

#### Kein Update des Virenschutzes – Vorsicht Haftungsfall!

- Warum sich der nachlässige Umgang mit den eigenen Schutzmaßnahmen rächen kann -

Fehlende oder nicht aktualisierte Antivirensoftware kann Haftungsfolgen gegenüber weiteren Infizierten mit sich bringen. Dieses Whitepaper behandelt:

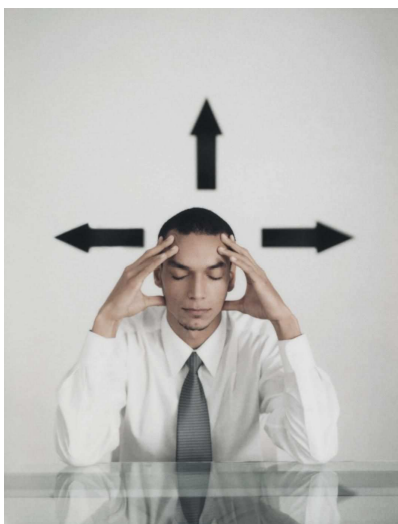
- [Entstehung einer Haftung](#)
- [Vermeidung der Haftung](#)
- [Wen diese Haftung trifft](#)

#### Problemaufriss:

In den letzten Jahren hat sich die Zahl der Schadprogramme drastisch erhöht. Während zu Beginn die meisten Viren, Würmer und Trojaner in erster Linie darauf ausgelegt waren, Zugang zu bestimmten Systemen zu erlangen und damit den jeweiligen Programmierern Selbstbestätigung zu beschaffen, haben die weitaus meisten Schadprogramme heutzutage einen rein kriminellen Hintergrund.

Dies führt in der Konsequenz leider immer häufiger dazu, dass bei den Betroffenen durch Vernichtung von Daten und Ausspähung von Passwörtern ein zum Teil erheblicher Schaden verursacht wird.

Was allerdings viele nicht wissen: Werden die Pflichten zur Einrichtung und regelmäßigen Erneuerung der Sicherungsprogramme wie Antivirensoftware oder Firewalls vernachlässigt, kann das einstige Opfer zum Täter werden und sich Haftungsansprüchen ausgesetzt sehen.



Gerne wird insbesondere in Unternehmen auf ein regelmäßiges Update der Sicherungssoftware verzichtet. Dies kann sie im Zweifel teuer zu stehen kommen.

#### Grundsatz der Verkehrspflichten gilt auch im Internet:

Derjenige, der eine Gefahrenlage schafft, ist dazu verpflichtet, sämtliche notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung Dritter zu vermeiden.

Dieser allgemeine zivilrechtliche Grundsatz zu den Verkehrspflichten gilt auch und gerade im Internet.

Das wahrscheinlich prominenteste Beispiel hierfür ist die von der Rechtsprechung entwickelte Störerhaftung des Anschlussinhabers bei Urheberrechtsverletzungen im Internet. Wer eine Gefahrenlage schafft, sei es durch eine Baustelle oder einen Internetanschluss, so die Rechtsprechung, müsse im Rahmen des Zumutbaren dafür Sorge tragen, dass davon keine Gefahr für die Rechte Dritter ausgeht. Im Fall des Internetanschlusses handelt es sich nach Ansicht einiger Gerichte u.a. um die Gefahrenlage „Verletzung möglicher Urheberrechte Dritter“, die es durch die Vornahme der entsprechenden Maßnahmen zu verhindern gilt.

Denkt man diesen Ansatz konsequent weiter, hören die Verkehrspflichten nicht bei der Verhinderung von Filesharing auf. So geht eine Gefahr für Rechte Dritter nicht nur durch die Nutzung von Filesharingsoftware durch die

eigenen Kinder, sondern auch durch mögliche bewusste, unbewusste oder jedenfalls geduldete Weiterleitung von Schadsoftware aus.

So kommt es regelmäßig vor, dass E-Mails mit Schadsoftware nicht nur aktiv weitergesendet werden, sondern sogar sich von selbst an alle im Adressbuch gespeicherten Kontakte versenden. Auch kann der eigene Rechner gekapert und zu Angriffen auf andere Computer missbraucht werden.

Für solche Angriffe haftet selbstverständlich zunächst einmal der direkte Verursacher. Darüber hinaus ist jedoch auch eine Haftung desjenigen möglich, dessen Computer für die Verbreitung von Schadsoftware missbraucht wurde. Dies jedenfalls dann, wenn er seine Verkehrspflichten nicht erfüllt hat, er also gerade nicht alles Notwendige und Zumutbare getan hat, um die Weiterleitung zu verhindern.

### **Wo hört jedoch das Zumutbare auf und wo fängt das Unzumutbare an?**

#### **Sicherungssoftware:**

Die hier beschriebenen Gefahren, die von den stetig wachsenden Angriffen von Schadsoftware ausgehen, sind eigentlich allen Internetnutzern hinlänglich bekannt. Dennoch sind viele äußerst nachlässig, wenn es um den Schutz des eigenen und damit letztlich auch fremder Rechner geht.

- Installation von Antivirensoftware bzw. einer Firewall -

Nach den allgemeinen Grundsätzen der Verkehrspflichten sind auch Internetnutzer verpflichtet, die entsprechenden notwendigen und zumutbaren Vorkehrungen

zu treffen, damit diese Schädlinge sich nicht weiter von dem eigenen Computer auf andere verbreiten.

Hat ein Nutzer kein Antivirenprogramm auf seinem Computer eingerichtet, so ist er seinen Verkehrspflichten bereits nicht nachgekommen und eine Haftung gegenüber den dadurch Betroffenen besteht. Zudem sollte eine Firewall installiert werden, die die entsprechenden Datentransfers auf und von dem jeweiligen Rechner überwacht. Eine Firewall allein soll jedoch den Anforderungen zur Erfüllung der Verkehrspflichten nicht genügen, da diese nur die Datentransfers überprüft, nicht jedoch den Computer auf einen bereits erfolgten Befall von Schadprogrammen durchsucht und diese gegebenenfalls unschädlich macht.

An die Auswahl des verwendeten Antivirenprogramms bzw. der Firewall sind jedoch keine besonders hohen Maßstäbe anzulegen. Die Überprüfung der Effektivität der einzelnen Angebote und die Auswahl des vermeintlich besten Programms gehört jedenfalls nicht mehr zu den Pflichten des Internetnutzers.

- Verpflichtung zum Update -

Die Verpflichtung ausreichende Vorkehrungen zu treffen, damit vom eigenen Computer keine Gefahren für die Systeme Dritter ausgehen, endet jedoch nicht bei der einmaligen Installation eines Antivirenprogramms bzw. einer Firewall. Laufend, im Grunde sekundlich, treten immer neue Schadprogramme auf, die von älteren Versionen der Antivirensoftware in der Regel nicht erkannt und damit auch nicht unschädlich gemacht werden können. Somit ist eine Haftung des Internetnutzers auch dann denkbar, wenn von seinem Computersystem

Dritte befallen werden und er seine Antivirensoftware zuvor nicht regelmäßig aktualisiert hat.

### **Wie oft hat denn ein Update zu erfolgen?**

Hier streiten sich die Geister. Es gibt jedoch noch keine Rechtsprechung zu der verlangten Frequenz der einzelnen Updates, sodass man aufgrund der sich immer schneller ändernden Gefährdungslage durch neue Schadsoftware jedenfalls davon ausgehen muss, dass jedenfalls ein Update jeden Monat unzureichend ist.

Mindestens sollte deshalb eine Aktualisierung der Antivirensoftware in einem häufigeren, wohl wöchentlichen, Rhythmus vorgenommen werden. Allerdings muss die Erfüllung der Verkehrssicherungspflicht zumutbar bleiben. Ob ein solches wöchentliches Update ausreicht, um den Verkehrspflichten des Internetnutzers zu genügen, muss die Rechtsprechung im Einzelfall entscheiden. Noch liegen jedoch keine Urteile vor, in welchen sich die Gerichte mit dem Rhythmus der zu verlangenden Aktualisierungen beschäftigt haben.

### **Beweisbarkeit - Update und dann?**

Wenn nunmehr eine regelmäßige Aktualisierung vorgenommen wurde, muss dies natürlich gegenüber dem jeweiligen Betroffenen bewiesen werden können. Die Durchführung der Updates muss deshalb aus den entsprechenden Log-Dateien entnommen und gegebenenfalls vorgelegt werden. Ist dies nicht der Fall, kann im Zweifel auch das regelmäßig durchgeführte Update keine Enthftung mit sich bringen.

Problematisch erscheint in diesem Zusammenhang, dass manche Programme, wie zum Beispiel das Betriebssystem Chrome von Google, die Updates unbe-

merkt vom Nutzer selbstständig durchführen. Diese im Hintergrund durchgeführten und deshalb auch „silent updates“ genannten Aktualisierungen fallen dem Nutzer nicht nur nicht auf, sondern sind auch nicht immer nachweisbar. Hier wird dringend geraten, dafür Sorge zu tragen, dass auch solche stillen Updates in den Logs protokolliert werden. Anderenfalls nutzt im Streitfall auch die regelmäßige Vornahme eines Updates nichts, wenn dieses nicht nachgewiesen werden kann.

Kann eine regelmäßige und lückenlose Aktualisierung der eigenen Antivirenprogramme nachgewiesen werden, so entfällt eine Haftung des Internetnutzers auch bei Infektionen anderer Computer aus den Gründen der Verletzung der Verkehrspflicht grundsätzlich dann, wenn die jeweils aktuelle Version der Antivirensoftware nichts hätte gegen das konkrete Schadprogramm ausrichten können. In diesem Fall wurde alles Notwendige und Zumutbare durch den Internetnutzer getan, um mögliche Verletzungen Dritter durch den eigenen Computer bzw. die Nutzung des Internets zu vermeiden. Größere Sorgfaltspflichten sollten hier auch nicht verlangt werden.

### **Verpflichtung auch für Privatnutzer?**

Noch ungeklärt ist die Frage, ob neben Unternehmen auch Privatpersonen die hier genannten Verpflichtungen zur regelmäßigen Erneuerung der eigenen Sicherheitssoftware zu erfüllen haben.

Die Rechtsprechung bezüglich der Störerhaftung des Anschlussinhabers bei Urheberrechtsverletzungen bei Internetausbörsen ist jedoch recht streng. Deshalb liegt die Vermutung nahe, dass eine Haftung für die Weiterverteilung von Schadprogrammen lediglich wegen der Nutzung der Gefahrenquelle „Internet“ von den Gerichten auch dann angenommen wird, wenn die

Verkehrspflichten nicht im notwendigen und zumutbaren Rahmen erfüllt wurden.

Dies dann auch unabhängig davon, ob es sich um ein Unternehmen oder eine Privatperson handelt.

### **Besteht sogar die Verpflichtung zur Beendigung der Internetverbindung?**

Ob die Verpflichtung durch die eigenen Gefahrenquelle (Internetverbindung) Schaden von anderen abzuwenden bzw. den Schadenseintritt zu vermeiden, im Einzelfall sogar darin münden könnte, dass die Verbindung durch den betroffenen Nutzer zum Internet gänzlich beendet wird, wird kontrovers diskutiert und wurde noch von keinem Gericht entschieden. Denkt man die sich aus den Grundsätzen der Verkehrspflicht ergebenden Verpflichtungen zu Ende, so lässt sich jedoch durchaus annehmen, dass zumindest im Fall der Feststellung eines schwerwiegenden Befalles von Schadsoftware zum Schutze der Rechtsgüter Dritter die Internetverbindung sofort getrennt werden müsste.

Ob auch die Gerichte diese Verpflichtung aufgreifen werden, wird sich in Zukunft zeigen.

### **Fazit:**

Die Gefahr für die eigenen und fremden Daten sowie die Funktionsfähigkeit des eigenen Computersystems machen es heutzutage unerlässlich, den Schutz vor Angriffen aus dem Internet so aktuell wie möglich zu halten. Für die eigenen Daten ist zwar jeder Einzelne verantwortlich, dass jedoch allein aus dem Umstand, das Anti-virenprogramm nicht regelmäßig aktualisiert zu haben, im Zweifel eine Haftungsfalle werden kann, ist den meisten allerdings nicht bewusst.

Jedenfalls wird diese Verpflichtung für Unternehmen wohl auch ohne bislang einschlägige Rechtsprechung anzunehmen sein. Gerade jedoch Unternehmen pflegen oftmals eine nachlässige Handhabung des eigenen Schutzes vor Schadprogrammen.

Dies kann zumindest dann, wenn ein Geschädigter den tatsächlichen Verursacher nicht greifen kann, zu unerwarteten und äußerst unangenehmen (Haftungs-)Folgen führen.



Weitere Informationen hierzu erteilt Ihnen gerne:

Herr Rechtsanwalt Sascha Faber, LL.M. (Medienrecht):

[faber@volke2-0.de](mailto:faber@volke2-0.de)

Fon: 02306/75684-0

Fax: 02306/75684-11

Der Autor, Herr Rechtsanwalt Sascha Faber LL.M. (Medienrecht) ist, wie alle Anwälte der Kanzlei Volke2.0, ausschließlich auf den Gewerblichen Rechtsschutz (Wettbewerbs-, Marken-, Gebrauchs-, Geschmacksmuster- und Patentrecht) im Internet und das IT-Recht spezialisiert. Das Team von Volke2.0 steht Ihnen gerne auch für weitere Fragen rund um diese Rechtsgebiete zur Verfügung.

**Bitte beachten Sie, dass dieses White Paper lediglich zur Information und Orientierung in dem entsprechenden Bereich des Rechts dient. Das Dokument kann nur als Hilfestellung verwendet werden. Im konkreten Einzelfall sollte eine rechtliche Beratung durch einen Rechtsanwalt in Anspruch genommen werden. Dieses White Paper ist nicht dazu gedacht, eine anwaltliche Beratung zu ersetzen. Eine Haftung kann daher nicht übernommen werden.**