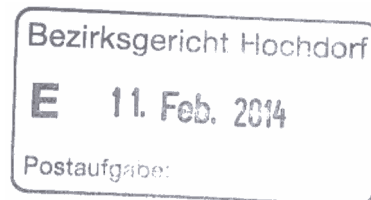


Anmerkung: Dieses Dokument wurde automatisch eingescannt und via OCR in Text umgesetzt. Wir entschuldigen uns für verbleibenden Fehler.

Einschreiben

Bezirksgericht Hochdorf
Bellevuestrasse 6
Postfach
6281 Hochdorf



lic. iur. **Marius Brem**
Rechtsanwalt und Notar
Fachanwalt **SAV**
Erbrecht

lic. iur. HSG et lic. oec.
HSG Peter Germann
Rechtsanwalt und Notar

Dr. iur. Franz Keller
Rechtsanwalt und
Notar
lic. iur. Monika Lütolf-
Geiser Rechtsanwältin

lic. iur. Urs
Lütol
Rechtsanwalt
lic. iur. HSG Dieter
Steiger '
Rechtsanwah und
Notar eidg. dipl.
Steuerexperte

Kriens, 10. Februar 2014

Klageantwort

für

Host Europe Suisse AG, D4 Platz 4, 6039 Root Längenbold, vertreten durch
Rechtsanwalt Urs Lütolf, Luzernerstrasse 51 a, 601 0 Kriens,

Beklagte,

gegen

1 **Herrn René Seeberger**, Im Geissacker 21, 8404 Winterthur, und
2 **Frau Margrit Seeberger**, Route des-Chenes 10, 1082 Corcelles-Le Jorat,

Kläger,

betreffend

Forderung (Fallnummer 1B3 13 34).

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren Bezirksrichterinnen und Bezirksrichter

Namens und irrn Auftrage der Beklagten reiche ich Ihnen innert erstreckten Frist die vorliegende Klageantwort ein mit folgenden

Anträgen-

- 1 Die **Klage** vom 22. Oktober **2013** sei abzuweisen
2. Unter Kosten- und Entschädigungsfolge zulasten der Kläger unter solidarischer Haftbarkeit.

Begründung

Zu Fomelle Angaben

Zu Ziff. 1 bis 3

Keine
Bemerkungen

Zu Ziff. 4

Die Kläger beziffern den Streitwert mit CHF 30'000.00. Dies steht im Widerspruch zu ihren Rechtsbegehren. In Antrag Ziff. 1 machen sie Schadenersatz über CHF 30'000.00 geltend und in Antrag Ziff. 3 verlangen sie zusätzlich die Webhosting-Vertragsgebühren ab 1. Juni 2013 zurück. Es ist somit offenkundig, dass die eingeklagte Summe den Streitwert von CHF 30'000.00 übersteigt. Bereits das Schadenersatzbegehren beträgt CHF 30'000.00. Es gilt somit nicht - wie in der Klageschrift verlangt (vgl. Titelblatt) - das vereinfachte Verfahren, sondern das ordentliche Verfahren (vgl. Art. 243 Abs. 1 ZPO).

Zu Einführung 1 Übersicht

Richtig ist, dass zwischen dem Kläger 1 und der Beklagten ein Webhosting-Vertrag bestand. Der Kläger 1 mietete auf den Servern der Beklagten Webspace (=Internet-Speicherplatz). Es besteht kein schriftlicher Vertrag. Der Kläger 1 hat bei der Beklagten das Produkt "WEB-Professional P3" gebucht zu CHF 14.90 pro Monat (vgl. KB 61 und 165).

Beweis: Urkunde: Bel. 1: Produkteübersicht Webhosting der Beklagten bzw. von dynamic net.ch AG

2. Falsch ist die Behauptung, die unter der Datenbanknummer web175 im Webpace der Beklagten vom Kläger 1 betriebenen Webseiten würden vom Hoster, d.h. von der Beklagten verwaltet. Die Verwaltung der Webseiten wie auch der E-Mail Postfächer ist ausschließlich Sache des Kunden, also des Klägers 1. Ergänzend wird auf die nachfolgenden Ausführungen zu Detailbegründung Ziff. 1 verwiesen.
3. Die Kläger führen aus, dass das Vertragsverhältnis bis Juli 2012 mit der dynamie net.ch AG bestand. Hierzu ist zu bemerken, dass die dynamic net.ch AG und die Beklagte identisch sind. Im Juli 2013 hat die dynamic net.ch AG ihre Firma in Host Europe Suisse AG geändert.

Beweis: Urkunde: Bel. 2: Internet-Handelsregisterauszug betr. Beklagte vom 20. Januar 2014

4. Weiter führen die Kläger in diesem Zusammenhang aus, dass anlässlich dieser Firmaänderung von der Beklagten keine Vertragsänderungen oder veränderte AGB's kommuniziert wurden. Die Kläger bestätigen damit, dass heute nach wie vor die zur Zeit der dynamic net.ch AG vereinbarten allgemeinen Geschäftsbedingungen unverändert Gültigkeit haben. Es ist bereits an dieser Stelle auf Ziff. 9 *Verantwortung und Haftung*' dieser AGB's hinzuweisen. Abs. 2 dieser Bestimmung lautet wie folgt:

"Dynamic-net haftet nur für vorsätzlich oder grobfahrlässig verursachte Schäden sowie für Personenschäden unbeschränkt. Ausgeschlossen ist die Haftung für Schäden infolge Höherer Gewalt oder Verzug. In keinem Fall haftet dynamic-net für Vermögens- und Folgeschäden, Datenverluste und entgangener Gewinn. Betragliche Obergrenze jeglicher Haftung der Dynamic-Net ist der mit dem Kunden in der betroffenen Vertragsperiode mit dem haftungsauslösenden Angebot erzielte Umsatz. Jede darüber hinausgehende Haftung von dynamic-net wird ausgeschlossen."

Beweis: Urkunde: Bel. 3 Allgemeine Geschäftsbedingungen dynamic net.ch AG

5. Selbst dann, wenn dem Kläger 1 durch die Virengeschichte vom Sommer 2013 einen Schaden entstanden wäre und auch die übrigen Haftungsvoraussetzungen (Vertragsverletzung, adäquater Kausalzusammenhang und Verschulden) gegeben wären, was von der Beklagten jedoch bestritten wird, bestünde keine Schadenersatzpflicht der Beklagten. Eine unbeschränkte Haftung würde nur dann greifen, wenn der Beklagten ein

grob-fahrlässiges oder sogar vorsätzliches Verhalten angelastet werden könnte, was vorliegend offenkundig nicht der Fall ist. Dieser Haftungsausschluss steht im Einklang mit Art. 100 Abs. 1 OR.

Wie nachfolgend darzulegen sein wird, trifft die Beklagte an dem von den Klägern behaupteten Schaden jedoch überhaupt kein Verschulden. Auch können der Beklagten keine Vertragsverletzungen vorgeworfen werden, geschweige denn solche, die zum behaupteten Schaden in einem adäquaten Kausalzusammenhang stünden. Wäre leichte Fahrlässigkeit zu bejahen, was jedoch wie gesagt bestritten ist, so wäre eine allfällige Haftung auf den vom Kläger 1 in der betroffenen Vertragsperiode erzielten Umsatz beschränkt. Die Webhosting-Vertragslaufzeit beträgt jeweils ein Jahr (vgl. auch KB 61). Somit wäre ein allfälliger Schadenersatz der Beklagten bestenfalls auf CHF 178.80 beschränkt (12 x CHF 14.90).

Beweis: **Urkunden:** Bel. 1 Produkteübersicht Webhosting der Beklagten bzw. von dynamic net.ch AG

Bel. 3: Allgemeine Geschäftsbedingungen dynamic net.ch AG

- 6 Die Klageschrift ist zudem ungenügend substantiiert. Insbesondere enthält die Klageschrift weder Ausführungen zum geltend gemachten Schaden noch zur verlangten Rückerstattung der Hosting-Gebühren. Lediglich als Beilage zur Klage findet sich eine tabellarische Zusammenstellung "History/Tatbestand-Beweismittel/Zeitaufwand/Kosten" datierend vom 21. Oktober 2013 und versehen mit der Fallnummer des Friedensrichterverfahrens FRH 13 148. Diese Zusammenstellung ist prozessual unbeachtlich. Die massgebenden Tatsachenbehauptungen müssen substantiiert in der Klage selbst erfolgen (Art. 221 Abs. 1 lit. d ZPO). Eine blosser Verweisung auf Beilagen ist unzureichend (Killias, Berner Kommentar ZPO 11; N 23 Alinea 4 zu Art. 221), wobei hier in der Klageschrift nicht einmal auf die genannte Beilage verwiesen wurde. Die Klage ist somit bereits mangels Substanziierung abzuweisen.
- 9
- 7, Im Gegensatz zum Kläger 1 steht die Beklagte mit der Klägerin 2 in keinem Vertragsverhältnis, was von den Klägern zu Recht auch nicht behauptet wird. Folglich kann die Klägerin 2 von der Beklagten weder Schadenersatz aus einer angeblichen Schlechterfüllung des Hosting-Vertrages mit dem Kläger 1 geltend machen noch vom Kläger 1 geleistete Hosting-Gebühren zurückverlangen. Der Klägerin 2 fehlt die Aktivlegitimation für die geltend gemachten Ansprüche, weshalb ihre Klage so oder so abzuweisen ist.

Zu Begründung

Zu Summarium 1 Index

Keine Bemerkungen

Zu Detailbegründung

Zu Ziff. 1

- 1 Die Kläger verkennen das Wesen und den Inhalt des zwischen der Beklagten und dem Kläger 1 abgeschlossenen Hosting-Vertrages. Sie führen aus, dass ihre Daten, welche entsprechend dem Vertrag der Beklagten „anvertraut“ wurden, nicht dem heutigen Stand der Technik entsprechend geschützt wurden. Diese Darstellung ist ebenso unzutreffend wie die auf Seite 3 der Klage (oben) gemachten Ausführungen, wonach die Webseiten und die E-Mail Postfächer vom Hostler, d.h. von der Beklagten verwaltet werden.

2. Beim Hosting-Vertrag mietet der Kunde auf Servern des Hosters Webspace. Dieser Internet-Speicherplatz wird vom Kunden selbst verwaltet und nach seinen Bedürfnissen für verschiedene Zwecke genutzt, z.B. für Homepages, Shopsysteme, Communitys, Bewerbungsstellen, Online Fotoalben, ebay Webspace, online Anwendungen. Die Verwendung des Webspaces obliegt alleine dem Kunden. Die Beklagte kann und darf - unter anderem aus Datenschutzgründen - auf die Kundendateien auf dem Server weder zugreifen noch diese einsehen oder gar ändern. Dies ist alleine Sache des berechtigten Administrators, hier des Klägers 1. Die Beklagte stellte dem Kläger 1 lediglich die technischen Grundlagen zur Verfügung. Sämtliche Softwareinstallationen inklusive Erstellung und Bearbeitung der Webseiten oder Datenbanken muss der Kunde hingegen selber erledigen. Dasselbe gilt auch für die E-Mail Postfächer. Die Vornahme der erforderlichen Einstellungen und Einrichtungen (z.B. die Einrichtung der E-Mail Konten) ist Sache des Kunden. Auf die Emaildaten der Kunden fehlt der Beklagten auch aus technischer Sicht jegliche Zugriffsmöglichkeit. Darauf basiert der zwischen den Parteien abgeschlossene Hosting-Vertrag.

Beweis: Urkunde: Bel. 1 Produkteübersicht Webhosting der Beklagten bzw. von dynamic net.ch AG

- 3 Die Server der Beklagten sind mit den üblichen Schutzmassnahmen versehen (Z.B. Spamschutz, Schutz vor DDoS-Attacken [= Angriffe, welche den Server infolge Überbelastung unerreichbar machen], etc.), obschon die Beklagte hierzu gegenüber ihren Kunden rechtlich nicht verpflichtet ist. Mit diesen Massnahmen ist die gesamte Infrastruktur der Beklagten und deren Funktionsfähigkeit geschützt. Diese Schutzmassnahmen

kommen somit auch den Kunden zugute. Sie bieten den Kunden für ihre Webseiten und Dateien jedoch nur einen bedingten Schutz.

4. Für weitere Schutzmassnahmen, insbesondere für den Virenschutz der Webseiten und Dateien ist der Kunde alleine verantwortlich. Er hat diese vor Viren aus dem Internet zu schützen. Die konkreten Schutzmassnahmen hängen davon ab, für welche Zwecke der Server vom Kunden genutzt wird, wie dieser betrieben wird und welche Software und welches Betriebssystem vom Kunden installiert werden. Darüber hat die Beklagte als Hosterin keine Detailkenntnisse, weshalb sie auch keine Möglichkeit hat, zusätzlichen Schutzmassnahmen sinnvoll einzusetzen.

Grundsätzlich sollte der Kunde seinen Server durch Zugriffe durch Dritte schützen, indem zunächst nur ein eingeschränkter Personenkreis überhaupt Zugriff auf den Server hat. Der Kläger 1 führt selbst aus, dass er anderen Personen, unter anderem der Klägerin 2, Zugriff auf den gemieteten Internet-Speicherplatz gewährte und Teile davon zur Verfügung gestellt hatte. Es ist durchaus wahrscheinlich, dass eine oder mehrere dieser Personen für den Virenbefall verantwortlich sind. Zudem ist wichtig, dass die Kunden stets aktuelle Software nutzen. Ältere Software haben oft Schwachstellen, die schnell ausgenutzt werden. Unabdingbar ist ferner, dass die Kunden auf ihre Bedürfnisse zugeschnittene Schutzsoftware (Virensoftware) verwenden. Diese hängt von der konkreten Nutzungsart der Kunden ab. Zu schützen sind von den Kunden selbstverständlich auch die Heim- oder Arbeitsplatzrechner, von welchen der Zugriff auf den Server erfolgt. Wenn diese befallen sind, ist es für einen Angreifer ein leichtes, die Zugangsdaten mitzulesen und damit ohne Probleme wie der Kunde selbst auf den Server zuzugreifen.

Dies wurde vom Kläger 1 offenbar nicht hinreichend vorgekehrt. Über die von ihm getroffenen Schutzmassnahmen schweigt er sich denn bezeichnenderweise auch aus. Ist der Virenschutz Sache des Klägers 1, so gilt dies selbstredend auch für die Beseitigung des Virenbefalls seiner Webseiten und Dateien.

5. Ob die Viren von den Klägern "eingeschleppt" oder von Dritten verursacht wurden, spielt auch keine Rolle. Bei einer Infizierung der Webseiten durch Dritte ist es ebenso Sache des Klägers 1, die Viren, Malware, etc. zu entfernen, wie wenn er diese selbst eingeschleppt hat.

Dies gilt auch dann, wenn der Kläger 1 das web175 zur fraglichen Zeit und kurz zuvor nicht besucht hätte, was bestritten ist. Viren nutzen normalerweise Schwachstellen in der Software aus, um sich selbständig von Server zu Server zu kopieren. Dabei können die Viren selbständig nach neuen Servern suchen, die entsprechende Schwachstellen aufweisen. Da dieser Vorgang also automatisch und unbemerkt vom Kunden läuft, macht es keinen Unterschied, ob der Kunde sich auf dem Server einloggt oder nicht. Meistens laufen Viren auch gerade so, dass der normale Betrieb des Servers nicht beeinträchtigt wird, um keine Aufmerksamkeit zu erregen.

Fbenso mit Nichtwissen bestritten ist die Behauptung, die PC-Infrastruktur der Klägerin 2 sei durch einen professionellen IT-Service gewartet, mit einem Virenschutzprogramm ausgerüstet und nach der Virenmeldung überprüft und als virenfrei bezeichnet worden.

Höchstwahrscheinlich wurden die Viren bzw. die schädliche Software denn auch von Dritten auf den Webseiten des Klägers 1 platziert. Darauf deuten auch die Ausführungen von SWITCH Internet Domains in der Mail vom 30. Mai 2013 (KB 6):

" ... Höchstwahrscheinlich wurde der Code zur Verbreitung der schädlichen Software unbemerkt von Dritten auf Ihrer Webseite platziert, zum Beispiel durch eine Sicherheitslücke auf Ihrer Webseite, ein schwaches Passwort oder durch Spionagesoftware auf Ihrem PC. ... Als Halter des genannten Domain-Namens bzw. als technischer Kontakt sind Sie für den Inhalt der Webseite verantwortlich. Deshalb fordern wir Sie auf, den Code zur Verbreitung der schädlichen Software umgehend, jedoch spätestens bis am 31. Mai 2013 13.32 zu entfernen. ... "

Für einen ungenügenden Virenschutz haben die Kläger einzustehen und nicht die Beklagte. Alles Abweichende wird bestritten.

6. Der Virenbefall gewisser Webseiten des Klägers 1 ist nicht auf eine Vertragsverletzung der Beklagten zurückzuführen. Dieser kann weder eine Sorgfaltspflichtverletzung noch eine andere Vertragsverletzung vorgeworfen werden. Der vorliegend aufgetretene Virenbefall fällt alleine in den Verantwortungs- und Risikobereich des Klägers 1. Alles Abweichende wird bestritten.

7. Die Kläger behaupten unter Hinweis auf Beiträge unter www.sellerforum.de, dass die Beklagte bereits im April 2012 solche Probleme gehabt habe (vgl. BB 155 und 156). In diesem Zeitpunkt firmierte die Beklagte nach wie vor unter dynamic net.ch AG und noch nicht unter Host Europe Suisse AG. Die entsprechende Firmaänderung ist erst im Juli 2012 erfolgt, was von den Klägern auf Seite 3 der Klageschrift auch so bestätigt wird. Die von der Klägerin zitierten Beiträge aus Deutschland, welche eine "Hosteuropa" betreffen, können somit nicht die Beklagte zum Gegenstand haben. Aber selbst dann, wenn dies die Beklagte betreffen würde, könnten die Kläger aus solchen Internetforen, deren Wahrheitsgehalt jeweils mehr als fraglich ist, nichts zu ihren Gunsten ableiten.

Beweis: Urkunde: Bel. 2:

Internet-Handelsregisterauszug betr. Beklagte vom
20.Januar2014

- 8 Dasselbe gilt auch für KB 161 und 162. Ob die Webseite www.appenzellersennenhunde.ch bei der Beklagten gehostet wurde, weiss die Beklagte nicht und tut hier auch nichts zu Sache. Jedenfalls lässt sich dem Vermerk in KB 162 entnehmen, dass der Code dieser Webseite durch einen böswilligen Angriff auf diese Webseite beschädigt wurde. Offenbar war auch diese Webseite gegen Malware, Viren, etc. vom verantwortlichen Betreiber zu wenig geschützt.

Zu Ziff. 2

Zutreffend ist, dass der Kundenservice der Beklagten in der fraglichen Zeitspanne nicht optimal funktionierte. Die Reaktionszeiten auf die Mails und Telefonanrufe der Kläger waren zum Teil zugegebenermassen etwas lange. Dies war auf eine Unterbesetzung des Supportteams und auf eine zeitliche Überbelastung der Mitarbeitenden zurückzuführen. Mit dem nicht in allen Teilen befriedigenden Kundenservice können die Kläger jedoch keine Schadenersatzforderungen gegen die Beklagte begründen. Alles Abweichende wird bestritten.

Zu Ziff. 2.1

- 1 Unabhängig vom Kläger 1 hat die Beklagte auch von der Nansys Informatik GmbH am 1. Juni 2013 Mitteilung erhalten, dass gewisse für den Kläger 1 gehastete Webseiten mit Malware (=schädliche Software) infiziert sind.

Beweis: Urkunde: Bel. 4: Mail Nansys Informatik GmbH 1 Beklagte vom 1. Juni 2013 mit pdf-Anhang

- 2 Die Mail des Klägers 1 vom Mittwoch, 29. Mai 2013, 23:46 Uhr, wurde am Montag, 3. Juni 2013, 17:13 Uhr beantwortet. Es wurden dem Kläger 1 diverse Lösungsvorschläge unterbreitet. Unter anderem wurde dem Kläger 1 empfohlen, sämtliche Passwörter zu ändern. Zudem wurde der Kläger 1 auf weitere Informationen zum Thema "Malware/Phishing" hingewiesen. Weitere Informationen hat der Kläger 1 auch von SWITCH erhalten (vgl. KB 6).

Beweis: Urkunde: Bel. 5: Mail Beklagte 1 Kläger 1 vom **3. Juni 2013**

3. Zu betonen ist hier nochmals, dass der Virenschutz und die Beseitigung der mit Viren, Malware, etc. befallenen Webseiten und Dateien Sache des Klägers 1 und nicht der Beklagten ist. Befallen mit Viren waren die Webseiten und Dateien des Klägers 1 (vgl. KB 2, 3 und 6). Folglich lag es nicht an der Beklagten, dem Kläger 1 konkret und einzelfallbezogen mitzuteilen, was im Einzelnen zur Behebung der Viren bzw. Malware vorzu- kehren ist, zumal die Beklagte auch keine Möglichkeit hatte, auf die Dateien des Klägers 1 zuzugreifen und diese einzusehen. Der von den Klägern monierte kostenlose Support

bezieht sich denn auch nur auf die eigenen Angebote der Beklagten (vgl. Ziff. 4 Abs. 3 der massgebenden AGB's), wozu die Virenbeseitigung auf den Kundenwebseiten nicht zählt. Alles Abweichende wird bestritten.

Beweis: Urkunden: Sel. 4: Mail Nansys Informatik GmbH 1 Beklagte vom 1. Juni 2013 mit pdf-Anhang

Bel. 3: Allgemeine Geschäftsbedingungen dynamic net.ch AG

Zu Ziff. 2.2

Dass die Kläger die betroffenen Webseiten und Dateien repariert haben, wird von ihnen nicht nachgewiesen und ist von der Beklagten auch bestritten.

Zu Ziff. 2.3

Die erste Antwort der Beklagten ist wie vorstehend ausgeführt am 3. Juni 2013 erfolgt. Am 4. Juni 2013 wurde dem Kläger 1 ergänzend mitgeteilt, dass die Beklagte auch von Dritten, namentlich von der Nansys Informatik GmbH, Kenntnis der infizierten Webseiten erhalten habe und es wurde der Kläger 1 aufgefordert, die nötigen Massnahmen zur Beseitigung einzuleiten verbunden mit dem Hinweis, dass andernfalls das Hosting deaktiviert werden müsste (BB 1 1). Mögliche Lösungsvorschläge wurden dem Kläger 1 nochmals aufgezeigt. Ergänzend wird auf die obigen Ausführungen zu Ziff. 2.1 verwiesen. Alles Abweichende wird bestritten.

Beweis: Urkunden: Bel. 5: Mail Beklagte 1 Kläger 1 vom 3. Juni 2013

Bel. 4: Mail Nansys Informatik GmbH 1 Beklagte vom 1. Juni 2013 mit pdf-Anhang

Zu Ziff. 2.4

Wie bereits erwähnt ist es Sache des Klägers 1, den Virenbefall der fraglichen Webseiten zu analysieren, deren Umfang festzustellen und die entsprechenden Massnahmen zur Beseitigung der Viren, Malware, etc. zu treffen. Die Beklagte hat keine Kenntnisse der Dateien auf ihrem Server und auch keine Zugriffs- und Änderungsmöglichkeiten auf diese Dateien. Welche und wie viele Dateien der Kläger mit Viren befallen waren, weiss die Beklagte nicht und wird deshalb mit Nichtwissen bestritten. Folglich handelt es sich bei den am 3. und 4. Juni 2013 unterbreiteten Lösungsvorschlägen wie gesagt um blosse grundsätzliche Empfehlungen. Hinzu kommt, dass der Kläger 1 angeblich vom Fach ist und offenbar seit mehr als 15 Jahren Erfahrung als Webmaster im Umgang mit Webseiten hat (vgl. Klage S. 3). Die Beklagte hat den Arbeitsaufwand der Kläger nicht erhöht, geschweige denn bewusst.

Bestritten ist insbesondere auch die unsubstanzierte Behauptung, dass die Beklagte den Virenbefall ermöglicht haben sollte und sie folglich für die Schadensbehebung verantwortlich sein sollte.

Für die Datensicherung sind die Kunden selbst verantwortlich (vgl. Ziff. 8 der massgebenden AGB's). Die Verwendung von Backups kann vom Kunden nicht verlangt werden und wurde vom Kläger 1 konkret auch nie beantragt. Es besteht optional die Möglichkeit, die Beklagte im Rahmen eines separaten, kostenpflichtigen Produktes mit der Erstellung von Backups zu beauftragen. Dieses Produkt wurde vom Kläger 1 jedoch nicht gebucht, was von ihm richtigerweise auch nicht behauptet wird. Abgesehen davon ist die unbeschränkte Erstellung von Backups von Kundendaten aus Sicht des Datenschutzes zumindest problematisch und aufgrund der riesigen Datenmengen auch kaum umsetzbar.

Beweis: Urkunde: Bel. 3: Allgemeine Geschäftsbedingungen dynamic net.ch AG

Zu Ziff. 2.5

Die Beklagte hat den erforderlichen Support gewährt, wenn auch in zeitlicher Hinsicht mit etwas Verzögerung. Ergänzend wird auf das oben zu Ziff. 2.1 und 2.4 Gesagte verwiesen. Alles Abweichende wird bestritten.

Zu Ziff. 2.6

Dass die Beklagte seit einer Woche keine Telefonanrufe entgegengenommen haben soll, ist unzutreffend und bestritten.

Dafür, dass die Mail vom 6. Juni 2013 erst am 17. Juni 2013 beantwortet wurde, entschuldigte sich die Beklagte. Die Beklagte ersuchte die Klägerin 2 um eine Konkretisierung ihrer Anfrage, was in der Folge nicht geschehen ist. Eine Beantwortung Ihrer Mail vom 6. Juni 2013 bezeichnete die Klägerin 2 gegenüber dem Kläger 1 selber als unnütz. Offenbar ging es den Klägern dabei einzig darum, Stoff für eine Klage gegen die Beklagte zu generieren (vgl. Mail Klägerin 2 an den Kläger 1 vom 17. Juni 2013 [in KB 30]). Zudem ist die Klägerin 2 nicht Kundin und Vertragspartei der Beklagten, weshalb Sie keinen Anspruch auf (kostenlosen) Support hat. Alles Abweichende wird bestritten.

Zu Ziff. 2.7

Die erste Antwort der Beklagten ist wie bereits mehrfach erwähnt am 3. Juni 2013 erfolgt. Ergänzend wird auf das oben zu Ziff. 2.1 und 2.4 Gesagte verwiesen.

Zu Ziff. 2.8, 2.10, 2.12 und 2.14

Die Servicenummer 0800 66 99 66 und die Festnetznummer 041 455 59 10 funktionierten sehr wohl. Es wird bestritten, dass unter dieser Nummer konstant niemand erreichbar war. Gewisse Wartezeiten sind bei Hotline-Nummern unausweichlich. Alles Abweichende wird bestritten

Zu Ziff. 2.9

Die Mails des Klägers 1 vom 29. Mai 2013 und vom 3. Juni 2013 wurden von der Beklagten wie bereits dargelegt am 3. und 4. Juni 2013 beantwortet. Alles andere wird unter Verweisung auf die obigen Ausführungen zu Ziff. 2.1 bestritten.

Zu Ziff. 2.11

Richtig ist, dass der Kläger 1 am 6. Juni 2013 den Verwaltungsrat M. Brem kontaktiert hatte. Unzutreffend und bestritten ist jedoch, dass dieser dem Kläger 1 gesagt haben sollte, er habe selber Kontaktprobleme mit der Beklagten.

Zu Ziff. 2.13

Die Antwort der Beklagten findet sich nicht in KB 26, sondern in KB 23.

Zu Ziff. 2.15

Unter Hinweis auf die Ausführungen zu Detailbegründung Ziff. I/Unterziffern 7 und 8 bestritten.

Zu Ziff. 2.16

Der in KB 163 zu den Akten gegebene Bericht auf www.webgeist.de betrifft nicht die Beklagte, sondern Host Europe Deutschland. Ein Richard Sirch ist der Beklagten auch nicht bekannt. Der Inhalt dieses Berichts ist für das vorliegende Verfahren auch nicht relevant und von der Beklagten bestritten. Derartige Internet-Forenberichte sind denn auch nur mit sehr grosser Zurückhaltung zu würdigen. Der Wahrheitsgehalt derartiger Berichte ist zumindest zweifelhaft. Alles Abweichende wird bestritten.

Selbst dann, wenn der von der Beklagten erbrachte Support ungenügend gewesen sein sollte und darin eine Vertragsverletzung erblickt werden müsste, was bestritten wird, vermochte dies keine Schadenersatzfolgen auszulösen. Es wird auf die obigen Ausführungen zur Einführung 1 Übersicht Unterziffern 5 ff. verwiesen. Nochmals ausdrücklich bestritten wird an dieser Stelle, dass der Virenbefall der Webseiten der Kläger von der Beklagten zu vertreten ist und die Beklagte zur Beseitigung verpflichtet gewesen wäre. Die Kläger können denn nicht ernstlich meinen, sie könnten von der Beklagten Schadenersatz für den angeblich gehaltenen Zeitaufwand im Zusammenhang mit den Kontakten und Kontaktaufnahmen mit der Beklagten und mit der ohnehin ihnen obliegenden Behebung der Infizierung ihrer Webseiten geltend machen. Die Kläger unterlassen es denn auch, die behaupteten Schadenspositionen nachzuweisen und den ihnen angeblich entstandene Schaden rechtsgenügend zu belegen.

Zu Ziff. 3

[Die Kläger wiederholen sich. Es wird auf das dazu bereits Gesagte verwiesen, insbesondere zu Ziff. 2 ff. oben. Alles Abweichende wird bestritten.

Zu Ziff. 4

Zutreffend ist, dass die Beklagte das Webespace des Klägers 1 gesperrt hatte und zwar am 6. Juni 2013. Unzutreffend und bestritten ist indessen, dass die Sperrung grundlos und willkürlich erfolgt ist. Am 4. Juni 2013 hat die Beklagte unmissverständlich und keinesfalls bloss beiläufig die Deaktivierung des Hostings angekündigt und den Kläger 1 aufgefordert, sämtliche nötigen Massnahmen zur Beseitigung in die Wege zu leiten (KB 12).

Zu Ziff. 4.1

Die Beklagte bestreitet, dass die vom Kläger 1 über das web175 betriebenen Webseiten vor der vorgenommenen Sperrung virenfrei waren. Dies wird von den Klägern auch nicht nachgewiesen, auch nicht, dass dies von dritter Seite kontrolliert wurde.

Diese Behauptung der Kläger steht auch in grundsätzlicher Weise im Widerspruch zur Sperrung. Denn wären die Webseiten und Dateien des Klägers 1 im Zeitpunkt der Sperrung tatsächlich virenfrei gewesen, so wäre eine Sperrung offenkundig nicht notwendig gewesen und auch nicht erfolgt. Die Beklagte hätte keine Veranlassung zur Sperrung gehabt, wenn die Webseiten der Kläger effektiv virenfrei gewesen wären.

Der zuständige Fachbearbeiter bei der Beklagten, Herr Michel Herzog, hat am 6. Juni 2013 die fraglichen Webseiten nochmals überprüft und dabei festgestellt, dass diese zumindest teilweise nach wie vor infiziert und kompromittiert waren. Auch bei Aufrufung der fraglichen Webseiten kam von Google die Mitteilung, dass diese infiziert sind (vgl. auch BB 5). Dies wur-

de von Herrn Michel Herzog gleichentags am 6. Juni 2013 in einer internen Aktennotiz festgehalten. Alles Abweichende wird bestritten.

Beweis: Urkunde: Bel. 6: Aktennotiz von Michel **Herzog** vom **6. Juni 2013**

Zeuge: Herr Michel Herzog, Adresse wird nachgereicht

Bestritten und unzutreffend ist ferner, dass der Kläger 1 am 30. Mai 2013 das Zugangspasswort geändert hat. Dies wird von den Klägern bezeichnenderweise auch nicht belegt. Jedenfalls seit dem Übergang von dynamic net.ch AG zur Host Europe Suisse AG hat der Kläger kein einziges Mal das Passwort geändert, auch nicht, als er von der Beklagten hierzu auf- gefordert wurde (vgl. KB 1 1 und 12). Hätte der Kläger 1 das Passwort geändert, wäre dies in seiner History-Ticketübersicht ersichtlich. Darin wird unter anderem automatisch verzeichnet, wenn ein Kunde das Passwort ändert. In der History-Ticketübersicht des Klägers 1 findet sich jedoch kein entsprechender Vermerk. Dies im Gegensatz zu anderen Kunden, z.B. des Kunden Nr. 363115. Bei diesem findet sich unter dem 30. August 2013, 09.40 Uhr, der Vermerk ‚History-Ticket KIS‘ (ID 3569025). Im KIS-Ticket werden Änderungen an den Vertragsdaten festgehalten, also auch, wenn ein Kunde das Passwort ändert. Im entsprechenden Detail- Ausdruck zum Eintrag ID 3569025 ist beim genannten Beispielkunden Nr. 363115 der Ver- merk "Passwort geändert" ersichtlich. Hätte der Kläger 1 jemals das Passwort geändert, so würde sich auch in seinem History-Ticket ein entsprechender Eintrag finden. Dies ist auch ein weiteres Indiz dafür, dass der Kläger 1 keine bzw. nur ungenügende Virenbeseitigungs- und auch Virenschutzmassnahmen getroffen hat. Spätestens nach Kenntnis des Virenbefalls, allerspätestens nach den Aufforderungen der Beklagten hätte der Kläger 1 das Zugangspass- wort ändern müssen. Mit dem Passwortwechsel kann als erstes mit geringem Aufwand er- reicht werden, dass bisherige Angreifer, welche das Passwort kennen, ausgesperrt werden.

Beweis: Urkunden: Bei. 7: Printscreen der History-Ticketübersicht betr. Kläger 1

Bel. 8: Printscreen der History-Ticketübersicht des Kunden Nr. 363115 mit Detailausdruck zum Eintrag mit ID 3569025

Zu Ziff. 4.2

Die aufgelegten Switch-Bestätigungen (KB 7) sind kein Beweis dafür, dass die Viren vollständig entfernt wurden. Wie oben dargelegt, haben die Abklärungen der Beklagten zum gegenteiligen Resultat geführt.

[Diese bereits vom 31. Mai 2013 datierenden Switch-Bestätigungen stehen auch im Widerspruch zur Beurteilung Dritter, namentlich der Nansys Informatik GmbH. Diese hat die von Switch als virenfrei bezeichnete Webseite (www.top-info.ch) noch am 1. Juni 2013 als mit Malware infiziert beurteilt. Es ist auch in zeitlicher Hinsicht kaum vorstellbar, dass die Kläger in

der Lage waren, sämtliche infizierten Webseiten und Dateien innert eines Tages zu reparieren. Der Befall war ziemlich umfassend, was der Kläger 1 in seiner Mail vom 29. Mai 2013 selber bestätigt hat: *"Eine Kontrolle hat ergeben, dass z.B. alle ..html Dateien in www.Top-info.ch/Antik (und auch in www. Arlino.ch, etc.) vom Virus Java Script JSIBIacoleRef.CZ.20 geändert worden sind"*. Die Beseitigung der Infizierung dürfte technisch ziemlich komplex und aufwendig gewesen sein. In nur einem Tag wären die zahlreich und grossflächig infizierten Webseiten und Dateien wohl kaum fachgerecht und sicher wiederherzustellen gewesen. Die aufgelegten Bestätigungen von Switch sind auch nicht vollständig, so fehlen beispielsweise Bestätigungen für die nachweislich ebenfalls infizierten Webseiten www.arlino.ch (vgl. KB 3) und www.chats-chien.ch (KB 6).

Beweis: Urkunde: Bel. 4: Mail Nansys Informatik GmbH / Beklagte vom 1. Juni 2013 mit pdf-Anhang

0

Trotz Aufforderung haben die Kläger der Beklagten nie bestätigt, welche Massnahmen sie zur "Säuberung" der infizierten Webseiten und Dateien und welche Schutzmassnahmen sie zur Vermeidung von erneuten Infizierungen getroffen haben. Sie belassen es jeweils bei der pauschalen Behauptung alles sei „sauber“. Hätten sie effektiv die vorgefundenen Viren vollständig und in allen Dateien fachgerecht beseitigt und entsprechende Schutzmassnahmen vorgekehrt, was bestritten wird, hätten sie ohne weiteres zumindest kurz umreissen können, welche Vorkehrungen sie getroffen haben. Es wird darauf nachfolgend zurückgekommen. Alles Abweichende wird bestritten.

Zu Ziff. 4.3

Unter Hinweis auf die obigen und noch folgenden Ausführungen bestritten,

0

Zu Ziff. 4.4 bis 4.6

Ob und mit welchem Ergebnis die PC-Infrastruktur des Klägers (inkl. Virenschanner) überprüft wurde, weiss die Beklagte nicht und ist bestritten.

Es wird auch nochmals ausdrücklich bestritten, dass die Kläger vor der Mitteilung der Beklagten bzw. vor der Sperrung alle relevanten Massnahmen durchgeführt und die kompromittierten Dateien entfernt haben. Dies wird von ihnen zwar behauptet, aber nirgends nachgewiesen. In seiner Mail vom 6. Juni 2013 widerlegt der Kläger seine Aussagen selber indem er folgendes mitteilt: *"Nun haben Sie die Seite gesperrt und wir (recte: wir) können nichts verifizieren oder bereinigen oder reparieren"*. Damit bringt der Kläger 2 selber zum Ausdruck, dass die gesperrten Seiten (noch) nicht virenfrei waren. Nichts anderes ergibt sich auch aus seiner Mail vom 30. Mai 2013: *"Diese und die untenstehenden Webseiten wurden weitgehendst gesäubert"* (vgl. KS 6D). Dies hat wie gesagt am 6. Juni 2013 auch der zuständige Fachbearbeiter der

Beklagten, Herr Michel Herzog, festgestellt, ansonsten die Seiten nicht gesperrt worden wären.

Beweis: Zeuge:

Herr Michel Herzog, Adresse wird nachgereicht

Auch aus KB 18 können die Kläger nichts zu ihren Gunsten ableiten. Es geht daraus überhaupt nicht hervor, welche Massnahmen sie zur Virenbehebung konkret getroffen haben. Dies obschon die Beklagte den Kläger zuvor, unter anderem in der Mail vom 6. Juni 2013 (KB 17), ausdrücklich aufgefordert hatte, schriftlich zu bestätigen, dass sie die relevanten Bereiche und nicht nur die 'Webseiten (d.h. auch Daten, Datenbanken, FTP-Benutzer und Mailpostfächer) nach der Sicherung per FTP von ihrem Webhosting entfernen bzw. reparieren werden. Eine solche Bestätigung hat die Beklagte nie erhalten.

Beweis: Zeuge:

Herr Michel Herzog, Adresse wird nachgereicht

Richtig ist, dass die Kläger nach der Sperrung keinen Zugriff mehr hatten und damit auch keine Möglichkeit, Daten auf dem Server zu bearbeiten, zu löschen oder zu ändern. Deshalb verlangt die Beklagte vom Kunden vorab schriftlich die Mitteilung, welche Massnahmen er zur Desinfizierung seiner Webseiten und sonstigen Dateien zu ergreifen gedenkt. Dies ermöglicht der Beklagten zu beurteilen, ob die Massnahmen ausreichend sind. Diesfalls wird die Deaktivierung insoweit aufgehoben, als dass der Kunde die erforderlichen Massnahmen ausführen kann. Weil die Beklagte vorliegend nie eine solche Mitteilung erhalten hatte, blieb es bei der Sperrung. Folglich konnten die Kläger seither auch keine Virenentfernung vornehmen.

Zu Ziff. 4.7

Eine Sperrung von 14 Tagen ist üblich und auch angezeigt. Infizierte Server werden in der Regel auf sogenannte "Blacklists" gesetzt. Dies mit der Folge, dass die betroffenen Server ignoriert werden, damit sich die Viren nicht weiterverbreiten können. Nach längstens 14 Tagen ohne neue Virusmeldung werden die betroffenen Server von der "Blacklist" wieder gelöscht. Mit der 14-tagsfrist wird daher sichergestellt, dass der betroffene Server nicht erneut wieder gelistet wird, oder eventuell sogar dauerhaft gesperrt wird auf Grund mehrfacher Verstösse, sollte doch noch ein Virenbefall bestehen. Auch besteht die Gefahr, dass oftmals nicht nur der betroffene Kundenserver auf die "Blacklist" gesetzt wird, sondern auch weitere Server aus demselben Verbund, wovon unter Umständen zahlreiche weitere Kunden betroffen wären. Es liegt somit im Interesse der Beklagten wie auch der übrigen Kunden, dass infizierte Kundenserver deaktiviert und nicht verfrüht wieder aufgeschaltet werden.

Inwiefern das Vorgehen der Beklagten vertragswidrig sein soll, ist nicht ersichtlich. Die Beklagte war aufgrund des Gesagten berechtigt und auch verpflichtet, den Kundenserver des Klägers 1 zu sperren. Dies ergibt sich zudem auch aus den massgebenden AGB's (siehe Ziff. 4 Abs. 2 und Ziff. 5 Abs. 2). Eine Vertragsverletzung hat vielmehr der Kläger 1 begangen, in-

dem er seine Webseiten und Dateien zu wenig geschützt und der Beklagten die angeforderte Mitteilung über die konkret ausgeführten bzw. beabsichtigten Behebungsmassnahmen verweigert hatte. Alles Abweichende wird bestritten.

Beweis: Urkunde: Bei. 3: Allgemeine Geschäftsbedingungen dynamic net.ch AG

Zu Ziff. 4.8

Der Kläger 1 wusste was zu tun ist. Er brauchte der Beklagten schriftlich zu erklären, welche Massnahmen er treffen werde, um die relevanten Bereiche und nicht nur die Webseiten (d.h. auch Daten, Datenbanken, FTP-Benutzer und Mailpostfächer) zu reparieren (vgl. KB 17). Am 10. Juni 2013 wurde dies dem Kläger 1 erneut mitgeteilt und er wurde nochmals aufgefordert, genau anzugeben, welche Massnahmen er unternommen habe, die Viren zu entfernen und was er konkret unternehmen werde, um solche Verstösse inskünftig zu verhindern (vgl. KB 23). Ohne sich nur ansatzweise dazu zu äussern, beharrte der Kläger 1 kommentarlos an der Wiederaufschaltung der Webseiten.

Zu Ziff. 4.9

Die Ausführungen der Kläger sind bestritten und auch nicht gehörig substantiiert und belegt.

Die Kläger behaupten, der Kunde www.coiffitif.ch konnte Kundenreservierungen nicht mehr entgegennehmen, weshalb diesem ein Umsatzverlust drohte. Der Kunde habe beim Kläger 1 eine Schadenersatzforderung von CHF 3'500.00 platziert. Abgesehen davon, dass die Webseite www.coiffitif.ch über kein online-Kundenreservationstool verfügt, ist nicht einzusehen, weshalb dieser Kunde durch den Ausfall der Webseite ein Umsatzverlust von CHF 3'500.00 entstanden sein soll. Dieser ist auch in keiner Weise belegt. Hinzu kommt, dass Vertragspartnerin dieses Kunden die Klägerin 2 ist, welche ihrerseits mit der Beklagten in keinem Vertragsverhältnis steht (vgl. zu Einführung i Übersicht Unterziffer 7 oben). Bezeichnenderweise richteten sich die Korrespondenzen des fraglichen Kunden vom 30. Juni und 19. Juli 2013 auch an die Klägerin 2. Der Klägerin 2 stünden somit gegenüber der Beklagten zum vornherein keine Vertragsansprüche zu. Alles Abweichende wird bestritten.

Beweis: Urkunde: Bel. 9: Auszug aus www.coiffitif.ch

Zu Ziff. 4.10

Bestritten.

Zu Ziff. 5

Zwar liessen sich mit Mehraufwand auch einzelne Seiten und Dateien sperren. Weil aber der Befall relativ umfassend war und zahlreiche Webseiten und Dateien erfasste und für die Beklagte nicht ersichtlich war, wo und in welchem Ausmass die Viren sass, war eine umfassende Sperre der einzig gangbare Weg.

Dies gilt auch für den E-Mailzugang um zu verhindern, dass sich die Viren nicht darüber verbreiten können. Auch bestand die Gefahr, dass es sich um Viren handelte, die Spam und Massenmails hätten versenden können. Daran vermag nichts zu ändern, dass die E-Maileingänge mit dem Kaspersky Virenschutz gefiltert werden. Das Problem lag vorliegend nicht bei den Mail-Eingängen, sondern bei den Mail-Ausgängen.

Was die Kläger nach erfolgter Sperrung vorgekehrt haben, wissen die Beklagten nicht und wird von den Klägern auch nicht gehörig substantiiert und bewiesen. Die Ausführungen der Kläger werden bestritten.

Zu Ziff. 6

Dasselbe gilt auch hier. Interessant ist, dass die Kläger offenbar bereits am 8. Juni 2013 einen neuen Hoster ausgewählt haben, obschon der Kläger 1 den Hoster-Vertrag mit der Beklagten erst rund drei Monate später am 2. September 2013 gekündigt hatte (vgl. KB 61).

Zu Ziff. 6.1

Auch diese Tatsachenbehauptungen werden von den Klägern nicht ansatzweise nachgewiesen. Diese sind von der Beklagten auch bestritten.

Zu Ziff. 6.2

Die Vorhaltungen, die Beklagte hätte sich unprofessionell und unhöflich verhalten, werden bestritten. Bestritten und auch tatsachenwidrig ist ferner die Behauptung, die Beklagte hätte kein einziges der E-Mails der **Kläger** sorgfältig gelesen und beantwortet.

Unter den gegebenen Verhältnissen entschied sich die Beklagte, die Kündigung des Klägers 1 vom 2. September 2013 (KB 61) zu akzeptieren. Zudem erklärte sie sich - ohne Anerkennung einer Rechtspflicht und ohne Präjudiz - bereit, die Kündigung auf den 30. Juni 2013 zurück zu beziehen und dem Kläger 1 die auf die Zeit ab dem 1. Juli 2013 bis 2. März 2014 bezahlten Gebühren von CHF 122.03 zuzüglich Mehrwertsteuer zurückzuerstatten (vgl. KB 164 und 165).

Zu Ziff. 7

Der Kläger 1 mietete bei der Beklagten wie gesagt Webespace zur eigenen Verwendung und Verwaltung (**vgl.** zu Ziff. 1 Unterziffer 2 oben). Wer Eigentümer der vom Kläger 1 auf dem Webespace der Beklagten platzierten Domains, Webseiten und Dateien ist, ist unerheblich.

Der Hosting-Vertrag des Klägers 1 war auch nicht speziell auf eine bestimmte Situation ausgelegt. Es war ein normaler Hosting-Vertrag. Der Kläger 1 mietete 2'000 MB Speicherplatz mit unlimitierten Mail/Map, FTP-Zugängen und Traffic. Wie der Speicherplatz genutzt wird, ist jeweils dem Kunden überlassen.

Beweis: Urkunde: Bel. 1: Produkteübersicht Webhosting der Beklagten bzw.
von dynamic net.ch AG

Die Domains müssen einzeln gebucht werden, was technisch bedingt ist, da Server und Domain zwei unterschiedliche Sachen sind, wie z.B. Auto und Nummernschild. Was die Kläger daraus ableiten wollen, ist nicht nachvollziehbar.

Ebenfalls nicht nachvollziehbar (und auch nicht relevant) sind die Ausführungen der Kläger zur Datenspeicherung. Dass die Daten der Kläger auf verschiedene Platten gespeichert wurden, mag sein. Selbst dann, wenn dies der Fall gewesen wäre, wäre es technisch nicht möglich gewesen, einfach die befallene/n Platte/n zu sperren. Im Unterschied zu einem "normalen" PC handelt es sich beim Server der Beklagten trotz mehrerer physischer Laufwerke nicht um getrennte Speicherorte. Vielmehr werden alle Platten zu einem grossen Speichermedium zusammengefasst. Die Dateien werden also vom System automatisch auf mehrere Medien verteilt, weshalb bei einem Befall einer Platte auch der Rest des Dateisystems betroffen ist. In Hölst betreibt die Beklagte kein Rechenzentrum.

Was die Kläger aus KB 160 ableiten wollen, ist nicht ersichtlich. Dieses aus dem Jahr 2012 stammende Dokument war der Beklagten nicht bekannt. Die Beklagte wäre auch nicht verpflichtet gewesen, bei allen Webseiten und Dateien der Kläger nachzuforschen, ob bei diesen ein Javascript verwendet wurde oder nicht. Die vom Kläger1 eingesetzte Software und Betriebssystem war der Beklagten nicht bekannt. Ergänzend wird auf die vorherigen Ausführungen zu Ziff. 5 verwiesen. Alles Abweichende wird bestritten.

Zu Ziff. 8

Alles was zum Zeitpunkt der Sperrung da war, ist nicht verloren, auch E-Mails. Die Kläger konnten nur nicht hierauf zugreifen, da die Dateien immer noch mit Viren befallen waren. Es wäre der Beklagten allenfalls möglich gewesen, Kopien dieser Daten herauszugeben. Solche wurden bei ihr von den Klägern jedoch niemals angefordert.

Zu Ziff. 9

Unter Verweisung auf das bereits Ausgeführte bestritten. Die Beklagte hat auch in diesem Punkt keine Vertragsverletzungen begangen.

Zu Ziff. 10

Worin die Kläger eine fahrlässige Geschäftsführung der Beklagten erblicken wollen, ist nicht ersichtlich und von der Beklagten auch bestritten.

Zu Ziff. 10.1

Zu Pos. 1

Die Meldung erfolgte sowohl vom Kläger 1 als auch von Dritten (vgl. zu Ziff. 2.1 oben).

Beweis: Urkunde: Bel. 4:

Mail Nansys Informatik GmbH 1 Beklagte vom 1. Juni 2013 mit pdf-Anhang

Zu Pos. 2

Daraus, dass die Sperrung erst am 6. Juni 2013 erfolgt ist, können die Kläger nichts ableiten,

Zu Pos. 3

Wie bereits mehrfach ausgeführt, war die Entfernung der Viren, welche die Webseiten des Klägers befallen hatten, Sache des Klägers 1 und nicht der Beklagten. Wenn für die Kläger von Anfang an klar war, wie die von Viren befallenen Dateien zu säubern sind, weshalb haben Sie die Beklagte denn überhaupt angefragt?

Zu Pos. 4

Die Kläger wussten, was sie zu tun hatten (vgl. Ziff. 4.4 bis 4.6 und 4.8 oben).

Zu Pos. 5

Es wurde dargelegt, dass einzelne Webseiten im Zeitpunkt der Sperrung noch mit Viren befallen waren. Nach erfolgter Sperrung konnten die Webseiten gar nicht mehr repariert werden, da die Kläger keinen Zugriff mehr hatten (vgl. zu Ziff. 4.1 und 4.4. bis 4.6 oben). Recherchen von Herrn Michel Herzog haben ergeben, dass die Webseite www.top-info.ch des Klägers 1 am 13. August 2013 bei Google als infiziert gelistet war, obschon der Kläger 1 in der Zwischenzeit den Hoster gewechselt hatte! Alles Abweichende wird bestritten.

Beweis: zeuge:

Herr Michel Herzog, Adresse wird nachgereicht

Zu Pos. 6

Der Stundenansatz von CHF 200.00 ist in keiner Weise begründet und belegt. Dieser ist von der Beklagten denn auch bestritten.

Zu Pos. 7

Weder ist belegt, dass die Hardware/Software der Beklagten bereits vor dem 16. Mai 2013 infiziert war, noch dass die Webseiten und Dateien des Klägers 1 über den Server der Beklagten infiziert wurden. Die Beklagte hat oben zu Ziff. 1 Unterziffer 3 dargelegt, dass sie selber über einen hinreichenden Schutz verfügt. Aus den Beilagen KB 161 und 162 können die Kläger aus den vorstehend zu Ziff. 1 Unterziffern 7 und 8 und zu Ziff. 2.16 genannten Gründen nichts für sich ableiten. Zudem ist aktenkundig, dass die Webseiten des Klägers¹ befallen wurden und nicht der Server der Beklagten. Es wird auf die obigen Ausführungen zu Ziff. 1 Unterziffer 5 verwiesen. Die Beklagte hat deshalb auch nicht für die angeblichen Aufwendungen der Kläger im Zusammenhang mit der Abklärung und Entfernung der Viren und Malware auf ihren Webseiten und Dateien aufzukommen.

Zu Pos. 8

Der Standpunkt der Beklagten ist korrekt. Alles Abweichende wird bestritten

Zu Pos. 9

Jedenfalls führte dies dazu, dass mehrere Personen auf den Server der Beklagten Zugriff hatten mit der Folge eines eindeutig höheren Vireninfectionsrisikos (vgl. zu Ziff. 1 Unterziffer 4 oben).

Zu Ziff. 10.2

Bei der Mail vom 20. September 2013 handelte es sich um eine Standardmail. Diese hat der Kläger versehentlich erhalten, weil die tags zuvor am 19. September 2013 bestätigte Vertragsauflösung (vgl. KB 164) im System noch nicht vermerkt war. Daraus können die Kläger nichts zu ihren Gunsten arbeiten.

Zu Ziff. 10.3

Das gleiche gilt auch für die Rechnung vom 20. September 2013.

Zu Ziff. 10.4

Auch damit lassen sich keine Schadenersatzforderungen begründen,

Schlussbemerkungen

Abschliessend ist zusammenfassend nochmals folgendes festzuhalten

- 1 Mit der Klägerin 2 steht die Beklagte in keinem Vertragsverhältnis, weshalb die Klägerin 2 gegenüber der Beklagten auch keine Vertragsverletzungen begangen haben konnte. Folglich können der Klägerin 2 auch keine Schadenersatzansprüche gegen die Beklagte zustehen. Die Klage ist in Bezug auf die Klägerin 2 bereits in dieser Hinsicht ohne weiteres abzuweisen.
- 2, Auch gegenüber dem Kläger 1 hat die Beklagte keine Vertragsverletzungen begangen. Weder ist sie dafür verantwortlich, dass die Webseiten des Klägers 1 mit Viren infiziert wurden, noch war sie vertraglich verpflichtet, die Entfernung der Viren von den Webseiten der Kläger vorzunehmen. Zudem hat die Beklagte zu Recht vom Kläger 1 eine nachvollziehbare und detaillierte Bestätigung über die Entfernung der Viren und die getroffenen Massnahmen und Schutzmassnahmen verlangt und den Zugang webl 75 solange zu Recht gesperrt. Lediglich in Bezug auf die Kommunikation hat sich die Beklagte in zeitlicher Hinsicht gewisse Vorhaltungen gefallen zu lassen, welche jedoch keine Schadenersatzpflicht rechtfertigen können und zu den von den Klägern behaupteten Schäden auch in keinem adäquaten Kausalzusammenhang stehen. Dieser ist ebenso wie die behaupteten Vertragsverletzungen von den Klägern nicht nachgewiesen.
- 3 Selbst dann, wenn der Beklagten ein vertragswidriges Verhalten angelastet werden müsste, was jedoch bestritten ist, ist darauf hinzuweisen, dass die Parteien die Haftung der Beklagten nach oben beschränkt haben, nämlich auf einen vom Kläger 1 erzielten Jahresumsatz. Dieser liegt bei CHF 178.80. Dass die Beklagte der von den Klägern behauptete Schaden grobfahrlässig oder sogar absichtlich herbeigeführt hätte, ist offenkundig nicht der Fall und wird von den Klägern zu Recht auch nicht behauptet. Der Kläger 1 bestätigt, dass die zur Zeit der dynamic net.ch AG eingegangenen allgemeinen Geschäftsbedingungen nach wie vor gültig sind, somit auch Ziff. g. Dort wurde zudem vereinbart, dass die Beklagte in keinem Fall haftet für Vermögens- und Folgeschäden, Datenverluste und entgangener Gewinn.
4. Schliesslich brauchen die Haftungsvoraussetzungen der Vertragsverletzung, des Verschuldens und des adäquaten Kausalzusammenhanges auch nicht näher geprüft zu werden, weil es offenkundig am weiteren Erfordernis des Schadens fehlt. Die Kläger behaupten zwar in Antrag Ziff. 1 einen Schaden von CHF 30'000.00. Sie unterlassen es

jedoch, diesen rechtsgenügend zu substantizieren und zu beweisen. Die Klage enthält diesbezüglich praktisch keine Ausführungen. Es wurde oben zu Einleitung/ Übersicht Ziff. 6 unter Hinweis auf Art. 221 ZPO dargelegt, dass die relevanten Tatsachenbehauptungen Bestandteil der Klage sein müssen. Eine blosser Verweisung auf Beilagen ist un- zureichend und nicht statthaft. Die tabellarische Zusammenstellung "History/Tatbestand- Beweismittel/Zeitaufwand/Kosten" datierend vom 21. Oktober 2013 ist somit prozessual unbeachtlich, zumal darauf in der Klageschrift nicht einmal verwiesen wird.

Rein vorsorglich ist zu dieser Zusammenstellung vom 21. Oktober 2013 an dieser Stelle kurz folgendes zu bemerken:

- Die von den Klägern aufgeführten externen Kosten sind nicht substantiiert und in keiner Weise belegt. Diese sind von der Beklagten sowohl in grundsätzlicher als auch in masslicher Hinsicht bestritten. Insbesondere ist bestritten, dass Kunden der Kläger Umsatzverluste bzw. Kundenverluste erlitten haben. Derartige Schadenspositionen könnten gegenüber der Beklagten auch nicht geltend gemacht werden und schon gar nicht von der Klägerin 2.
- Der Kläger 1 macht einen eigenen Schaden von CHF 19'830.00 geltend, basierend auf einem Aufwand von 99.15 Stunden und einem Stundenansatz von CHF 200.00. Sowohl der angegebene Stundenaufwand als auch der erwähnte Stundenansatz ist von der Beklagten ebenfalls grundsätzlich und masslich bestritten. Wie bereits ausgeführt ist ein Stundenansatz von CHF 200.00 bestritten. Dieser ist offenkundig überrissen und auch in keiner Weise belegt.

Dasselbe gilt auch für den behaupteten Arbeitsaufwand von 99.15 Stunden. Dieser enthält auch Positionen, welche zum vornherein nicht ersatzfähig wären. Dies gilt insbesondere für die Aufwendungen im Zusammenhang mit der Zusammentragung des Prozessstoffes, der Vorbereitung und Durchführung des Schlichtungsverfahrens und des vorliegenden Gerichtsverfahrens (Seiten 5 und 6). Zudem können Aufwendungen im Zusammenhang mit der Virenbefreiung der Webseiten und der Informationsbeschaffung der Beklagten gegenüber sicher nicht geltend gemacht werden, da die Beklagte hierzu nicht verpflichtet war (Seiten 1 bis 3). Aber auch die unter B) Tatbestand aufgeführten Aufwendungen (Seite 4) wären nicht zu vergüten, auch wenn diese hinreichend substantiiert wären, da persönliche Zeitaufwendungen rechtlich überhaupt nicht ersatzpflichtig sind.

- Der Aufwand der Klägerin 2 wird mit 81.55 Stunden deklariert und unter Anwendung eines Stundensatzes von ebenfalls CHF 200.00 auf CHF 16'310.00 berechnet. Es gilt das unter dem vorstehend ausgeführten Punkt Ausgeführte analog.

5. Die Klage ist somit abzuweisen unter Kosten- und Entschädigungsfolge zulasten der Kläger unter solidarsicher Haftbarkeit.

Mit freundlichen Grüßen



Urs Lütolf
uluetolf@anwaelte-kriens.ch

Beilagen.- - **gemäss separatem** Beilagenverzeichnis

Kopie z.K. an: - Mandantin

dreifach

Beilagenverzeichnis

- Bel. 1 Produkteübersicht Webhosting der Beklagten bzw. von dynamic net.ch AG
- Bel. 2: Internet-Handelsregisterauszug betr. Beklagte vom 20. Januar 2014
- Bel. 3: Allgemeine Geschäftsbedingungen dynamic net.ch AG
- Bel. 4: Mail Nansys Informatik GmbH 1 Beklagte vom 1. Juni 2013 mit pdf-Anhang
- Bel 5: Mail Beklagte / Kläger 1 vom **3. Juni 2013**
- Bel. 6: Aktennotiz von Michel Herzog vom 6. Juni 2013
- Bel 7: Printscreen der History-Ticketübersicht betr. Kläger 1
- Bel. 8: Printscreen der History-Ticketübersicht des Kunden Nr. 363115 mit Detailausdruck zum Eintrag mit ID 3569025
- Bel. 9: Auszug aus www.coiff.tif.ch

ENDE