

## Verstecken Sie Ihre Daten hinter einem Internetschutzwall

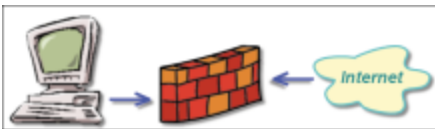
Da Ihr Rechner, sobald Sie mit dem Internet verbunden sind, ein potentielles Angriffsziel darstellt und Sie es wohl kaum schaffen werden, immer auf dem aktuellsten Stand zu sein, was alle möglichen Gefahren angeht, muss ein wirkungsvoller Schutzmechanismus her, der Sie und Ihre Daten so gut wie möglich vor den aktuellsten Trojanischen Pferden, Phonehome-Programmen und Script-Kiddies etc. schützt.

Im Bauwesen haben sich zum Schutz vor übergreifenden Gefahren Brandmauern bewährt: Sollte ein Gebäudeteil Feuer fangen, kann es nicht auf die anliegenden Komplexe übergreifen, wenn eine solide Mauer dazwischen steht. Solche Brandmauern (engl. Firewall) gibt es auch für Computer und Netzwerke. Und wenn Sie vertrauliche Informationen auf Ihrem Rechner gespeichert haben oder einfach etwas gegen unerlaubte Zugriffe und Datenspione haben, dann bieten Firewalls hervorragenden Schutz, damit der Aufenthalt im Web nicht zu Verfolgungswahn führt und Sie wieder beruhigt surfen können.

## Wie eine Firewall Sie schützen kann

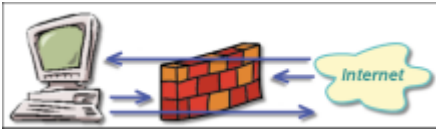
Waren Firewalls bis vor kurzem noch etwas, womit sich nur Systemadministratoren großer Firmen auseinander setzen mussten und konnten, hat sich die Technik mittlerweile so sehr gewandelt, dass eigentlich kein PC-Besitzer, der im Internet surft, mehr ohne auskommen kann, denn immer mehr Menschen scheinen es besonders darauf abgesehen zu haben, anderen Schaden zuzuführen.

Eine Firewall arbeitet nach einem einfachen Prinzip: Das Programm schaltet sich zwischen PC und Internet und blockiert einfach den gesamten Datenverkehr. So können keine Angriffe zum Computer durchkommen und keine Daten herausgelangen.



## Verstecken Sie Ihre Daten hinter einem Internetschutzwall

Diese Radikallösung ist allerdings nicht sinnvoll, denn dann können Sie ja gar keine Daten mehr mit dem Internet austauschen und ebenso die Verbindung abbauen. Aus diesem Grund wird eine Firewall so konfiguriert, dass sie zwar immer noch die meisten Daten erst einmal abfängt, aber einiges auch durchlässt.



Dazu lauscht die Firewall an allen Verbindungen (den so genannten Ports) zwischen PC und Netzwerk. Schickt eine Applikation Daten ins Netz, der dies erlaubt wurde, passieren die Daten. Versucht aber eine Anwendung, die keine Freigabe besitzt, Daten zu senden, werden die Informationen abgefangen, und es erscheint ggf. eine Warnmeldung, damit Sie erfahren, wer da kommunizieren will.

Ebenso schützt die Firewall vor Daten aus dem Netz: Treffen Datenpakete ein, die angefordert wurden und an eine freigegebene Anwendung gerichtet sind, dürfen sie passieren. Alle anderen Versuche, zu dem Rechner durchzukommen, scheitern, worüber Sie ebenfalls informiert werden können, damit Sie mögliche Attacken erkennen und reagieren können.

### Info

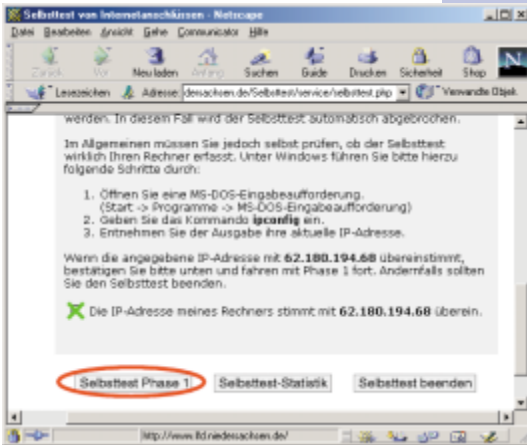
#### Firewalls bieten Rundum-Schutz

Nicht nur gegen Attacken aus dem Internet helfen Firewalls. Auch in lokalen Netzwerken können sie sinnvoll sein, da der gesamte Datenverkehr zwischen Ihrem PC und allen Netzwerkkomponenten kontrolliert werden kann.

Neben den zahlreichen Programmen, wie Sie im Kapitel über Viren & Co. ab Seite 119 vorgestellt wurden und die gern heimlich Daten ins Netz schicken, schützt eine Firewall auch vor den sehr beliebten Portscans. Dabei läuft auf einem Rechner des Angreifers ein einfaches Programm, das IP-Adressen ermittelt und dann alle möglichen Verbindungen Ihres PCs abklappert, ob zufällig eine offene Verbindung besteht. Über so einen Port können dann Attacken gestartet werden. Je nachdem, welcher Port offen ist, lassen sich auf Ihrem Rechner Programme ausführen oder Daten sammeln. Ohne Firewall bekommen Sie davon nichts mit, bis Sie sich wundern, warum Ihr PC Daten verliert oder Ihre Kontoauszüge im Web veröffentlicht werden.

## Wie eine Firewall Sie schützen kann

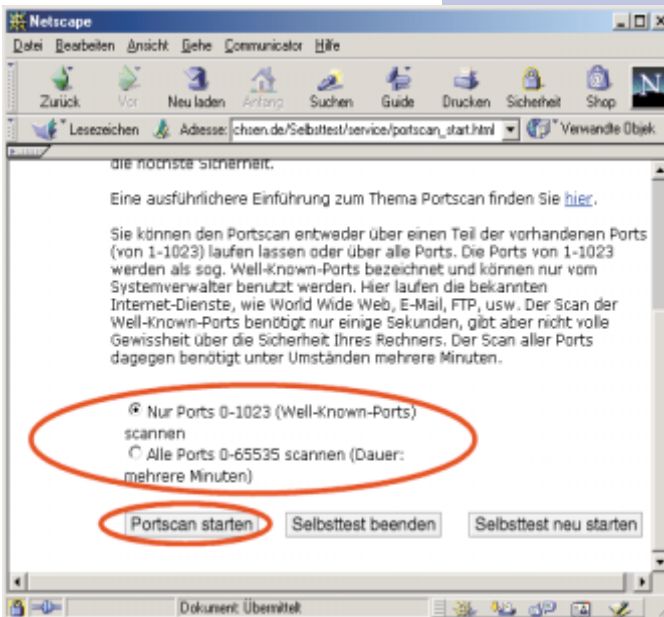
Auf der Webseite des Landesbeauftragten für den Datenschutz Niedersachsen können Sie einen solchen Angriff auf Ihrem Rechner auslösen und feststellen, welche Ports zurzeit ein Sicherheitsrisiko bilden.



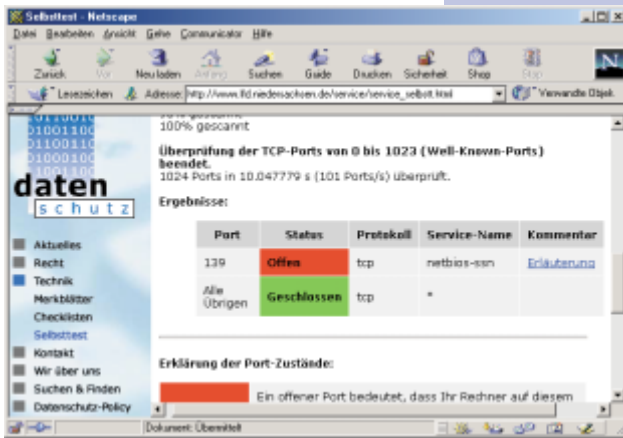
**1** Starten Sie den Test auf der Webseite [http://www.lfd.niedersachsen.de/service/service\\_selbstt.html](http://www.lfd.niedersachsen.de/service/service_selbstt.html).

Dazu müssen Sie am Seitenende überprüfen, ob Ihre IP-Adresse korrekt ermittelt wurde und dann ein Häkchen setzen. Mit *Selbsttest Phase 1* starten Sie den Selbstversuch.

**2** Die folgenden Tests informieren Sie über weitere Sicherheitsrisiken auf Ihrem PC. Der eigentliche Portscan findet in *Phase 3* statt. Sie können wählen, ob Sie nur die Standardports (Well-Known-Ports) oder alle 65.536 Ports überprüfen wollen, was einige Minuten dauert.



## Verstecken Sie Ihre Daten hinter einem Internetschutzwall



**3** Nach dem Test erhalten Sie einen Report, in dem alle offenen Ports aufgeführt sind. Je nachdem, welches Protokoll an dem Port aktiv ist, gehen unterschiedliche Gefahren davon aus, über die Sie sich weiter informieren können, wenn Sie den jeweiligen Links in der Spalte *Kommentar* folgen.

## Kostenlose Firewall installieren

Firewalls gibt es zahlreiche, und die Spanne reicht von kostenlos bis teuer und von unverständlich bis anwenderfreundlich. Eins der für private Anwender beliebtesten Firewall-Programme vereint zwei markante Vorteile in sich: Es ist kostenlos und benutzerfreundlich. Daher spricht also nichts gegen eine sofortige Installation, damit Sie wieder in Ruhe surfen können.



Auf der Webseite <http://www.zonelabs.com> finden Sie den knapp 2 MByte großen kostenlosen Download von ZoneAlarm (nur wenn Sie das Programm beruflich nutzen wollen, benötigen Sie die Pro-Version).



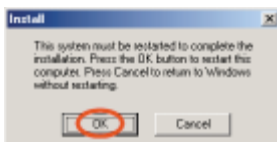
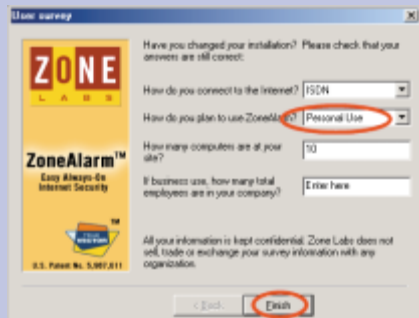
**1** Starten Sie das Setup-Programm nach dem Download durch Doppelklick auf den Dateinamen im Explorer.

**2** Lesen Sie sich die Informationen auf den ersten zwei Dialogfeldern durch und geben Sie anschließend Ihren Namen etc. in die Felder ein. Wenn Sie sich bei ZoneAlarm registrieren lassen, bekommen Sie Infos per E-Mail und automatisch Updates, die Sie sich aber auch manuell besorgen können.



**3** Akzeptieren Sie den Lizenzvertrag und wählen Sie im nächsten Schritt den Installationspfad mit *Browse* bzw. belassen Sie es bei der Standardangabe.

**4** Nach der Installation werden noch ein paar Benutzerdaten erfragt, von denen die wichtigste ist, dass Sie *Personal Use* einstellen.



**5** Haben Sie alle Schritte ausgeführt, muss zum Schluss nur noch der Rechner neu gestartet werden, damit Ihre persönliche Firewall aktiv wird, was Sie am Symbol im Traybar erkennen können.



### Info

#### Datentransfer immer unter Kontrolle

Mithilfe der zwei Bargraph-Anzeigen im ZoneAlarm-Symbol haben Sie immer einen Überblick darüber, ob gerade Daten ins Netz geschickt (rot) oder von dort empfangen (grün) werden. Je weiter die Anzeige ausschlägt, desto höher ist die Transfer-rate.

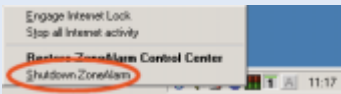
## Die Firewall im Surfalldag

Nach der Installation von ZoneAlarm werden erst einmal alle Zugriffe aus und vom Netzwerk 100%ig abgeblockt. Dadurch erhalten Sie zwar die höchste Sicherheit, jedoch können Sie auch nicht mehr ins Internet. Deshalb müssen Sie die Firewall ein wenig konfigurieren, sodass einige Programme dann doch mit dem Internet kommunizieren können.

### Info

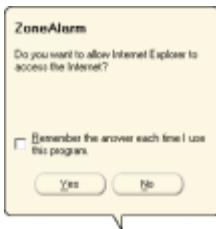
#### Auch Ihr lokales Netzwerk ist betroffen

Haben Sie zu Hause mehrere Computer zum Beispiel für Mehrbenutzerspiele untereinander vernetzt, werden diese Computer von ZoneAlarm erst einmal ausgesperrt. Die Hilfe zeigt Ihnen, wie Sie die Rechte für Netzwerke anpassen können. Haben Sie keine Internetverbindung aktiviert, können Sie auch mit einem Rechtsklick auf das Symbol die Firewall beenden (*Shutdown ZoneAlarm*).



## Zugriffsrechte für Programme festlegen

Sobald Sie mit einem Programm auf ein Netzwerk zugreifen wollen, registriert ZoneAlarm dieses Anliegen und erkennt, ob das Programm dazu berechtigt ist oder nicht.



**1** Sobald eine Anwendung Daten verschicken will, erscheint eine Warnmeldung, die Sie über den Zugriff informiert. Lesen Sie sich die Informationen genau durch, denn es kann sich durchaus um ein Programm handeln, was nichts im Netz verloren hat und geheime Daten versenden will.

**2** Wollen Sie dem Programm (hier: Internet Explorer) den Zugriff aufs Internet erlauben, klicken Sie auf *Yes*, ansonsten auf *No*.

**3** ZoneAlarm kann sich Ihre Entscheidung merken, was bei einigen Standardanwendungen praktisch ist, da Sie sonst bei jedem neuen Zugriff mit der Rückfrage genervt werden. Bei aktivierter Option *Remember the answer each time ...* merkt sich die Firewall, ob Sie *Yes* oder *No* anklicken, und verwendet die Wahl in Zukunft automatisch.

Da Sie am Anfang noch keinerlei Rechte eingestellt haben, werden Sie in den ersten Tagen vermehrt solche Meldungen erhalten, bis Sie für alle Programme die Einstellungen festgelegt haben.

### Info

#### Rechte zurückhaltend vergeben

Bei der Freigabe von Zugriffsrechten aufs Internet sollten Sie sehr knauserig sein. Viele Programme wollen gern ins Internet Daten senden, brauchen dies aber eigentlich gar nicht. Ihre Browse- und E-Mail-Programme sind sicherlich dauerhaft berechtigt; Werbeprogramme wie TSAdBot ganz bestimmt nicht. Und dann gibt es noch die große Zahl der Programme, bei denen Sie lieber jedes Mal aufs Neue entscheiden sollten. So z. B. beim Mediaplayer, der nur dann ins Netz gehen muss, wenn er einen neuen Treiber oder Ähnliches braucht, es aber auch sonst ganz gern macht, um Daten über Sie zu verschicken. Auch wenn die Rückfragen von ZoneAlarm etwas Zeit kosten, so erhöhen sie doch die Sicherheit. Geben Sie also nicht pauschal alles frei, sondern schauen Sie erst mal, wann welches Programm mit dem Internet kommunizieren will.

Wollen Sie einmal getroffene Entscheidungen korrigieren oder allgemein feststellen, welche Programme mit welchen Rechten arbeiten, dann bietet ZoneAlarm hierzu einen einfachen Dialog an:






**1** Starten Sie den Konfigurationsdialog von ZoneAlarm durch Doppelklick auf das Programmsymbol im Traybar.

**2** Klicken Sie auf *Programms*, um alle Programme zu sehen, die bereits von ZoneAlarm

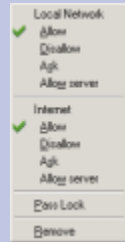
## Verstecken Sie Ihre Daten hinter einem Internetschutzwall



registriert wurden. In der Spalte *Allow connect* sehen Sie die Rechte des jeweiligen Programms fürs lokale Netzwerk und das Internet. Die Symbole haben dabei folgende Bedeutung:

-  **Ask** – Bei jedem Zugriff wird erneut nachgefragt.
-  **Allow** – Es dürfen immer Daten ausgetauscht werden.
-  **Disallow** – Es dürfen keine Daten ausgetauscht werden.

**3** Die Rechte können Sie jederzeit abändern, indem Sie mit der rechten Maustaste auf einen Programmeintrag klicken und im Kontextmenü die neuen Einstellungen wählen. Mit *Remove* erhalten Sie weiterhin die Möglichkeit, ein Programm aus der Liste zu entfernen, wenn Sie es beispielsweise komplett deinstalliert haben.



## Pausenlose Attacken? – Keine Panik!

ZoneAlarm kontrolliert nicht nur Daten, die von Ihrem Rechner hinaus ins Netzwerk geschickt werden, sondern auch solche, die auf Ihrem Computer eintreffen. Sollte beispielsweise ein Hacker versuchen, gegen Sie vorzugehen, während Sie online sind, steht ihm die Firewall wirksam im Weg.

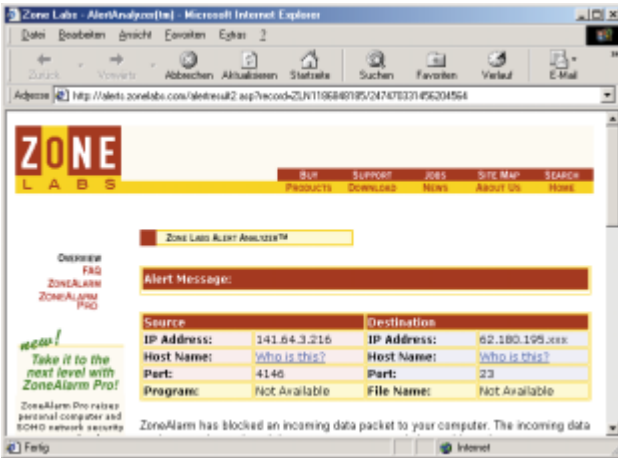
Mit installierter Firewall haben Sie so auch einen guten Schutz gegen Bugs in Programmen, die bisher noch nicht öffentlich bekannt sind oder für die es keine Lösung gibt, wie zum Beispiel das Loch in Microsoft NetMeeting, das es einem Angreifer erlaubt, per Denial-of-service-Attack den PC des Opfers zu 100 % auszulasten, und so das weitere Arbeiten unmöglich macht. Mit einer Firewall sind Sie vor solchen Umtrieben sicher.

Zum Beispiel versuchte hier (s. Abbildung) ein Nutzer von [hrz.tfh-berlin.de](http://hrz.tfh-berlin.de) mit der IP-Adresse *141.64.3.216* per Telnet Zugriff auf den Computer zu erzielen, was von ZoneAlarm verhindert wurde.





ZoneAlarm öffnet bei jedem potentiellen Angriffsversuch einen Hinweis, in dem detailliert beschrieben wird, welcher Service von wo gerade auf Ihren PC zugreifen wollte. Dadurch haben Sie die Chance zu erkennen, ob es sich um eine ernste Bedrohung handelt. Für weitere Informationen können Sie sich über die Schaltfläche *More info* mit der ZoneLabs-Webseite verbinden lassen.



Eine Eigenart von Firewalls ist es, dass es durchaus passieren kann, dass Sie eine Verbindung zu einer Webseite beendet haben (zum Beispiel durch Beenden der Sitzung und kurz danach einem erneuten Aufbau der Verbindung) und daraufhin zahllose Warnmeldungen bei Ihnen eintreffen. Das liegt daran, dass die ursprüngliche Webseite immer noch Daten sendet, diese aber nicht mehr an den kor-

<http://alerts.zonelabs.com/t>

rekten Port adressiert werden, der bei der ersten Sitzung verwendet wurde. Von derartigen Datenpaketen geht zum Glück keinerlei Gefahr aus, doch können solche Fehlermeldungen auf Dauer nerven. Unterdrücken Sie sie einfach mit der Option *Don't show this dialog again*.

## So erwischen Sie jeden Hacker

Häufen sich die Attacken von einem einzelnen System aus, was Sie an der gleich bleibenden IP-Adresse erkennen, können Sie sich auch zur Wehr setzen und gegen den vermeintlichen Hacker vorgehen, denn auch wenn Sie keinen Schaden nehmen, da Sie durch die Firewall geschützt sind, kann es anderen Anwendern doch schlimm ergehen, wenn der Hacker sein Unwesen weitertreibt.

Da Sie den Hacker nicht direkt ermitteln können – schließlich wird er kaum seinen Namen verraten und auch kaum der Besitzer der IP-Adresse sein, von der aus er seinen Angriff unternimmt (das wäre zu einfach und es müsste sich

## Verstecken Sie Ihre Daten hinter einem Internetschutzwall

schon um einen äußerst dummen Hacker handeln) –, können Sie sich nur an den Systemadministrator des Computers wenden, von dem der Angriff ausging. Informieren Sie ihn so genau wie möglich über den Angriff auf Ihr System. Mit den konkreten Informationen kann dieser dann in seinen Log-Dateien nachsehen und mit hoher Wahrscheinlichkeit den Angreifer identifizieren. Da kaum ein Systemverwalter Hacker leiden kann, wird er schon von sich aus motiviert sein und auch eine entsprechende Strafverfolgung in Erwägung ziehen. Reicht Ihnen das nicht, können Sie sich immer noch eigene rechtliche Schritte überlegen.

Auf jeden Fall müssen Sie folgende Informationen sichern und dem Administrator zukommen lassen:

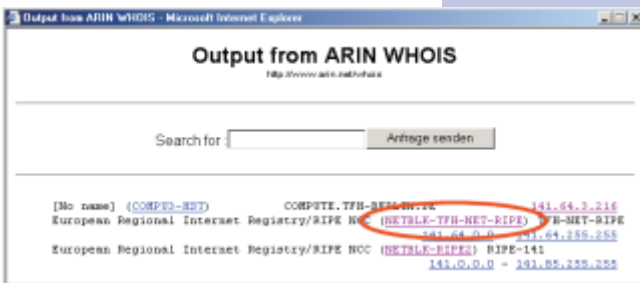
- die (auf die Sekunde) genaue Uhrzeit des Angriffs und das Datum,
- die Art der Attacke (zum Beispiel Telnet, Ping etc.),
- die IP-Adresse und der Port, von dem der Angreifer kam.

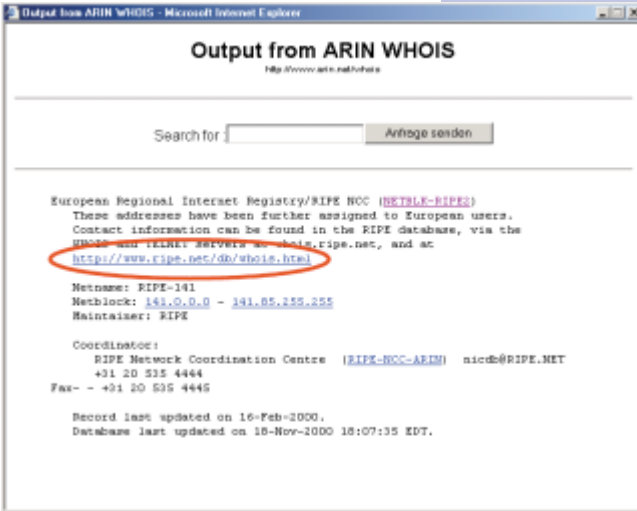
Wie Sie sehen, sind das genau die Daten, die Ihnen die Warnmeldung von ZoneAlarm auch ausgibt, und Sie brauchen die Informationen nur noch abzuschreiben. Ein Screenshot kann zusätzlich nicht schaden. Dazu drücken Sie die Taste **Druck** und fügen das Bild aus der Zwischenablage in ein Grafikprogramm ein, um es dann abzuspeichern.

Haben Sie das „Beweismaterial“ gesichert, müssen Sie nur noch herausbekommen, wer eigentlich für das System des Angreifers verantwortlich ist. Dazu informieren Sie sich wie zuvor beschrieben am besten durch einen Klick auf *More info* in der Warnmeldung auf den Webseiten von ZoneLabs.

**1** In der Tabelle (s. o.) können Sie dann in der Spalte *Source* durch Anklicken des Links *Who is this* den Inhaber des Computers ermitteln.

**2** Dazu wird eine Whois-Datenbankabfrage an die American Registry for Internet Numbers-Organisation (ARIN) gestellt (<http://www.arin.net/whois>). Entweder die Suche kann direkt beantwortet werden oder ARIN lie-





fert einen Hinweis auf die zuständige Verwaltungsstelle für die IP-Adresse.

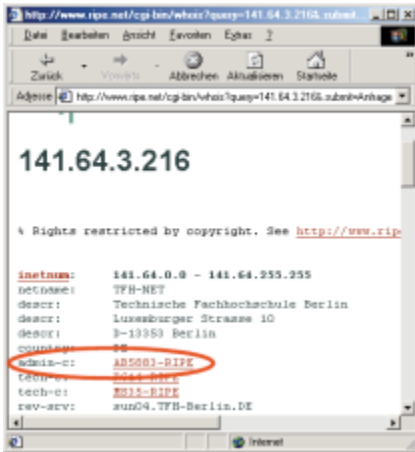
**3** Für europäische Adressen ist dies zum Beispiel das RIPE (Réseaux IP Européens, <http://www.ripe.net>), dessen URL durch Anklicken des Links im Suchergebnis von ARIN angezeigt wird.



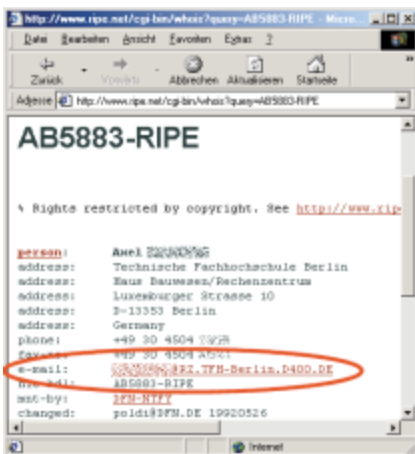
**4** Durch Eingabe der IP-Adresse in das Suchformular der angegebenen Verwaltungsstelle (in diesem Beispiel beim RIPE) kommen Sie in Ihrer Suche nach dem Systembesitzer einen Schritt weiter.

<http://www.ripe.net/cgi-bin/whois>

## Verstecken Sie Ihre Daten hinter einem Internetschutzwall



**5** Nach erfolgreicher Suche werden Ihnen anschließend alle Informationen preisgegeben, die in der Datenbank gespeichert sind. Jetzt wissen Sie immerhin schon einmal, wer als Besitzer des angreifenden Computers eingetragen wurde bzw., genauer gesagt, des Netzservers, hinter dem sich der Angreifer versteckt.



**6** Um den Namen und die E-Mail-Adresse des Administrators zu ermitteln, müssen Sie nur noch auf den Link hinter *admin-c* klicken, und Sie haben alle Informationen, um Ihren Hacker anzuschwärzen.