

Schließen

## Cyber Patrol für Fun Online

*Cyber Patrol für Fun Online* ist eine Software für den privaten Benutzer, mit der Sie den Zugang zu Internet-Diensten freigeben oder sperren können.

[Was ist Cyber Patrol für Fun Online?](#)

[Funktionen von Cyber Patrol für Fun Online](#)

[Cyber Patrol für Fun Online installieren](#)

[Cyber Patrol registrieren](#)

[Cyber Patrol deinstallieren](#)

[Cyber Patrol erneut installieren oder aktualisieren](#)

## Was ist Cyber Patrol für Fun Online?

**Cyber Patrol für Fun Online** ist eine Software, die eigens für Fun Online Mitglieder angeboten wird. Mit dieser Software können Sie den Zugang zu Internet-Diensten freigeben oder sperren.

Cyber Patrol wird Ihnen von Fun Online mit einer Option zur Registrierung zur Verfügung gestellt, die in der kommerziellen Standard-Version von Cyber Patrol nicht enthalten ist.

## Funktionen von Cyber Patrol für Fun Online

**Cyber Patrol für Fun Online** ist eine Software, die eigens für Fun Online Mitglieder angeboten wird.

Mit Cyber Patrol kann der Zugriff auf Internet-Inhalte kontrolliert werden, wie z. B. auf Internet Newsgroups, auf die Sie mit einem externen News Reader zugreifen können, und auf Internet Relay Chat Groups, auf die Sie mit einer externen Chat Group-Software zugreifen.

Außerdem können Sie mit Cyber Patrol festlegen, wann und wie lange Ihre Kinder Fun Online benutzen dürfen.

---

Mit folgenden Mitteln können Sie je nach Inhalt den Zugang zu Internet-Sites und Internet-Diensten sperren lassen:

- [CyberNOT-Liste](#)
- Bereichsbeschränkungen SafeSurf
- [IRC-Sperrphrasen-Liste](#)

---

Sie haben außerdem die Möglichkeit, die Zugangszeiten festzulegen:

- Sie können festlegen, zu welchen Zeiten Fun Online benutzt werden und wann im Internet gesurft werden darf.
- Sie können die Benutzung von Fun Online und den Zugang zum Internet auf eine maximale Zeitdauer pro Tag oder Woche beschränken.

---

Sie können Benutzern ein [Assistenten](#)-Kennwort geben, um ihnen vollen, unbegrenzten Zugang zu den Fun Online und Internet-Diensten zu gewähren.

## Cyber Patrol für Fun Online installieren

**Cyber Patrol für Fun Online** wird mit Standard-Einstellungen für die Verwendung mit Fun Online geliefert.

---

### So laden Sie Cyber Patrol herunter

In der ReadMe-Datei finden Sie Hinweise, wie Sie die Software bei Fun Online herunterladen können.

---

### So installieren Sie Cyber Patrol

*Melden Sie sich bei Fun Online an, bevor Sie die Installation beginnen.*

Wenn Sie das Installationsprogramm für eine spätere Installation heruntergeladen haben:

1. Stellen Sie eine Verbindung zu Fun Online her, um Cyber Patrol zu installieren und registrieren zu lassen.
2. Starten Sie das Installationsprogramm CP-SETUP.EXE.
3. Registrieren Sie Ihre Kopie von Cyber Patrol.
4. Überprüfen Sie die Liste der Anwendungen im Dialogfeld *Spiele & Anwendungen*, und vergewissern Sie sich, daß das von Ihnen verwendete Fun Online Programm dort enthalten ist.

Wenn Sie direkt von Fun Online installieren:

1. Stellen Sie eine Internet-Verbindung mit Fun Online her, um Cyber Patrol zu installieren und registrieren zu lassen.
2. Befolgen Sie die Anweisungen von Fun Online.
3. Registrieren Sie Ihre Kopie von Cyber Patrol.
4. Überprüfen Sie die Liste der Anwendungen im Dialogfeld *Spiele & Anwendungen*, und vergewissern Sie sich, daß das von Ihnen verwendete Fun Online Programm dort enthalten ist.

---

### So registrieren Sie Cyber Patrol

**Lesen Sie auch:** [Cyber Patrol registrieren](#)

---

## Hotline für Fun Online

### Hotline

Die Hotline für Fun Online ist täglich von 8 bis 23 Uhr erreichbar unter:

**0 18 05 / 26 26 47**

---

Schließen

## Neues in Cyber Patrol

**Cyber Patrol 3.1** umfaßt folgende Funktionen:

[Proxy Server einrichten](#)

[Automatische Downloads aktivieren/deaktivieren](#)

---

**Cyber Patrol 3.0** umfaßt folgende Funktionen:

[Automatische Zugangskennwortabfrage](#)

[ChatGard](#)

[Beschreibung der CyberNOT-Kategorien](#)

[CyberYES-Liste](#)

[Filter für Domänen](#)

[Cyber Patrol-Symbol](#)

[Sperrmeldungen und -codes](#)

[Mehrere Benutzer einrichten](#)

[Profile ausdrucken](#)

[PICS-Bewertungsstandard: RSACi](#)

[Das Dialogfeld Bereichsbeschränkungen für SafeSurf SS~~](#)

[Änderungen der Systemfunktionen](#)

[Systembeschränkungen](#)

[Akustisches Signal](#)

## Änderungen der Systemfunktionen

Folgende Systemfunktionen haben sich geändert:

- Als "Zusätzlich erlaubte Bereiche" aufgeführte Sites werden nun grundsätzlich zugelassen. Bisher war es möglich, daß in diesem Feld aufgeführte Sites aufgrund von IRC-Sperrphrasen oder SafeSurf PICS-Bewertungsstandards dennoch gesperrt wurden.
- Spiele & Anwendungen unterstützt nun 32-Bit-Anwendungen.
- Cyber Patrol kann nun auch mit 32-Bit-Browsern verwendet werden.
- Es sind mehr Einträge pro Liste und mehr Zeichen pro Eintrag möglich.
- Die Aktualisierung der CyberNOT- und CyberYES-Listen nimmt weniger Zeit in Anspruch. Sie bemerken diese erhöhte Geschwindigkeit z. B., wenn Sie in den Dialogfeldern *WWW, FTP & andere Dienste* oder *Newsgroup-Kontrolle* den Feldern *Zusätzlich erlaubte Bereiche* oder *Zusätzlich gesperrte Bereiche* Bereiche hinzufügen.
- Mit der Option Nutzungsprofil (gesamt) wird nun die Nutzung aller im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen angezeigt.



## **Cyber Patrol für Fun Online - Inhalt der Hilfe**

### **Erste Schritte**

"Welche Schritte führe ich zuerst aus?" und weitere Fragen für neue Benutzer.

### **Cyber Patrol registrieren**

Wie registriere ich mich bei Cyber Patrol?

### **Filtermöglichkeiten**

Aktivierung von Filtern und Anpassung der Filter an die persönlichen Bedürfnisse. Umgang mit den Cyber-Listen. Überwachung von Spielen und Anwendungen.

### **Zeit-Management**

Festlegung der Nutzungsdauer.

### **Online- und Druckprofile**

Verwendung von Grafiken online und Drucken von Internet Nutzungsprofilen.

### **Mit Cyber Central verbinden**

Kundendienstleistungen, die Sie bei der Benutzung und Pflege von Cyber Patrol in Anspruch nehmen können.

### **Referenzhinweise**

Beschreibung der Dialogfelder und Menüs von Cyber Patrol.

## Neues in Cyber Patrol

Schließen

## Referenzhinweise

[Regeln für den Internet-Zugang](#)

[Hacker-Schutz](#)

---

### Optionen des Menüs *Datei*

[Internet-Nutzungsprofil drucken](#)

[Steuerpult drucken](#)

[Kennwörter festlegen](#)

[Freigabe für Assistent](#)

[Internet sperren](#)

[Automatischen Empfang aktivieren/deaktivieren](#)

[CyberNOT-Liste aktualisieren](#)

[Benutzer \[Benutzername\] als ...](#)

[Cyber Patrol deinstallieren](#)

---

### Optionen des Menüs *Inspektion*

[Bereichsbeschränkungen](#)

[SafeSurf SS~~ Beschränkungen festlegen](#)

[RSACi Beschränkungen festlegen](#)

[Filter für Domäne auswählen](#)

[Internet Relay Chat](#)

[ChatGard Einstellung](#)

[WWW, FTP & andere](#)

[Newsgroups](#)

[Spiele & Anwendungen](#)

---

### Optionen des Menüs *Optionen*

[Proxy- & SOCKS-Einstellungen](#)

[Online-Registrierung](#)

[Fehlerberichte / Kommentare online](#)

[Inspektionsmeldung](#)

[Nutzungsprofile](#)

[Symbol ausblenden](#)

---

### Das Cyber Patrol-Symbol

[Das Symbolmenü und die Symbole von Cyber Patrol](#)

[Das Dialogfeld Cyber Patrol-Berechtigungsabfrage](#)

[Das Dialogfeld Cyber Patrol benutzerdefinierte Berechtigungsabfrage](#)



## Erste Schritte

### Einführung

[Funktionen von Cyber Patrol](#)

Liste mit Cyber Patrol Funktionen.

[Was neue Benutzer wissen sollten](#)

Antworten auf die von neuen Benutzern häufig gestellten Fragen.

[Welche Möglichkeiten bietet Ihnen Cyber Patrol?](#)

Gründe, warum Cyber Patrol Ihnen helfen kann, Ihre private und geschäftliche Umgebung zu schützen.

---

### Benutzer und Kennwörter

[Das Dialogfeld Cyber Patrol-Kennwörter](#)

Einstellung des [Steuerpults](#) und Festlegung der Kennwörter der [Assistenten](#).

[Mehrere Benutzer einrichten](#)

Festlegung von Benutzernamen und [Zugangskennwörtern](#).

---

### Installation

[Die Cyber Patrol Installation überprüfen](#)

Informationen dazu, wie sich überprüfen lässt, ob Internet-Sites wie gewünscht gesperrt werden.

[Cyber Patrol deinstallieren](#)

Informationen dazu, wie sich Cyber Patrol *leicht* und *sicher* löschen lässt.

[Das Dialogfeld Proxy- & SOCKS-Einstellungen](#)

Informationen dazu, wie Sie Cyber Patrol konfigurieren müssen, damit Sie mit einer [Firewall](#) arbeiten können.

[Cyber Patrol erneut installieren und aktualisieren](#)

Informationen dazu, wie Sie Cyber Patrol erneut installieren oder Ihre alte Version aktualisieren können.

---

### Cyber Patrol-Symbol und Symbolmenü

[Das Symbolmenü und die Symbole von Cyber Patrol](#)

Bedeutung der verschiedenen Varianten des Cyber Patrol-Symbols. Verwendung des Symbolmenüs von Cyber Patrol.

[Cyber Patrol-Beschränkungen freigeben](#)

Informationen darüber, wie Sie auf das Internet zugreifen können, ohne der Cyber Patrol-Kontrolle zu unterliegen.

[Gesamten Internet-Zugang sperren](#)

Informationen darüber, wie Sie den Internet-Zugang für jeden anderen Benutzer sperren können.

[Steuerpult beenden und Cyber Patrol schließen](#)

Informationen darüber, wie Sie die Überwachung durch Cyber Patrol beenden können.

---

### Anmerkungen und Empfehlungen

[So senden Sie uns Ihre Anmerkungen und Empfehlungen](#)

Gerne nehmen wir Ihre Anregungen, Vorschläge und Fehlerberichte entgegen!



## Was neue Benutzer wissen sollten

### Wie starte ich Cyber Patrol?

Cyber Patrol wird nach der Installation automatisch gestartet.

Unter Windows 3.1 wird das Cyber Patrol-Symbol links oben auf Ihrem Desktop angezeigt. Möglicherweise wird es von anderen Fenstern verdeckt. Sie können das Symbol auf dem Desktop an eine beliebige Stelle ziehen. Klicken Sie mit der linken Maustaste auf das Symbol, um das Cyber Patrol-Symbolmenü anzeigen zu lassen.

Unter Windows 95 wird Cyber Patrol in der Windows 95 Task-Leiste angezeigt. Klicken Sie mit der rechten Maustaste auf das Symbol in der Task-Leiste, um das Cyber Patrol-Symbolmenü anzeigen zu lassen.

---

### Voreinstellungen

- **Kennwort**  
Cyber Patrol wird mit einem speziell für Sie vergebenen Kennwort ausgeliefert, welches Sie bei unserer [Hotline](#) erfragen können. Es ist empfehlenswert, so bald wie möglich sich eigene Kennwörter zu vergeben. **Lesen Sie auch:** [Cyber Patrol-Kennwörter](#)
- **Zugangsbeschränkungen**  
Cyber Patrol wird mit voreingestellten Zugangsbeschränkungen hinsichtlich zulässiger Betriebszeiten, täglicher und wöchentlicher Nutzungsdauer sowie inhaltlich problematischer Bereiche ausgeliefert. Wenn Sie Cyber Patrol während einer nicht erlaubten Tageszeit installieren, müssen Sie zuerst den Internet-Zugang freigeben.  
Wenn Sie die Einstellungen ändern möchten, **gehen Sie zu:** [Zeit-Management](#) und [Filtermöglichkeiten](#).

---

### Was passiert, wenn jemand die Cyber Patrol-Dateien manipuliert?

- Lesen Sie auch:** [Cyber Patrol deinstallieren](#)  
[Hacker-Schutz](#)  
[Cyber Patrol erneut installieren oder aktualisieren](#)

---

### Wie kann ich die Cyber Patrol-Zugangsbeschränkungen freigeben?

Freigeben von Cyber Patrol:

1. Klicken Sie einmal auf das minimierte Cyber Patrol-Symbol.  
**Ergebnis:** Sie sehen das Cyber Patrol-Symbolmenü.
2. Wählen Sie die Option *Freigabe für Assistent*.  
**Ergebnis:** Sie sehen das Dialogfeld *Cyber Patrol-Berechtigungsabfrage* und werden nach einem Kennwort gefragt.
3. Geben Sie IHR Kennwort ein. Haben Sie sich noch kein eigenes Kennwort vergeben, so fragen Sie bei unserer [Hotline](#) nach Ihrem persönlichen Kennwort. Klicken Sie auf die Schaltfläche *Kennwort prüfen*, oder drücken Sie die Eingabetaste.  
**Ergebnis:** Das Cyber Patrol-Symbol ändert sich in ein *rotes "X" auf einem blauweißen "P"*, und Sie haben freien Internet-Zugang.

---

### Was bedeutet es, wenn das "P" des Cyber Patrol-Symbols rot ist und die Internet-Dienste gesperrt werden?

Wenn nach der Installation von Cyber Patrol das Cyber Patrol-Symbol als rotweißes "P" angezeigt wird, haben Sie die Installation während einer zugriffsbeschränkten Zeit durchgeführt. Sie haben dann die Möglichkeit, die Zugangsbeschränkungen mit Hilfe der Option *Freigabe für Assistent* zu umgehen oder im Cyber Patrol-Steuerpult die Einstellungen für die Nutzungsdauer zu ändern.

---

### **Wie öffne ich das Cyber Patrol-Steuerpult?**

1. Klicken Sie auf das minimierte Cyber Patrol-Symbol.

**Ergebnis:** Sie werden im Dialogfeld *Cyber Patrol-Berechtigungsabfrage* nach einem Kennwort gefragt.

2. Geben Sie IHR Kennwort ein. Haben Sie sich noch kein eigenes Kennwort vergeben, so fragen Sie bei unserer [Hotline](#) nach Ihrem persönlichen Kennwort. Klicken Sie auf die Schaltfläche *Kennwort prüfen*, oder drücken Sie die Eingabetaste.

**Ergebnis:** Sie befinden sich im Cyber Patrol-Steuerpult. Dort können Sie u.a. die Einstellungen verändern, Nutzungsprofile und Grafiken anzeigen sowie Kennwörter festlegen.

---

### **Wie vergebe ich Zugangs- und Assistentenkennwörter?**

Zur Vergabe dieser beiden Kennwörter wählen Sie im Steuerpult aus dem Menü *Datei* den Befehl *Kennwörter festlegen*. Im nun angezeigten Dialogfeld können Sie zwei Kennwörter vergeben:

- Das Zugangskennwort wird zur Änderung der Cyber Patrol-Einstellungen benötigt.
  - Das Assistentenkennwort ermöglicht eine Umgehung der Cyber Patrol-Zugangsbeschränkungen und damit unbegrenzten Internet-Zugang.
- 

### **Löschen des Browser-Cachespeichers**

Nach einer freien Internet-Sitzung dürfen Sie niemals vergessen, den Cachespeicher Ihres Browsers zu löschen, damit Ihr Kind keinen Zugang zu den von Ihnen bei Ihrer letzten Internet-Sitzung gespeicherten Seiten hat.

**Lesen Sie auch:** [Auf dem Rechner gespeicherte Daten löschen](#)

## Regeln für den Internet-Zugang

**Cyber Patrol erlaubt den Zugriff auf eine Internet-Site, wenn:**

- ▶ die Gesamtstundenzahl pro Woche NICHT überschritten wurde UND
- ▶ die Gesamtstundenzahl pro Tag NICHT überschritten wurde UND
- ▶ sich die aktuelle Zeit mit der erlaubten Betriebszeit deckt UND
- ▶ eine der folgenden Bedingungen erfüllt ist:
  1. *Der Zugang zu dem spezifischen Internet-Dienst ist auf Voll gesetzt.*  
- ODER -
  2. *Der Zugang zu dem spezifischen Internet-Dienst ist auf Selektiv gesetzt, und Sie haben die Site in die Liste Erlaubte Chat Groups eingefügt.*  
- ODER -
  3. *Der Zugang zu dem spezifischen Internet-Dienst ist auf Selektiv gesetzt, und Sie haben die Site nicht ausdrücklich eingeschränkt und entweder:*
    - wird die Site NICHT in der CyberNOT-Liste unter einer der gewählten Bereichsbeschränkungen aufgeführt, oder
    - der Site-Name enthält keine IRC-Sperrphrase.

## Hacker-Schutz

Cyber Patrol ist mit einem zweistufigem Sicherheitssystem ausgestattet:

- **Hohe Sicherheit (empfohlen)**  
Bei hoher Sicherheitsstufe interpretiert Cyber Patrol jeden Versuch, die Cyber Patrol-Dateien zu löschen oder zu verändern, als unerlaubte Manipulation. Diese Sicherheitsstufe soll Kinder oder Schüler davon abhalten, den Cyber Patrol-Schutz ohne Autorisierung zu entfernen. Wenn Sie diese Sicherheitsstufe wählen, können Sie nur mit dem Cyber Patrol-Befehl *Deinstallieren* die Cyber Patrol-Dateien von Ihrem Computer-System entfernen.
- **Niedrige/Mittlere Sicherheit**  
Bei niedriger/mittlerer Sicherheitsstufe können Sie die Cyber Patrol-Dateien und Symbole ohne den Cyber Patrol-Befehl *Deinstallieren* von Ihrem System entfernen. (Deinstallieren wird jedoch empfohlen.)

Bei der Installation von Cyber Patrol bestimmen Sie, welche Sicherheitsstufe implementiert wird. Bei der Installation von Fun Online - Das Netz ist automatisch die hohe Sicherheitsstufe eingestellt.

---

### Hohe Sicherheit: Cyber Patrol-Dateien dürfen NICHT gelöscht oder verändert werden

**Warnung!** Cyber Patrol wurde mit einem ausgeklügelten **Hacker-Schutz** ausgestattet. Cyber Patrol-Dateien dürfen NICHT gelöscht oder geändert werden, da Cyber Patrol dies sonst als unerlaubte Manipulation interpretieren würde.

---

### Was passiert, wenn Cyber Patrol eine unerlaubte Manipulation erkennt?

Wenn Cyber Patrol unerlaubte Manipulationen erkennt, deaktiviert es den Internet-Zugang. Methoden zur Wiederherstellung erfahren Sie von der [Hotline](#).

Abhängig davon, welche unerlaubten Änderungen vorgenommen wurden, kann Cyber Patrol auch den Zugriff auf Windows sperren.

**Hinweis für Windows 95:** Wenn der Zugriff auf Windows gesperrt wurde, ist für eine Wiederherstellung eventuell eine Neuinstallation von Windows 95 notwendig.

## Auf dem Rechner gespeicherte Daten löschen

Einige Internet-Browser speichern bestimmte Materialien auf der Festplatte Ihres Computers. Wenn Sie Cyber Patrol implementieren, sollten Sie sicherstellen, daß eventuell anstößiges Material von der Festplatte Ihres Computers gelöscht wird oder Ihre Kinder darauf keinen Zugriff haben.

Einige Beispiele dafür sind:

- ▶ **Cache des Web-Browsers löschen**

Microsoft Internet Explorer und einige andere Internet-Browser speichern Daten, die in der letzten Zeit gelesen wurden, in einem **Cache**-Bereich auf der Festplatte Ihres Computers. Löschen Sie den lokalen Cache, bevor Sie Cyber Patrol einsetzen.

- ▶ **Heruntergeladene Nachrichten sperren**

Agent und einige andere Hilfsprogramme für den Internet-Zugang laden Nachrichten auf Ihren Computer herunter, damit sie offline gelesen werden können. Sie können den Zugriff Ihrer Kinder auf Agent sperren.

## Cache des Web-Browsers löschen

Einige Internet-Browser, z. B. Microsoft Internet Explorer, speichern die zuletzt geladenen Web-Seiten in einem sogenannten Cache auf der Festplatte Ihres Computers. Wenn Sie die Sperrliste von Cyber Patrol ändern und einen Browser verwenden, löschen Sie unbedingt den lokalen Cache des Browsers sowohl auf der Festplatte als auch im Arbeitsspeicher um die neue Cyber Patrol-Konfiguration zu aktivieren. Dadurch wird verhindert, daß Ihre Kinder unter Umständen anstößiges Material aus dem Cache lesen.

Löschen Sie den Cache außerdem immer, wenn Sie die Einstellungen für Cyber Patrol ändern.

---

### **Beispiel: So löschen Sie den Cache des Internet Explorers**

Wenn Sie z. B. Microsoft Internet Explorer verwenden, löschen Sie den lokalen Cache wie folgt:

1. Wählen Sie aus dem Internet Explorer Menü *Ansicht* den Eintrag *Optionen*.
2. Klicken Sie im Fenster *Optionen* auf die Registerkarte *Erweitert*.
3. Klicken Sie im Bereich *Temporäre Internet-Dateien* auf die Schaltfläche *Einstellungen*.
4. Klicken Sie im Dialogfeld *Einstellungen* auf die Schaltfläche *Ordner leeren*. Daraufhin wird der Cache gelöscht. Dieser Vorgang kann einige Zeit in Anspruch nehmen.

## Heruntergeladene Nachrichten sperren

Agent und einige andere Hilfsprogramme für den Internet-Zugriff laden Nachrichten auf die Festplatte Ihres Computers, damit sie offline gelesen werden können. Sobald Nachrichten auf die Festplatte Ihres Computers heruntergeladen wurden, sind sie nicht mehr durch die Standardeinstellungen für den Internet-Zugriff von Cyber Patrol geschützt. Statt dessen können Sie den Zugriff auf diese Daten beschränken, indem Sie die Benutzung des Hilfsprogramms für den Internet-Zugriff vollständig für Ihre Kinder sperren (eventuell ist es nötig, ein separates Hilfsprogramm für den Internet-Zugriff für ihre Zwecke zu installieren).

---

### So sperren Sie die Benutzung des Hilfsprogramms für den Internet-Zugriff:

1. Markieren Sie im Dialogfeld *Cyber-Patrol-Steuerpult für Spiele & Anwendungen* das Optionsfeld *Kein*.  
**Grund:** Sie sperren damit den Zugriff auf alle Anwendungen aus der Liste der Spiele und Anwendungen.
1. Wählen Sie aus dem Menü *Inspektion* die Option *Spiele & Anwendungen*.
3. Geben Sie das Hilfsprogramm in das Dialogfeld [Spiele & Anwendungen](#) ein (klicken Sie auf die Schaltfläche *Hilfe* im Dialogfeld, um weitere Informationen anzuzeigen), und speichern Sie Ihre Änderungen.

## Welche Möglichkeiten bietet Ihnen Cyber Patrol?

Das Internet oder Cyberspace, wie es manchmal genannt wird, ist eine Umgebung für Informationen, Ressourcen, Referenzmaterialien, bietet Möglichkeiten, anderen Menschen zu begegnen, und steht Teilnehmern in der ganzen Welt zur Verfügung.

Allerdings ist das Internet eine offene Umgebung ..., d. h. es gibt Gutes aber auch Schlechtes, wie überall auf der Welt. Deshalb gibt es im Internet auch Dateien, deren Inhalt für Kinder nicht geeignet ist, oder die sich Ihre Mitarbeiter nicht während der Arbeitszeit ansehen sollten. Ebenso sollten sich Teilnehmer über das Internet miteinander unterhalten können, ohne dabei irgendwelche persönlichen Informationen preisgeben zu müssen.

Cyber Patrol wurde entwickelt, um den Zugang zum Internet sinnvoll zu beschränken und um Ihnen zu helfen, die Internet-Umgebung zu kontrollieren und Ihre Kinder zu schützen.

▶ Weitere Informationen zu den verschiedenen Schutztypen, die von Cyber Patrol angeboten werden, finden Sie unter [Funktionen von Cyber Patrol](#).

▶ Weitere Informationen zu den Regeln für den Internet-Zugriff von Cyber Patrol finden Sie unter [Regeln für den Internet-Zugriff](#)

---

**Lesen Sie auch:** [So schützen Sie Ihre Kinder](#)

## So schützen Sie Ihre Kinder

Da immer mehr Kinder PCs für ihre Ausbildung oder zum Spielen benutzen, wird die Verwendung von Programmen, die die Benutzung von PCs durch Kinder sinnvoll kontrollieren, immer wichtiger. Es reicht aber nicht aus, wenn diese Programme lediglich den Zugang zu Online-Diensten und dem immer populärer werdenden Internet steuern. Eine Überwachung anderer Programme, z. B. von Computerspielen oder Dienstprogrammen von Online-Diensten (z. B. CompuServe oder America Online) ist ebenso notwendig. Ziel der entsprechenden Kontrollprogramme ist es, daß Kinder Computer für produktive Zwecke einsetzen. Ohne ein solches Kontrollprogramm könnten Ihre Kinder Zugang zu für sie ungeeignete Materialien erhalten oder übermäßig viel Zeit beim Spielen oder in den Online-Diensten zubringen.

Zum Lieferumfang vieler Computer, die heute verkauft werden, gehört ein Modem und die zunächst kostenlose Anmeldung bei Online-Diensten, CompuServe, America Online und anderen. Viele Eltern wünschen sich aber, daß ihre Kinder den Computer optimal und sinnvoll nutzen.

Wenn Ihre Kinder mit dem Internet oder einem Online-Dienst verbunden sind und dabei die vielfältigen Online-Informationen durchforsten, die Tiefen eines Computer-Programms erkunden oder ein spannendes Computerspiel spielen, können sie Zeit und Raum leicht vergessen. Dann kann der Computer den Fernseher leicht ersetzen. Sicher empfinden Sie es als positiv, daß Ihr Kind, anstatt unzählige Stunden passiv vor dem Fernseher zu verbringen, seine Kreativität erprobt und seine Computer-Kenntnisse vertieft.

Es wäre zu einfach, Ihrem Kind völlige Freiheit bei der Beschäftigung mit Online-Diensten, dem Internet und Computerspielen zu lassen. Denn so wie Sie überwachen, wieviel Zeit ihre Kinder vor dem Fernseher verbringen und welche Sendungen sie sich ansehen, so sollten Sie auch nicht einfach darauf vertrauen, daß über Online-Dienste ausschließlich für Kinder geeignetes Material verfügbar ist. Achten Sie auch darauf, daß Ihre Kinder nicht übermäßig viel Zeit mit einem Computerspiel verbringen oder stundenlang in einem Online-Dienst zubringen.

Sie können Verschiedenes tun, um zu kontrollieren, wie Ihr Kind den Computer verwendet. Folgende Tips sollen dazu beitragen, daß sich Ihre Kinder auf solche Aktivitäten konzentrieren, die sie weiterbilden und die Spaß machen:

- **Regeln festlegen**  
Sie sollten klare Regeln für Ihre Kinder festlegen. Genauso wie Sie Ihnen beibringen, das Telefon zu beantworten oder sich von verdächtigen Fremden fernzuhalten, sollten Sie Ihre Kinder anweisen, nicht bereitwillig Ihre Adresse oder Telefonnummer ohne Ihre Erlaubnis preiszugeben. Sie sollten auch die Zeiten festlegen, zu denen das Kind einen Online-Dienst oder ein Computerspiel benutzen darf. Sie sollten Ihren Kindern beispielsweise nicht erlauben, auch nach der Zeit zum Schlafengehen Computerspiele zu spielen.
- **Ständigen Dialog fördern**  
Ermutigen Sie Ihr Kind, davon zu berichten, was es im Netzwerk erlebt hat, welche Unterhaltungen es mit anderen geführt und welche interessanten Dinge es in der letzten Zeit im Netzwerk gefunden hat. Während Sie erfahren, was Ihre Kinder tun, können Sie ihr Verhalten, ihre Art den Computer zu benutzen und die Verbindungen zu Online-Diensten korrigieren und abstimmen.
- **Online-Gewohnheiten Ihrer Kinder überwachen**  
Verbringen Sie Zeit mit Ihren Kindern, während Sie das Netzwerk oder ein Computerspiel erforschen. Lassen Sie sich von Ihren Kindern zeigen, was sie gemacht haben.
- **Den Zugang Ihrer Kinder mit Hilfsprogrammen kontrollieren**  
Cyber Patrol wurde entwickelt, um beobachten zu können, auf welche Bereiche ihr Kind gewöhnlich zugreifen möchte. Wenn ein Kind versucht, in einen Bereich zu gelangen, der eingeschränkt wurde, weil er für Kinder ungeeignetes Material enthält oder versucht, ein Spiel über eine sinnvolle Zeitdauer hinaus zu spielen, wird es durch eine Sperre daran gehindert.

Wir hoffen, daß es Ihnen gelingt, mit Hilfe der oben beschriebenen Vorschläge und einem Hilfsprogramm wie Cyber Patrol die Aktivitäten Ihrer Kinder im Netzwerk zu überwachen. Sie und Ihre Kinder werden

durch viele angenehme und sichere Stunden bei der Erforschung der Online-Informationdienste und anderer Computerprogramme belohnt.

## Funktionen von Cyber Patrol

Mit Cyber Patrol können Sie den Internet-Zugang kontrollieren.

- Sie können den Zugang begrenzen auf:
  - Tageszeit
  - Gesamtstunden pro Tag
  - Gesamtstunden pro Woche
- Sie können den Zugang zu folgenden Diensten/Programmen einschränken/sperrern:
  - Arten der Internet-Dienste, z. B. Internet Relay Chat (IRC)
  - Internet-Sites mit anstößigem Material (auf Grundlage der Master-CyberNOT-Liste, die Sie zum Schutz Ihrer Kinder ergänzen und überschreiben können)
  - Provider von Online-Diensten, z. B. CompuServe oder America Online
  - Spiele oder andere Anwendungen, die sich auf Ihrem Computer befinden.
- Sie können jedoch allen, denen Sie das Assistentenkennwort geben, unbegrenzten Internet-Zugang gewähren.

## Die Cyber Patrol Installation überprüfen

Nach der Installation von Cyber Patrol können Sie auf folgende Weise testen, ob Internet-Sites wie gewünscht gesperrt werden.

---

### Sperrt Cyber Patrol den Internet-Zugang korrekt?

**Test:** Versuchen Sie, auf die Cyber Patrol-Testsite zuzugreifen:

**HTTP://www.microsys.com/TEST/**

**Erwartetes Ergebnis:** Sie sollten eine Cyber Patrol [Sperrmeldung](#) erhalten.

---

### Können Sie die Zugangsbeschränkung für die Cyber Patrol-Testsite freigeben?

**Test:** Versuchen Sie, die Cyber Patrol-Zugangsbeschränkungen freizugeben.

- Klicken Sie auf das Cyber Patrol-Symbol.
- Wählen Sie die Option *Freigabe für Assistent*.
- Geben Sie im Dialogfeld *Cyber Patrol Kennwortabfrage* das Zugangs- oder Assistentenkennwort ein, und klicken Sie dann auf die Schaltfläche *Kennwort prüfen*.
- Versuchen Sie, auf die Cyber Patrol-Testsite zuzugreifen: **HTTP://www.microsys.com/TEST/**

**Erwartetes Ergebnis:** Sie sollten die Webseite **Cyber Patrol Test Restriction (Zugangsbeschränkung durch Cyber Patrol)** sehen.

---

### Löschen des Browser-Cachespeichers

Vergessen Sie nach einer freien Internet-Sitzung niemals, den Cachespeicher Ihres Browsers (z. B. Microsoft Internet Explorer) zu löschen, damit die darin gespeicherten Informationen gelöscht werden.

Lesen Sie auch: [Auf dem Rechner gespeicherte Daten löschen](#)

---

## Das Dialogfeld Proxy- & SOCKS-Einstellungen

Im Dialogfeld *Proxy- & SOCKS-Einstellungen* geben Sie Informationen ein, mit deren Hilfe Cyber Patrol die [Firewall](#)-Konfiguration passieren kann.

---

### So geben Sie die Proxy- & SOCKS-Einstellungen ein:

Tragen Sie in folgende Felder Informationen ein:

#### **Proxy-Server Adresse:**

Geben Sie die [IP](#)- oder [URL](#)-Adresse des Proxy-Servers ein, auf den vom lokalen Netzwerk aus zugegriffen werden kann.

#### **Proxy-Portnummer:**

Geben Sie die vom Proxy Server bei der Kommunikation mit Winsock verwendete [Service Portnummer](#) ein.

#### **SOCKS-Server Adresse:**

Geben Sie die IP- oder URL-Adresse des SOCKS-kompatiblen Servers ein, auf den vom lokalen Netzwerk aus zugegriffen werden kann.

#### **SOCKS-Portnummer:**

Geben Sie die vom SOCKS-kompatiblen Server bei der Kommunikation mit Winsocks verwendete Port-Nummer ein.

#### **SOCKS-Accountname:**

Geben Sie Ihren SOCKS-Accountnamen ein.

und klicken Sie auf die Schaltfläche *Einstellungen speichern*.

## Das Dialogfeld *Cyber Patrol benutzerdefinierte Berechtigungsabfrage*

Im Dialogfeld *Cyber Patrol benutzerdefinierte Berechtigungsabfrage* melden Sie sich bei Cyber Patrol als definierter Benutzer an.

Geben Sie Ihren Benutzernamen und Ihr Zugangskennwort ein, und klicken Sie anschließend auf eine der beiden Schaltflächen:

- **Kennwort prüfen**

Klicken Sie auf diese Schaltfläche, um sich bei Cyber Patrol anzumelden.

- **Abfrage beenden**

Klicken Sie auf diese Schaltfläche, um das Dialogfeld *Cyber Patrol benutzerdefinierte Berechtigungsabfrage* zu schließen.

---

### Wann wird dieses Dialogfeld angezeigt?

Dieses Dialogfeld wird nur dann angezeigt, wenn Sie mehrere Benutzer (nicht nur den einen Standard-Benutzer) als Benutzer für Cyber Patrol eingerichtet haben.

Ist dies der Fall, wird es bei folgenden Aktionen automatisch aufgerufen:

- Wenn ein Benutzer auf das Internet zugreift (d. h. wenn der Browser oder Dialer die Winsock lädt).
- Beim Programmaufruf von Cyber Patrol (gewöhnlich wird Cyber Patrol beim Start von Windows aufgerufen).

Sie können dieses Dialogfeld mit Hilfe des Dialogfelds *Benutzer festlegen* deaktivieren. **Lesen Sie auch:** [Mehrere Benutzer einrichten](#).

## Das Dialogfeld *Cyber Patrol-Berechtigungsabfrage*

Im Dialogfeld *Cyber-Patrol-Berechtigungsabfrage* tragen Sie Ihr Kennwort ein, um mit Cyber Patrol zu arbeiten oder die Zugriffskontrolle freizugeben.

Nachdem Sie Ihr Kennwort eingegeben haben, klicken Sie auf eine der folgenden Schaltflächen:

• **Kennwort prüfen**

Klicken Sie auf diese Schaltfläche, um die Aktion durchzuführen, die Sie gerade begonnen haben. Klicken Sie z. B. auf diese Schaltfläche, um das Steuerpult zu öffnen, Cyber Patrol freizugeben oder andere Symbolmenü-Optionen von Cyber Patrol auszuführen.

• **Abfrage beenden**

Klicken Sie auf diese Schaltfläche, um das Dialogfeld *Cyber Patrol-Berechtigungsabfrage* ohne weitere Aktionen zu verlassen.

---

**Lesen Sie auch:**     [Kennwörter festlegen](#)

## Das Dialogfeld *Cyber Patrol-Kennwörter*

### Cyber Patrol-Kennwörter

Bei Cyber Patrol gibt es verschiedene Arten von Kennwörtern.

[Zugangskennwort](#)

[Assistentenkennwort](#)

[Anmeldekennwort](#)

Die Zugangs- und Assistentenkennwörter legen Sie im Dialogfeld *Cyber Patrol-Kennwörter* fest. Die Anmeldekennwörter der einzelnen Benutzer werden im Dialogfeld [Benutzer festlegen](#) definiert.

---

### So legen Sie ein Kennwort fest oder verändern es

Gehen Sie wie folgt vor, um ein Kennwort festzulegen oder zu verändern:

1. Öffnen Sie das Cyber Patrol-Steuerpult.
2. Wählen Sie aus dem Menü *Datei* die Option *Kennwörter festlegen*.
3. Geben Sie im nun angezeigten Dialogfeld *Cyber Patrol-Kennwörter* die gewünschten Kennwörter ein.
4. Klicken Sie auf *OK*, um Ihre Auswahl zu speichern.

---

### Regeln für Kennwörter

Kennwörter können aus Buchstaben und Ziffern bestehen.

Obwohl Kennwörter aus einer beliebig langen Buchstaben- oder Zahlenfolge bestehen können, werden nur die ersten 8 Zeichen von Cyber Patrol benutzt.

---

**Lesen Sie auch:** [Informationen zu Kennwörtern](#)

## Kennwörter festlegen

Gehen Sie wie folgt vor, um Kennwörter festzulegen oder zu ändern:

1. Wählen Sie aus dem Menü *Datei* den Befehl *Kennwörter festlegen*.
2. Das Dialogfeld *Cyber Patrol-Kennwörter* erscheint. Geben Sie Kennwörter Ihrer Wahl ein.
3. Klicken Sie auf *OK*, um Ihre Auswahl zu speichern.

---

**Lesen Sie auch:** [Das Dialogfeld Cyber Patrol-Kennwörter](#)

## Zugangskennwort

Mit dem Zugangskennwort können Sie alle Funktionen und Programme von Cyber Patrol aufrufen. Dazu gehören:

- das Cyber Patrol-Steuerpult,
- alle Symbol-Menüoptionen von Cyber Patrol und
- Freigabe von Cyber Patrol-Einschränkungen.

Beispiel: Eltern, die die Cyber Patrol-Kontrolle einrichten, benutzen das Zugangskennwort.

## Assistentenkennwort

Mit dem Assistentenkennwort können Sie das Cyber Patrol-Steuerpult nicht aufrufen. Sie können jedoch alle Symbol-Menüoptionen von Cyber Patrol benutzen. Dazu gehören:

- Festlegen der Option *Internet-Zugang sperren*,
- Freigabe einer Sperrmeldung
- Freigabe von Cyber Patrol-Beschränkungen.

Beispiel: Eventuell wollen Sie älteren Jugendlichen ungeschützten Internet-Zugang gewähren, jedoch die Kontrollen für jüngere Kinder aufrechterhalten. Geben Sie in diesem Fall älteren Jugendlichen das Assistentenkennwort. Behalten Sie jedoch das Zugangskennwort für sich, damit ältere Jugendliche nicht die Cyber Patrol-Zugriffskontrolle ändern können.

## **Benutzerdefinierte Zugangskennwörter**

Bei der Festlegung verschiedener Profile für die einzelnen Benutzer Ihres Rechners weisen Sie jedem Benutzer einen eindeutigen Namen und ein eindeutiges Zugangskennwort zu. Meldet sich ein Benutzer dann mit seinem Namen und seinem eindeutigen Kennwort bei Cyber Patrol an, gelten für ihn die von Ihnen festgelegten Einstellungen.

## Informationen zu Kennwörtern

Wählen Sie Ihre Kennwörter sorgfältig. Wählen Sie kein Kennwort, das jemand, der Sie gut kennt oder Ihren Computer benutzt, erraten könnte. Benutzen Sie z. B. nicht Ihre Telefonnummer, den zweiten Vornamen, die Lieblingsfernsehserie oder ein anderes geläufiges Wort.

Merken Sie sich das Kennwort. (Stellen Sie sicher, daß das von Ihnen notierte Kennwort nicht gefunden werden kann!) Sollten Sie jedoch Ihr Zugangskennwort vergessen, wenden Sie sich bitte an die [Hotline](#).

## Cyber Patrol deinstallieren

Um Cyber Patrol zu deinstallieren, wählen Sie aus dem Menü *Datei* oder aus dem Cyber Patrol-Symbolmenü den Befehl *Cyber Patrol deinstallieren*. Das Deinstallationsprogramm von Cyber Patrol entfernt Cyber Patrol vom Desktop.

Cyber Patrol hat ein ausgeklügeltes Hacker-Schutzsystem. Versuchen Sie deshalb NICHT, die Cyber Patrol-Dateien oder die Einträge in der Datei WIN.INI selbst zu entfernen. Benutzen Sie statt dessen DEINSTALLIEREN von Cyber Patrol.

## Das Symbolmenü von Cyber Patrol

## Das Symbolmenü und die Symbole von Cyber Patrol

Das Symbol "Cyber Patrol" erscheint auf dem Desktop, wenn Cyber Patrol aktiv ist. Sie können es verschieben oder hinter anderen Fenstern verbergen, aber Sie können es nur mit dem Kennwortschutz-Hilfsprogramm schließen.

---

### Das Symbolmenü von Cyber Patrol

Mit Hilfe des Symbolmenüs von Cyber Patrol können Sie das Cyber Patrol-Steuerpult öffnen und andere Funktionen von Cyber Patrol aufrufen. Weitere Informationen finden Sie unter [Das Symbolmenü und die Symbole von Cyber Patrol](#).

---

### Varianten des Cyber Patrol-Symbols

Es gibt verschiedene Versionen des Cyber Patrol-Symbols. Sie zeigen an, ob der Internet-Zugang unter der Cyber Patrol-Zugangskontrolle gerade geschützt, völlig deaktiviert oder freigegeben ist. Lesen Sie auch: [Varianten des Cyber Patrol-Symbols](#)

---

### Aktualisierung Ihrer Kopie von Cyber Patrol

Wenn das Cyber Patrol-Symbol vom normalen "P"-Symbol zu einem blauen "U"-Symbol wechselt, bedeutet dies, daß bei Cyber Central eine neuere Version von Cyber Patrol vorhanden ist. Weitere Informationen finden Sie unter: [Cyber Patrol aktualisieren](#)

---

#### Lesen Sie auch:

[Erste Schritte](#)

[Inhalt der Hilfe](#)

[Steuerpult beenden und Cyber Patrol schließen](#)

## Menüoptionen des Cyber Patrol Steuerpults

Mit dem Cyber Patrol-Symbolmenü rufen Sie das Cyber Patrol-Steuerpult auf, geben Einschränkungen durch Cyber Patrol frei oder sperren den Internet-Zugang vollständig.

---

Folgende Optionen stehen im Symbolmenü zur Verfügung:

### **Steuerpult**

Klicken Sie auf die Option *Steuerpult*, um das Cyber Patrol-Steuerpult aufzurufen. Geben Sie anschließend im Dialogfeld *Cyber Patrol Berechtigungsabfrage* das Zugangskennwort ein.

### **Schließen**

Klicken Sie auf diese Option, um das Programm "Cyber Patrol" auf dem Desktop zu beenden. Geben Sie anschließend im Dialogfeld *Cyber Patrol Berechtigungsabfrage* das Zugangskennwort ein.

### **Freigabe für Assistent**

Klicken Sie auf diese Option, um alle Einschränkungen von Cyber Patrol freizugeben. Geben Sie anschließend im Dialogfeld *Cyber Patrol Berechtigungsabfrage* entweder das Zugangs- oder Assistentenkennwort ein.

### **Internet sperren**

Klicken Sie auf diese Option, um den Internet-Zugang zu sperren. Es wird kein Internet-Zugang gewährt. Geben Sie anschließend im Dialogfeld *Cyber Patrol Berechtigungsabfrage* entweder das Zugangs- oder das Assistentenkennwort ein.

### **Deinstallieren**

Klicken Sie auf diese Option, um alle Cyber Patrol-Dateien von Ihrem PC zu entfernen. Geben Sie anschließend im Dialogfeld *Cyber Patrol Berechtigungsabfrage* das Zugangskennwort ein.

## Varianten des Cyber Patrol-Symbols

Es gibt verschiedene Varianten des Cyber Patrol-Symbols:



- Blaues und weißes "P"  
Cyber Patrol arbeitet normal.
- Rotes und weißes "P"  
Internet-Zugang ist deaktiviert. Eventuell ist der Zugang deaktiviert, weil die täglichen oder wöchentlichen Zeitbeschränkungen überschritten wurden oder der Zugang zu dieser Zeit gesperrt ist, oder weil die Option *Internet sperren* aktiviert wurde.
  - Rotes "X" auf einem blauen und weißen "P"  
Die Cyber Patrol-Zugangskontrolle wird umgangen.
- Blaues "U"  
Eine aktuellere Version von Cyber Patrol befindet sich im Cyber Central. Cyber Patrol sucht immer nach einer neueren Version, wenn Sie die CyberNOT-Liste aktualisieren. Für weiterführende Informationen lesen Sie auch: [Cyber Patrol aktualisieren](#).

---

### Lesen Sie auch:

[Mit Cyber Central verbinden](#)

[Das Symbolmenü und die Symbole von Cyber Patrol](#)

[Tägliche Zeitbegrenzungen festlegen](#)

[Wöchentliche Zeitbegrenzungen festlegen](#)

[Nutzungszeiten festlegen](#)

## Cyber Patrol-Symbol ausblenden

Sie haben die Möglichkeit, das Cyber Patrol-Symbol auf Ihrem Desktop auszublenden. Wählen Sie hierzu aus dem Menü *Optionen* den Befehl *Symbol ausblenden*.

Wenn das Symbol wieder angezeigt werden soll, wählen Sie aus dem Menü *Optionen* den Befehl *Symbol anzeigen*.

---

### **So öffnen Sie das Cyber Patrol-Steuerpult, wenn das Symbol ausgeblendet ist**

Wenn Sie das Cyber Patrol-Steuerpult bei ausgeblendetem Cyber Patrol-Symbol öffnen möchten, wählen Sie aus der Programmgruppe der Cyber Patrol-Programme die Option *Cyber Patrol*.

---

### **So schließen Sie das Cyber Patrol-Steuerpult, wenn das Symbol ausgeblendet ist**

Wenn Sie das Cyber Patrol-Steuerpult bei ausgeblendetem Cyber Patrol-Symbol schließen möchten, klicken Sie im Dialogfeld *Cyber Patrol benutzerdefinierte Berechtigungsabfrage* auf die Schaltfläche *Schließen*. Diese Schaltfläche steht nur dann zur Verfügung, wenn das Symbol ausgeblendet wurde.

---

**Lesen Sie auch:** [Das Symbolmenü und die Symbole von Cyber Patrol](#)

## Cyber Patrol-Beschränkungen freigeben

Über das Kennwort für die Freigabe für den Assistenten können Sie die Cyber Patrol-Beschränkungen freigeben oder vermeiden. Dadurch können Sie sich oder einem anderen Benutzer Ihres PCs vollen, uneingeschränkten Zugang zum Internet gewähren.



Wenn auf Ihrem PC die Freigabe für den Assistenten aktiviert ist, wird auf dem minimierten Cyber Patrol-Symbol ein großes rotes X angezeigt.

---

### So geben Sie das Kennwort für den Assistenten über das Cyber Patrol-Symbol ein:

1. Klicken Sie einmal auf das Cyber Patrol-Symbol. Das Cyber Patrol-Symbolmenü erscheint.
2. Klicken Sie auf den Befehl *Freigabe für Assistent*.
3. Wenn Sie aufgefordert werden, ein Kennwort einzugeben, geben Sie das Kennwort für den Assistenten ein.

---

### So geben Sie das Kennwort für den Assistenten über das Menü *Steuerpult* ein:

1. Wählen Sie aus dem Menü *Datei* den Befehl *Freigabe für den Assistent*. Das Cyber Patrol-Symbol ändert sich und zeigt an, daß die Cyber Patrol-Zugangskontrolle umgangen wird.

---

### Lesen Sie auch:

[Das Symbolmenü und die Symbole von Cyber Patrol](#)  
[Varianten des Cyber Patrol-Symbols](#)

## Gesamten Internet-Zugang sperren

Sie können den gesamten Internet-Zugang sperren.

---

### So sperren Sie den gesamten Internet-Zugang:

1. Klicken Sie einmal auf das Cyber Patrol-Symbol. Das Cyber Patrol-Symbolmenü erscheint.
  2. Klicken Sie auf den Befehl *Internet sperren*.
  3. Wenn Sie dazu aufgefordert werden, geben Sie entweder das [Assistenten-](#) oder [Zugangskennwort](#) ein.
- 

### So heben Sie die Vollsperrung des Internet-Zugangs auf:

1. Klicken Sie einmal auf das Cyber Patrol-Symbol. Das Cyber Patrol-Symbolmenü erscheint.
2. Klicken Sie auf den Befehl *Internet sperren*.
3. Wenn Sie dazu aufgefordert werden, geben Sie das Zugangskennwort ein.

Beachten Sie, daß Sie mit dem Assistenten-Kennwort den Internet-Zugang zwar sperren, den Zugang damit jedoch nicht erneut aktivieren können.

## Steuerpult beenden und Cyber Patrol schließen

*Beenden* und *Schließen* sind unterschiedliche Befehle.

---

Um das Cyber Patrol-Steuerpult zu beenden, wählen Sie aus dem Menü *Datei* den Befehl *Beenden*. Mit diesem Befehl wird das Cyber Patrol-Steuerpult geschlossen, aber Cyber Patrol bleibt weiter als Symbol auf dem Desktop aktiv.

---

Um Cyber Patrol vollständig zu schließen, wählen Sie den Befehl *Schließen* aus dem Cyber Patrol-Symbolmenü. Sie werden aufgefordert, das Zugangskennwort einzugeben. Mit diesem Befehl wird Cyber Patrol vollständig vom Desktop entfernt und die Überwachung durch Cyber Patrol beendet.

## Mehrere Benutzer einrichten

Sie können für bis zu 9 Benutzer oder Benutzergruppen eigene Profile in Cyber Patrol festlegen. Neben diesen Benutzern ist ein Standard-Benutzer definiert.



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.

---

### [Definition von Benutzerprofilen](#)

Informationen zur Festlegung von Benutzernamen, Zugangskennwörtern und Einstellungen.

### [Informationen zum Standard-Benutzer](#)

Eine Beschreibung der Einstellungen für den Standard-Benutzer.

### [Benutzeranmeldung bei Cyber Patrol](#)

Informationen dazu, wie sich ein Benutzer unter eigenem Benutzernamen und mit seinem eigenen Zugangskennwort bei Cyber Patrol anmeldet.

---

### **So deaktivieren Sie die automatische Aufforderung zur Benutzeranmeldung**

Wenn Sie die automatische Aufforderung zur Benutzeranmeldung deaktivieren möchten, markieren Sie im Dialogfeld *Benutzer festlegen* das Kontrollkästchen *Kennworteingabeaufforderung ausschalten*. Soll die Aufforderung zur Benutzeranmeldung automatisch angezeigt werden, entfernen Sie die Markierung aus dem Kontrollkästchen.

Weitere Informationen über die automatische Aufforderung zur Benutzeranmeldung finden Sie unter [Das Dialogfeld Cyber Patrol benutzerdefinierte Berechtigungsabfrage](#).

## Definition von Benutzerprofilen

Für jeden Benutzer wird ein eindeutiger Name und ein eindeutiges Zugangskennwort festgelegt. Der Benutzer wird anhand dieses Namens und dieses Kennworts identifiziert, und Cyber Patrol ordnet dem Benutzer ein bestimmtes Profil zu.

Ein Benutzer meldet sich mit seinem eigenen Namen und seinem Zugangskennwort bei Cyber Patrol an. Für diesen Benutzer gilt dann das für seinen Namen und sein Kennwort definierte Profil, und gemäß der Einstellungen dieses Profils werden seine Aktionen von Cyber Patrol überwacht.

*Tip: Sie sollten sich als Benutzer mit vollständigem Zugang zu allen Inhalten definieren.*

---

### Was ist ein Benutzer?

Bei einem Benutzer kann es sich um eine einzelne Person oder um eine Gruppe handeln.

Kontext	Beispiel
Zu Hause	Familienmitglieder
Schule	Klassenstufe, Projekt, Themenbereich
Unternehmen	Marketing, Technischer Kundendienst

---

### So definieren Sie einen Benutzer

Gehen Sie folgendermaßen vor, um einen Benutzer hinzuzufügen, zu entfernen oder das Zugangskennwort eines bestehenden Benutzers zu ändern:

1. Wählen Sie aus dem Menü *Datei* die Option *Benutzer [Benutzername] als ...* aus.
  2. Wählen Sie aus dem nun angezeigten Menü die Option *Benutzer festlegen*.
  3. Daraufhin wird das Dialogfeld *Benutzer festlegen* angezeigt. Wenn Sie einen neuen Benutzer hinzufügen möchten, geben Sie im Feld *Benutzer* den Namen des Benutzers ein, und drücken Sie die Eingabetaste. Wenn Sie einen Benutzer entfernen oder das Kennwort eines bestehenden Benutzers ändern möchten, wählen Sie den gewünschten Benutzernamen aus der Liste aus.
  4. Wenn Sie einen Benutzer hinzufügen oder ein Kennwort ändern, geben Sie das Kennwort des Benutzers in das Feld *Kennwort* ein, und drücken Sie die Eingabetaste.  
Bei der Eingabe des Kennworts werden nur Sternchen (\*) angezeigt. Sie haben die Möglichkeit, das tatsächliche Kennwort zu sehen, indem Sie das Kennwortfeld hervorheben.
  5. Wenn Sie einen bestehenden Benutzer entfernen, klicken Sie auf die Schaltfläche *Einträge löschen*.
  6. Nachdem Sie alle gewünschten Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche *Änderungen speichern*.
- 

### So ändern Sie ein Benutzerprofil

Gehen Sie folgendermaßen vor, um ein Benutzerprofil zu ändern:

1. Wählen Sie aus dem Menü *Datei* die Option *Benutzer [Benutzername] als ...* aus.
2. Wählen Sie aus dem nun angezeigten Menü den Benutzernamen aus.
3. Nehmen Sie in den verschiedenen Dialogfeldern die gewünschten Änderungen vor. Die von Ihnen festgelegten neuen Einstellungen gelten nur für den zuvor ausgewählten Benutzer.

Jedes Dialogfeld verfügt über eine Schaltfläche zum Sichern der Einstellungen, und für jedes Dialogfeld gelten spezielle Regeln für die Änderung der Einstellungen.



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer

festgelegt werden können.

---

**So ermöglichen Sie E-Mail-Zugang mit der CyberYES-Liste**

**Lesen Sie auch:** [Verwendung von CyberYES-Liste und E-Mail](#)

## Informationen zum Standard-Benutzer

Cyber Patrol verfügt über eine Einstellung für den Standardbenutzer.

- Der Benutzername lautet STANDARD. Ein Kennwort ist nicht erforderlich und auch nicht zulässig.
- Zu Beginn ist mit den Einstellungen für den Standardbenutzer nur ein SELEKTIVER Internet-Zugang möglich, d. h. es gelten die restriktivsten Einstellungen. Außerdem wird die CyberYES-Liste verwendet.
- Diese Standardeinstellungen können von Ihnen geändert werden.

*Tip: Die Einstellungen für den STANDARD-Benutzer sollten restriktiver sein als die der definierten Benutzer.*

---

### Automatischer Wechsel zu dem Standard-Benutzerprofil

Bei folgenden Gegebenheiten wechselt Cyber Patrol automatisch zum Standard-Benutzerprofil:

- Beim Programmaufruf von Cyber Patrol (gewöhnlich wird Cyber Patrol beim Start von Windows aufgerufen).
- Um Mitternacht.
- Wenn Sie auf das Internet zugreifen (d. h. wenn der Browser oder Dialer die Winsock lädt).

## Benutzeranmeldung bei Cyber Patrol

### Automatische Aufforderung zur Benutzeranmeldung

Immer wenn ein Benutzer auf das Internet zugreift (d. h. wenn der Browser oder Dialer die Winsock lädt), wird er zur Eingabe seines Benutzernamens und seines Kennworts aufgefordert. **Lesen Sie auch:** [Das Dialogfeld Cyber Patrol benutzerdefinierte Berechtigungsabfrage](#)

Mit Hilfe des Dialogfelds *Benutzer festlegen* können Sie die automatische Aufforderung zur Benutzeranmeldung deaktivieren. **Lesen Sie auch:** [Mehrere Benutzer einrichten](#).

---

### So wechseln Sie zum Profil eines anderen definierten Benutzers

Gehen Sie folgendermaßen vor, um bei der Anmeldung zum Profil eines anderen definierten Benutzers zu wechseln:

1. Wählen Sie aus dem Cyber Patrol-Symbolmenü die Option *Benutzerprofil wechseln* aus.
2. Wählen Sie aus dem nun angezeigten Menü den Benutzernamen aus.
3. Geben Sie im nun angezeigten Dialogfeld das Zugangs- oder Assistenkennwort ein. **Lesen Sie auch:** [Das Dialogfeld Cyber Patrol benutzerdefinierte Berechtigungsabfrage](#)

## Verwendung von CyberYES-Liste und E-Mail

Wenn für einen Benutzer die Verwendung der CyberYES-Liste festgelegt wurde, der Benutzer jedoch elektronische Post (E-Mails) versenden oder empfangen möchte, müssen Sie den Zugang zur E-Mail-Adresse dieses Benutzer in Cyber Patrol freigeben.

Wenn Sie den Zugang nicht freigeben, wird der E-Mail-Zugang dieses Benutzer durch Cyber Patrol gesperrt, weil die Adresse des Benutzers nicht in der CyberYES-Liste enthalten ist.

---

### So ermöglichen Sie E-Mail-Zugang mit der CyberYES-Liste

Gehen Sie folgendermaßen vor, um den E-Mail-Zugang für einen Benutzer freizugeben:

1. Klicken Sie im Cyber Patrol-Steuerpult auf die Schaltfläche *WWW, FTP & andere*. Daraufhin wird das Dialogfeld *WWW, FTP & andere Dienste* angezeigt.
2. Geben Sie im Feld *Zusätzlich gesperrte Bereiche* die Server-Adresse ein. (Hierbei handelt es sich um den Teil, der auf das @ folgt. Wenn Ihre E-Mail-Adresse beispielsweise **myname@xyzabc.com** lautet, geben Sie als Server-Adresse **xyzabc.com** ein.)
3. Drücken Sie die Eingabetaste.
4. Wiederholen Sie die Schritte 2 und 3 für die E-Mail-Adresse jedes Benutzers.
5. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

## Benutzereinstellungen

Folgende Einstellungen können für die einzelnen Benutzer festgelegt werden:

### Im Steuerpult

- Zugriff auf Internet-Dienste: *Voll, Kein* oder *Selektiv*
- Zeit-Management: *Ein* oder *Aus*
- Nutzungszeiten: Tageszeiten, zu denen der Internet-Zugang zugelassen bzw. gesperrt werden soll.
- Stunden pro Tage: Gesamtnutzungsdauer pro Tag.
- Stunden pro Kalenderwoche: Gesamtnutzungsdauer pro Woche.

### Im Dialogfeld Internet Relay Chat - IRC-Kontrolle

- Aktivieren oder Deaktivieren des Filters.

### Im Dialogfeld ChatGard

- Aktivieren oder Deaktivieren des Filters.

### Im Dialogfeld WWW, FTP & andere Dienste

- Auswahl der Cyber-Liste (Diese Auswahl ist nur in der Desktop-Version möglich.\*)

### Im Dialogfeld Newsgroup-Kontrolle

- Auswahl der Cyber-Liste (Diese Auswahl ist nur in der Desktop-Version möglich.\*)

### Im Dialogfeld Bereichsbeschränkungen

- Auswahl der Kategorien für die CyberNOT-Liste.

### Im Dialogfeld PICS Bereichsbeschränkungen auswählen

- Aktivieren oder Deaktivieren des Filters.
- Auswahl des Bewertungsstandards und Festlegung, wie mit Sites ohne Einstufung verfahren werden soll.

### Im Dialogfeld Bereichsbeschränkungen für SafeSurf SS

- Aktivieren oder Deaktivieren des Filters.
- Auswahl des Bewertungsstandards und Festlegung, wie mit Sites ohne Einstufung verfahren werden soll.

---

***\*Bei der LAN-Version von Cyber Patrol müssen alle Benutzer dieselbe Cyber-Liste verwenden.***

*Wenn Sie das vollständige Hilfethema anzeigen lassen möchten, klicken Sie auf das Fenster des Haupthilfethemas. Das Fenster mit dem vollständigen Hilfetext wird dann über diesem Fenster angezeigt.*

*Sie können anschließend das Fenster mit dem vollständigen Hilfetext schließen und zum Cyber Patrol-Steuerpult zurückkehren. Dieses Fenster wird jedoch so lange angezeigt, bis Sie es schließen.*



Wenn Sie die Liste dieses Fensters ausdrucken möchten, klicken Sie auf diese Schaltfläche, und wählen Sie anschließend aus dem Menü *Datei* die Option *Thema drucken*.

## Benutzereinstellungen

Folgende Einstellungen können für die einzelnen Benutzer festgelegt werden:

### Im Steuerpult

- Zugriff auf Internet-Dienste: *Voll, Kein* oder *Selektiv*
- Zeit-Management: *Ein* oder *Aus*
- Nutzungszeiten: Tageszeiten, zu denen der Internet-Zugang zugelassen bzw. gesperrt werden soll.
- Stunden pro Tage: Gesamtnutzungsdauer pro Tag.
- Stunden pro Kalenderwoche: Gesamtnutzungsdauer pro Woche.

### Im Dialogfeld Internet Relay Chat - IRC-Kontrolle

- Aktivieren oder Deaktivieren des Filters.

### Im Dialogfeld ChatGard

- Aktivieren oder Deaktivieren des Filters.

### Im Dialogfeld WWW, FTP & andere Dienste

- Auswahl der Cyber-Liste (Diese Auswahl ist nur in der Desktop-Version möglich.\*)

### Im Dialogfeld Newsgroup-Kontrolle

- Auswahl der Cyber-Liste (Diese Auswahl ist nur in der Desktop-Version möglich.\*)

### Im Dialogfeld Bereichsbeschränkungen

- Auswahl der Kategorien für die CyberNOT-Liste.

### Im Dialogfeld PICS Bereichsbeschränkungen auswählen

- Aktivieren oder Deaktivieren des Filters.
- Auswahl des Bewertungsstandards und Festlegung, wie mit Sites ohne Einstufung verfahren werden soll.

### Im Dialogfeld Bereichsbeschränkungen für SafeSurf SS

- Aktivieren oder Deaktivieren des Filters.
- Auswahl des Bewertungsstandards und Festlegung, wie mit Sites ohne Einstufung verfahren werden soll.

***\*Bei der LAN-Version von Cyber Patrol müssen alle Benutzer dieselbe Cyber-Liste verwenden.***

## • **Zeit-Management**

In Cyber Patrol stehen Ihnen folgende Zeit-Management-Funktionen zur Verfügung:

Tägliche Zeitbeschränkungen festlegen Sie können festlegen, wie lange das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen insgesamt pro Tag zugänglich sein sollen.

Wöchentlichen Zeitbeschränkungen festlegen Sie können festlegen, wie lange das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen insgesamt pro Woche zugänglich sein sollen.

Nutzungszeiten festlegen Sie können die Zeiten festlegen, während derer das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen zugänglich sind..

Zeit-Management ein-/ausschalten Sie haben die Möglichkeit, die Zeit-Management-Funktionen ein- oder auszuschalten.

---

### **Definierte Benutzerprofile**



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.

## Zeit-Management ein-/ausschalten

Das Cyber Patrol Zeit-Management bietet Ihnen folgende Möglichkeiten:

- Sie können festlegen, wie lange das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen insgesamt pro Tag zugänglich sein sollen.
- Sie können festlegen, wie lange das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen insgesamt pro Woche zugänglich sein sollen.
- Sie können die Betriebszeiten festlegen, während derer das Internet und die im Dialogfeld *Spiele & Anwendungen* aufgeführten Anwendungen zugänglich sind.

Mit Hilfe der Schaltfläche *Zeit-Mgmt.[Ein/Aus]* im Dialogfeld *Cyber Patrol-Steuerpult* können Sie die Zeit-Management-Optionen ein- oder ausschalten.

Wenn die Optionen ausgeschaltet sind, gelten keine Beschränkungen für die Dauer der Zugangszeit bzw. für die Betriebszeiten.

---

### Überschreitung des vorgegebenen Zeitlimits

Wenn das vorgegebene Zeitlimit überschritten wird oder eine zugangsbeschränkte Uhrzeit erreicht wird, wird der Internet-Zugang automatisch gesperrt.

*Hinweis: Die Verbindung zum Internet Provider (wie z. B. Fun Online oder CompuServe) wird dabei NICHT automatisch getrennt. Sie sollten daher die Verbindung nach der Zugangssperre UNBEDINGT trennen, da ansonsten hohe Telefon- und Verbindungsgebühren auf Sie zukommen können.*

Wenn Sie die Verbindung zu Ihrem Internet Provider automatisch trennen möchten, müssen Sie das Programm, mit dem Sie sich über Ihren Provider in das Internet einwählen, im Dialogfeld [Spiele & Anwendungen](#) auflisten. Außerdem müssen Sie in dem gleichen Dialogfeld den COM-Port des Programms eingeben.

Cyber Patrol gibt eine Vorwarnung, kurz bevor der Internet-Zugang aufgrund eines Zeitlimits gesperrt wird. Sie können diese Vorwarnzeit im Dialogfeld *Cyber Patrol-Steuerpult* einstellen, indem Sie im Feld *Vorwarnung* die Pfeiltasten auswählen.

Sollte das vorgegebene Zeitlimit überschritten werden, zeigt Cyber Patrol eine Nachricht an. Weitere Hilfe zu dieser Meldung finden Sie im Hilfethema [Die Meldung Vorgegebenes Zeitlimit überschritten!](#).

**Your time is up! jump**

\*\*\* do not translate this topic \*\*\*

## **Die Meldung Vorgegebenes Zeitlimit überschritten!**

Wenn das vorgegebene Zeitlimit überschritten wird oder eine zugangsbeschränkte Uhrzeit erreicht ist, wird der Internet-Zugang sofort gesperrt.

*Die Verbindung zum Internet Provider wird dabei NICHT automatisch getrennt. Sie sollten daher die Verbindung nach der Zugangssperre UNBEDINGT trennen.*

---

### **Wie trenne ich die Verbindung zu meinem Internet Provider?**

Das von Ihnen verwendete Programm zur Herstellung einer Verbindung zum Internet sollte eine Funktion enthalten, mit der Sie die Verbindung trennen können.

Wenn Sie mit Hilfe dieses Programms die Verbindung nicht trennen können, beenden Sie Windows, schalten Sie ihren Computer aus, und starten Sie ihn neu. (Vergessen Sie nicht, vorher alle Anwendungen zu schließen.)

---

### **Kann ich die Verbindung automatisch trennen lassen?**

Sie können Cyber Patrol so konfigurieren, daß die Verbindung automatisch getrennt wird. Weitere Informationen hierzu finden Sie im Cyber Patrol Hilfethema *Zeit-Management* ein-/ausschalten.

## Nutzungszeiten festlegen

**Lesen Sie auch:** [Regeln für Internet-Zugang](#)

Sie können die Nutzung des Internets und der Anwendungen in der Liste des Dialogfelds *Spiele & Anwendungen* auf bestimmte Tageszeiten beschränken. Außerhalb der zugelassenen Zeiten erscheint bei Zugriffsversuchen auf das Internet oder eine geschützte Anwendung eine Meldung und der Zugang wird verweigert.

---

### Beispiel für tägliche Zeitbeschränkungen

Sie wollen an Schultagen nur einen Zugriff von 20:00 Uhr bis 21:00 Uhr erlauben, an Wochenenden jedoch von 7:00 Uhr bis 23:00 Uhr.

---

### So legen Sie Nutzungszeiten fest:

Die maximalen Betriebszeiten legen Sie mit Hilfe des Cyber Patrol-Steuerpults fest.

1. Klicken Sie auf die Schaltfläche *Nutzungsdauer festlegen*. Nun können Sie alle Zeiteinstellungen vornehmen.
  2. Die Zeitgrafik gibt die Betriebszeiten an. **Zeiten, in denen der Zugang erlaubt ist, erscheinen grün. Zeiten, in denen der Zugang gesperrt ist, erscheinen rot.**
  3. Bewegen Sie den Mauszeiger auf den Wochentag, für den Sie die Zeiteinstellung ändern wollen.
  3. Ziehen Sie den Mauszeiger bei gedrückter Maustaste über die Zeiten, in denen der Zugang gesperrt werden soll.
  4. Klicken Sie auf die Schaltfläche *Einstellungen speichern*.
- 

### Zeitintervalle

Die Zugriffszeiten können in 30-Minuten-Intervallen festgelegt werden.

---

### Löschen der Zeiteinstellungen

Zum Löschen der aktuellen Zeiteinstellungen klicken Sie auf die Schaltfläche  für den betreffenden Tag.

## Tägliche Zeitbeschränkungen festlegen

**Lesen Sie auch:** [Regeln für Internet-Zugang](#)

Sie können die Nutzung des Internets und der Anwendungen in der Liste des Dialogfelds *Spiele & Anwendungen* auf Tagesbasis zeitlich beschränken. Nach Ablauf der maximalen Nutzungsdauer erscheint bei Zugriffsversuchen auf das Internet oder eine geschützte Anwendung eine Meldung und der Zugang wird verweigert.

---

### Beispiel für Zeitbeschränkungen auf Tagesbasis

Sie wollen die Nutzung des Internets und der Anwendungen von Montag bis Freitag nicht mehr als 1 Stunde pro Tag und an Wochenenden maximal 3 Stunden pro Tag zulassen.

---

### Vorgehensweise:

Sie legen die maximalen Betriebszeiten mit Hilfe des Cyber Patrol-Steuerpults fest.

1. Klicken Sie auf die Schaltfläche *Nutzungsdauer festlegen*. Nun können Sie alle Zeiteinstellungen vornehmen.
2. Die Spalte *Freigabe Std./Tag* zeigt die maximalen Betriebszeiten für jeden Wochentag an.
3. Klicken Sie auf die Schaltflächen rechts neben dem zu ändernden Eintrag, bis die für diesen Tag vorgesehene Zeitdauer angezeigt wird.
4. Klicken Sie auf die Schaltfläche *Einstellungen speichern*.

Die Zeiten können in 15-Minuten-Intervallen verändert werden.

## Wöchentliche Zeitbeschränkungen festlegen

### Lesen Sie auch: [Regeln für Internet-Zugang](#)

Sie können die Nutzung des Internets und der Anwendungen in der Liste des Dialogfelds *Spiele & Anwendungen* auf [Wochenbasis](#) zeitlich beschränken. Nach Ablauf der maximalen Nutzungsdauer erscheint bei Zugriffsversuchen auf das Internet oder eine geschützte Anwendung eine Meldung und der Zugang wird verweigert.

---

### Beispiel für Zeitbeschränkungen auf Wochenbasis

Sie wollen den Zugang auf maximal 6 Stunden pro Woche beschränken.

---

### Vorgehensweise:

Sie legen die maximalen Betriebszeiten mit Hilfe des Steuerpults fest.

1. Klicken Sie auf die Schaltfläche *Nutzungsdauer festlegen*. Nun können Sie alle Zeiteinstellungen vornehmen.
2. Das Feld *Std./Kalenderwoche* gibt die maximale Nutzungsdauer pro Woche an.
3. Klicken Sie auf die Schaltflächen rechts neben dem Feld, bis die gewünschte wöchentliche Zeitdauer angezeigt wird.
4. Klicken Sie auf die Schaltfläche *Einstellungen speichern*.

Die Zeiten können in 15-Minuten-Intervallen verändert werden.

## - **Filtermöglichkeiten**

Cyber Patrol bietet zahlreiche Möglichkeiten, Inhalt und Internet-Zugang zu filtern. Die Software wird mit Standardeinstellungen geliefert. Sie haben jedoch die Möglichkeit, diese Standardeinstellungen an Ihre Bedürfnisse anzupassen.

---

### **Zugangsberechtigungen**

#### [Zugangsberechtigungen für Internet-Dienste festlegen](#)

Legen Sie für jede Gruppe von Diensten eigene Zugangsberechtigungen fest.

---

### **Newsgroups, WWW, FTP & andere Dienste**

#### [Cyber-Listen](#)

Hier erfahren Sie, wie Sie mit Hilfe der CyberNOT- und CyberYES-Listen Internet-Sites nach Inhalt filtern können.

#### [Bereichsbeschränkungen](#)

Hier erfahren Sie, welche Inhaltskategorien zum Filtern zur Verfügung stehen.

#### [WWW, FTP & andere Dienste](#)

Hier erfahren Sie, wie Sie zusätzliche Sites sperren oder zulassen können und wie Sie eine Cyber-Liste auswählen.

#### [Newsgroup-Kontrolle](#)

Hier erfahren Sie, wie Sie zusätzliche Newsgroups sperren oder zulassen können und wie Sie eine Cyber-Liste auswählen.

#### [Filter für Domänen](#)

Hier erfahren Sie, wie Sie eine Liste mit Bestandteilen von Internet-Adressen (z. B. **.edu**) für Sites anlegen, die zugelassen oder gesperrt werden sollen.

---

### **PICS-Bewertungssystem**

#### [Bereichsbeschränkungen für SafeSurf SS~~](#)

Hier erfahren Sie, wie Sie das Bewertungssystem SafeSurf einrichten.

#### [PICS-Bewertungsstandard: RSACi](#)

Hier erfahren Sie, wie Sie das Bewertungssystem RSACi PICS einrichten.

---

### **Internet Relay Chat und ChatGard**

#### [Internet Relay Chat -IRC-Kontrolle](#)

Hier erfahren Sie, wie Sie eine Liste der [IRC-Sperrphrasen](#) erstellen. Anhand dieser Liste werden die Namen der [IRC-Chat Groups](#) und Internet-Sites geprüft und dementsprechend gesperrt oder zugelassen.

#### [ChatGard](#)

Hier erfahren Sie, wie Sie eine Liste von Wortteilen erstellen, mit deren Hilfe von ChatGard die Eingabe privater (oder sonstiger) Informationen verhindert wird.

---

### **Spiele & Anwendungen**

#### [Spiele & Anwendungen](#)

Hier erfahren Sie, wie Sie Filter für Spiele und andere Anwendungen auf Ihrem Rechner einrichten.

## Zugangsberechtigungen für Internet-Dienste festlegen

Cyber Patrol teilt Sites und andere Anwendungen in mehrere Gruppen von Internet-Diensten ein. Sie können im Steuerpult unterschiedliche Zugangsberechtigungen für jede Gruppe von Diensten vergeben.

---

### Zugangsberechtigungen für *Internet Relay Chat*; *WWW*, *FTP* & *andere* sowie *Newsgroups*:

Für jede Gruppe können Sie eine der folgenden Zugangsberechtigungen wählen:

**Voll:** Zugang ist zu allen Sites der Gruppe möglich.

**Kein:** Zugang ist zu allen Sites der Gruppe gesperrt.

**Selektiv:** Einige Sites der Gruppe sind anwählbar. Ist ein Site in der Cyber Patrol **CyberNOT-Liste** eines zugangsbeschränkten Bereichs aufgeführt, so wird der Zugang verweigert. (Die CyberNOT-Liste ist modifizierbar. Sie können bestimmte gesperrte Sites freigeben oder Sites zusätzlich sperren.)

---

### Zugangsberechtigungen für *Spiele & Anwendungen*

Für den Bereich *Spiele & Anwendungen*, können Sie folgende Zugangsberechtigungen vergeben:

**Voll:** Zugang zu allen Anwendungen der Liste *Spiele & Anwendungen* ist möglich.

**Kein:** Zugang zu allen Anwendungen der Liste *Spiele & Anwendungen* ist gesperrt.

**Selektiv:** Der Zugang zu den Anwendungen der Liste *Spiele & Anwendungen* wird gemäß Ihrer Zeiteinstellungen freigegeben. Ein Starten der Anwendungen in dieser Liste ist nur zu den erlaubten Tageszeiten möglich. Wird eine tägliche oder wöchentliche Zeitbegrenzung überschritten, ist der Zugang ebenfalls gesperrt.

---

### Zugangsberechtigungen erteilen

1. Klicken Sie im Cyber Patrol-Steuerpult auf die Kreissymbole im Gruppenfeld *Zugriff auf Internet-Dienste*. Die Schaltfläche *Nutzungsdauer festlegen* verschwindet und wird durch die Schaltflächen *Einstellungen speichern* und *Abbrechen* ersetzt.
2. Klicken Sie auf *Einstellungen speichern*, um die neuen Zugangsberechtigungen zu speichern.

---

### Zugangsbeschränkungen nach Inhalten anpassen

Wenn Sie *Selektiv* als Zugangsmodus festlegen, können Sie den Zugang nach Inhalten sperren.

#### Beschränkungen nach Inhalten

Zum Festlegen von zugangsbeschränkten Bereichen für *WWW*, *FTP* & *andere* sowie *Newsgroups* wählen Sie den Menübefehl *Bereichsbeschränkungen* im Menü *Inspektion*. Weitere Informationen finden Sie unter [Das Dialogfeld Bereichsbeschränkungen](#).

#### SafeSurf-Bereichsbeschränkungen

Zum Festlegen von zugangsbeschränkten Bereichen gemäß der SafeSurf-Klassifizierung wählen Sie den Menübefehl *SafeSurf~~ Beschränkungen festlegen* im Menü *Inspektion*. Weitere Einzelheiten finden Sie unter [Das Dialogfeld SafeSurf SS~~ Beschränkungen festlegen](#).

#### Internet Relay Chat

Zum Ändern der [IRC-Sperrphrasen](#) oder Hinzufügen weiterer erlaubter IRC-Gruppen klicken Sie auf die Schaltfläche *Internet Relay* und nehmen die entsprechenden Einstellungen im [Dialogfeld Internet Relay Chat \\_IRC-Kontrolle](#). vor.

#### WWW, FTP & andere

Zum Hinzufügen zusätzlicher erlaubter oder gesperrter Sites sowie anderer Sperr-Einstellungen klicken Sie auf die Schaltfläche *WWW, FTP & andere* und nehmen die entsprechenden Einstellungen im [Dialogfeld WWW, FTP & andere Dienste](#) vor.

### **Newsgroups**

Zum Hinzufügen zusätzlicher erlaubter oder gesperrter Newsgroups sowie anderer Sperr-Einstellungen klicken Sie auf die Schaltfläche *Newsgroups* und nehmen die entsprechenden Einstellungen im [Dialogfeld Newsgroup-Kontrolle](#) vor.

### **Spiele & Anwendungen**

Zum Anzeigen der zu überwachenden Anwendungen klicken Sie auf die Schaltfläche *Spiele & Anwendungen* und nehmen die gewünschten Einstellungen im Dialog [Spiele & Anwendungen](#) vor.

---

### **Lesen Sie auch:**

[Funktionen von Cyber Patrol](#)

[Regeln für Internet-Zugriff](#)

[Informationen zur CyberNOT-Liste](#)

[Auf dem Rechner gespeicherte Daten löschen](#)

## Cyber-Listen

Sie können die Zugangsberechtigungen für Internet-Sites oder Newsgroups entweder über eine [CyberYES-Liste](#) oder über eine [CyberNOT-Liste](#) steuern.

---

### Cyber-Listen

[WWW, FTP & andere Dienste](#)

Hier erfahren Sie, wie Sie zusätzliche Sites sperren oder zulassen können und wie Sie eine Cyber-Liste auswählen.

[Newsgroup-Kontrolle](#)

Hier erfahren Sie, wie Sie zusätzliche Newsgroups sperren oder zulassen können und wie Sie eine Cyber-Liste auswählen.

[CyberNOT-Liste aktualisieren](#)

Hier erfahren Sie, wie Sie die Cyber-Listen aktualisieren.

---

### CyberNOT-Liste

[Informationen zur CyberNOT-Liste](#)

Zusammenfassende Informationen zur CyberNOT-Liste.

[Beschreibung der CyberNOT-Kategorien](#)

Beschreibungen der einzelnen Inhaltskategorien.

[Bereichsbeschränkungen](#)

Hier erfahren Sie, wie Sie die Inhaltskategorien auswählen, mit deren Hilfe Sites von der CyberNOT-Liste gesperrt werden.

---

### CyberYES-Liste

[Informationen zur CyberYES-Liste](#)

Zusammenfassende Informationen zur CyberYES-Liste.

[Beschreibung der CyberYES-Kategorien](#) Beschreibungen der einzelnen Inhaltskategorien.

[Verwendung von CyberYES-Liste und E-Mail](#)

Hier erfahren Sie, wie Sie verhindern, daß Ihre E-Mail-Adresse durch die CyberYES-Liste gesperrt wird.

---

### Definierte Benutzerprofile



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.

## Informationen zur CyberNOT-Liste

Die CyberNOT-Liste ist eine verschlüsselte Liste mit Internet-Sites, die nach bestimmten Bereichen sortiert sind und Material enthalten, dessen Zugang Sie kontrollieren möchten.

Bei der Bewertung, ob eine Site in die Liste mit aufgenommen werden soll, gehen wir von der Wirkung dieser Site auf ein 12-jähriges Kind aus, das das Internet ohne Aufsicht durch die Eltern oder eine Lehrkraft durchsucht.

---

### Was ist in der CyberNOT-Liste enthalten?

- Bestimmte Sites, die gemeldet wurden, weil sie möglicherweise anstößiges Material verbreiten.
- Sites, deren Namen vermuten lassen, daß sie eventuell anstößiges Material enthalten.

---

### Hinweis zur Genauigkeit und Vollständigkeit

Microsystems Software, Inc. hat im Rahmen ihrer Möglichkeiten alle Anstrengungen unternommen, um CyberNOTs zu identifizieren und zu kategorisieren. Für die Qualität und Vollständigkeit des Schutzes kann jedoch keine Garantie von Cyber Patrol übernommen werden. Außerdem wird jede Verantwortung für etwaige Fehler oder Auslassungen abgelehnt. Wenn Sie glauben, einen Fehler oder eine Auslassung bei der Identifizierung oder Klassifizierung einer Site gefunden zu haben, melden Sie diese bitte mit Hilfe des Dialogfelds [Inspektionsmeldung](#).

---

### Aktualisierungen der CyberNOT-Liste

Die Master-CyberNOT-Liste wird regelmäßig durch Cyber Central aktualisiert. Sie können Aktualisierungen auf Wunsch herunterladen.

---

### Anpassen der CyberNOT-Liste

Sie können die CyberNOT-Liste folgendermaßen anpassen:

- Indem Sie weitere Sites auflisten, die gesperrt werden sollen.
- Indem Sie bestimmte Sites auflisten, die zugelassen werden sollen.

Sie können empfehlen, daß eine bestimmte Site der Master-CyberNOT-Liste von Cyber Central hinzugefügt oder aus ihr gelöscht werden soll.

---

### Lesen Sie auch:

[CyberNOT-Liste aktualisieren](#)

[Das Dialogfeld Bereichsbeschränkungen](#)

[Beschreibung der CyberNOT-Kategorien](#)

[Zugangsberechtigungen für Internet-Dienste festlegen](#)

## Beschreibung der CyberNOT-Kategorien

Folgende Inhaltsbereiche stehen zur Verfügung:

- **Gewalt/Obszönität**  
Extreme Grausamkeit, physische oder emotionale Gewalttaten gegen Tiere oder Personen. Texte in denen bestimmte Begriffe (obszöne Begriffe, Anspielungen und Flüche) öfter als einmal in 50 Meldungen oder Seiten vorkommen.
- **Teilweise nackte Körper**  
Vollständige oder teilweise Entblößung der menschlichen Anatomie mit Ausnahme der Genitalien.
- **Vollständig nackte Körper**  
Jede Entblößung von menschlichen Genitalien.
- **Sexuelle Handlungen (Bild oder Text)**  
Bildmaterial oder Texte, in denen Menschen oder Tiere beim expliziten sexuellen Akt und bei anstößigem und laszivem Verhalten gezeigt werden, inkl. Masturbation, Kopulation, Sex mit Kindern, Intimitäten, bei denen nackte oder teilweise nackte Personen bei heterosexuellen, bisexuellen, lesbischen oder homosexuellen Begegnungen gezeigt werden. Dazu gehören auch Werbung für Telefonsex, Begleit- und Vermittlungsagenturen, Erwachsenenmagazine, CD-ROMs und Videos.
- **Anstößige Darstellungen (Bild oder Text)**  
Bildmaterial oder beschreibende Texte von Menschen, Tieren oder Sachen, die äußerst vulgäres, die Menschenwürde verachtendes oder obszönes Fehlverhalten zeigen. Dazu gehören die Darstellung von Verstümmelungen, besonders grausame Szenen und unanständige Darstellung von Körperfunktionen.
- **Rassismus/Ethnische Ausgrenzungen**  
Vorurteile und Diskriminierung einer Volksgruppe oder ethnischen Kultur. Ethnische oder rassistische Witze und Verleumdungen. Alle Texte, die eine Volksgruppe über eine andere stellen.
- **Satanismus/Sekten**  
Teufelsverehrung, Affinität für das Böse und Boshafte. Sekten oder Gruppen, von denen angenommen wird, daß sie Individuen zum Beitritt zwingen oder Mitglieder unlauter anwerben.
- **Drogen & Drogenkultur**  
Themen, die sich mit der Verwendung oder dem Vertrieb illegaler Drogen beschäftigen. Ausgenommen davon sind zur Zeit illegale Drogen, die für medizinische Zwecke verwendet werden (z. B. Drogen, die bei der Behandlung von AIDS-Patienten eingesetzt werden). Dazu gehören Substanzen mit dem primären Zweck, den Bewußtseinszustand eines Individuums zu ändern, z. B. Klebstoff-Schnüffeln.
- **Militarismus/Extremismus**  
Besonders aggressives und streitlustiges Verhalten, Radikalismus, Engagement für extremistische politische Meinungen. Dazu gehören extremistische politische Gruppierungen, die Gewalt als Möglichkeit zur Verwirklichung ihrer Ziele propagieren oder billigen.
- **Glücksspiel**  
Glücksspiel in Form von Lotterien, Casinos, Wetten, Zahlenspiele, Online-Sportwetten oder Wetten mit Geldeinsatz und nicht mit Geld verbundene Mutproben.
- **Anrüchiges/Illegales**  
Material oder Aktivitäten zweifelhafter Natur, die ungesetzlich in einer oder allen Jurisdiktionen sind, wie z. B. illegale Geschäftspraktiken, Kettenbriefe, Raubkopieren von Software und Copyright-Verletzungen.
- **Alkohol, Bier, Wein & Tabak**  
Material, das mit dem Verkauf oder Verzehr von alkoholischen Getränken zu tun hat.



# Beschreibung der CyberYES-Kategorien

## Hinweis zur Genauigkeit und Vollständigkeit

Microsystems Software, Inc. hat im Rahmen ihrer Möglichkeiten alle Anstrengungen unternommen, um CyberYESs zu identifizieren und zu kategorisieren. Für die Qualität und Vollständigkeit des Schutzes kann jedoch keine Garantie von Cyber Patrol übernommen werden. Außerdem wird jede Verantwortung für etwaige Fehler oder Auslassungen abgelehnt. Wenn Sie glauben, einen Fehler oder eine Auslassung bei der Identifizierung oder Klassifizierung einer Site gefunden zu haben, melden Sie diese bitte mit Hilfe des Dialogfelds [Inspektionsmeldung](#).

---

## Beschreibungen der Kategorien:

### **Spiele & Spielzeuge**

Bilder, Texte und Klänge mit Informationen zum Basteln von oder Spielen mit Spielen oder Spielzeugen. Hierunter fallen außerdem Sites, auf denen man Spiele herunterladen kann. Mit diesen Spielen kann anschließend online oder offline gespielt werden.

### **Kunst, Bücher & Musik**

Bilder, Texte und Klänge über Kunst, Büchern und Musik. Hierzu zählen z. B. Biographien und herunterladbare Bilder, Klänge und Texte zu Künstlern, Autoren und Musikern. Librettos mit anstößiger Sprache werden ausgeschlossen.

### **Film & Fernsehen**

Bilder, Texte und Klänge mit Informationen zu Film und Fernsehen. Hierzu gehören Informationen zu Film- und Fernseh-Stars, Regisseuren, der Produktion von Filmen und Fernseh-Shows, Kritiken und Programmen. Zu dieser Kategorie zählen außerdem Informationen zu Theaterproduktionen.

### **Spiele im Freien & Sport**

Bilder, Texte und Klänge mit Informationen zu Spielen im Freien und zu Sport. In diese Kategorie fallen Informationen zu Aktivitäten wie Camping, Wandern und Zeltlagern und alle weiteren organisierten und nicht organisierten Freizeitaktivitäten.

### **Haustiere, Tiere & Dinos**

Bilder, Texte und Klänge zum Thema Haustiere, Tiere und Dinosaurier. Hierzu zählen Informationen zur Pflege von Haustieren oder dazu, welches Tier wie gepflegt werden muß. Zu dieser Kategorie gehören außerdem Informationen zu Lebensräumen, Umweltbedingungen und Ernährungsweise vieler verschiedener Tierarten (auch die der ausgestorbenen Arten) sowie die Geschichte und Evolution verschiedener Spezies (auch die der bereits ausgestorbenen Spezies).

### **Urlaub & Reisen**

Bilder, Texte und Klänge zum Thema Urlaub und Reisen. In diese Kategorie fallen Informationen zu Reisezielen, Sehenswürdigkeiten sowie die besten Anreisemöglichkeiten und die voraussichtlichen Reisekosten. Diese Kategorie enthält außerdem Informationen zur Bevölkerung, Lage, zu den Produkten und zum Tourismus der einzelnen Regionen, Länder und Staaten.

### **Rätsel & Hobbies**

Bilder, Texte und Klänge zum Thema Rätsel und Hobbies. Hierzu zählen Informationen für Sammler von Erinnerungsstücken und Tips zur Aufarbeitung alter Gegenstände. In diese Kategorie fallen Sites, auf denen Rätsel heruntergeladen werden können, oder auf denen man sich selbst Rätsel ausdenken oder entwerfen kann.

### **Hausaufgaben**

Bilder, Texte und Klänge mit Unterrichtsunterlagen. Hier finden Sie ein umfassendes Angebot an Informationen zu allen möglichen Kursangeboten für Schüler von Grund-, Haupt- Realschulen

und Gymnasien. Das Kursangebot umfaßt Fächer wie Mathematik, Naturwissenschaften, Englisch, Landeskunde, Sprachen, Sozialwissenschaften und Geschichte.

### **Ratschläge & Hilfe**

Bilder, Texte und Klänge mit Informationen zu freiwilliger Nachbarschaftshilfe und zum Thema Freundschaftsdienste.

### **Nachschlagewerke**

Bilder, Texte und Klänge mit Informationen zu verschiedenen Arten von Nachschlagewerken. Hierzu gehören beispielsweise Wörterbücher, Thesauren, Atlanten und Enzyklopädien.

### **Schulen im Internet**

Bilder, Texte und Klänge, die von Grund-, Haupt-, Realschulen, Gymnasien, Schulklassen oder einzelnen Schülern in das Internet hochgeladen wurden.

### **Eltern & Lehrer**

Bilder, Texte und Klänge mit Informationen über Kindererziehung für Eltern und Lehrer. Diese Kategorie wird möglicherweise als **KINDER/JUGENDLICHE** neu definiert.

### **Weitere interessante Materialien**

Bilder, Texte und Klänge mit Informationen, die keiner der anderen Kategorien zugeordnet werden konnten.

## CyberNOT-Liste aktualisieren

Ihre Kopie der [CyberNOT-Liste](#) wird alle 10 Tage automatisch aktualisiert. Aktualisierungen überschreiben keine Einträge in der Liste, die von Ihnen individuell ausgewählt wurden.

Des Weiteren können Sie Ihre Kopie der CyberNOT-Liste jederzeit selbst aktualisieren. Um eine neue Version zu laden:

- Wählen Sie aus dem Menü *Datei* den Befehl *CyberNOT-Liste aktualisieren*.
  - Oder: -
  - Klicken Sie im Dialogfeld *Bereichsbeschränkungen* auf die Schaltfläche *Neue CyberNOT-Liste laden*.
- Cyber Patrol stellt automatisch eine Verbindung zu [Cyber Central](#) her und lädt die Liste herunter.

---

### Lesen Sie auch:

[Informationen zur CyberNOT-Liste](#)

[Das Dialogfeld Bereichsbeschränkungen](#)

## Das Dialogfeld *Bereichsbeschränkungen*

Im Dialogfeld *Bereichsbeschränkungen* können Sie selektiv bestimmte Bereiche auf Basis von Inhalten sperren. Cyber Patrol verweigert den Zugriff auf alle Sites, von denen bekannt ist, daß sie Material dieses Inhalts verbreiten.

Ihre Auswahl gilt für alle Internet-Dienste, für die Sie im Cyber Patrol-Steuerpult die Zugangsberechtigung *Selektiv* vergeben haben. Die Inhaltsbeschränkungen gelten nicht für *Internet Relay Chat* sowie für *Spiele & Anwendungen*.

---

### Sperren bestimmter Inhalte

1. Markieren Sie dieses Optionsfeld bevor Sie Inhaltsbereiche sperren.
  2. Klicken Sie auf die Schaltfläche *Beschränkungen speichern*.
- 

### Aktualisieren der CyberNOT-Liste

Zum Aktualisieren der CyberNOT-Liste klicken Sie auf die Schaltfläche *CyberNOT-Liste aktualisieren*. Cyber Patrol wählt sich automatisch bei [Cyber Central](#) ein und lädt die neueste Version der CyberNOT-Liste herunter.

---

### Lesen Sie auch:

- [Informationen zur CyberNOT-Liste](#)
- [Beschreibung der CyberNOT-Kategorien](#)
- [Regeln für Internet-Zugriff](#)
- [CyberNOT-Liste aktualisieren](#)

## Filter für Domänen

Sie haben die Möglichkeit, Sites nach Bestandteilen ihrer [Domäne](#) zu filtern. Sie können z. B. den Zugang zu allen Sites sperren, deren Domäne ein COM enthält.

Der Filter für Domänen wird von den Einträgen im Feld *Zusätzlich erlaubte Bereiche* der Dialogfelder *WWW, FTP & andere Dienste* und *Newsgroup-Kontrolle* und von den Einträgen der CyberYES-Liste überschrieben.

---

### So geben Sie Teile der Domäne ein

Gehen Sie folgendermaßen vor, um einen Teil einer Domäne einzugeben:

1. Wählen Sie aus dem Menü *Inspektion* die Option *Filter für Domäne auswählen*.
  2. Geben Sie im Feld *Domänenbestandteile* den gewünschten Teil der Domäne ein, und drücken Sie die Eingabetaste.
  3. Wiederholen Sie Schritt 2 für jeden Domänenbestandteil, den Sie eingeben möchten.
  4. Klicken Sie auf die Schaltfläche *Änderungen speichern*, um die von Ihnen eingegebenen Domänenbestandteile zu speichern.
- 

### Regeln für die Eingabe von Domänenbestandteilen

Im Feld *Domänenbestandteile* können bis zu 32 Domänenbestandteile eingegeben werden.

Ein Domänenbestandteil darf maximal 3 Zeichen umfassen, muß aber mindestens aus 2 Zeichen bestehen.

Der Domänenbestandteil muß vollständig eingegeben werden, d. h. es ist nicht möglich, nur einen Teil einer Domäne einzugeben.

---

### Auswahl einer Filtermethode

Sie können die in der Liste aufgeführten Domänenbestandteile entweder alle zulassen oder alle sperren. Es es nicht möglich, einige Bestandteile zuzulassen und andere zu sperren.

Sie haben folgende Möglichkeiten, die Domänenbestandteile zu filtern:

- Wenn Sie die unter *Domänenbestandteile* aufgeführten Namen sperren möchten, markieren Sie das Optionsfeld *gesperrte Domänen*.
  - Wenn Sie die Namen in der Liste der Domänenbestandteile zulassen möchten, markieren Sie das Optionsfeld *erlaubte Domänen*.
- 

### Beispiel

Wenn Sie alle Sites sperren möchten, in deren Domäne der Bestandteil COM enthalten ist, markieren Sie das Optionsfeld *gesperrte Domänen* und geben Sie *COM* in das Feld *Domänenbestandteile* ein. Es werden nun alle Sites gesperrt, deren Adresse folgendermaßen aussehen: **www.abcxyz.com**, **www.com.abc**, oder **com.abc.xyz**. Der Domänenbestandteil COM kommt in vielen Adressen kommerzieller Sites vor.

---

### Definierte Benutzerprofile



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.

## Das Dialogfeld *SafeSurf~~ Beschränkungen festlegen*

Cyber Patrol unterstützt den SafeSurf-Klassifizierungsstandard des Internets. Dieser stuft alle Sites nach Prüfung des angebotenen Materials in eine Eignungsklasse für Minderjährige ein. Gemäß dem SafeSurf-Standard besitzt jeder Site eine Einstufungsklasse. Cyber Patrol sperrt Sites, die unter Ihre Sperrkriterien fallen, oder noch unbewertet sind.

Zum Festlegen einer SafeSurf-Bereichsbeschränkung, wählen Sie aus dem Menü *Inspektion* des Cyber Patrol-Steuerpults die Option *SafeSurf~~ Beschränkungen festlegen*. Im Dialogfeld *Festlegen der PICS Bereichsbeschränkungen für* markieren Sie die Optionsfelder für die gewünschten Bereiche und Prioritäten. Wird einem Bereich die Priorität 1 oder höher zugeordnet, so werden alle Sites dieser Einstufung und höher gesperrt. Markieren Sie beispielsweise die Sperrpriorität 4, so sind auch die Prioritäten 5 bis 9 gesperrt.

Versuchen Sie zum Testen des SafeSurf-Standards sich in die SafeSurf-Testsite der Cyber Central einzuwählen: [www.microsys.com/SSTEST/](http://www.microsys.com/SSTEST/)

Die Bereichsbeschränkung für diese Site ist: Bereich *0 - Altersbereich*, Sperrpriorität *8 - Nur Erwachsene*. Wenn Sie Priorität *8 - Nur Erwachsene* oder niedriger wählen, sollten Sie nicht in der Lage sein, auf den Testsite zuzugreifen; wenn Sie *9 - Explizit für Erwachsene* oder *0 - Altersbeschränkung ignorieren* wählen, sollten Sie auf den Cyber Central-Testsite zugreifen können.

Um den SafeSurf-Standard außer Kraft zu setzen, wählen Sie aus dem Menü *Inspektion* des Cyber Patrol-Steuerpults die Option *SafeSurf~~ Beschränkungen festlegen* und markieren das Optionsfeld *SafeSurf SS~~ inaktiv*.

Einzelheiten über den SafeSurf-Standard finden Sie unter: [www.safesurf.com](http://www.safesurf.com)

Sie können wählen, ob nur die SafeSurf-Standards, nur die Bereichsbeschränkungen nach CyberNOT-Liste oder beide Verfahren Anwendung finden sollen.

## PICS-Bewertungsstandard: RSACi

Cyber Patrol unterstützt den Internet-Bewertungsstandard des Recreational Software Advisory Council (RSAC). Mit Hilfe des RSACi-Standards werden Sites anhand der Kategorien *Gewalt*, *Sex*, *Nackte Körper* und *Sprache* bewertet.

Alle Sites werden nach diesem Standard bewertet. Durch Ihre Auswahl der zu erlaubenden bzw. zu sperrenden Bewertungskategorien legen Sie fest, welche Sites von Cyber Patrol gesperrt werden.

Wenn Sie den RSACi-Standard nicht verwenden möchten, wählen Sie im Dialogfeld Cyber Patrol-Steuerpult aus dem Menü *Inspektion* die Option *RSACi Beschränkungen festlegen*, und markieren Sie anschließend die Option *RSACi deaktivieren*.

Auf der Test-Site von Cyber Central RSACi können Sie den RSACi-Bewertungsstandard testen. Sie finden diese Test-Site unter folgender Adresse: [www.microsys.com/RTEST/](http://www.microsys.com/RTEST/)

## Das Dialogfeld *Internet Relay Chat Groups* **IRC-Kontrolle**

In diesem Dialogfeld können Sie zusätzliche Internet Relay Chat Groups sperren oder über Sperrphrasen gesperrte Chat Groups einzeln freigeben. Die Einstellungen werden nur dann wirksam, wenn Sie im Cyber Patrol-Steuerpult die Zugangsberechtigung *Selektiv* für diesen Dienst gewählt haben.

Cyber Patrol sperrt Chat Groups, die bestimmte Textteile (Sperrphrasen) in ihrem Namen enthalten, wie z. B. "Sex" oder "uck".

---

### So sperren Sie zusätzliche Chat Groups

Gehen Sie folgendermaßen vor, um eine [IRC-Sperrphrase](#) hinzuzufügen:

1. Geben Sie den gewünschten Text im Feld *Sperrphrasen* ein.  
Beispiel: **Sex**
2. Drücken Sie die Eingabetaste.
3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### So lassen Sie einzelne Chat Groups zu

Cyber Patrol ermöglicht den selektiven Zugriff auf einzelne Chat Groups. Um eine Chat Group freizugeben, gehen Sie wie folgt vor:

1. Geben Sie den Namen der Chat Group im Feld *Erlaubte Chat Groups* ein.  
Sie müssen den vollen Gruppennamen eingeben.  
Beispiel: **#duckhunt**
2. Drücken Sie die Eingabetaste.
3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

**Lesen Sie auch:**      [Regeln für Internet-Zugriff](#)

## ChatGard

Mit ChatGard kann verhindert werden, daß nicht für die Allgemeinheit geeignete Informationen (z. B. Adressen oder Kreditkartennummern) online weitergegeben oder daß ungeeignete Wörter online verwendet werden.

ChatGard überwacht die Eingabe über die Tastatur. Dabei wird verhindert, daß die im Dialogfeld *ChatGard - Chat Kontrolle* aufgeführten [Wörter](#) richtig eingegeben werden können. Die Eingabe der [Carlin 7-Wörter](#) wird automatisch unterbunden.

Wenn Sie versuchen ein Wort aus der ChatGard-Liste der zu sperrenden Wörter oder Sätze einzugeben, werden die einzelnen Buchstaben des Wortes durch das Zeichen "x" ersetzt. Wenn z. B. ein zu sperrendes Wort "apz" lautet, erscheint beim Eingabeversuch dieses Wortes die Zeichenfolge "xxx".

*Hinweis: Die Tastatureingabe wird von ChatGard ununterbrochen kontrolliert, solange Sie sich im Internet bewegen (d. h. wenn die Winsock oder das entsprechende Element geladen ist). Dadurch werden nicht nur die Wörter überprüft, die Sie im Internet-Browser oder in Ihrem E-Mail-Programm eingeben, sondern auch alle Wörter, die Sie für Textverarbeitungsprogramme, Tabellenkalkulationsprogramme oder sonstige Rechneranwendungen eingeben.*

---

### So geben Sie ChatGard-Wörter ein und löschen sie

Gehen Sie folgendermaßen vor, um ein zu sperrendes Wort hinzuzufügen:

1. Wählen Sie aus dem Menü *Inspektion* die Option *ChatGard Einstellung*, oder klicken Sie im Dialogfeld *Cyber Patrol-Steuerpult* auf die Schaltfläche *ChatGard*.
2. Geben Sie das Wort in das Feld *Weitere Sperrphrasen* oder in eines der Felder des Bereichs *Besondere Einträge* ein, und drücken Sie die Eingabetaste.
3. Wiederholen Sie Schritt 2 für jedes Wort, das Sie eingeben möchten.
4. Klicken Sie auf die Schaltfläche *Änderungen speichern*, um die von Ihnen eingegebenen Wörter zu speichern.

Wenn Sie ein Wort aus der Liste der Wörter im Feld *Weitere Sperrphrasen* löschen möchten, markieren Sie das Wort, und klicken Sie anschließend auf die Schaltfläche *Einträge löschen*.

Wenn Sie ein Wort aus einem der Felder im Bereich *Besondere Einträge* löschen möchten, markieren Sie das Wort, und klicken Sie anschließend auf die Schaltfläche *Einträge löschen*.

---

### So deaktivieren Sie ChatGard

Wenn Sie die Überwachung mit ChatGard deaktivieren möchten, markieren Sie das Kontrollkästchen *ChatGard inaktiv*.

---

### Regeln für die Eingabe von ChatGard-Wörtern

Im Feld *Weitere Sperrphrasen* können bis zu 32 Wörter eingegeben werden. Sechs der 32 Wörter sind bereits vorgegeben. Bei diesen vorgegebenen Wörtern handelt es sich um die Carlin 7-Wörter. Diese Carlin 7-Wörter können weder geändert noch gelöscht werden.

Jedes Wort darf aus maximal 32 Zeichen bestehen.

Mit ChatGard werden nur alphabetische und numerische Zeichen überwacht. Leerschritte, Satzzeichen sowie andere nicht alphanumerische Zeichen werden automatisch aus dem ChatGard-Feldern entfernt und bleiben somit bei der Überwachung durch Cyber Patrol unberücksichtigt.

---

## Definierte Benutzerprofile



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.

## Das Dialogfeld WWW, FTP & andere Dienste

Dieses Dialogfeld dient zur Anpassung der [CyberNOT-Liste](#) in Verbindung mit dem [World Wide Web](#), [FTP](#), und anderen Internet-Diensten. Die Einstellungen werden nur dann wirksam, wenn Sie im Steuerpult die Zugangsberechtigung *Selektiv* für diesen Dienst gewählt haben.

Cyber Patrol sperrt Sites, von denen bekannt ist, daß sie potentiell anrüchiges Material anbieten.

Sie können:

- Zusätzliche Sites sperren.
- Bestimmte gesperrte Sites freigeben.
- Sites über [IRC-Sperrphrasen](#) sperren.
- Die CyberNOT-Liste außer Kraft setzen.
- Ports für Internet-Dienste sperren.

---

### So sperren Sie zusätzliche Sites

Zusätzlich zu den über die CyberNOT-Liste gesperrten Sites können Sie weitere Sites wie folgt sperren:

1. Geben Sie die Site-Adresse ([URL](#)) im Feld *Zusätzlich gesperrte Bereiche* ein.
2. Drücken Sie die Eingabetaste.
3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### So geben Sie bestimmte Sites frei

Sie können einzelne Sites freigeben, selbst wenn diese in der CyberNOT-Liste enthalten sind:

1. Geben Sie die Site-Adresse ([URL](#)) im Feld *Zusätzlich erlaubte Bereiche* ein.
2. Drücken Sie die Eingabetaste.
3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### Können Sites auch nur teilweise gesperrt bzw. freigegeben werden?

Ja. Da Cyber Patrol die Adressen bis auf Verzeichnis- und Seitenebene überwacht, können Sie eine beliebig genaue Adreßangabe eingeben. Beispielsweise können Sie **WWW.ABC.EDU** eingeben, wenn Sie die gesamte Site WWW.ABC.EDU bezeichnen wollen. Oder Sie verwenden **WWW.ABC.EDU/JOKES**, um nur den Witzebereich (und alles, was er unter /JOKES enthält) den Site anzugeben.

---

### Wie gebe ich eine Adresse ein?

Jede Adresse wird eingegeben als:

*site\_adresse*/PORT: *service\_port\_number*

wobei *site\_adresse* die URL der Site bezeichnet, einschließlich aller gewünschten Erweiterungen, wie z. B. *WWW.ABC.EDU* oder *WWW.ABC.EDU/JOKES* oder *FTP.abcxyz.com*.

und */PORT: service\_port\_number* den Kommunikations-[Service-Port](#) für den betreffenden Internet-Dienst. Dieser Teil der Adresse **muß** für die Dienste FTP, Gopher, Telnet, SMTP, Finger und weitere Internet-Dienste angegeben werden. Für World Wide Web-Sites wird diese Angabe **nicht benötigt**.

Service-Portnummern werden vom Internet-Standardisierungskomitee vergeben. Standard Service-Portnummern sind:

#### Service-Portnummer

FTP            21

Telnet	23
SMTP	25
Gopher	70
Finger	79

**Beispiele:**     **ftp.abcxyz.com/PORT:21**  
                  **www.abcxyz.com**  
                  **www.abcxyz.com/TEST**

**Protokoll:** Üblicherweise enthalten Adressen zusätzlich ein Protokoll-Präfix, wie http://, ftp://, oder gopher://. Die Angabe des Protokolls entfällt jedoch in diesem Dialog.

---

### **Sperren von Sites über IRC-Sperrphrasen**

Sie können Cyber Patrol anweisen, alle Sites zu sperren, deren Adressen Textelemente aus der Liste der Sperrphrasen für IRC Chat Groups enthalten. Wenn Sie diese Option wählen und "sex" als Sperrphrase festgelegt wurde, so würde ein Site mit der Adresse **WWW.ABC.EDU/AdultSex** gesperrt werden.

Um Sites über Sperrphrasen zu sperren, markieren Sie das Optionsfeld *IRC-Sperrphrasen auf URL-Namen anwenden*.

---

### **Deaktivieren der CyberNOT-Liste**

Sie können Cyber Patrol anweisen, nur diejenigen Sites zu überwachen, die in den Listen für zusätzlich gesperrte bzw. erlaubte Bereiche aufgeführt sind. Markieren Sie dazu das Optionsfeld *CyberNOT-Liste deaktivieren*.

---

### **Sperren von Internet-Serviceports**

Sie können jegliche Kommunikation über einen bestimmten Internet-[Serviceport](#) sperren. Diese Funktion kann beispielsweise sehr effektiv in Betrieben eingesetzt werden, um bestimmte Dienste für die Mitarbeiter unzugänglich zu machen, oder einen innerbetriebliche [Firewall](#) zu verstärken. Auf typischen Heimcomputern wird diese Funktion eher selten genutzt, solange nicht auf betriebliche Netze zugegriffen wird oder eine [RPC](#) -Unterstützung installiert ist.

**Siehe:** [Sperren eines Internet-Service-Ports](#)

---

### **Regeln für die Listen**

Sie können sowohl bei den erlaubten als auch bei den gesperrten Sites maximal 32 Adressen angeben, die jeweils bis zu 64 Zeichen lang sein dürfen.

---

#### **Siehe auch:**

- [Informationen zur CyberNOT-Liste](#)
- [Regeln für Internet-Zugriff](#)
- [Das Dialogfeld Internet Relay Chat -IRC-Kontrolle](#)

## Das Dialogfeld *Newsgroup-Kontrolle*

Dieses Dialogfeld erlaubt die Anpassung der [CyberNOT-Liste](#) für [Newsgroups](#). Sie können zusätzliche Internet Newsgroups sperren oder freigeben. Die Einstellungen werden nur dann wirksam, wenn Sie im Steuerpult die Zugangsberechtigung *Selektiv* für diesen Dienst gewählt haben.

Cyber Patrol sperrt Newsgroups, von denen bekannt ist, daß sie potentiell anstößiges Material anbieten.

---

### So sperren Sie zusätzliche Newsgroups

Zusätzlich zu den Sites, die über die CyberNOT-Liste gesperrt sind, sperrt Cyber Patrol alle Newsgroups, die Sie hier angeben:

1. Geben Sie die Adresse ([URL](#)) im Feld *Zusätzlich gesperrte Bereiche* ein.  
Cyber Patrol sperrt dabei immer ab dem letzten angegebenen Adreßteil.  
Beispiel: Zum Sperren der Newsgroup **comp.home.hacking** geben Sie folgendes ein:  
**comp.home.hacking..**  
Beispiel: Zum Sperren aller Newsgroups im Bereich **comp.home** geben Sie nur **comp.home** ein.  
In diesem Fall werden alle Newsgroups gesperrt, die mit **comp.home** beginnen.  
Beispiel: Zum Sperren aller Newsgroups im Bereich **comp.home**, die mit "hack" beginnen, geben Sie **comp.home.hack** ein. Dies sperrt auch "hacking", "hacker", etc.
  2. Drücken Sie die Eingabetaste.
  3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.
- 

### So geben Sie zusätzliche Newsgroups frei

Sie können einzelne Sites freigeben, auch wenn diese in der CyberNOT-Liste enthalten sind:

1. Geben Sie die Adresse ([URL](#)) im Feld *Zusätzlich erlaubte Bereiche* ein.  
Beispiel: Zum Freigeben aller Newsgroups im Bereich **comp.home** geben Sie **comp.home** ein.  
In diesem Fall werden alle Newsgroups freigegeben, die mit **comp.home** beginnen.
  2. Drücken Sie die Eingabetaste.
  3. Klicken Sie auf die Schaltfläche *Änderungen speichern*.
- 

### Sperrungen von Newsgroups über IRC-Sperrphrasen

Sie können Cyber Patrol anweisen, alle Newsgroups und Foren zu sperren, deren Adressen (Namen) Textelemente aus der Liste der Sperrphrasen für Internet Relay Chat Groups enthalten. Wenn Sie diese Option wählen und "sex" als Sperrphrase festgelegt wurde, so würde eine Newsgroup mit der Adresse **alt.sexy.captains** gesperrt werden.

Um Sites über Sperrphrasen zu sperren, markieren Sie das Optionsfeld *IRC-Sperrphrasen auf URL-Namen anwenden*.

---

### Deaktivieren der CyberNOT-Liste

Sie können Cyber Patrol anweisen, nur diejenigen Adressen zu überwachen, die in den Listen für zusätzlich gesperrte bzw. erlaubte Bereiche aufgeführt sind. Markieren Sie dazu das Optionsfeld *CyberNOT-Liste deaktivieren*.

---

### Regeln für die Listen

Sie können sowohl bei den erlaubten als auch bei den gesperrten Adressen maximal 32 Adressen angeben, die jeweils bis zu 64 Zeichen lang sein dürfen.

---

**Siehe auch:** [Informationen zur CyberNOT-Liste](#)  
[Regeln für Internet-Zugang](#)  
[Das Dialogfeld Internet Relay Chat - IRC-Kontrolle](#)

## Zusätzliche Sites oder Newsgroups zulassen oder sperren

Im Dialogfeld *WWW, FTP & andere Dienste* können Sie zusätzliche Internet-Sites, die zugelassen oder gesperrt werden sollen, in die entsprechenden Listen eintragen.

Tragen Sie auch die Newsgroups, die zusätzlich zugelassen oder gesperrt werden sollen, in die entsprechenden Listen dieses Dialogfelds ein.

Die Cyber-Listen werden von Ihren Einträge überschrieben.

---

### So sperren Sie zusätzliche Sites oder Newsgroups

Cyber Patrol sperrt alle Sites, die Sie hier angeben:

1. Geben Sie die Adresse ([URL](#)) im Feld *Zusätzlich gesperrte Bereiche* ein.
2. Drücken Sie die Eingabetaste.
3. Wiederholen Sie die Schritte 1 und 2 für jede Site, die Sie sperren möchten.
4. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### So geben Sie zusätzliche Sites oder Newsgroups frei

Cyber Patrol gibt alle Sites frei, die Sie hier angeben:

1. Geben Sie die Adresse ([URL](#)) im Feld *Zusätzlich erlaubte Bereiche* ein.
2. Drücken Sie die Eingabetaste.
3. Wiederholen Sie die Schritte 1 und 2 für jede Site, die Sie freigeben möchten.
4. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### Können Sites oder Newsgroups auch nur teilweise gesperrt bzw. freigegeben werden?

Ja. Da Cyber Patrol die Adressen bis auf Verzeichnis- und Seitenebene überwacht, können Sie eine beliebig genaue Adreßangabe eingeben.

Beispielsweise können Sie **WWW.ABC.EDU** eingeben, wenn Sie die gesamte Site WWW.ABC.EDU bezeichnen wollen. Oder Sie verwenden **WWW.ABC.EDU/JOKES**, um nur den Witzebereich (und alles, was er unter /JOKES enthält) der Site anzugeben.

---

### Wie gebe ich eine Adresse ein in das Dialogfeld Newsgroup-Kontrolle ein?

Jede Adresse wird eingegeben als: *news\_group\_address*

wobei

*news\_group\_address* für den Teil der Adresse der Newsgroup-Hierarchie steht, den Sie sperren oder freigeben möchten. Cyber Patrol wendet den Filter von der obersten Ebene der Hierarchie ausgehend bis zu der von Ihnen angegebenen Verzweigung an.

#### Beispiele:

**comp.home.hacking**

Sperrt oder erlaubt den Zugang zu **comp.home.hacking** und allen Ebenen "unter" .hacking.

**comp.home**

Sperrt oder erlaubt den Zugang zu **comp.home** und allen Ebenen "unter" .home.

**comp.home.hack**

Sperrt oder erlaubt den Zugang zu allen Newsgroups unter **comp.home**, die mit "hack" beginnen. Hierzu gehören beispielsweise "hacking", "hacker" etc.

## Wie gebe ich eine Adresse in das Dialogfeld WWW, FTP & andere Dienste ein?

Jede Adresse wird eingegeben als:

*site\_address*/**PORT:***service\_port\_number*

wobei

*site\_address* die URL der Site bezeichnet, einschließlich aller gewünschten Erweiterungen, wie z. B. **WWW.ABC.EDU** oder **WWW.ABC.EDU/JOKES** oder **FTP.abcxyz.com**

und

**/PORT:** *service\_port\_number* den Kommunikations-**Service-Port** für den betreffenden Internet-Dienst. Dieser Teil der Adresse muß für die Dienste FTP, Gopher, Telnet, SMTP, Finger und weitere Internet-Dienste angegeben werden. Für World Wide Web-Sites wird diese Angabe nicht benötigt.

Service-Portnummern werden vom Internet-Standardisierungskomitee vergeben. Standard-Service-Portnummern sind:

<b>Service</b>	<b>Portnummer</b>
FTP	21
Telnet	23
SMTP	25
Gopher	70
Finger	79

**Beispiele:**     **ftp.abcxyz.com/PORT:21**  
                  **www.abcxyz.com**  
                  **www.abcxyz.com/TEST**

**Protokoll:** Üblicherweise enthalten Adressen zusätzlich ein Protokoll-Präfix, wie http://, ftp:// oder gopher://. Die Angabe des Protokolls entfällt jedoch in diesem Dialog.

---

### Regeln für die Listen

Sie können sowohl bei den erlaubten als auch bei den gesperrten Sites maximal 64 Adressen angeben, die jeweils bis zu 64 Zeichen lang sein dürfen.

## Sites mit Hilfe von IRC-Sperrphrasen sperren

Sie können Cyber Patrol so einrichten, daß alle Sites und Newsgroups gesperrt werden, deren Erweiterungen eine der [IRC-Sperrphrasen](#) enthalten.

Bei Internet-Sites werden die Verzeichnisse oder Informationen anhand der IRC-Sperrphrasen überprüft, die auf die [Domäne](#) folgen. Die Domäne selbst wird nicht geprüft.

Bei Newsgroups werden alle Adreßteile anhand der IRC-Sperrphrasen überprüft.

---

### Beispiele

Wenn "toy" eine IRC-Sperrphrase ist, gilt folgendes:

Dienst	Adresse	Ergebnis
Internet-Site	<b>WWW.ABC.COM/shopping/toys</b>	Diese Site wird gesperrt, da "toy" Teil des Verzeichnisses ist, das auf die Domäne WWW.ABC.COM folgt.
Internet-Site	<b>WWW.TOYS.COM/sports</b>	Diese Site wird <i>nicht</i> gesperrt, da "toy" Teil der Domäne ist.
Newsgroup	<b>alt.shopping.toys</b>	Diese Site wird gesperrt, da "toy" Teil der Adresse ist.

---

### Sperren von Internet-Sites und Newsgroups über IRC-Sperrphrasen

Wenn die Internet-Sites anhand der IRC-Sperrphrasen gefiltert werden sollen, aktivieren Sie im Dialogfeld *WWW, FTP & andere Dienste* das Kontrollkästchen *IRC-Sperrphrasen auf URL-Namen anwenden*.

Wenn Sie Newsgroups anhand der IRC-Sperrphrasen filtern lassen möchten, aktivieren Sie im Dialogfeld *Newsgroup-Kontrolle* das Kontrollkästchen *IRC-Sperrphrasen auf NG-Namen anwenden*.

---

**Lesen Sie auch:** [Das Dialogfeld Internet Relay Chat - IRC-Kontrolle](#)

## Cyber-Listen auswählen oder umgehen

In den Dialogfeldern *WWW, FTP & andere Dienste* und *Newsgroup-Kontrolle* können Sie die Cyber-Liste auswählen, die Sie verwenden möchten, oder die Verwendung der Cyber-Listen umgehen. Die hier von Ihnen ausgewählte Liste wird zum Sperren von Sites und Newsgroups verwendet.

---

### So wählen Sie eine Liste aus

1. Wählen Sie aus dem Dropdown-Listefeld *Cyber-Liste* den gewünschten Eintrag aus:

<b>Eintrag</b>	<b>Beschreibung</b>
None	Es wird keine Cyber-Liste verwendet.
CyberYES	Die Sites und Newsgroups werden anhand der CyberYES-Liste gefiltert.
CyberNOT	Die Sites und Newsgroups werden anhand der CyberNOT-Liste gefiltert.
<i>cyber_list</i>	Es wird eine benutzerdefinierte Cyber-Liste verwendet. Einige Versionen enthalten benutzerdefinierte Cyber-Listen; dies gilt jedoch nicht für alle Versionen.

2. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

Die von Ihnen gewählte Cyber-Liste gilt automatisch sowohl für Internet-Sites als auch für Newsgroups. Es ist nicht möglich, für Newsgroups und Sites unterschiedliche Listen zu verwenden.

---

### So umgehen Sie eine Liste

Wenn Sie eine Liste umgehen möchten, dann wählen Sie den Eintrag **Kein** aus. Was letztendlich angezeigt wird hängt davon ab, was genau Sie in *WWW, FTP & andere Dienste* ausgewählt haben.

<b>WWW, FTP &amp; andere Dienste</b>	<b>Auswahl der Newsgroups</b>	<b>Ergebnisse*</b>
Kein	CyberNOT Liste oder angepaßte CyberNOT list	Newsgroups werden mit der CyberNOT-Liste überwacht.  WWW, FTP & andere Dienste werden anhand keiner Liste gefiltert. Es werden alle Sites, die im Feld <i>Zusätzlich gesperrte Bereiche</i> aufgeführt sind, gesperrt. Alle anderen Sites werden zugelassen.
Kein	CyberYES Liste oder angepaßte CyberYES Liste	Newsgroups werden mit der CyberYES-Liste gefiltert.  WWW, FTP & andere Dienste werden anhand keiner Liste gefiltert. Es werden alle Sites, die im Feld <i>Zusätzlich erlaubte Bereiche</i> aufgeführt sind, zugelassen. Alle anderen Sites werden gesperrt.
CyberNOT-Liste oder angepaßte CyberNOT-Liste	Kein	WWW, FTP & andere Dienste werden mit der CyberNOT-Liste überwacht.  Newsgroups werden anhand keiner Liste gefiltert. Es werden alle Sites, die im Bereich <i>Zusätzlich gesperrte Bereiche</i> aufgeführt sind, gesperrt. Alle anderen Sites werden zugelassen.

CyberYES-Liste oder angepaßte CyberYES-Liste	Kein	<p>WWW, FTP &amp; andere Dienste werden mit der Cyber NOT-Liste überwacht.</p> <p>Newsgroups werden anhand keiner Liste gefiltert. Es werden alle Sites, die im Bereich <i>Zusätzlich erlaubte Bereiche</i> aufgeführt sind, erlaubt. Alle anderen Sites werden gesperrt.</p>
Kein	Kein	<p>Wenn die zuletzt ausgewählte Liste die CyberYES-Liste war, werden nur die Sites und Newsgroups zugelassen, die im Feld <i>Zusätzlich erlaubte Bereiche</i> aufgeführt sind. Alle anderen Sites und Newsgroups werden gesperrt.</p> <p>Wenn die zuletzt ausgewählte Liste die CyberYES-Liste war, werden nur die Sites und Newsgroups gesperrt, die im Feld <i>Zusätzlich gesperrte Bereiche</i> aufgeführt sind. Alle anderen Sites und Newsgroups werden zugelassen.</p>

\* Andere Filter, wie z. B. PICS oder Domänenfilter, bleiben weiterhin aktiv.

---

### Definierte Benutzerprofile



Klicken Sie hier, um eine Liste der Einstellungen anzeigen zu lassen, die für einzelne Benutzer festgelegt werden können.



## Internet-Service-Ports sperren

Sie können jegliche Kommunikation über einen bestimmten Internet-[Service-Port](#) sperren:

- Sperren des [Finger](#)-Dienstes, um Mitarbeiter daran zu hindern Informationen über andere Firmen abzufragen.
- Außenstehende daran hindern mit dem Finger-Dienst in Ihr System einzudringen.
- Sperren eingehender [RPC](#) -Befehle.
- Sperren des Zugangs auf Ihre Unternehmensdatenbank, wenn diese sich der gleichen Kommunikationstechnik bedient, wie ein Internet-Site.

Hacker, die Informationen stehlen oder vernichten wollen, können leicht in Firmennetze eindringen. Ein Weg, auf dem sich Hacker in Netzwerke einschleusen, ist über Service-Ports. Das Sperren eines Service-Ports für eingehende Zugriffe kann vor einem Hackerangriff über diesen Port schützen.

Heimcomputer sind von diesen Problemen eher selten betroffen, sofern keine Verbindungen mit Firmennetzen aufgebaut werden oder RPC-Unterstützung installiert ist.

---

### So sperren Sie abgehende Zugriffe für einen Service-Port:

1. Wählen Sie aus dem Menü *Inspektion* die Option *WWW, FTP & andere*.
2. Geben Sie nachfolgende Adresse im Feld *Zusätzlich gesperrte Bereiche* ein:

0.0.0.0/ **port-type:service\_port\_number**

**Dabei ist:**

**port-type** gleich **PORT**, wenn Sie abgehende Zugriffe sperren wollen, oder **IPOINT**, wenn Sie eingehende Zugriffe sperren wollen.

**service\_port\_number** bezeichnet die Nummer des zu sperrenden Ports.

3. Drücken Sie die Eingabetaste.
4. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

Nachfolgend die Portnummern einiger Dienste:

Dienst	Portnummer
FTP	21
Finger	79
Sun RPC für PC-NFS	111
Encore RPC für PC-NFS	121

---

**Beispiele:** **0.0.0.0/port:21**  
sperrt abgehende FTP-Zugriffe. Jeder Versuch, eine Datei herunterzuladen wird zurückgewiesen.

**0.0.0.0/port:79**  
sperrt abgehende Finger-Zugriffe. Jeder Versuch, Finger zu benutzen, wird zurückgewiesen.

**0.0.0.0/iport:79**  
sperrt eingehende Finger-Zugriffe. Alle Finger-Anfragen auf Ihren Computer werden zurückgewiesen.

**0.0.0.0/iport:111**  
sperrt eingehende RPC-Anfragen in einer Sun PC-NFS-Umgebung.

---

**Lesen Sie auch:** [Das Dialogfeld WWW, FTP & andere Dienste](#)



## Das Dialogfeld *Spiele & Anwendungen*

In diesem Dialogfeld können Sie den Zugang auf bestimmte [Spiele](#) und [Anwendungen](#) sperren. Dabei kann es sich um jede Windows-basierte Anwendung auf Ihrem Computer handeln, wie z. B.:

- Spiele
- Anwendungen für Ihren persönlichen Gebrauch (z. B. Ihr Buchhaltungsprogramm).
- Online-Dienste, wie z. B. CompuServe.

---

### Anwendungen von Online-Diensten

Zum Überwachen eines Online-Dienstes nehmen Sie die jeweilige Zugangssoftware des Dienstes in die Sperrliste auf. Für weitere Beispiele **siehe auch:** [Beispiele für Programme von Online-Diensten](#).

---

### Sperren von Spielen, Anwendungen und Online-Diensten

Tragen Sie die gewünschten Anwendungen im Dialogfeld *Spiele & Anwendungen* in die Sperrliste ein.

Wählen Sie eine Zugriffsart im Cyber Patrol-Steuerpult.

Legen Sie im Cyber Patrol-Steuerpult wahlweise Zeitbeschränkungen fest.

**Siehe auch:** [Sperrmechanismen für Spiele & Anwendungen](#)

---

### Aufnehmen von Spielen, Anwendungen und Online-Diensten in die Sperrliste

Cyber Patrol sperrt alle Anwendungen, die in der Sperrliste eingetragen sind:

1. Klicken Sie auf die Schaltfläche *Neue Anwendung aufnehmen*. **Ergebnis:** Sie sehen einen Windows-Standarddialog zur Dateiauswahl.
2. Wählen Sie die ausführbare Datei der zu sperrenden Anwendung.  
Beispiel: Zum Sperren von Solitaire (ein Kartenspiel im Lieferumfang von Windows), wählen Sie die Datei **SOL.EXE**
3. Heben Sie die Datei in der Sperrliste hervor.
4. Klicken Sie auf eine der Optionen für Kommunikationsschnittstellen unter *Gewählte Anwendung verwendet*.

Wenn Ihre Anwendung eine Verbindung mit dem Internet oder anderen Diensten aufbaut, ist es wichtig, die benutzte COM-Schnittstelle anzugeben, damit Cyber Patrol die Verbindung trennen oder sperren kann. Kann Cyber Patrol die Verbindung nicht unterbrechen, fallen womöglich weiterhin Gebühren von Seiten des Online-Dienstes an.

Die Optionen sind:

- **Keinen COM-Port.** Die Anwendung läuft rein lokal und baut keine Verbindungen ins Internet oder anderswohin auf.
- **Com1.** Die Anwendung benutzt die Schnittstelle COM1.
- **Com2.** Die Anwendung benutzt die Schnittstelle COM2.
- **Com3.** Die Anwendung benutzt die Schnittstelle COM3.
- 5. Klicken Sie auf die Schaltfläche *Änderungen speichern*.

---

### Löschen einer Anwendung aus der Sperrliste

Heben Sie die gewünschte Anwendung in der Liste hervor und drücken Sie die Taste <Entf>.

---

### Regeln für die Sperrliste

- Die Sperrliste kann maximal 8 Einträge enthalten, einschließlich der bei Auslieferung von Cyber Patrol voreingestellten. Sie können letztere jedoch aus der Liste löschen und durch andere Anwendungen

ersetzen.

- Jeder Anwendungsname darf bis zu 32 Zeichen lang sein.
- Nehmen Sie keine 32-Bit-Anwendungen in die Liste auf. Cyber Patrol kann keine 32-Bit-Anwendungen überwachen.

---

**Siehe auch:** [Regeln für Internet-Zugang](#)

## Sperrmechanismen für Spiele & Anwendungen

Da sich lokale Anwendungen anders verhalten, als Internet-Sites, benutzt Cyber Patrol für erstere unterschiedliche Sperrmechanismen.

---

### Wann werden Spiele & Anwendungen gesperrt?

Der Zeitpunkt ist abhängig von den bei *Spiele & Anwendungen* vergebenen Zugangsberechtigungen:

- *Voll*: Die Anwendungen in der Sperrliste werden nie gesperrt.
- *Selektiv*: Die Anwendungen in der Sperrliste werden gemäß der festgelegten Zeitbeschränkungen gesperrt bzw. freigegeben. Dies gilt sowohl für tageszeitliche als auch für kumulative (tägliches bzw. wöchentliches Limit) Zeitbeschränkungen.
- *Kein*: Die Anwendungen der Sperrliste sind immer gesperrt. Sie müssen das Assistentenkennwort benutzen, um die Anwendungen zu starten.

### Beispiel:

Enthält die Sperrliste die Datei SOL.EXE (das Windows-Spiel Solitaire) und Sie markieren das Optionsfeld *Kein* als Zugangsberechtigung für *Spiele & Anwendungen*, so kann niemand ohne Kenntnis des Assistentenkennwortes Solitaire starten.

Enthält die Sperrliste die Datei WINCIM.EXE (CompuServe) und Sie markieren das Optionsfeld *Selektiv* als Zugangsberechtigung für *Spiele & Anwendungen*, so können Sie die Betriebszeiten so wählen, daß ein Internet-Zugang (ein Starten von WINCIM) nur an Wochentagen zwischen 19:00 Uhr und 21:00 Uhr möglich ist.

---

### Wirkungsweise der Anwendungssperre

Cyber Patrol überprüft alle 30 Sekunden, ob Anwendungen laufen, die in der Sperrliste aufgeführt sind und beendet diese gegebenenfalls.

Deshalb können Sie eine zugangsbeschränkte Anwendung zwar starten, diese wird jedoch nach spätestens 30 Sekunden gesperrt d. h. abgebrochen.

---

### Lesen Sie auch:

[Das Dialogfeld Spiele & Anwendungen](#)  
[Nutzungszeiten festlegen](#)

## Beispiele für Programme von Online- Diensten

Einige Beispiele für Programme, mit denen Sie Zugang zu einem Online-Dienst erhalten:

### **America Online**

WAOL.EXE

### **CompuServe**

AIRMOS.EXE (Internet Browser)

CID.EXE (CompuServe Dialer)

WINCIM.EXE (CompuServe Information Manager)

CS3.EXE (CompuServe 3.0.2)

### **Prodigy**

PRODIGY.EXE

Die Programme, die Sie benutzen, um Zugang zu Ihrem Online-Dienst zu erhalten, können von den oben genannten abweichen.

- **Online- und Druckprofile**

Sie haben folgende Möglichkeiten, Nutzungsinformationen einzusehen:

[Profile ausdrucken](#)

Sie können die Profile ausdrucken.

[Nutzungsprofile anzeigen](#)

Sie können die Nutzungsprofile online anzeigen lassen.

## Profile ausdrucken

Sie können Profile ausdrucken, die die Nutzung des Internets zeigen.

---

### Druckereinrichtung

Wählen Sie aus dem Menü *Datei* den Befehl *Druckereinrichtung*, um den Drucker oder Druckeroptionen zu ändern.

---

### Internet Nutzungsprofil

Dieses Profil zeigt die Zeiten, in denen das Internet benutzt wurde. Um dieses Profil zu drucken, wählen Sie aus dem Menü *Datei* den Befehl *Internet-Nutzungsprofil drucken*. Weitere Informationen finden Sie unter [Das Dialogfeld Profileinstellungen](#).

---

### Das Dialogfeld *Cyber Patrol-Steuerpult*

Im Dialogfeld *Cyber Patrol-Steuerpult* werden die aktuellen Einstellungen für die Zeitbeschränkung und den Zugang zu Internet-Diensten angezeigt. Um den Inhalt des Dialogfelds *Cyber Patrol-Steuerpult* auszudrucken, wählen Sie aus dem Menü *Datei* den Befehl *Internet-Nutzungsprofil drucken*.

## Nutzungsprofile anzeigen

Sie erhalten eine grafische Darstellung der Nutzungsprofile Ihrer Kinder, wenn Sie im Dialogfeld *Cyber Patrol-Steuerpult* einen der folgenden Befehle aus dem Menü *Optionen* wählen.

[Profil \(Freigabe\)](#)

[Profil \(Geschützt\)](#)

[Profil \(Gesamt\)](#)

---

### Was Sie im Nutzungsprofil sehen können

Im Nutzungsprofil wird folgendes angezeigt:

1. In der Zeitkarte wird die Tageszeit angezeigt, in der auf das Internet zugegriffen wurde.
  - **Grau** = Auf das Internet wurde während dieser Zeit nie zugegriffen.
  - **Grün** = Auf das Internet wurde mit Cyber Patrol-[Zugriffskontrolle](#) zugegriffen.
  - **Rot** = Auf das Internet wurde unter Freigabe der Cyber Patrol-[Zugriffskontrolle](#) zugegriffen.
2. Die Gesamtstunden pro Tag werden in der Spalte *Freigabe Std./Tag* angezeigt.
3. Die Gesamtstunden pro Woche werden im Feld *Std./Kalenderwoche* angezeigt.

---

### So kehren Sie zum Normalbetrieb zurück

Um das Nutzungsprofil zu verlassen und zum Normalbetrieb zurückzukehren, klicken Sie auf eine der folgenden Schaltflächen, die entsprechend dem aktuellen Nutzungsprofil angezeigt werden:

- die Schaltfläche *Profil (Freigabe) schließen*.
- die Schaltfläche *Profil (Geschützt) schließen*.
- die Schaltfläche *Profil (Gesamt) schließen*.

---

### So drucken Sie das Nutzungsprofil aus

Um das Nutzungsprofil zu drucken, wählen Sie aus dem Menü *Datei* den Befehl *Steuerpult drucken*.

---

### Regeln für die Berechnung der Gesamtstunden

Die Zeit wird in 5-Minuten-Abschnitten gemessen. Wenn Sie auf das Internet von 10:55 bis 11:05 zugreifen, wird dies als 10 Minuten Benutzung gerechnet. Wenn Sie jedoch auf das Internet von 10:58 bis 11:02 zugreifen, wird dies auch als 10 Minuten Benutzung gerechnet, weil Sie sich im Zeitsegment von 10:55-11:00 und im Zeitsegment von 11:00-11:05 im Internet befanden.

Die Zeit im Betriebsstunden-Diagramm wird in 30-Minuten-Abschnitten berechnet. Wenn Sie zwischen 10:55 bis 11:05 auf das Internet zugreifen, zeigt das Diagramm eine Benutzung von 10:30-11:30 an, weil Sie sich in den Zeitsegmenten von 10:30-11:00 und 11:00-11:30 im Internet befanden.

Im Profil (Gesamt) wird ein 30-Minuten-Abschnitt nur in der Rubrik für die Freigabe der Zugriffskontrolle angezeigt, wenn zu dieser Zeit sowohl unter der Zugriffskontrolle als auch unter Freigabe derselben auf das Internet zugegriffen wurde.

---

### Statistische Daten zu Cyber Patrol

Cyber Patrol speichert die Daten zur Benutzung 120 Tage lang.



## **Profil (Freigabe)**

In diesem Diagramm wird die Zeitdauer dargestellt, in der auf das Internet unter Freigabe der Cyber Patrol-Zugriffskontrolle zugegriffen wurde.

## **Profil (Geschützt)**

In diesem Diagramm wird die Zeitdauer dargestellt, in der von Benutzern, die die Cyber Patrol-Zugangskontrolle nicht aufheben können, auf das Internet mit Cyber Patrol-Zugriffskontrolle zugegriffen wurde.

## **Profil (Gesamt)**

In diesem Diagramm wird die Gesamtzeit dargestellt, in der sich Benutzer im Internet befanden, inkl. Freigabe und geschütztem Zugriff.

## **So senden Sie uns Ihre Anmerkungen und Empfehlungen**

Sie können Anmerkungen, Empfehlungen und Problemlberichte an Cyber Central senden. Weitere Informationen finden Sie unter [Mit Cyber Central verbinden](#).

## **Das Kontrollkästchen *Systemkonfiguration beifügen***

Für die Bearbeitung von Fehlerberichten / Kommentaren brauchen wir einige Informationen über Ihre Systemkonfiguration. Wir benötigen diese Informationen, damit wir unsere Produkte ständig verbessern und alle Probleme, die mit Cyber Patrol auftreten, lösen können.

Wenn Sie das Kontrollkästchen *Systemkonfiguration beifügen* aktiviert haben, werden einige Informationen über Ihr PC-System zusammen mit anderen Informationen an Cyber Central gesandt: *Bitte beachten Sie, daß diese Informationen sich auf die in folgendem Beispiel genannten Angaben beschränken:*

---

### **Ermittelte System Information (Beispiel)**

BIOS = 1985-1993,AMIAmerican Megatrends Inc. Alle Rechte vorbehalten.

CPU = 80486

AT-Geschwindigkeit = 435 Mhz

BILDSCHIRM; = 800x600x65536

Controller = STB Vision Display Meta Driver

SPEICHER = 8

CD-ROM = Nein

DOS Version = 6.22

Windows Version = 3.10

Netzwerk = Novell NetWare (Shell-Version 3.26 oder höher)

Soundkarte = Creative Sound Blaster Pro Waveform und Midi

Plattengröße = C: 0404-0093;

## Das Dialogfeld *Inspektionsmeldung*

In diesem Dialogfeld können Sie Internet-Sites angeben, die der CyberNOT-Liste hinzugefügt oder aus der CyberNOT-Liste entfernt werden sollen.

---

### **So bereiten Sie eine Inspektionsmeldung vor und senden sie:**

Tragen Sie Informationen in die folgenden Felder ein:

**Ihre E-Mail-Adresse:**

Hier tragen Sie Ihre vollständige Internet-E-Mail-Adresse ein.

**Site-Adresse:**

In dieses Feld geben Sie die Adresse der Sites ein, der hinzugefügt oder entfernt werden soll.

**Gründe:**

Hier geben Sie Gründe an, warum der Standort hinzugefügt oder entfernt werden soll.

Klicken Sie dann auf die Schaltfläche *Inspektionsmeldung absenden*. Cyber Patrol sendet automatisch eine Meldung mit den eingegebenen Informationen an [Cyber Central](#).

---

**Lesen Sie auch:** [Mit Cyber Central verbinden](#)

## Fehlerberichte / Kommentare online

Mit diesem Dialogfeld melden Sie Cyber Central einen [Bug](#) von Cyber Patrol. Sie können uns auch Empfehlungen oder andere Anmerkungen zu dem Produkt senden.

---

### So bereiten Sie einen Fehlerbericht / Kommentar vor und senden ihn:

1. Tragen Sie Informationen in folgende Felder ein. Die Informationen helfen dem Kundendienstmitarbeiter von Cyber Patrol, sich mit Ihnen in Verbindung zu setzen, falls weitere Informationen nötig sind.

#### Ihre E-Mail-Adresse:

Hier tragen Sie Ihre vollständige Internet-E-Mail-Adresse ein.

#### Ihr Name:

In dieses Feld geben Sie Ihren Namen ein.

#### Tel.:

Hier tragen Sie Ihre Telefonnummer ein.

2. Füllen Sie das folgende Feld aus:

#### Problem oder Kommentar:

Hier können Sie eine Anmerkung oder Problembeschreibung eingeben.

3. Aktivieren Sie das Kontrollkästchen [Systemkonfiguration beifügen](#) (optional).
4. Klicken Sie auf die Schaltfläche *Bericht / Kommentar absenden*. Cyber Patrol sendet automatisch eine Meldung mit den eingegebenen Informationen an [Cyber Central](#).

---

**Lesen Sie auch:** [Mit Cyber Central verbinden](#)

## Das Dialogfeld *Profileinstellungen*

Mit Hilfe des Dialogfelds *Profileinstellungen* drucken Sie ein Nutzungsprofil für einen bestimmten Kalendermonat aus.

---

### Was wird in diesem Profil angezeigt

Das Nutzungsprofil für einen Monat zeigt an, wie lange jeden Tag auf das Internet zugegriffen wurde inklusive der Gesamtnutzungsdauer für diesen Monat. Getrennte Zugriffszeiten werden für folgende Punkte berechnet:

- **Profil (Freigabe)**  
Die Gesamtzeit, in der auf das Internet unter [Freigabe](#) der Cyber Patrol-Zugriffskontrolle zugegriffen wurde.
  - **Profil (Geschützt)**  
Die Gesamtzeit, in der sich Benutzer im Internet befanden, während die Cyber Patrol [Zugriffskontrolle](#) aktiviert war.
  - **Profil (Gesamt)**  
Die Gesamtzeit, in der sich Benutzer im Internet befanden, d. h. Zugriff unter Zugriffskontrolle und unter Freigabe.
- 

### So drucken Sie ein Profil aus

So drucken Sie ein Profil aus:

1. Wählen Sie aus dem Menü *Datei* des Cyber Patrol-Steuerpults die Option *Nutzungsprofil drucken*.
2. Wählen Sie für das Feld *für den Monat* einen Monat für das Profil.
3. Klicken Sie auf die Schaltfläche *Profil drucken*.

Das Profil wird auf dem aktuell unter Windows gewählten Drucker gedruckt.

---

**Lesen Sie auch:**     [Profile ausdrucken](#)

## Sperrmeldungen und -codes

Es gibt zahlreiche Gründe, warum der Zugriff von Cyber Patrol gesperrt wird. Im Fall einer Zugriffssperrung wird eine Fehlermeldung und ein numerischer Code angezeigt. Die Bedeutung der einzelnen numerischen Codes ist im folgenden beschrieben.

Code	Beschreibung
CODE:1	Die Site wurde aufgrund ihrer <a href="#">IP-Adresse</a> gesperrt. Beispiel: Wenn die Site <b>www.abcxyz.com/lmnop</b> unter Anzeige der Meldung CODE:1 gesperrt wird, wurde die Adresse aufgrund des Adreßteils <b>www.abcxyz.com</b> gesperrt.
CODE:2	Die Site wurde aufgrund eines ihrer Verzeichnisse gesperrt. Beispiel: Wenn die Site <b>www.abcxyz.com/lmnop/</b> unter Anzeige der Meldung CODE:2 gesperrt wird, wurde die Adresse aufgrund des Verzeichnisses <b>lmnop</b> gesperrt.
CODE:3	Die Site wurde aufgrund des SafeSurf SS~~-Bewertungsstandards gesperrt. (Eine von SafeSurf PICS hervorgerufene Sperre wird mit CODE:4 und nicht mit CODE:3 gekennzeichnet.)
CODE:4	Die Site wurde aufgrund des PICS-Bewertungsstandards gesperrt.
CODE:5	Die Site wurde aufgrund einer <a href="#">IRC-Sperrphrase</a> in einem Teil der von Ihnen eingegebenen URL gesperrt. Bei den Internet-Sites werden die Verzeichnisse oder Daten, die nach der <a href="#">Domäne</a> stehen auf IRC-Sperrphrasen durchsucht. Die Domäne selbst wird dabei nicht auf IRC-Sperrphrasen getestet. Bei Newsgroups werden die IRC-Sperrphrasen auf alle Teile der Adresse angewendet.
CODE:6	Die Site wurde von Cyber Sentry, einem weiteren Produkt von Microsystems Software Inc., gesperrt.
CODE:7	Dieser Code ist für den zukünftigen Gebrauch reserviert.
CODE:8	Die Site wurde aufgrund des Filters für Domänen gesperrt.

## Systembeschränkungen

Im folgenden werden die Systembeschränkungen beschrieben:

---

### Anzahl der möglichen Einträge pro Feld:

In den Feldern für die zusätzlich gesperrten und zusätzlich erlaubten Bereiche kann pro Feld folgende Anzahl an Einträgen vorgenommen werden:

Dialogfeld	Cyber Patrol 3.x	
	Zus. gesperrte Bereiche	Zus. erlaubte Bereiche
WWW, FTP & andere Dienste:	64	64
Newsgroup-Kontrolle:	64	64
Internet Relay Chat - IRC-Kontrolle:	64	64
Spiele & Anwendungen:	16	n/a
ChatGard:	32*	n/a

*\* einschließlich 6 standardmäßig gesperrter Phrasen*

---

### Anzahl der möglichen Zeichen pro Eintrag:

In den Feldern für die zusätzlich gesperrten und zusätzlich erlaubten Bereiche kann pro Eintrag folgende Anzahl an Zeichen eingegeben werden:

Dialogfeld	Cyber Patrol 3.x	
	Zus. gesperrte Bereiche	Zus. erlaubte Bereiche
WWW, FTP & andere Dienste:	64	64
Newsgroup-Kontrolle:	64	64
Internet Relay Chat - IRC-Kontrolle:	20	64
Spiele & Anwendungen:	16	n/a
ChatGard:	32	n/a

## **Akustisches Signal**

Bei der Installation von Cyber Patrol wird in der Windows-Systemsteuerung unter *Akustische Signale* ein akustisches Ereignis angelegt. Dieses Ereignis tritt immer dann ein, wenn der Zugriff von Cyber Patrol gesperrt wird.

Sie können dieses Ereignis mit einer beliebigen Datei verknüpfen.

Der Name des Ereignisses lautet Cyber Patrol Intercept.

**Cyber Patrol für Fun Online, Hilfe - März 13, 1997**

## Cyber Patrol registrieren

### So registrieren Sie Cyber Patrol für Fun Online

Gehen Sie wie folgt vor:

1. Stellen Sie eine Internet-Verbindung mit Fun Online her.
2. Klicken Sie mit der rechten Maustaste auf das Cyber Patrol-Symbol. Das Menü wird angezeigt.
3. Wählen Sie die Option *Steuerpult*.
4. Bei der Kennwortabfrage geben Sie IHR Kennwort ein. Haben Sie sich noch kein eigenes Kennwort vergeben, so fragen Sie bei unserer [Hotline](#) nach Ihrem persönlichen Kennwort. Klicken Sie auf die Schaltfläche *Kennwort prüfen*, oder drücken Sie die Eingabetaste. Nun können Sie das Steuerpult benutzen.
5. Wählen Sie aus Menü *Optionen* den Befehl *Online-Registrierung*.
6. Folgen Sie den Anweisungen im Dialogfeld [Online-Registrierung](#).

---

### Hilfe! Eine Registrierung ist nicht möglich, da Cyber Patrol meinen Fun Online Zugang beschränkt!

Wenn Sie Cyber Patrol nicht sofort bei der Installation registriert haben, kann Cyber Patrol Ihren Internet- und Fun Online Zugriff beschränken.

Wenn im Cyber Patrol-Symbol ein **rotes P** erscheint, ist der Zugriff beschränkt. Cyber Patrol befindet sich im Betriebsmodus *Internet-Zugang sperren*.

Behebung des Problems:

1. Klicken Sie mit der rechten Maustaste auf das Cyber Patrol-Symbol. Es erscheint ein Menü.
2. Wählen Sie den Befehl *Schließen*. Dadurch entfernen Sie Cyber Patrol vom Desktop, ohne es zu deinstallieren.
3. Bei der Kennwortabfrage geben Sie IHR Kennwort ein. Haben Sie sich noch kein eigenes Kennwort vergeben, so fragen Sie bei unserer [Hotline](#) nach Ihrem persönlichen Kennwort. Klicken Sie auf die Schaltfläche *Kennwort prüfen*, oder drücken Sie die Eingabetaste.
4. Stellen Sie eine Internet-Verbindung mit Fun Online her.
5. Öffnen Sie die Gruppe der Cyber Patrol Programmsymbole. Klicken Sie zweimal auf das Cyber Patrol-Symbol. Nun wird Cyber Patrol wieder auf Ihrem Desktop angezeigt.
6. Klicken Sie mit der rechten Maustaste auf das Cyber Patrol-Symbol. Es erscheint ein Menü.
7. Wählen Sie die Option *Steuerpult*.
8. Bei der Kennwortabfrage geben Sie IHR Kennwort ein. Haben Sie sich noch kein eigenes Kennwort vergeben, so fragen Sie bei unserer [Hotline](#) nach Ihrem persönlichen Kennwort. Klicken Sie auf die Schaltfläche *Kennwort prüfen*, oder drücken Sie die Eingabetaste. Nun können Sie das Steuerpult benutzen.
9. Wählen Sie aus Menü *Optionen* den Befehl *Online-Registrierung*.
10. Folgen Sie den Anweisungen im Dialogfeld [Online-Registrierung](#).

## Das Dialogfeld Online-Registrierung

Mit diesem Dialogfeld können Sie Ihre Cyber Patrol-Kopie elektronisch bei Cyber Central registrieren lassen.

---

### So registrieren Sie Ihre Cyber Patrol-Kopie

1. Geben Sie Ihren Fun Online Namen im Feld *Fun Online Name* ein.
2. Erfragen Sie Ihre BID-Nummer bei unserer [Hotline](#) und tragen Sie diese in das dafür vorgesehene Feld ein.
3. Geben Sie Ihren Namen, Ihre Adresse und Ihre Telefonnummer in die dafür vorgesehenen Felder ein.
4. Klicken Sie auf die Schaltfläche *Registrierungsdaten absenden*. Cyber Patrol stellt nun automatisch eine Verbindung zu Cyber Central her und leitet eine Nachricht mit Ihren Registrierungsdaten an Cyber Central weiter. Diese Nachricht wird aus Sicherheitsgründen verschlüsselt übertragen.

---

**Lesen Sie auch:** [Cyber Patrol registrieren](#)

## Cyber Patrol erneut installieren oder aktualisieren

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, daß Sie Cyber Patrol beendet haben, bevor Sie eine aktuellere Version von Cyber Patrol installieren. **Lesen Sie auch:** [Steuerpult beenden und Cyber Patrol schließen](#)
2. Deaktivieren Sie alle Anti-Virus und Schutzprogramme. Stellen Sie sicher, daß Sie nicht mehr mit dem Internet verbunden sind. Die Installation von Cyber Patrol kann nicht ordnungsgemäß erfolgen, wenn die oben angeführten Programme noch geöffnet sind.
3. Laden Sie die aktuellste Version von Cyber Patrol für Fun Online herunter , oder legen Sie eine Diskette mit der neuesten Cyber Patrol-Version ein.  
  
Cyber Patrol wird in Form eines einzelnen Programms angeboten, das sich bei der Installation selbst entpackt.
4. Führen Sie das Installationsprogramm von Cyber Patrol unter Windows aus.
  - Wenn Sie Windows 95 verwenden, suchen Sie dazu im Windows-Explorer nach dem Cyber Patrol-Setup-Programm (setup.exe), und doppelklicken Sie dann zweimal auf das Symbol oder auf den Dateinamen. Wenn Sie Windows 3.x verwenden, finden Sie das Cyber Patrol Setup-Programm in Ihrem Datei-Manager.
  - Nach der Installation können Sie Cyber Patrol von Ihrem Startmenü aus (Windows 95) oder aus Ihrer Programmgruppe (Windows 3.x) aufrufen.
5. Nun können Sie Ihre Anti-Virus-Software und die Systemschutzprogramme erneut aktivieren.

Bei einer Aktualisierung werden alle Cyber Patrol-Dateien durch neue ersetzt. Eine erneute Registrierung ist nicht erforderlich, und alle bereits eingegebenen Benutzerinformationen bleiben erhalten.

**Warnung: Stellen Sie sicher, daß Sie neue Versionen nur von Fun Online herunterladen, da sonst Ihre Registrierung beschädigt werden könnte. Laden Sie keine Kopien von anderen Quellen herunter.**

## Mit Cyber Central verbinden

Sie können [Cyber Central](#) entweder direkt über das Steuerpult erreichen.

---

### So erreichen Sie Cyber Central direkt vom Cyber Patrol-Steuerpult aus:

- Wählen Sie aus dem Menü *Optionen* die Option [Fehlerberichte / Kommentare online](#), um eine Support-Anfrage zu senden oder ein Problem mit Cyber Patrol zu melden.
- Wählen Sie aus dem Menü *Optionen* die Option [Inspektionsmeldung](#), um einen Site zu empfehlen, der der [CyberNOT-Liste](#) hinzugefügt oder aus der Liste entfernt werden soll.

## Sites für Cyber-Listen empfehlen

Sie haben die Möglichkeit, Sites vorzuschlagen, die in die [CyberNOT-Liste](#) oder in die [CyberYES-Liste](#) aufgenommen oder aus den Listen entfernt werden sollen. Wählen Sie hierzu im Cyber Patrol-Steuerpult aus dem Menü *Optionen* den Eintrag *Inspektionsmeldung*, und geben Sie im daraufhin angezeigten Dialogfeld [Inspektionsmeldung](#) die entsprechende Site-Adresse ein.

## **Glossar**

[Anwendung](#)

[Assistent](#)

[BID-Nummer](#)

[Browser](#)

[Cache](#)

[Carlin 7-Wörter](#)

[Cyber Central](#)

[CyberNOT-Liste](#)

[CyberYES-Liste](#)

[Deinstallieren](#)

[Dialogfeld](#)

[Domäne](#)

[FAQ-Liste](#)

[Bug](#)

[Finger](#)

[Firewall](#)

[Freigabe](#)

[FTP](#)

[Geschützt](#)

[Gopher](#)

[Internet Relay Chat \(IRC\)](#)

[Internet-Dienste](#)

[Internet-Zugang sperren](#)

[IP-Adresse](#)

[IRC-Sperrphrase](#)

[MSI](#)

[Newsgroups](#)

[PICS](#)

[Ping](#)

[Online-Dienste](#)

[Registrierung](#)

[RPC \(remote procedure calls\)](#)

[RSACi](#)

[SafeSurf](#)

[Service-Port](#)

[Sperren](#)

[Sperrmeldung](#)

[Spiele](#)

[Steuerpult](#)

[Testdauer](#)

[URL-Adresse](#)

[Woche](#)

[Word \(ChatGard\)](#)

WWW (World Wide Web)

## Anwendung

Eine Anwendung ist ein Software-Programm für Computer. Oft besteht eine Anwendung aus einem Hauptprogramm, das andere Programme aufruft. In diesem Fall sind das Hauptprogramm und seine untergeordneten Programme Teile derselben Anwendung.

Beispiele für Anwendungen sind: Word für Windows (Textverarbeitung), Quicken (Finanzmanagement) und WinGIF (Viewer für Grafikdateien).

## **BID-Nummer**

Die BID-(Bundle ID-)Nummer ist eine eindeutige Nummer, die Sie von Ihrem Cyber Patrol-Händler bei der Registrierung von Cyber Patrol erhalten. Die BID-Nummer ist der Nachweis, daß Sie Ihre Kopie von Cyber Patrol käuflich erworben haben.

## **Sperrern**

Sperrern bedeutet, daß der Zugang zu einem Dienst oder die Benutzung eines Dienstes, einer Anwendung oder eines Programms deaktiviert und der Benutzer zurückgewiesen wird. Möglicherweise werden Sie durch ein Dialogfeld oder eine Meldung im Web-Browser auf die Sperrung hingewiesen.

## **Bug**

Ein Bug ist ein Fehler, der in einer Software-Anwendung oder im Zusammenhang mit einer Software-Anwendung auftritt.

## **Freigabe**

Freigabe bedeutet, daß Sie die Einschränkungen durch Cyber Patrol aufheben und umgehen können. Bei einer Freigabe werden die Nutzungsbeschränkungen bezüglich Gesamtzeit und Tageszeit nicht berücksichtigt. Eine Freigabe bleibt bis Mitternacht oder so lange in Kraft, bis Windows erneut geladen oder bis derselbe Menübefehl erneut aufgerufen und die Freigabe entfernt wird.

## **Cache**

Der Cache ist ein temporärer Speicherbereich auf Ihrem Rechner, in dem erst kürzlich verarbeitete Daten gespeichert werden. Die entsprechenden Daten werden häufig im Arbeitsspeicher des Rechners, auf der Festplatte oder sowohl im Arbeitsspeicher als auch auf der Festplatte zwischengespeichert.

## **Cyber Central**

Cyber Central bezeichnet die Internet-Site, über die Cyber Patrol verwaltet und gepflegt wird. Cyber Central erfüllt folgenden Aufgaben:

- Stellt Aktualisierungen der CyberNOT-Liste (der Liste zur Kontrolle von Internet-Sites) zur Verfügung.
- Verwaltet die Cyber Patrol-Registrierung.
- Nimmt Empfehlungen für Sites entgegen, die der CyberNOT-Liste hinzugefügt oder aus ihr entfernt werden sollen.
- Nimmt Fehlerberichte und Kommentare entgegen.

## **CyberNOT-Liste**

Die CyberNOT-Liste ist eine verschlüsselte Liste mit Internet-Sites, die nach bestimmten Bereichen sortiert sind und Material enthalten, dessen Zugang Sie kontrollieren möchten.

## **Testdauer**

Cyber Patrol ist auch ohne Registrierung während der Testdauer völlig funktionstüchtig.

Während dieses Zeitraums können Sie Cyber Patrol jederzeit über das Dialogfeld *Cyber Patrol-Registrierung* registrieren.

Am Ende der Testdauer wird der Internet-Zugang eventuell gesperrt, bis Sie Cyber Patrol registrieren oder das Produkt entfernen.

## **Assistent**

Ein Assistent bei Cyber Patrol ist ein Benutzer, der das Assistentenkennwort kennt. Ein Assistent kann Cyber Patrol freigeben und hat uneingeschränkten Zugriff auf das Internet. Außerdem kann ein Assistent die Option *Internet sperren* aus dem Cyber Patrol-Symbolmenü aktivieren.

## **Dialogfeld**

Dialogfeld bezeichnet ein Fenster, das über das Cyber Patrol-Steuerpult geöffnet wird. Über Dialogfelder geben Sie Informationen an das Programm, wählen Optionen und führen Befehle in Programm-Dialogfeldern aus.

## **Internet-Zugang sperren**

Sperrern, wie im Befehl *Internet sperren*, bedeutet, daß kein Zugang zum Internet gewährt wird.

## **FAQ-Liste**

FAQ (Frequently Asked Questions) steht für *häufig gestellte Fragen*. Eine FAQ-Liste besteht aus den häufig von Kunden gestellten Fragen und den jeweiligen Antworten zu einem Produkt, zu Problemen mit dem Produkt oder zur Anwendung eines Produkts.

## **Finger**

Finger ist ein Programm, das Ihnen Wege aufzeigt oder Informationen gibt, die Sie benötigen, um in einen entfernten PC oder ein Netzwerk einzubrechen. Zum Beispiel können Sie mit Finger den Namen einer Person mit einem Netzwerk-Account und das entsprechende Login-Verzeichnis ermitteln, wenn der Besitzer eingeloggt ist. Hacker sind der Meinung, daß Finger ein sehr nützliches Programm ist.

## **Firewall**

In einer unternehmensweiten Umgebung bedeutet Firewall ein System, das den direkten Zugriff auf PCs innerhalb eines geschlossenen Systems verhindert. Firewalls wurden konstruiert, um Hacker daran zu hindern, auf ein Netzwerk zuzugreifen.

## **FTP**

FTP bedeutet File Transfer Protocol. Im Internet befinden sich auf einem FTP-Site viele Dateien, die Sie auf Ihren PC herunterladen können. Unter den Dateien, die sich auf einem FTP-Site befinden, kann sich auch anstößiges Material befinden.

## **Spiele**

Spiele sind Software-Programme, die zur Unterhaltung programmiert wurden. Spiele können so spannend sein, daß Sie sich stundenlang damit die Zeit vertreiben.

## Gopher

Gopher ist ein Programm, mit dem Sie im Internet bestimmte Sites finden können oder mit dem Sie Sites finden können, die bestimmte Kriterien erfüllen. Gopher ist kostenlos und steht seit vielen Jahren auf dem Internet zur Verfügung.

Die Verwendung von Gopher wird im Dialogfeld *WWW, FTP & andere Dienste* eingeschränkt.

## **Steuerpult**

Als Steuerpult wird der Cyber Patrol-Eingangsbildschirm bezeichnet, mit dem Sie die Zugangskontrolle festlegen und Cyber Patrol von Ihrem PC aus verwalten können. Zugang haben nur Personen, die das Zugangskennwort kennen.

## **Sperrmeldung**

Wenn jemand versucht, auf eine Internet-Site zuzugreifen oder ein Programm aufzurufen, die bzw. das durch Cyber Patrol gesperrt wurde, dann erscheint eine Meldung, die besagt, daß der Zugang verweigert wurde. Bei der Meldung handelt es sich entweder um eine Meldung des Web-Browsers oder um eine Meldung von Cyber Patrol.

## **Internet Relay Chat (IRC)**

Internet Relay Chat ist ein Internet-Dienst, mit dessen Hilfe sich Teilnehmer elektronisch miteinander unterhalten können.

IRC ist ein beliebter Freizeitsport von Jugendlichen, aber vielleicht auch der gefährlichste. Grundsätzlich ist es nicht möglich, Name, Geschlecht oder Alter der Teilnehmer von IRC zu ermitteln. Es ist aber bekannt, daß es Teilnehmern von IRC dennoch gelungen ist, wertvolle Informationen von Kindern zu erfahren, z. B. Adresse, Kreditkartennummer und persönliche Daten.

## **Internet-Dienste**

Internet-Dienste beziehen sich auf Dienste, die von Computern angeboten werden, die an das Internet angeschlossen sind. Beispiele für Internet-Dienste sind:

- WWW (World Wide Web), für Web-Zugriff und Ansicht
- FTP, für Dateiübertragung
- IRC (Internet Relay Chat)
- Gopher, Veronica, Archie und WAIS für die Informationssuche
- Telnet, für Terminalzugriff
- Newsgroups

## **IP-Adresse**

IP (Internet Protocol) ist eine Internet-Adresse, die aus einer Zahlenfolge besteht, wie z. B. 199.103.160.100

## **IRC-Sperrphrase**

IRC-Sperrphrase bezeichnet Buchstabenfolgen in der Liste, mit denen Internet-Relay-Gesprächsrunden (Chat Groups) gesperrt werden. Alle Chat Groups, in deren Namen diese Buchstabenfolge enthalten ist, können mit Cyber Patrol gesperrt werden.

## **MSI**

MSI steht für Microsystems Software Inc. Von dieser Firma wurde Cyber Patrol programmiert.

## **Newsgroups**

Newsgroups sind virtuelle Orte, an denen Benutzer Nachrichten lesen, Dateien austauschen und Nachrichten an andere Teilnehmer versenden können. Viele Newsgroups beschäftigen sich mit einem bestimmten Thema.

Da Newsgroups zumeist von keinem Sysop verwaltet werden, können sie Dateien und Diskussionen enthalten, die möglicherweise nicht für Ihre Kinder geeignet sind.

## **Online-Dienste**

Online-Dienste sind Firmen, die eigene Online-Informationendienste, oft auch einen Internet-Zugang anbieten. Normalerweise erfordern diese Online-Dienste eine Mitgliedschaft, so z. B. CompuServe, America Online oder T-Online.

Diese Online-Dienste sind in bezug auf Zugriffsmöglichkeiten, Funktionen und Höhe der Gebühren sehr unterschiedlich.

## **Ping**

Ping ist ein Hilfsprogramm (nicht in Cyber Patrol enthalten), mit dem Sie eine Meldung an einen entfernten Site senden, um eine Empfangsbestätigung (return acknowledgement) zu erhalten. Mit diesem Hilfsprogramm können Sie überprüfen, ob die Kommunikationssoftware auf beiden Sites richtig funktioniert.

Cyber Patrol beeinflusst nicht die Funktionsweise von Ping. Durch Ping werden keine schädlichen Informationen vom Sender oder Empfänger übermittelt.

## **Geschützt**

Geschützt bedeutet, daß jemand auf das Internet unter aktiver Cyber Patrol-Zugriffskontrolle zugreift und Cyber Patrol nicht umgeht. Alle Cyber Patrol-Beschränkungen sind damit in Kraft.

## **Registrierung**

Registrierung bedeutet, daß Sie Ihre Kopie von Cyber Patrol käuflich erworben haben. Neben anderen Vorteilen sind Sie damit berechtigt, die CyberNOT-Liste (die Master-Liste der potentiell anstößigen Sites) während der Dauer des Abonnements zu aktualisieren.

## **RPC (remote procedure calls)**

RPC (remote procedure calls) ist ein Protokoll, um Befehle von einem Computer in eine andere Client-Server-Umgebung zu senden. In der Regel installiert der Netzwerkverwalter eines unternehmensweiten Netzwerks einen RPC-Dienst, um andere PCs in der Firma leichter von seinem PC aus zu steuern. Nur wenige private Benutzer haben eine RPC-Unterstützung installiert.

Obwohl es sehr praktisch ist, kann RPC auch Hackern Einlaß in ein Firmennetzwerk bieten.

## Service-Port

Jedem Internet-Dienst, den Sie installieren, wird eine *Schnittstelle* oder *Service-Port*-Nummer zugewiesen.

Service-Port-Nummern werden vom Internet Standards Committee zugewiesen und sind für alle Benutzer gleich. Zum Beispiel lautet die Service-Port-Nummer für FTP-Zugriff immer 21.

---

### **So finden Sie eine Service-Port-Nummer**

Unter den Dateien, die bei der Installation des Internet-Browsers auf den PC kopiert wurden, sollte sich auch eine Liste der Dienste und Port-Nummern befinden. Da jeder Internet-Browser andere Dateien und Verzeichnisse verwendet, können wir Ihnen keine genauen Dateinamen nennen.

## **Deinstallieren**

Deinstallieren bedeutet, daß das Programm von Ihrem PC entfernt wird.

## URL-Adresse

Eine URL (Uniform Resource Locator) ist eine Internet-Adresse, wie z. B.

**<http://www.abcxyz.com/CYBER/>**

Viele Internet-Sites sind nach ihrer URL-Adresse bekannt. Beachten Sie, daß in einigen URL-Adressen die Groß-/Kleinschreibung von Bedeutung ist.

Eine URL kann aus einigen oder allen der folgenden Teile bestehen:

### ***Protokoll***

mit dem Protokoll werden Dateien gelesen und übertragen, z. B. **http:** für eine Web-Seite, **ftp:** für einen FTP-Site oder **telnet:** für einen TELNET-Site.

**/**

Jeder Schrägstrich (/) bedeutet eine Ebene in der Adressenhierarchie. Ein Schrägstrich am Ende einer Adresse ist wie ein Platzhalter, der für alle Adresse steht, die sich auf einer niedrigeren Hierarchieebene befinden.

### ***Domäne***

die registrierte Adresse von Sites, die in der Regel verschiedene Teile enthält, z. B. **www** für World Wide Web; **.abcxyz** für den Site-Namen und **.com** für ein Unternehmen. (Andere gebräuchliche Endungen lauten **.edu** für Bildungsinstitutionen und **.gov** für Regierung.)

### ***Erweiterung der Domäne***

ein Name nach der Site-Adresse steht für einen speziellen Bereich auf dieser Site.

### ***Service-Port-Nummer***

die Nummer des Service-Ports, der diesem Internet-Dienst zugewiesen wurde.

## Woche

Eine Woche ist in Cyber Patrol als eine Kalenderwoche definiert. Sie beginnt Sonntag morgens um Mitternacht und endet am Abend des darauffolgenden Samstags (um Mitternacht).

## **WWW (World Wide Web)**

WWW ist eine Abkürzung für World Wide Web, auch als "das Web" bekannt. Das World Wide Web ist ein Internet-Dienst, der allen an das Internet angeschlossenen Teilnehmern die Benutzung eines Web-Browsers (z. B. Microsoft Internet Explorer) erlaubt, um tausende Seiten mit Text, Dateien, Bildern und sogar Ton- oder Video-Clips anzuzeigen. Von einer Web-Seite können Sie problemlos eine Verbindung zu anderen Web-Seiten aufbauen, die tausende Meilen entfernt sind.

Das bei der Kommunikation mit einem Web Server verwendete Protokoll wird HTTP genannt. Die Adresse einer Web-Seite wird URL genannt.

## **Browser**

Ein Browser ist eine Anwendung, mit der Sie Internet-Sites, FTP-Sites und andere Elemente des World Wide Web anzeigen lassen können. Netscape, MOSAIC oder Microsoft Internet Explorer sind z. B. Browser.

## **Carlin 7-Wörter**

Als Carlin 7-Wörter wird eine Liste von Wörtern bezeichnet, die in einer Fernsehsendung in den siebziger Jahren zensiert wurden. Diese Liste wurde vom amerikanischen Komödianten George Carlin zusammengestellt.

## **CyberYES-Liste**

Bei der CyberYES-Liste handelt es sich um eine verschüsselte Liste, die für Kinder geeignete Internet-Sites und Newsgroups sortiert nach Inhaltsbereichen enthält.

## Domäne

Die Domäne ist ein Bestandteil von Internet-Adressen (URLs).

***Domäne:***

Die für eine Site registrierte Adresse. Gewöhnlich besteht die Domäne aus mehreren Bestandteilen, z. B **www** für World Wide Web, **.abcxyz** für den Namen der Site und **.com** zur Kennzeichnung eines kommerziellen Unternehmens.

Bei der Adresse **http://www.abcxyz.com/CYBER/** lautet die Domäne beispielsweise **www.abcxyz.com**.

## **PICS**

PICS steht für Platform for Internet Content Selection. Hierbei handelt es sich um eine aus Vertretern mehrerer Industriezweige bestehenden Arbeitsgruppe, die ein Bewertungssystem für interaktive Medien (dies umfaßt auch das Internet) erarbeitet hat.

Das PICS-Bewertungssystem wird u. a. in RSACi und SafeSurf verwendet.

## **RSACi**

RSACi bezeichnet den Internet-Bewertungsstandard des Recreational Software Advisory Council (RSAC). Mit Hilfe des RSACi-Standards werden Sites anhand der Kategorien Gewalt, Sex, Nackte Körper und Sprache bewertet.

## **SafeSurf**

Cyber Patrol unterstützt den Internet-Bewertungsstandard SafeSurf. Mit Hilfe des SafeSurf-Standards werden Sites nach ihrer Eignung für Erwachsene oder Kinder bewertet.

## **Wort (ChatGard)**

In ChatGard wird jede beliebige Kombination alphabetischer oder numerischer Zeichen als Wort bezeichnet. So gelten in ChatGard beispielsweise apple, 9000, 301A, éle usw. als Wörter.

- **Wichtige Informationen**

**Danke, daß Sie [Cyber Patrol für Fun Online](#)**

**- die Nummer 1 der Internetfilter -  
installiert haben.**

## **Löschen Sie auf keinen Fall Teile dieser Software!!!**

- Wenn Sie die Software sicher von Ihrem Rechner entfernen möchten, wählen Sie die Option *Cyber Patrol deinstallieren*.

**Cyber Patrol für Fun Online ist mit einem ausgefeilten Hacker Schutz versehen!  
Ein Löschen - auch von Teilen von Cyber Patrol - kann zum Blockieren von Windows führen.  
Dies kann eine Neuinstallation von Windows erforderlich machen.**

## **Deinstallieren ist nur mit dem Elternkennwort möglich!**

Durch die Anmeldung bei Fun Online - Das Netz hat das Kind seinen Benutzernamen und sein Kennwort per Telefon oder per Post erhalten. Ein paar Tage später erfahren die Eltern in einer getrennten Postsendung ihren Benutzernamen und ihr **Elternkennwort**.

- wenn Sie Ihr Kennwort vergessen haben... rufen Sie die [Hotline](#) an.
- Sollte Ihr Internetzugang blockiert sein... rufen Sie die [Hotline](#) an.

---

### **Wichtige unterstützende Informationen:**

Klicken Sie hier, um zu erfahren, wie Sie sich [<Mit Cyber Central verbinden>](#) können.

Klicken Sie hier, um Informationen zu den [<Ersten Schritten>](#) zu erhalten.

Klicken Sie hier, um zu erfahren, [<Was neue Benutzer wissen sollten>](#).

Klicken Sie hier, um zu erfahren, wie Sie [<Cyber Patrol deinstallieren>](#).

