



IIS dicht machen

Hacker ohne Grenzen

Nach dem Apache ist der IIS der am **meisten verbreitete Web-Server**. Eine richtige IIS-Installation ist **nicht unsicherer** als ein Apache. Wie Sie Ihren IIS sicher machen, zeigt dieser Beitrag.

THOMAS WÖLFER

Wenn man sich Web-Server unter dem Gesichtspunkt Sicherheit anschaut, scheint der IIS wirklich schlecht darzustellen. Während in Apache-Server praktisch nie eingebrochen wird, geschieht das bei IIS-Maschinen relativ oft. Das hat mehrere Gründe: Zum einen ist Microsoft-Software als Angriffsziel einfach be-

le möglichen mods mit in den Vergleich einbeziehen.

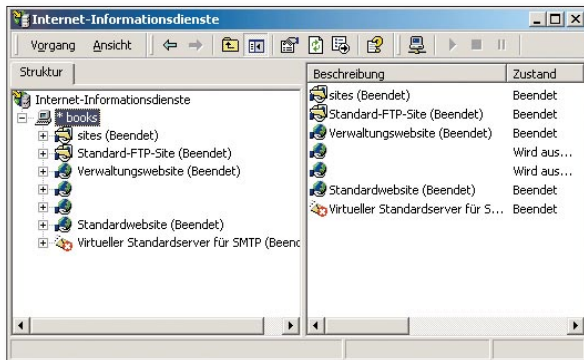
Wie auch immer: IIS-Installationen sind ein Fact of Life und eigentlich auch gar nicht so schwer zu sichern, wenn Sie sich an ein paar relativ einfache Vorgehensweisen halten.

Nach der Installation der Internet-Informationdienste sollten Sie sich über einige Dinge im Klaren sein: Sie installieren damit nicht nur einen Web-Server, sondern auch einen FTP-Server und einen SMTP-Server.

Wenn irgend möglich, sollten Sie die Verwendung mehrerer Server-Dienste auf einem Rechner vermeiden. Zumindest auf den FTP-Dienst sollten Sie verzichten. Unterbinden Sie auf jeden Fall den freien Zugang zum FTP-Dienst von beliebigen Rechnern. Das Gleiche gilt für den SMTP-Dienst, zu dem Sie übrigens einen ausführlichen Artikel an anderer Stelle in diesem Sonderheft finden.

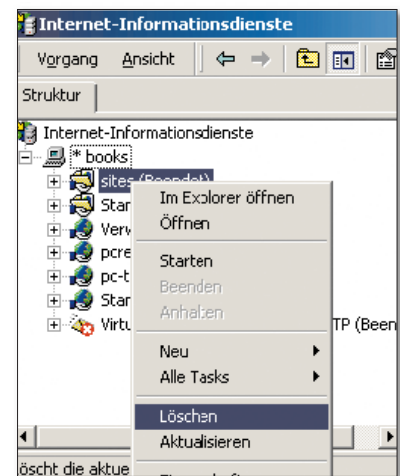
Am besten ist es, wenn Sie die Dienste einfach abschalten. Das geht direkt im IIS-Snap-in. Dort brauchen Sie bloß den richtigen Dienst auszuwählen, und ihn mit der *Stop*-Taste beenden. Wenn Sie aus irgend einem Grund einen der Dienste für lokale Operationen benötigen, geht das natürlich nicht. Ein Beispiel dafür wäre das Hochladen von Dateien auf den Web-Server oder der lokale Versand von E-Mails. Möchten Sie et-

wa auf dem Web-Server eine Seite unterbringen, mit der der Surfer weitere Informationen per Mail anfordern kann,



BEI DER INSTALLATION DES IIS installieren Sie neben dem Web-Server auch einen FTP-Server und einen SMTP-Server. Diese sollten Sie besser nicht laufen lassen.

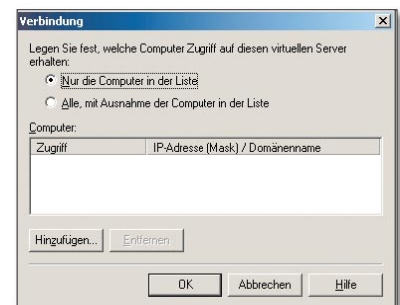
lieber. Zudem ist der Apache deutlich älter als der IIS – und das macht ihn „fehlerfreier“. Der IIS ist relativ einfach zu installieren und zu verwalten – die Default-Installation ist aber alles andere als „dicht“. Schließlich sind IIS und Apache vom Leistungsumfang her gar nicht zu vergleichen. Ein sehr großes Maß an Funktionalität, die beim IIS von Haus aus integriert wird, bekommt man beim Apache nur durch externe Module und Sprachen – oder gar nicht. Um bei Vergleichen einigermaßen fair zu bleiben, dürfte man den Apache nicht mit dem IIS vergleichen, sondern müsste zum Apache noch mindestens PHP und Perl, Datenbank-Anbindungsmodule in verschiedenen Sprachen und al-



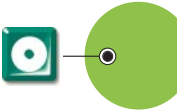
NICHT BENÖTIGTE DIENSTE mit den gemappten Sites sollten Sie nicht nur anhalten, sondern ganz löschen. Das gilt im Besonderen für die virtuellen Verzeichnisse der IIS-Beispiele.

brauchen Sie dazu den SMTP-Dienst, denn die Mail muss auf irgendwie vom Web-Server verschickt werden.

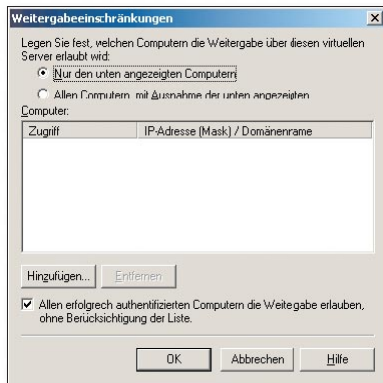
Sie können sowohl den FTP als auch den SMTP-Dienst auf bestimmte IP-



WENN DER DIALOG so aussieht wie abgebildet, kann kein Rechner Ihren SMTP-Server benutzen.



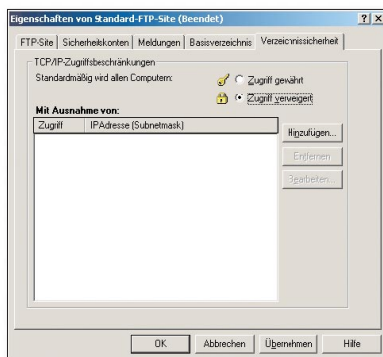
Adressen beschränken. Auf dem *Eigenschaften*-Dialog der Dienste finden Sie



WENN SIE DEN SMTP-DIENST laufen lassen, sollten Sie keine E-Mail weiterleiten – zumindest nicht für unbekannte Rechner.

dazu den Reiter *Verzeichnissicherheit*. Dort können Sie festlegen, welche Rechner auf den Dienst Zugriff haben sollen. Für den SMTP-Dienst würde es hier ausreichen, nur dem Server-Rechner selbst Zugriff zu gewähren. Das geht durch die Angabe der IP-Adresse dieses Rechners, nachdem Sie die Option *Standardmäßig wird allen Computern Zugriff verweigert* ausgewählt haben.

Im Falle des angeführten FTP-Beispiels würden Sie nur dem Rechner, von dem aus Sie die Dateien hochladen möchten, Zugriff gewähren – alle anderen Computer werden dann abgeblockt, wenn sie versuchen auf den Port des Dienstes zuzugreifen. Ein weiterer



LASSEN SIE KEINE FTP-Zugriffe zu. Wenn der Dienst schon laufen muss, dann nur für Ihren eigenen Rechner.

Dienst, der unter Umständen auf Ihrem Server betrieben wird, ist der Telnet-Dienst. Den sollten Sie auf jeden Fall abschalten. Hätte ein möglicher Angreifer Zugriff auf Ihren Telnet-Server, würde der Rechner in kürzester Zeit den Ad-

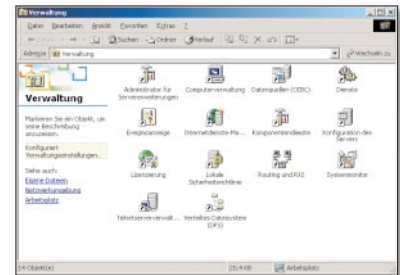
ministrator wechseln, denn Telnet ermöglicht es, die Kontrolle so über den Rechner auszuüben, als würden Sie direkt vor der Maschine sitzen und eine Konsole benutzen. Telnet verwendet außerdem eine unsichere Methode zur Authentifizierung. Wenn Sie aber aus bestimmten Gründen dennoch eine Remote-Kontrolle über den Rechner benötigen, verwenden Sie eine SSH-Lösung wie zum Beispiel das Programm *putty*. (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>).

Vom Hersteller von Putty gibt es übrigens auch einen Ersatz für FTP. Wenn möglich, sollten Sie Ihre Dateitransfers besser mit *pscp* durchführen als mit FTP. Beide Programme finden Sie auf der Heft-CD.

■ Wichtiger Unterschied: 4 oder 5 ?

Prinzipiell ist der IIS5 von Haus aus ein wenig besser gesichert, als der IIS4. Daher ist es nicht nur wegen des deutlich größeren Leistungsumfanges besser, den IIS5 und nicht die Version 4 einzusetzen. Wenn Sie aber auf den IIS4 nicht verzichten können, sollten Sie auf jeden Fall die IIS4 „Security-Checklist“ durcharbeiten. Diese führt Sie Schritt für Schritt zu einem „sichereren“ Server. Sie finden die Checkliste unter <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iischk.asp>

Beim IIS5 gibt es ein paar spezielle Werkzeuge, die das Sichern des Web-Servers deutlich vereinfachen. Man mag sich fragen, weshalb die Default-Installation des IIS5 diese Tools nicht automatisch anwendet. Die Antwort darauf ist relativ einfach. Die Anwendung von „höheren“ Sicherheitsregeln beeinträchtigt teilweise die Funktionalität des Web-Servers. Viele Installationen daraus befinden sich in einer relativ „sicheren“ Umgebung – also in einem LAN –, in der die höheren Sicherheitsanforderungen nicht ziehen oder erwünscht sind. Trotzdem kann es auch bei solchen Installationen nicht schaden, die Einstellungen zu überprüfen – und

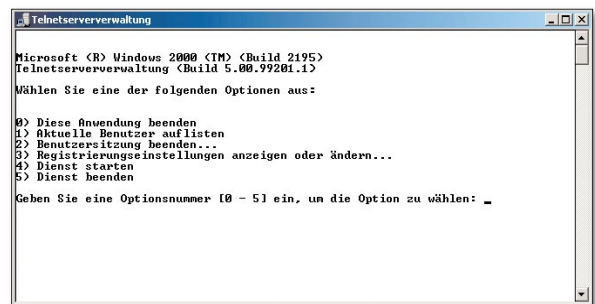


DIE TELNET-SERVER-VERWALTUNG finden Sie in der Systemsteuerung. Der Telnet-Server sollte möglichst nicht laufen.

sei dies nur, um die Ausbreitung von Würmern oder Trojanern, die sich auf anderem Weg in Ihre LAN eingeschmuggelt haben, einzudämmen.

■ Allgemeine Sicherheitseinstellungen

Der erste Schritt zu einem relativ sicheren Web-Server ist die Anwendung von



DIES IST DAS BENUTZER-INTERFACE für den Telnet-Server. Wie man sieht hat sich Microsoft nicht gerade viel Mühe mit diesem Programm gegeben.

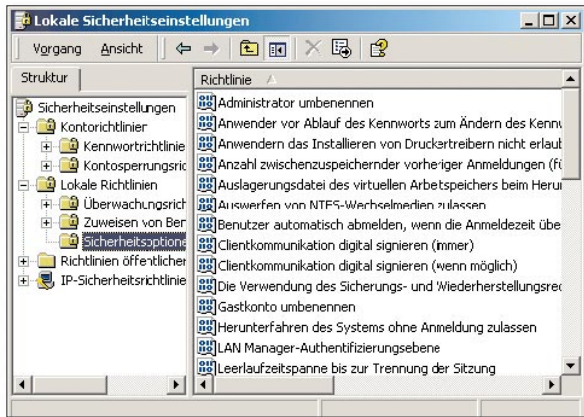
„HiSecWeb“. Dabei handelt es sich um ein Security-Template, das in Form einer .INF-Datei vorliegt. Dieses Template konfiguriert eine ganze Reihe von systemweiten Windows-2000-Einstellungen. HiSecWeb finden Sie unter <http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe> und auch auf der Heft-CD. (Wir danken Microsoft für die Freigabe, allerdings bitten wir unsere Leser sich bei Fragen nicht an Microsoft zu wenden, sondern uns zu kontaktieren unter urohde@wekanet.de).

Zur Anwendung dieses Template extrahieren Sie es zunächst aus der Exe-Datei, und kopieren Sie die daraus resultierende .INF Datei nach %windir%\security\templates.

Die .INF Datei können Sie mit dem „Security Configuration And Analy-



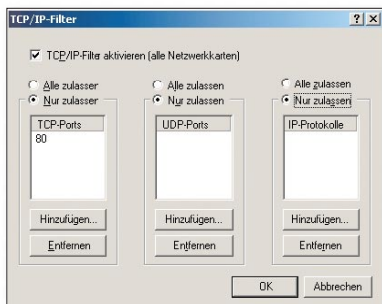
sis“-Werkzeug laden und per „Analyse now“ die Auswirkungen der neuen Einstellungen überprüfen. Vermutlich müssen Sie Teile des Templates an Ihre lokalen Bedürfnisse anpassen – wenn Sie mit den Einstellungen zufrieden sind, können Sie die Einstellungen per „Configure Computer Now“ gültig machen.



DAS HISECWEB.INF TEMPLATE setzt die lokalen Sicherheitseinstellungen so, wie Sie das von der Server-Administrierung gewohnt sind.

Danach können Sie das Template auf beliebig vielen anderen IIS-Rechnern verwenden.

Im nächsten Schritt sollten Sie alle TCP/IP-Ports sperren, die Sie nicht explizit benötigen. Bei einem öffentlichen Web-Server ist es zum Beispiel denkbar,



FÜR IHREN WEB-SERVER benötigen Sie ausschließlich einen Port. Das ist Port 80 für TCP.

dass Sie ausschließlich den Port 80 für http öffnen und alle anderen Ports schließen. Das tun Sie über die Eigenschaften des Netzwerkes, unter den TCP/IP-Einstellungen. Dort finden Sie auf dem Reiter *Optionen* die Möglichkeit *Eigenschaften* von TCP/IP-Filtern einzustellen. Bei einem reinen Web-Server sollten Sie hier alle Ports für alle Protokolle schließen und nur Port 80 für TCP zulassen. Sie leeren alle Listen auf

diesem Dialog, wählen dreimal die Option *Nur zulassen* und tragen ausschließlich unter *TCP-Port* den Port 80 ein. Damit können direkte Angriffe auf den Rechner aus dem Netz nur noch über den IIS selbst erfolgen.

Alternativ – oder besser sogar zusätzlich – sollten Sie sich überlegen, ob die Nutzung von IPSec-Richtlinien nicht angebracht wären. (Das ist eigentlich immer der Fall!). IPSec ist allerdings ein etwas aufwändiges Thema, daher hier nur der Hinweis: IPSec steht Ihnen als weiteres Sicherheits-Hilfsmittel zur Verfügung, und es wäre sicherlich nicht klug, ein zur Verfügung stehendes Werkzeug nicht zu benutzen.

Wenn Sie sich entgegen des Ratschlages, den wir weiter oben gegeben haben, entschlossen haben den Telnet-Server-Dienst auf Ihrem Rechner anzubieten, sollten Sie wenigstens sicher stellen, dass nur eine klar definierte Gruppe von Anwendern auf diesen Dienst zugreifen kann. Trotz der mäßigen Dokumentation für den Telnet-Server ist das relativ einfach möglich. Alles was Sie tun müssen, ist eine neue lokale Benutzergruppe einzurichten. Nennen Sie diese Gruppe „TelnetClients“, und fügen Sie nur die Benutzer zur Gruppe hinzu, die auch Zugriff per Telnet erhalten sollen. Wenn diese lokale Gruppe existiert – und nur dann – wird der Telnet-Server den Telnet-Zugriff auf diese klar definierte Anwender-Gruppe beschränken.

■ IIS spezifisch

Bei Ihrer IIS-Site sollten Sie die beteiligten Dateien nach dem Datei-Typ sortieren und in eigenen Verzeichnissen unterbringen. Sie sollten zum Beispiel alle CGI-Dateien (*.exe, *.dll, *.pl) in einem „cgi“-Verzeichnis, alle ASP-Dateien in einem anderen Verzeichnis, Include-Dateien (.inc..) in einem dritten und statische Inhalte (.html, .gif) in einem weiteren Verzeichnis unterbringen. Danach stellen Sie sicher, dass die Access Control Lists für diese virtuellen Verzeichnisse richtig gesetzt sind. Für die statischen Inhalte reicht es beispielsweise

aus, wenn *Everyone* nur *Read* (Lese-Berechtigung) hat. *Full Control* sollte grundsätzlich nur das „System“ und der Administrator haben.

Ebenso sollten Sie die Zugriffsrechte auf die verschiedenen IIS-Logdateien überprüfen. Dabei ist es sinnvoll, das Log-in beim IIS einzuschalten, falls das noch nicht der Fall sein sollte.

■ Wichtig: Beispiele weg

Der IIS kommt mit einer ganzen Reihe an Beispielprogrammen und auch einer kompletten auf HTML-basierenden Server-Verwaltung. Diese Beispiele sind schön und gut und als Hilfe auf Ihrem Staging-Server sicherlich gut aufgehoben. Das gilt jedoch nicht für den Produktions-Server, denn der hängt am In-



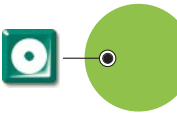
WENN SIE DEN TELNET-SERVER doch betreiben wollen, sollten Sie mindestens die lokale Gruppe „TelnetClients“ anlegen.

ternet! Bei den Beispielen handelt es sich ausschließlich um Beispiele und nicht um Anwendungen, die Außenstehenden zur Verfügung stehen sollten. Soweit es um die Beispiele geht sind drei Verzeichnisse betroffen, und diese sollten Sie komplett entfernen:

- \IISamples (\inetpub\iissamples)
- \IISHelp (\winnt\help\iishelp)
- \MSADC (\programme\common files\system\msadc)

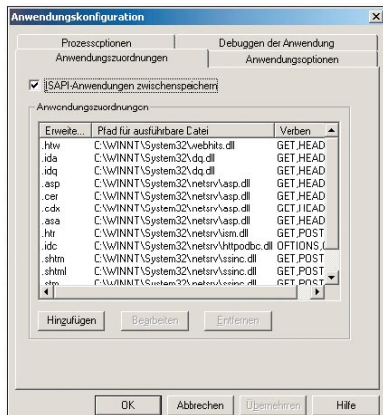
Entfernen Sie dabei sowohl die virtuellen Verzeichnisse (in der Liste oben als erstes angegeben) als auch die tatsächlichen Verzeichnisse auf Ihrer Festplatte.

Wenn irgend möglich, entfernen Sie auch das auf HTML basierende Administrations-Interface mit allen zugehörigen virtuellen Verzeichnissen. So angenehm dieses Interface sein mag, jedermann hat Zugriff darauf, die Lage der Software auf Ihrer Platte und die Namen der beteiligten virtuellen Verzeichnisse



sind bekannt. Wenn Sie auf keinen Fall auf dieses Tool verzichten wollen, sollten Sie zumindest die Namen der virtuellen Verzeichnisse ändern, in denen sich die Tools befinden.

Entfernen Sie auch alle anderen virtuellen Verzeichnisse, die nichts mit Ihrer Webseite zu tun haben, im Besonderen das Verzeichnis IISADMPWD. (Die-

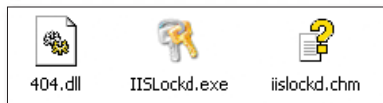


SO SIEHT ES AUS, wenn es „schlecht aussieht“. Vermutlich brauchen Sie keine dieser Datei-Erweiterungen für Ihren IIS. Also entfernen Sie sie.

ses Verzeichnis liegt dann bei Ihnen vor, wenn Sie Ihre IIS Installation durch ein Upgrade von IIS4 erhalten haben.)

■ Script-Mappings entfernen

Bei der Installation wird der IIS so konfiguriert, dass er auf die Anforderung spezieller Dateien mit speziellen Reaktionen antwortet. So gibt es etwa eine besondere Unterstützung für .htr-, .idc- und .printer-Dateien. In der IIS-Terminologie spricht man dabei von „Script Mappings“. Dabei geht es darum, dass



MIT DEM IISLOCKDOWN-TOOL stellen Sie sicher, dass Ihre IIS-Installation nur die Dienste anbietet, die Sie wünschen.

der IIS bei der Anforderung solcher Dateien bestimmte DLLs lädt und Funktionen darin aufruft. Je mehr Funktionen aus DLLs von außen aufgerufen werden können, um so mehr Angriffsfläche bietet Ihr Server. Im Normalfall werden Sie aber keine der per Default konfigurierten Script-Mappings ver-

wenden: Entfernen Sie sie! Das geht mit dem *Eigenschaften*-Dialog des IIS. Hier finden sie unter den *Haupteigenschaften* den WWW-Dienst. Klicken Sie dort auf *Bearbeiten* und dann auf den Reiter *Basisverzeichnis*.

Hier finden Sie den Button *Konfiguration*. Dieser öffnet den passenden Dialog, auf dem Sie den Reiter *Anwendungszuordnung* finden. Entfernen Sie hier alle Datei-Erweiterungen, die Sie bei Ihrer Webseite nicht benötigen. Das sind zum Beispiel .htw, .ida und .idq für den Index-Server, .printer für Internet-Printing und .idc für den Internet Database Connector.

■ User-Input validieren

Wenn Sie den Surfern auf Ihrer Webseite die Möglichkeit geben, Daten einzugeben, die auf Ihrem Server in irgendeiner Form weiterverarbeitet werden, sollten Sie alle vorhandenen Eingaben testen. Das ist am einfachsten, wenn Sie die Gruppe der zulässigen Zeichen einschränken. Angenommen, Sie wollen nur ein kleines Nachrichtensystem betreiben, ist es völlig ausreichend, wenn die Surfer alphanumerische Zeichen verwenden können und weiter nichts.

Das geht sowohl in JavaScript als auch in VBScript mit dem Regular-Expression-Mechanismus. Das folgende Beispiel entfernt etwa alle Zeichen aus einem String, die nicht im Bereich 0-9, a-z und A-Z liegen:

```
Set reg = new RegExp
reg.Pattern = "[^0-9a-zA-Z]"
strSicher = reg.Replace( str
  ↳ Unsicher, "")
```

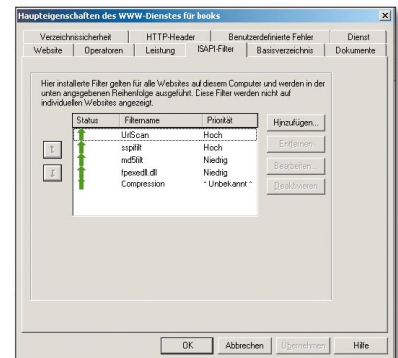
Ferner sollten Sie noch drei Tools von Microsoft einsetzen: Das sind IISLockdown, URLScan und HFNChek.

IISLockDown ist dabei ein ähnliches Werkzeug wie das HiSecWeb Template, allerdings ist es deutlich einfacher zu bedienen. Im Gegensatz zu HiSecWeb.inf betrachtet IISLockDown nur die IIS-Einstellungen und gibt Ihnen die Möglichkeit, auf einfachem Wege nur die Funktionen im IIS zu aktivieren, die Sie tatsächlich wünschen. IIS hat dabei zwei Modi. Der eine ist automatisch und verwendet einen „sicheren“ Satz an Voreinstellungen. Der zweite Modus erlaubt es Ihnen, den gewünschten Funktionsumfang selbst zu wählen. (Der automatische Modus schützt einen Web-Server übrigens so, dass er von den kürzlichen Angriffen von CodeRed und einer Vielzahl von anderen bekannten Angriffsformen geschützt ist, selbst

dann, wenn die zugehörigen Patches gar nicht installiert wurden.). Ausführliche Informationen zu IISLockdown finden Sie unter <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp> das Tool finden Sie auf der Heft-CD.

Mit HFNChek können Sie mehr oder weniger automatisiert sicherstellen, dass ein Server auf dem aktuellen Stand der Patches ist. Dabei können Sie sowohl den lokalen als auch entfernte Server überprüfen. Mehr Informationen zu diesem Tool finden Sie unter <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfncchk.asp>

Schließlich gibt es noch das URLScan-Werkzeug. Damit können Sie „merkwürdige“ Requests an Ihren Server von



DAS URLSCAN TOOL ist eines der mächtigsten Sicherheits-Tools für Ihre IIS-Installation. Es hat zwar keine Benutzeroberfläche, aber wenn es installiert ist, taucht es in der Liste der ISAPI-Erweiterungen an erster Stelle auf.

vornherein ausfiltern. (Die meisten Angriffe erfolgen über solche Requests.) Genau wie IISLockDown sollten Sie URLScan auf jeden Fall einsetzen. Mehr Informationen zu URLScan finden Sie unter <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/URLscan.asp>

In diesem Beitrag haben Sie erfahren, wie Sie Ihren IIS Server besser schützen können. Wenn Sie den Vorgehensweisen aus diesem Beitrag folgen, werden Sie einen verhältnismäßig sicheren Web-Server erhalten.

Sie sollten aber nicht dem Irrtum verfallen dadurch auf alle Zeiten gesichert zu sein – zumindest die Security-Information Mailing-Liste zum IIS sollten Sie auf jeden Fall regelmäßig lesen und bei Bedarf neue Patches auch tatsächlich einspielen. ✓ UR