, 2 Ob 107/08m

OGH 24.2.2009, 9 Ob 3/08v

(Phishing)

Sachverhalt

- > Bk stellt sich als „Finanzdienstleister“ für die Weiterüberweisung von Provisionen zur Verfügung
- > Mit PIN und TAN von Phishing-Opfer wird auf Konto der Bk überwiesen
- > Phishing-Opfer überzeugt Bank, dass nicht seine Überweisung
- > Bank storniert Gutschrift und klagt Debetsaldo ein

OGH dazu (1)

- > Auch gutgläubiger Empfänger (Bk) nicht von Kondiktion geschützt, da **schutzwürdige Interessen des scheinbar Überweisenden**
- > Nur dann **Ausnahme**, wenn scheinbar Überweisender
 - gegenüber dem Empfänger
 - in zurechenbarer Weise
 - Anschein einer im Augenblick der Zahlung noch gültigen Anweisung erweckt
- > Vertrauen des Empfängers auf Rechtsgültigkeit beruhte aber nicht auf Verhalten des scheinbar Überweisenden, sondern nur auf **Versprechungen Dritter**

OGH dazu (2)

- > Selbst wenn fahrlässiges Ermöglichen der Phishing-Attacke vorzuwerfen wäre, ist das Vertrauen des Empfängers auf zweifelhaftes Angebot nicht schützenswert
- > **Kein Verhalten** des Phishing-Opfers festgestellt, das **zum Anschein beigetragen** haben könnte, er habe selbst gehandelt (zB unzureichende Geheimhaltung von PIN und TAN)
- > Daher kein gültiger Überweisungsauftrag

OGH dazu (3)

- > Kann auf sich beruhen, ob vom Institut der Anscheinsvollmacht unabhängige Rechtsscheinzurechnung oder Risikozurechnung
 - Käme - wenn überhaupt - nur im Falle einer **ganz erheblichen Sorglosigkeit** des Kontoinhabers in Betracht
 - Erhebliche Sorglosigkeit nicht schon wegen Herausgabe der TAN infolge betrügerischer Aktion zu unterstellen

Schlüsse für Verbraucher



- > Zurechnung von Folgen einer Phishing-Attacke setzt grobe Fahrlässigkeit des Phishing-Opfers voraus
- > Technische Möglichkeit einer Internet-Transaktion begründet keine Rechtsscheinhaftung



OGH 16.4.2009, 2 Ob 137/08y
(Online-Auktion)

Sachverhalt

- > Käufer erwirbt Heizung bei Online-Auktion
- > Lieferant geht in Konkurs
- > Käufer fordert Kaufpreis von Auktionsplattform zurück

OGH dazu



- > **Vorleistungspflicht** des Käufers in AGB unter Gesichtspunkt des § 879 Abs 3 ABGB und § 6 Abs 1 Z 6 KSchG **unbedenklich**, da
 - Sachlich begründete Verkehrssitte
 - Verkäufer hätte sonst Gefahr der Nichtbezahlung trotz Lieferung und Kosten für Verpackung und Versand zu tragen
- > **Keine** Sorgfaltspflicht des Plattformbetreibers zur **Überprüfung der Bonität**, sofern
 - Keine Kenntnis über drohende Insolvenz
 - Keine Häufung von Beschwerden

Schlüsse für Unternehmer und Verbraucher

- > „Verkehrssicherungspflichten“ des Plattformbetreibers gering
- > Für Risikobegrenzung muss man sich selbst informieren

Deutsche Judikatur strenger



- > OLG Brandenburg 16.11.2005, 4 U 5/05, CR 2006, 124:
 - Der Betreiber einer Internet-Auktionsplattform haftet als Störer für durch Auftreten unter Verwendung fremder Kontaktdaten begangene Namensanmaßungen eines Nutzers, wenn er auf die Rechtsverletzung hingewiesen wurde und keine wirksame Vorsorge gegenüber weiteren gleichartigen Verletzungen - etwa durch Überwachung der Anmeldeprozedur neuer Mitglieder - getroffen hat



OGH 13.6.2005, 10 Ob 54/04w

OGH 27.2.2007, 1 Ob 1/07i

Kreditkartenmissbrauch

Sachverhalt

- > Identitäts- und Legitimationsprüfung bei ausländischen Kreditkarten beim eingesetzten System durch öst Kreditkartenunternehmen nicht möglich
- > Interneteinkäufe mit gestohlenen Kreditkartendaten
- > Kreditkartenunternehmen fordert von Online-Händler geleistete Zahlungen zurück

OGH dazu



- > Missbrauch durch Vertragspartner des Vertragsunternehmens
- > => Kreditkartenmissbrauch eher der **Sphäre des Vertragsunternehmens** zuzurechnen
- > Besondere Missbrauchsanfälligkeit durch offenes Netzwerk
- > Risiko betrügerischer Bestellungen = **typisches Risiko des Fernabsatzgeschäftes**, mit dem Händler seit jeher umzugehen haben
- > Alleinige Zuweisung des Risikos an Vertragsunternehmen in AGB sachlich gerechtfertigt



OGH 22.1.2008, 4 Ob 194/07v
Filesharing durch Tochter

Sachverhalt

- > Vater im Ausland und lässt Tochter surfen
- > Tochter macht Filesharing im großen Stil
- > Verwertungsgesellschaft klagt

OGH dazu (1)

- > Für Haftung muss Sachverhalt bekannt sein, der den Vorwurf gesetzwidrigen Verhaltens begründet oder eine diesbezügliche **Prüfpflicht** verletzt werden
- > Prüfpflicht ist auf **grobe und auffallende Verstöße** beschränkt

OGH dazu (2)

- > Bk musste mangels Anhaltspunkten **nicht damit rechnen**, dass seine Tochter bei Nutzung des Internets in Urheber- und/oder Werknutzungsrecht eingreifen würde
- > Funktionsweise von Internetaustauschbörsen und Filesharing-Systemen kann **bei Erwachsenen nicht als allgemein bekannt** vorausgesetzt werden. Bk musste nicht wissen, dass dadurch Verletzung von Verwertungsrechten
- > Bk daher **nicht verpflichtet, die Internetaktivitäten seiner Tochter von vornherein zu überwachen**

Deutsche Judikatur strenger

- > BGH 11.3.2009, 1 ZR 114/06
 - Benutzt ein Dritter ein fremdes Mitgliedskonto bei eBay zu Schutzrechtsverletzungen und Wettbewerbsverstößen, nachdem er an die Zugangsdaten dieses Mitgliedskonto gelangt ist, weil der Inhaber diese nicht hinreichend vor fremdem Zugriff gesichert hat, muss der Inhaber des Mitgliedskontos sich wegen der von ihm geschaffenen Gefahr einer Unklarheit darüber, wer unter dem betreffenden Mitgliedskonto gehandelt hat und im Falle einer Vertrags- oder Schutzrechtsverletzung in Anspruch genommen werden kann, so behandeln lassen, als ob er selbst gehandelt hätte
 - *„Passwort zu seinem Mitgliedskonto nicht unter Verschluss gehalten, sondern in dem auch seiner Ehefrau zugänglichen Schreibtisch so verwahrt, dass diese ohne Schwierigkeiten davon Kenntnis nehmen konnte“*



> RA Dr. Ralf Blaha LL.M.

Domplatz 1

9020 Klagenfurt am Wörthersee

Tel: 0463/500232

Fax: 0463/265526-4945

blaha@edvrecht.at

www.edvrecht.at