52 C 15528/10

Beglaubigte Abschrift

Amtsgericht Düsseldorf

Beschluss

In dem einstweiligen Verfügungsverfahren

des Herrn Jörg Reinholz, Hafenstraße 67, 34125 Kassel,

Antragstellers,

g e g e n

die Euroweb Internet GmbH, vertr. d. d. Gf., Hansaallee 299, 40549 Düsseldorf,

Antragsgegnerin,

wird gemäß §§ 935, 940 ZPO im Wege der einstweiligen Verfügung wegen Dringlichkeit ohne mündliche Verhandlung angeordnet:

Der Antragsgegnerin wird im Wege der einstweilige Verfügung aufgegeben, es zu unterlassen

a)

Durch wiederholtes Abrufen und Übertragen von Daten von/zu vom Antragsteller betriebenen oder benutzten Webservern deren Sicherheit oder Funktion sowie die Sicherheit der dort gespeicherten Daten oder Programme zu beeinträchtigen oder dies zu versuchen

b)

Einen Einbruch in sicherheitsrelevante Bereiche der Internetpräsenzen des Antragstellers zu versuchen und dabei zu versuchen Daten des Antragstellers oder Dritter zu erlangen,

verändern oder zu beschädigen oder ohne Aufforderung des Antragsteller zu testen oder testen zu lassen, ob dies möglich ist.

Die Kosten des Verfahrens werden dem Antragsgegner auferlegt.

Der Streitwert wird auf 4.000,00 € festgesetzt.

Düsseldorf, 22.12.2010
Amtsgericht

Hermeler, Richter am Amtsgericht

Beglaubigt
Vorwerk
Justizhauptsekretärin

28

Jörg Reinholz
Hafenstr. 67
34125 Kassel
Tel. 0561 317 22 77
Fax: 0561 217 22 76

Land- und Amtsgericht Düsseldorf
Eing. 21. Dez. 2010
Briefannahmestelle
..... € Kostenm. ..... Anl.

Jörg Reinholz, Hafenstr. 67, 34125 Kassel

per Telefax
Amtsgericht Düsseldorf
Zivilkammern

DRINGENDER ANTRAG

(Antrag auf den Erlaß einer einstweiligen Verfügung ohne Anhörung der Antragsgegnerin)

des

– Antragsteller –

Jörg Reinholz
Hafenstr. 67
34125 Kassel

gegen die

– Antragsgegnerin –

Euroweb Internet GmbH
Hansaallee 299
40549 Düsseldorf

wegen

Unterlassung von störenden Eingriffen in das Recht an der Führung seines Unternehmens

Streitwert für die einstweilige Verfügung: 4000 Euro

ANTRAG

ch beantrage der Dringlichkeit wegen gemäß § 944 ZPO gegen die Antragsgegnerin durch die oder den Vorsitzenden der zuständigen Kammer allein und ohne mündliche Verhandlung folgende Einstweilige Verfügung zu unterlassen wobei ich unter Bezugnahme auf § 938 ZPO folgende Beschlussfassung anrege:

1. **Der Antragsgegnerin wird verboten:**

   a) Durch wiederholtes Abrufen und Übertragen von Daten von/zu vom Antragsteller betriebenen oder benutzten Webservern deren Sicherheit oder Funktion sowie die Sicherheit der dort gespeicherten Daten oder Programme zu beeinträchtigen oder dies zu versuchen
   b) Einen Einbruch in sicherheitsrelevante Bereiche der Internetpräsenzen des Antragstellers zu versuchen und dabei zu versuchen Daten des Antragstellers oder Dritter zu erlangen, zu verändern oder zu beschädigen oder ohne Aufforderung des Antragstellers zu testen oder testen zu lassen, ob dies möglich ist.

wie es am 06. Dezember 2010 geschehen ist.

2. Für jeden Fall der Zuwiderhandlung gegen Ziffer 1

wird der Antragsgegnerin ein Ordnungsgeld in Höhe von bis zu 250.000 Euro, im Falle der Uneinbringlichkeit Ordnungshaft von bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu vollstrecken am Geschäftsführer Christoph Preuß, angedroht.

3. Der Antragsgegnerin auferlegt die Kosten des Verfahrens aus einem Streitwert von 4000 Euro zu tragen.

10

Begründung

I. Das Unterlassungsbegehren folgt aus §§ 823, 1004 BGB.

Am 6.12.2010 wurden beginnend um 15:43 von mehreren Rechnern aus dem Firmennetzwerk der Antragsgegnerin Internetpräsenzen des Antragstellers angegriffen. Der Antragsteller erhielt darauf hin 35 automatisch erstellte eMails durch welche der Angriff der Antragstellerin dokumentiert wird. Von diesen werden aus Gründen der Übersichtlichkeit nur 3 als Anlage 1a bis 1e beigefügt, die weiteren sind aber ebenfalls gespeichert und stehen im Falle des Bestreitens zur Glaubhaftmachung zur Verfügung.

Das als Anlage 2 beigefügte, für das Gericht gefilterte und sonst nicht veränderte, Protokoll/Logfile des Dienstleister Variomedia AG (Berlin) beweist, dass diese Abrufe von einem Rechner mit der IP-Adresse 217.6.222.114 aus ausgeführt wurden. Diese IP-Addresse ist im Mathematisch- wissenschaftlichen Sinne „eineindeutig". Der Rechner mit der IP 217.6.222.114 gehört ausweislich der whois Daten des Netzwerkes zu dem Netzwerk der Euroweb Internet GmbH. Es handelt sich hierbei nicht um eine „dynamische", sondern um eine (durch den Dienstleister Telekom) an den Geschäftskunde Euroweb Internet GmbH dauerhaft zugeteilte, statische IP. Der folgende whois-Abruf ist zur Glaubhaftmachung/zum Beweis jederzeit möglich, zugleich wird die Telekom AG nichts anderes bezeugen:

```
whois -B 217.6.222.114
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Information related to '217.6.222.112 - 217.6.222.127'

inetnum:        217.6.222.112 - 217.6.222.127
netname:        EUROWEB-INTERNET-DUESSELDORF-NET
descr:          Euroweb Internet GmbH
country:        DE
admin-c:        CP1840-RIPE
tech-c:         CP1840-RIPE
status:         ASSIGNED PA
mnt-by:         DTAG-NIC
notify:         lir.nic@t-com.net
changed:        lir.nic@t-com.net 20070926
source:         RIPE

person:         Christoph Preuss
address:        Euroweb Internet GmbH
address:        Neumannstr. 2
address:        D-40235 Duesseldorf
address:        Germany
phone:          +49 211 301290
fax-no:         +49 211 30129111
```

Eine umgekehrte Namensauflösung mit nslookup unter Benutzung des durch die DENIC eG. veröffentlichten DNS-Servers dns1.euroweb.de liefert den Name des Rechners „hq01.euroweb.de“:

```
nslookup 217.6.222.114 dns1.euroweb.net
Server:         dns1.euroweb.net
Address:  91.199.247.11#53

Non-authoritative answer:
114.222.6.217.in-addr.arpa    name = hq01.euroweb.de.
```

Auch dieser Vorgang ist jederzeit wiederholbar und beweist, dass der Rechner zum Netzwerk der Euroweb Internet GmbH, die auch als Webadresse „www.euroweb.de“, also die bei der DENIC registrierte Second-Level-Domain „Eurweb.de“ benutzt, gehört. Ein Bestreiten ist hier nicht zu erwarten.

Aus dem Fakt, das dieser Rechner nicht auf Pings reagiert und sämtliche UDP und TCP/IP- Ports geschlossen sind kann als wahrscheinlichstem Grund gefolgert werden, dass dieser Rechner eine sogenannte Firewall ist, der mittels NAT (Network-Adress-Translating) die wohl zahlreichen Rechner des Unternehmens am Hauptstandort der Antragsgegnerin in Düsseldorf einerseits mit Internet versorgt, andererseit dazu dient, diese sonst schwach gesicherten Rechner mit dem veraltetem Betriebssystem Windows XP aus dem Internet nicht oder weniger angreifbar zu machen.

Für den Antrag kommt es hierauf nicht an, so dass der Antragsteller auf die umfangreichen technischen Darlegungen zur Glaubhaftmachung oder dem Beweis verzichtet. Der Beweis für die Störung ist bereits dadurch erbracht, dass die Störung aus dem Netzwerk der Antragsgegnerin, also vom Host mit der IP stammt.

Zugleich wurde aus dem Netzwerk der Euroweb Internet GmbH, ausgehend vom Rechner der selben IP-Adresse auch weitere Seiten abgerufen:

Das Protokoll/Logfile des Webauftrittes von „www.dieWohnung.de“, einer ebenfalls vom Antragsteller betriebenen Internetpräsenz zeigt (u.a.) folgende Zugriffe:

```
217.6.222.114 - - [06/Dec/2010:15:44:41 +0100] "GET
/administration HTTP/1.1" 404 102 "-" "Mozilla/5.0 (Windows; U;
Windows NT 5.1; de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12"

217.6.222.114 - - [06/Dec/2010:15:45:15 +0100] "GET /admin
HTTP/1.1" 404 102 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1;
de; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12"
```

Die folgenden Seiten, welche 1.) gar nicht vorhanden sind und 2. deshalb nicht verlinkt sind

http://www.diewohnung.de/administration

p://www.diewohnung.de/admin

urden versucht abzurufen, es wurde also durch „trial & error" versucht, herauszufinden, o sich der Administrationsbereich befindet.

Beweis hierüber kann durch Vorlage des Protokolls/Logfiles der Variomedia AG erbracht werden.

Insbesondere die Internetpräsenz „diewohnung.de" enthält personenbezogene Daten zahlreicher Dritter, darunter Adressen, Rufnummern, Mailadressen und Passwörter, die der Antragsteller berechtigt dort speichert. Es handelt sich um eine Inserateseite, woe diese Dritten Immobilien Käufern oder Mietern anbieten können. Der Antragsteller hat das Recht und die Pflicht, diese Daten zu schützen.

2. Strafbarkeit der Handlung der Antragsgegnerin

Offensichtlich dienten diese Handlungen der Vorbereitung eines weiteren Angriffs, denn hinter diesen Adressen befinden sich oft besonders empfindliche und geschützte Bereiche. Dass die Antragsgegnerin diese angreifen wollte ergibt sich aus dem zeitlgleichen Angriff auf das Mailformular, respektive das dessen Eingaben verarbeitende Skript.

Ausweislich des Inhaltes der Eingaben, die durch die Emails weiter gegeben wurden, teils auch in den Protokollen/Logfiles ersichtlich sind, werden handelt es sich um eine XSS-Attacke, die im Online-Lexikon „wikipedia" wie folgt beschrieben ist:

> ***Cross-Site Scripting** (**XSS**) bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden.*
>
> *Ziel ist es meist, an sensible Daten des Benutzers zu gelangen, um beispielsweise seine Benutzerkonten zu übernehmen (Identitätsdiebstahl).*

Insbesondere die Eingaben

```
<META HTTP-EQUIV=\"Set-Cookie\"
Content=\"USERID=<SCRIPT>document.vulnerable=true</SCRIPT>\">

<meta http-equiv=\"refresh\"
content=\"0;url=javascript:document.vulnerable=true;\">

<SCRIPT>document.vulnerable=true;</SCRIPT>

<META HTTP-EQUIV=\"Set-Cookie\"
Content=\"USERID=<SCRIPT>document.vulnerable=true</SCRIPT>\">

<IMG SRC=\"jav ascript:document.vulnerable=true;\">
```

DY onload!#$%&()*~+-_.,:;?@[/|\\]^`=document.vulnerable=true;>
jeweils ohne weitere Inhalte mitzusenden in den Emails sichtbar werden, beweisen, ss hier ein solcher Angriff versucht wurde.

Insbesondere wurde versucht ein Cookie zu setzen – (und demnach auch lesen zu können) und eine Umleitung auf einen anderen Host zu bewirken. Das genau sind nach dem Wissenstand des Antragstellers Merkmale einer Vorbereitung (hier noch Tests einzelner Schritte) eines XSS-Angriffes. Ein sachverständiger Gutachter wird dies im möglicherweise notwendig werdenden Hauptsacheverfahren bestätigen.

Da diese Angriffe sich gegen ein Mailformular richteten kann auch davon ausgegangen werden, dass nicht nur die Webseiten, sondern auch der vom Antragsteller zum Empfangen von Emails benutzte Rechner, alternativ sein Webmailkonto bei seinem Hoster oder einem Dritten angegriffen werden sollte, denn es gab tatsächlich Mailprogramme/Webmailer bei denen sich auf vergleichbare Art Daten entführen ließen. Auch ist hinsichtlich des Dilletantismus anzumerken, dass sich der Angriff noch im Stadium des Suchens nach einer angreifbaren Stelle in der Software des Antragstellers befand, mithin also gerade noch rechtzeitig entdeckt und unterbunden wurde.

Beginnend am 6.12.2010 um 16:37 Uhr hat der Antragsteller nach Abruf seiner Emails nämlich seine sämtlichen Internetpräsenzen so konfiguriert, dass die Rechner des Netzwerkes der Antragsgegnerin vom Abruf der Webseiten ausgeschlossen sind, mithin keine weiteren Angriffe aus deren Netzwerk heraus möglich waren. Nur deshalb erfolgten keine weiteren Versuche.

Dies ist auch aus der Anlage 2 ersichtlich, denn ab 16:37 Uhr erfolgte auf jeglichen Abruf hin nur die Antwort, dass der Abruf „Forbidden", also verboten sei. Dies ist im Protokoll Logfile durch den Zahlencode „403" dokumentiert, es handelt sich hierbei um einen HTTP-Statuscode der in der RFC 2616 genormt ist (http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html).

Der Unterzeichner hatte, infolge des Angriffs folgenden Aufwand:

1. Herausfinden der Quelle des Angriffes
2. Herausfinden des Netzwerkes aus dem der Angriff stammt
3. Berechnen der Netzwerkmaske für die IP 217.6.222.114 und das Netzwerk (= 217.6.222.112/28
4. Hinzufügen der Zeilen:

   ```
   # attacks from Euroweb Internet GmbH
   deny from 217.6.222.112/28
   ```

   in mehr als 10 Dateien „.htaccess" auf den jeweiligen Webservern, durch welche die Zugriffe unterbunden werden. (Beweis: Öffentlich verfügbare Dokumentation des Webservers Apache unter der Adresse http://httpd.apache.org/docs/2.2/howto/access.html) – für jede Internetpäsenz und für jede Subdomain.

Der Antragsteller hat die Antragsgegnerin zu keiner Zeit aufgefordert oder sonst berechtigt die störende oder die Straftat vorbereitende oder ähnliche Handlungen vorzunehmen.

)4

Abwehr dem Antragsteller bereits erheblicher personeller Aufwand entstanden und es begründet auch seinen Unterlassungsanspruch aus dem ungerechtfertigten Eingriff in einen Geschäftsbetrieb und ohnehin aus der unerlaubten Handlung der Antragsgegnerin, die nur der Vorbereitung von Straftaten nach §§ 202a, 202b, 202c, 301a, 303b StGB dienen konnte. Das Misslingen ist hier jedenfalls der technischen Kompetenz, der zufälligen Verfügbarkeit und dem schnellen Eingreifen des Antragstellers zu verdanken.

3. Abmahnung des Antragstellers an die Antragsgegnerin

Der Netzwerkadministrator der Euroweb Internet GmbH, ein Herr Nippert wurde am 6.12.2010 um 16:49 auf die Störung/den Angriff aufmerksam gemacht. Dies wird durch Anlage 3 glaubhaft gemacht.

Die Antragsgegnerin wurde durch Email vom 6.12.2010 um 17:20 auf ordnungsgemäß Unterlassung in Anspruch genommen und hat hierauf in keiner Weise reagiert, die Frist verstrich fruchtlos. Die Antragstellerin hat also auch nicht erklärt, dass diese irgendwelche Maßnahmen ergriffen habe um derlei Tätigkeiten „wild gewordener Mitarbeiter" auszuschließen. Die Antragstellerin hat insbesondere nicht bestritten, verantwortlich zu sein.

Die Abmahnung wird als Anlage 4 beigefügt.

Beide Emails wurden vom Mailserver der Antragsgegnerin angenommen und auch sonst nicht reklamiert, sind also im Machtbereich der Antragsgegnerin zugegangen. Die Antragsgegnerin hätte also erklären können, dass diese die Störung oder den Angriff unterbindet, auch wenn eigenmächtig handelnde Angestellte ursächlich waren.

4. Wiederholungsgefahr, mögliche Einreden

Als Kaufmann trägt die Antragsgegnerin aber auch Verantwortung für das Handeln ihrer Erfüllungsgehilfen und die Antragsgegnerin betreibt ausweislich ihres Geschäftszweckes gerade kein Internetcafe und auch keinen öffentlich zugänglichen Proxyserver mit welchem Dritte die Webseiten des Antragstellers angreifen konnten. Insbesondere hat der Antragsteller den unter der IP-Adresse 217.6.222.114 adressierbaren Server der Antragsgegnerin mit – nach dem Angriff - legalen Methoden (Portscanner nmap) hin auf Eigenschaften geprüft, die auf einen Angriff Dritter schließen können, aber keinen auf der Internetseite(!) offenen Port (Zugang) gefunden, wodurch sich ein solcher Missbrauch sicher ausschließen lässt. Aus dem Firmennetzwerk wird dieser Server sehr wohl erreichbar sein, denn es handelt sich nach vernünftigem Ermessen um eine Firewall mit NAT-Funktion oder einen Proxy-Server, der für das Netzwerk am Firmensitz der Antragsgegnerin den Internetzugang ermöglicht.

Die Wiederholungsgefahr ist nicht dadurch ausgeschlossen, dass der Antragsteller die IP-Adressen der Antragsgegnerin ausgeschlossen hat, denn diese könnte sich weitere IP-Adressen besorgen und benutzen, einen alternativen Zugang benutzen, von anderen Orten aus tätig werden oder Proxy-Server benutzen, wodurch die Sperre umgangen werden kann. Es ist dem Antragsteller auch nicht zuzumuten, dass er sich dauerhaft oder zeitweilig darum kümmern muss, dass er die Antragsgegnerin ausschließt. Zudem müsste er dazu stets Informationen darüber haben, welche IP-Adressen die Antragsgegnerin

möglich noch oder künftig benutzt. Hier hilft nach der erfolgslosen Abmahnung nur die Androhung einer empfindlichen Strafe durch das Gericht, die auch wo weit wie beantragt zu fassen ist, denn es kann nicht angehen, dass die Antragsgegnerin nunmehr andere Selbpräsenzen des Antragstellers angreift. Ohnehin ist die Vorgehensweise auch bei Angriffen sogar Dritten gegenüber als strafbare Handlung von Anfang an zu unterlassen.

5. Eilbedürftigkeit

Seit dem 6.12. sind weniger als 7 Tage vergangen, die Sache an sich ist eilbedürftig, es geht um die Unterlassung eines Eingriffs in den Geschäftsbetrieb des Antragstellers, der naturgegeben ein Interesse daran hat, sich nicht mit technischem Aufwand gegen derlei Angriffe zu erwehren. Zudem verfolgt die Antragsgegnerin mit den zu unterlassenden Handlungen eine erkennbare Schädigungsabsicht.

6. Durch die erforderliche Verfügung werden keine Rechte der Antragsgegnerin verletzt.

Es besteht kein Recht kriminelle Handlungen oder auch Störungen des Geschäftsbetriebes Dritter vorzunehmen oder auch nur vorzubereiten. Dies ist auch und gerade dann der Fall, wenn und weil der Antragsteller die Antragsgegnerin zuvor in der Sache 31 C 14650/10 des Amtsgerichtes Düsseldorf (20 T 59/10 des LG Düsseldorf) erfolgreich in Anspruch nehmen musste und es sich bei dem Angriff um eine Rachehandlung handelt. Das die – anwaltlich stets beratene – und dem Gericht aus ca. 1500 Verfahren bekannte Antragsgegnerin dem Antragsteller gegenüber höchst böswillig ist ergibt sich daraus, dass diese trotz der klaren Rechtslage die geforderte Anerkennung der obigen Verfügung als endgültige Regelung trotz vernünftiger Fristsetzung nicht geleistet hat – und das obwohl der Antragsteller sich auch hierbei nicht vertreten ließ, was sonst Kosten verursacht hätte.

7.) Das Amtsgericht Düsseldorf ist als Sitz der Antragsgegnerin örtlich, dem Streitwert von 4000 Euro zu folge auch sachlich zuständig.

Die bis jetzt eingetretene Störung rechtfertigt keinen höheren Streitwert als 4000 Euro.

Zudem sollen einfache Rechtssachen auch vor den Amtsgerichten verhandelt werden um die höheren Gerichte nicht unnötig zu belasten.

8.) Ich bitte um telefonische Benachrichtigung, wenn die Verfügung erlassen wurde, damit die Zustellung unverzüglich bewirkt werden kann. Sollte nach Ansicht des Gerichtes weiterer Sachvortrag erforderlich sein, so bitte ich um entsprechenden Hinweis, der telefonisch (auch Anrufbeantworter), per Fax oder Brief erfolgen kann.

Mit freundlichen Grüßen

Jörg Reinholz
Kassel, am 13. Dez. 2010

Amtsgericht Düsseldorf

)ezember 2010

52 C 15528/10

Jörg Reinholz
Hafenstr. 67
34125 Kassel

52

Jörg Reinholz, Hafenstr. 67, 34125 Kassel

Amtsgericht Düsseldorf
Kammer 52 C

In Sachen 52 C 15528/10
Versicherung an Eides statt

In Kenntnis der Strafbarkeit der Abgabe einer vorsätzlich oder fahrlässig falschen Versicherung an Eides statt versichere ich wie folgt an Eides statt:

Ich habe die Euroweb Internet GmbH und auch sonst niemanden in irgend einer Form, nicht öffentlich oder nichtöffentlich darum gebeten oder sonst wie ersucht oder berechtigt, die Sicherheit meiner Internetpräsenzen zu überprüfen.

Richtig ist, dass ich vor den Angriffen bereits eine Unterlassungsverfügung gegen die Euroweb Internet GmbH erwirkte. (AG Düsseldorf, Az. 31 C 14650/10; LG Düsseldorf Az. 20 T 59/10).

Demnach habe ich eine rechtswidrige Rachehandlung hierfür zu vermuten.

Jörg Reinholz
Kassel, am 20. Dez. 2010

Jörg Reinholz
Hafenstr. 67
34125 Kassel

57

Original

Jörg Reinholz, Hafenstr. 67, 34125 Kassel

Amtsgericht Düsseldorf
Kammer 52 C

In Sachen 52 C 15528/10
Versicherung an Eides statt

In Kenntnis der Strafbarkeit der Abgabe einer vorsätzlich oder fahrlässig falschen Versicherung an Eides statt versichere ich wie folgt an Eides statt:

Ich bin seit dem Jahr 2000 als Privatdozent im Rahem der Erwachsenfortbildung im IT-Bereich tätig. Ich halte Seminare, Workshops und Trainings. In der Vergangenheit habe ich u.a. bei Einrichtungen der Bundeswehr, der Marine und der Luftwaffe Seminare zum Thema „IT-Sicherheit" gehalten. Ferner habe ich eine Vielzahl von Seminaren zum Thema PHP und Apache Webserver gehalten. Dazu gehört auch die Abwehr und das Erkennen von Angriffen. Ich habe also das fachliche Wissen und bin sachverständig genug, um folgende Aussage tätigen zu können:

Die im Antrag vom 13.12.2010 als Auszug aus dem Logfile dargestellten Zugriffe vom 6.12.2012, insbesondere die dabei aus dem Netzwerk der Euroweb Internet GmbH übertragenen Daten, zeigen auf, dass es sich hierbei nur

- um einen Versuch, durch wiederholtes Abrufen und Übertragen von Daten von/zu vom Antragsteller betriebenen oder benutzten Webservern deren Sicherheit oder Funktion sowie die Sicherheit der dort gespeicherten Daten oder Programme zu beeinträchtigen und
- um einen versuchten Einbruch in sicherheitsrelevante Bereiche der Internetpräsenzen des Antragstellers handeln kann.

Es wurde ganz offensichtlich – wenngleich erfolglos – versucht, Daten des Antragstellers oder seiner Kunden zu erlangen, zu verändern oder zu beschädigen oder zumindest ohne Aufforderung des Antragstellers zu testen ob dies möglich ist. Bereits dies ist aber ein unzulässiger Eingriff in meinen Geschäftsbetrieb, das gilt auch dann, wenn die überwiegende Anzahl der Versuche auf Grund offensichtlich mangelnder technischer Kenntnis der Angreifer von Anfang an erfolglos bleiben musste.

Eine weitere Beeinträchtigung trat durch die Belästigung und den Eingriff in meinen Geschäftsbetrieb ein, der sich aus dem Versand von 35 Emails über das Webformular ergibt, hier bei war dem Angreifer aus dem Firmennetzwerk der Euroweb Internet GmbH klar, dass diese Emails auch versendet wurden, denn diese Erfolgsbestätigung wurde dem Angreifer nach jedem Versand auch angezeigt. Der Angreifer aus dem Netzwerk der

:uroweb Internet GmbH hat also bewusst gestört.

Aus dem Logfile, welches als Anlage beigefügt war ergibt sich ferner, dass an diesem Angriff mindestens 6 Personen beteiligt waren, denn anders sind die 6 Zugriffe zu dem Zeitpunkt „06/Dec/2010:15:57:42 +0100" bis „06/Dec/2010:15:57:43", also vom 6. Dezember 2010 um 15 Uhr 57 Minuten und 42 bis 43 Sekunden mitteleuropäischer Zeit nicht zu erklären. Dieses Muster setzt sich auch fort.

Die gleichzeitigen Versuche, vom „06/Dec/2010:15:44:41 +0100" und „06/Dec/2010:15:45:15 +0100", also von 15:44:41 und 15:45:15, die nicht vorhandenen, nicht verlinkten und nicht abrufbaren Ressourcen

http://www.diewohnung.de/administration

und

http://www.diewohnung.de/admin

abzurufen, lassen gar keinen anderen Schluss, als den auf eines versuchten Angriffs auf die Sicherheit meiner Daten sowie die meiner Kunden mehr zu.

Es wird ferner an Eides statt versichert, dass die im Antrag und als Anlage beigefügten Auszüge solche aus den Logfiles der Variomedia AG sind, dass ich auf diese Logfiles keinen schreibenden Zugriff habe, dass die gefertigten Auszüge mit dem Werkzeug „grep" gemacht wurden, mit welchem sich aus Textdateien, wie es die Logfiles sind, zeilenweise – also Eintragsweise – erwünschte oder unerwünschte Inhalte filtern lassen, so dass der Auszug nur die Auswahl der als für den Antrag als relevant anzusehenden Abrufe darstellt, die aber an sich unverändert sind.

Für die Richtigkeit der vorstehenden Angaben in dieser eidesstattlichen Versicherung.

Jörg Reinholz
Kassel, am 20. Dez. 2010


Amtsgericht
179
Düsseldorf