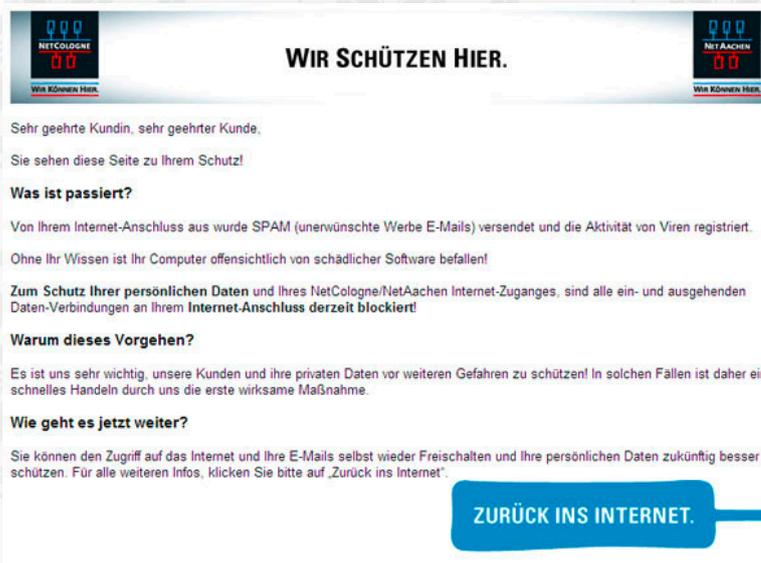


# INTERNET-SICHERHEIT

## ABUSE SICHERHEITSSPERRE INTERNET



**Sie erhalten die nebenstehende Seite angezeigt, sobald Sie irgendeine Internetseite öffnen wollen?**

Im dem Fall wurde Netzmissbrauch - engl. Abuse - ausgehend von Ihrem Internetzugang festgestellt und der Zugang aus Sicherheitsgründen gesperrt.

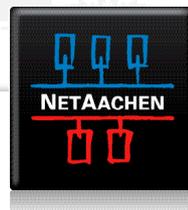
In der Regel geschieht dieser Netzmissbrauch im Hintergrund, ohne Ihr Wissen.

### **Häufig auftretende, schädliche Aktivitäten, die von Ihrem PC ausgehen können:**

- Über Ihren PC wurden Spam-E-Mails oder E-Mails mit Virenanhang versendet. (Spam-Proxy/Würmer)
- Ihr PC ist mit einem Virus infiziert, der sich selbständig weiter versendet, da dieser nicht durch Schutzsoftware blockiert wird. (Trojaner/Würmer)
- Ihr PC wurde missbraucht, um andere Rechner im Netz durch sogenannte Distributed-Denial-of-Service-Attacken zu beschädigen. (DDoS-Attacken, hervorgerufen durch Würmer/Trojaner)
- Sie haben Ihren PC aktiv benutzt, um z.B. Portscans oder jegliche Form anderer Attacken gegen Nutzer innerhalb und/oder außerhalb des NetCologne-Netztes auszuführen.

Sobald Sie sich entschieden haben, mit Ihrem Rechner online zu arbeiten, muß Ihnen auch bewußt sein, dass Ihr PC von nun an, für jeden der über das technische Know-how verfügt, angreifbar ist.

Das bedeutet nicht, dass das Arbeiten im Internet generell gefährlich ist, es bedeutet vielmehr, daß es absolut sinnvoll ist, persönliche Daten und Unterlagen vor dem Zugriff Dritter zu schützen.



### Wie kann ein solcher sinnvoller Schutz aussehen?

1. Der erste wichtige Schritt stellen die **Sicherheitsupdates für Ihr Betriebssystem** dar. Updates für Ihr Microsoft Windows Betriebssystem finden Sie zum Beispiel unter:

<http://windowsupdate.microsoft.com/>

Beachten Sie unbedingt, dass für alle älteren Betriebssysteme der Support vom Hersteller Microsoft eingestellt worden ist!

Dies führt dazu, dass diese Betriebssysteme nicht die gleiche Sicherheit bieten können wie neuere Versionen. Windows 98 und ME sind ältere Betriebssysteme, die Sicherheitsbedrohungen gegenüber anfälliger sind als neuere Betriebssysteme. Da Microsoft keine Sicherheits-Updates für diese Betriebssysteme mehr veröffentlicht, ist jeder PC, auf dem eines dieser Betriebssysteme installiert ist, wesentlich stärker gefährdet!

Wir empfehlen Ihnen dringend, ein aktuelles Betriebssystem zu nutzen. Damit erhöht sich nicht nur die Sicherheit Ihres Systems, auch stehen Ihnen durch moderne Techniken eine erhöhte Bedienungsfreundlichkeit sowie ein verbesserter Funktionsumfang zur Verfügung.

2. Der zweite wichtige Schritt ist der Einsatz eines **Antiviren-Schutzprogramms**.

3. Drittens sollten Sie Ihren Rechner durch den Einsatz einer **Firewall** weiter schützen.

4. Weiterhin empfiehlt sich der **Schutz vor** so genannter **Spyware**.

Wir empfehlen Ihnen unser **NetAachen Sicherheitspaket**, das viele dieser Bereiche absichert. Sie können das NetAachen Sicherheitspaket bequem von zu Hause aus bestellen und installieren. Wie das geht erfahren Sie [hier](#).

Eine Anleitung zur Durchführung einer Intensivprüfung finden Sie hier: [Intensivprüfung bei Befallsverdacht/ABUSE - Sicherheitssperre Internet](#)

**Weitere Informationen** zur Internet-Sicherheit finden Sie auf

den Seiten des [Anti-Botnetz-Beratungszentrum](#), das wir als Partner unterstützen  
den Seiten des [bsi, Bundesamt für Sicherheit in der Informationstechnik](#)