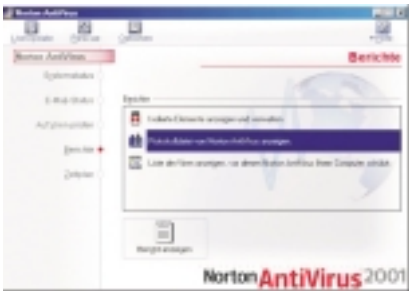
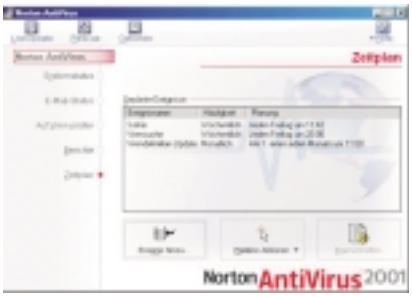
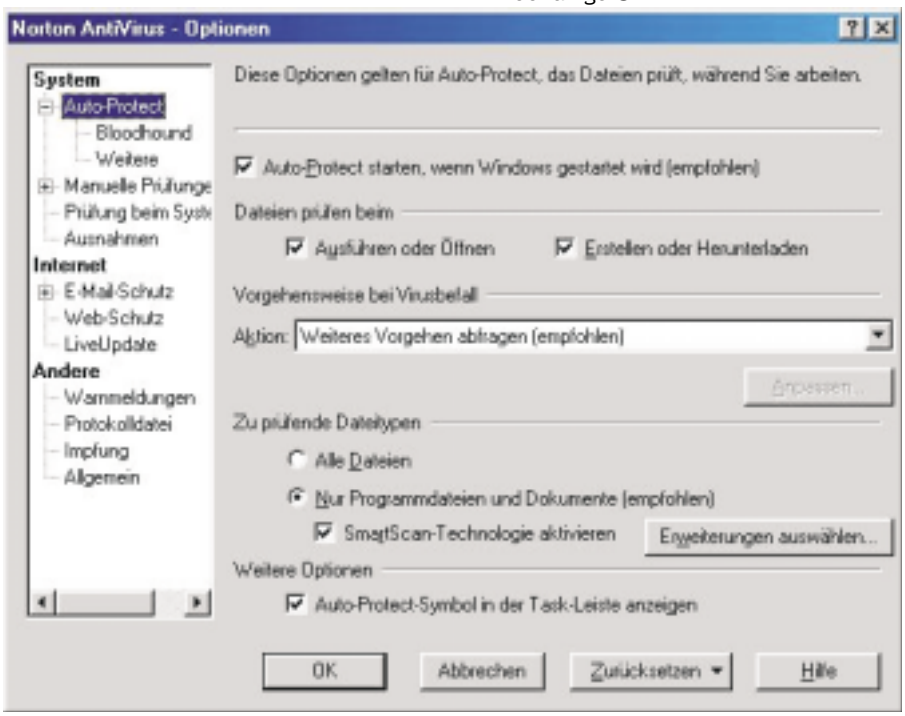


- Durch die Erstellung eines Zeitplans können sowohl regelmäßige Virenscans als auch Aktualisieren der Virendefinitionen und anderer Komponenten, aber auch automatische Starts anderer Programme und das Anzeigen von beliebigen Meldungen veranlasst werden!



Im Optionen–Fenster können sowohl Umfang der Auto-Protect-Funktion als auch vielfältige andere Einstellungen verändert werden.



Funktionen und Programmablauf

Neben der provisorischen Untersuchung von Emails und dem kontinuierlichen Schutz im Hintergrund durch automatische Prüfung aller Dateien, die verändert werden (optional) konzentriert sich das Programm auf die Erkennung bösartiger Codes wie ActiveX-Code, Java-Applets und Trojanische Pferde

Mittels Heuristischer Bloodhound-Technologie – sollen auch neue und unbekannte Viren aufgespürt werden.

Die Bloodhound-Technologie untersucht die Gesamtstruktur, Programmierlogik, Instruktionen, Dateidaten und weitere Attribute eines Programms und bewertet dann mit Hilfe von heuristischer Logik die Wahrscheinlichkeit einer Virusinfektion.

Saubere Dateien werden durchgelassen, „verseuchte“ Dateien hingegen gestoppt, bevor sie Schaden anrichten können.

Bei Eintreffen eines Virus erfolgt eine grafische Alarmierung. Der Reparaturassistent leitet Anwender durch weitere Schritte.

Neue, verbesserte Funktionen

- Automatische Aktualisierung von Virusdefinitionen über das Internet sobald Online-Verbindung aufgebaut wird (optional)
- SmartScan™-Technologie – verbessert die Leistung beim Prüfen von Dateien und verringert die Systembelastung, die durch die permanente Überwachung entstehen. (schneller)
- Umfassender Schutz durch Prüfung von E-Mail-Dateianhängen noch vor dem Öffnen oder Speichern – zusätzliche Unterstützung für MSN®-Mail, Auflistung vorhandener E-Mail-Konten unter Angabe, ob der E-Mail-Schutz für diese Konten aktiviert ist.
- Bootfähige CD

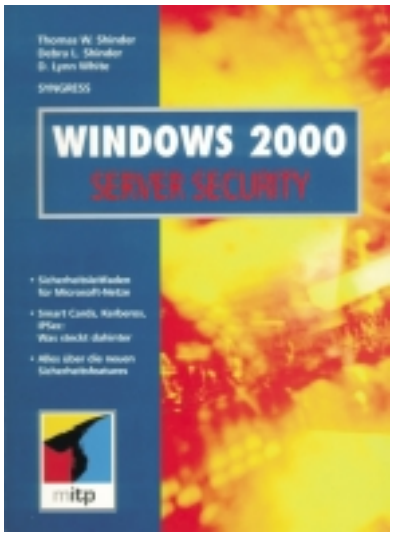
Bewertung

Das Benutzerhandbuch ist userfreundlich und übersichtlich gestaltet, verständlich verfasst und mit ergänzenden Screenshots ausgestattet.

Alles in allem ein leicht zu bedienendes Programm, das kaum merklich seine Arbeit zufriedenstellend verrichtet und hoffentlich auch im Ernstfall gut funktioniert.

Windows 2000 Server Security

Walter Kallinger



Thomas W. Shinder
Debra L.Shinder
D.Lynn White.
ISBN: 3-8266-4074-8

Da die Sicherheitsfeatures von Windows 2000 gegenüber den Vorgängerversionen um zahlreiche Sicherheitsfunktionen erweitert wurden, ist ein Buch wie dieses sicherlich für den fortgeschrittenen User von Interesse. Es beschreibt beispielsweise die Infrastruktur für öffentliche Schlüssel, das Kerberos v5-Authentifizierungsprotokoll, die Unterstützung von Smart Cards, das verschlüsselte Dateisystem und IPsec. In diesem Buch wird von einem Netzwerksicherheitsplan, dem zentrale Sicherheitskriterien für die Unternehmens-IT zu Grunde liegen, ausgegangen und so die neuen Sicherheitsfunktionen wie sie in Windows 2000 intergriert sind dargestellt. Beispiele für interessante Kapitel aus dem Inhalt sind:

- Migrationspfad zur Windows 2000 Serversicherheit
- Setzen der Standardausführungsrechte
- Authentifizierung des Kerberos - Servers
- Verteilte Sicherheitsdienste
- Wekzeuge für die Konfiguration
- Encrypted Filesystem
- IPsec Architektur
- Smart Cards
- Public Key Infrastruktur

Am Ende jedes Kapitels finden sich FAQs, die eine ausgezeichnete Möglichkeit bieten, sich selbst zu überprüfen. Textstellen für den “sehr fortgeschrittenen User” sind grau unterlegt, was sicherlich eine didaktische Hilfe darstellt. Das Kapitel über Standardbenutzerrechte ist bestimmt für jeden der zum ersten Mal einen Win-2000 Server aufsetzt eine wertvolle Arbeitsanleitung für die Praxis.