

OA-Sodat 32 (Plus)

oder "Wie schütze ich meinen PC vor unbefugtem Zugriff?"

Franz Feichtl

PCs mit den Betriebssystemen WIN NT, NOVELL oder ähnlichem bieten umfangreiche Sicherheitsvorkehrungen mit denen man sich vor unsachgemäßer Behandlung, vor mutwilligen Attacken usw. schützen kann.

Was tun, wenn man aber PCs mit dem Betriebssystem WIN9X schützen möchte? Der im Betriebssystem integrierte Schutz ist mehr als dürftig und weitere Schutzmaßnahmen sind oftmals sehr aufwendig.

Eine sehr praktikable Lösung dieses Problems lässt sich mit dem Programm O(p)timal A(ccess)-Sodat 32 realisieren.

Dieses Programm schützt bereits installierte Software und Daten auf dem Computer, verhindert die Verwendung unerwünschter Speichermedien, verunmöglicht die Installation neuer Programme, schützt die Windows-Konfigurationsdateien, schützt teilweise vor Viren (speziell Master Boot Record Viren) und ist obendrein einfach zu bedienen. (Vgl. auch PCNEWS Nr. 61, Nr. 62)

Das Programm ist für die Betriebssysteme MS-DOS, Windows 3.1 und Windows 9x vorgesehen.

Mit dem Programm OA-Sodat 32 Plus kann der Schutz noch um eine Passwortfunktion erweitert werden. Hier ein Praxisbericht:

OA-Sodat 32

Bevor man mit der Installation beginnt, ist es wichtig, alle Virens Scanner und sonstigen Programme, die im Hintergrund laufen, zu deaktivieren. OA-Sodat 32 benötigt Zugriff auf den Master Boot Record und dabei käme es sonst zu Konflikten mit einem eventuellen Virens Scanner.

Das Programm schlägt dann vor, ein Backup des MBR auf eine Diskette zu machen (sehr zu empfehlen).

Da das Programm sehr klein (ca. 600 KB) ist, dauert die Installation nur sehr kurz. Nach der Installation des Programms müssen die eigentlichen Dienste des Programms installiert werden. Und nach einem Neustart sollte der Schutz des Systems bereits aktiviert sein.

Jetzt kann mit der Konfiguration des Programms und damit der Schutzvorkehrungen begonnen werden.

Folgende Schutzmöglichkeiten stehen zur Verfügung:

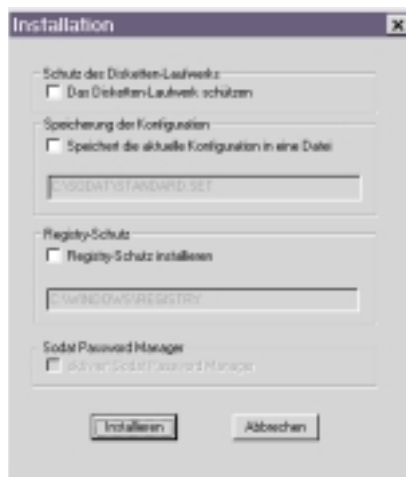


Abb. 1: Installation des Schutzsystems

- **Schutz des Diskettenlaufwerkes:** Diese Funktion unterbindet die Verwendung von nicht-„autorisierten“ Disketten (Disketten können über eine Programmfunktion autorisiert werden) und ist deshalb bestens geeignet die Kontrolle über die verwendeten Speichermedien auszuüben.
- **Schutz vor Zugriff auf die Festplatte:** Auf der Festplatte können verschiedene Dateien und/oder Verzeichnisse mit verschiedenen Attributen (read + write, read



Abb. 2: Attribute-Einstellung

only, Verzeichnis nicht benutzbar) versehen werden. Besonders praktisch in diesem Zusammenhang ist die Funktion „Verzeichnis nicht benutzbar“ da damit natürlich automatisch ein Schreib- und Leseschutz gegeben ist.

Leider lässt sich nicht eine ganze Festplatte auf einmal schützen. Erst auf der Verzeichnisebene kann man die darunterliegenden Verzeichnisse automatisch mit-schützen.

- **Schutz vor Zugriff auf die Registry:** Hier wird die Registrierungsdatenbank sehr wirkungsvoll geschützt und kann nicht mehr manipuliert werden.

• Schutz der Systemsteuerung:

Diese Funktion ist im Alltag außerordentlich nützlich und gewährleistet ein immer gleiches Erscheinungsbild des Computers. Dabei können die Benutzer durchaus Veränderungen an der Systemsteuerung durchführen, sie werden nur nicht wirksam.

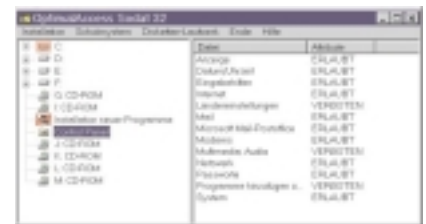


Abb. 3: Konfigurationseinstellungen

• Schutz vor der Installation neuer Programme:

Bei Aktivierung dieser Funktion ist es dem Benutzer nicht mehr möglich ein Programm zu installieren.

OA-Sodat 32 PLUS

Wem diese Schutzmaßnahmen noch zu wenig ausreichend sind, kann das Programm OA-Sodat 32 noch um das Programm OA-Sodat 32 PLUS erweitern.

OA-Sodat 32 PLUS ergänzt das Programm OA-Sodat 32 um einen Passwort-Manager und erlaubt nur noch dem durch ein Passwort autorisierten Benutzer den Zugriff. Dieser Schutz der Festplatte lässt sich auch durch die Installation der Festplatte auf einem anderen Computer nicht mehr umgehen.

Installation von OA-Sodat 32 Plus

Bevor das Programm installiert werden kann, muss der Schutzmechanismus von OA-Sodat 32 deaktiviert (=deinstalliert)

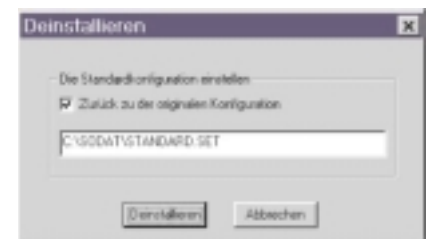


Abb. 4: Deinstallationsauswahl

werden. Nach dem notwendig gewordenen Warmstart kann mit der Installation begonnen werden. Auch hier fällt wieder der angenehm kurze Installationsvorgang auf. Nach dem neuerlichen Warmstart wird man bereits – noch bevor das Betriebssystem bootet – nach dem Passwort gefragt. Dieser Schutz erweist sich in der Praxis als sehr wirkungsvoll.

Fazit

Das Programm ist sehr einfach zu bedienen, arbeitet zuverlässig und schützt einen „Windows“-Rechner hervorragend

Weiterentwicklung von OA-Sodat 32:

Extension

Franz Feichtl

O(ptimal) A(ccess)-Sodat 32, das Programm zum Schutz des PC's vor unbefugtem Zugriff, wurde um eine weitere nützliche Programmkomponente namens Extension erweitert.

Wie sie bereits in der letzten Ausgabe der PCNEWS lesen konnten, ist das Programm OA-Sodat 32 bestens geeignet, einen PC mit den Betriebssystemen Windows 9x, Windows 3.1 oder MS-DOS gegen unsachgemäße Behandlung oder mutwillige Attacken zu schützen.

Sie haben die Möglichkeit, mit diesem Programm Diskettenlaufwerke, Festplatten, die Registry und die Systemsteuerung zu schützen. Außerdem kann man sich noch gegen das Installieren von Programmen schützen und mit der Programmiererweiterung OA-Sodat 32 Plus lässt sich der PC mit einem Passwortschutz versehen.

Mit der Programmiererweiterung OA-Sodat 32 Extension lassen sich noch zusätzlich folgende weitergehende Schutzmöglichkeiten realisieren:

OA-Sodat 32 Extension

Verstecken der Netzwerkumgebung

- Verstecken der Identifikationsseite in der *Systemsteuerung - Netzwerk*
- Verstecken des Symbols *Netzwerkumgebung*
- Sperren der Datei- und Druckerfreigabe
- Verstecken der Seite *Zugriffssteuerung* in der Systemsteuerung

Passwörter

Verstecken der Benutzerliste

- Verstecken der Seite *Kennwörter*

Drucker

- Deaktivieren der Möglichkeit, einen neuen Drucker zu installieren

- Deaktivieren der Möglichkeit einen installierten Drucker zu entfernen
- Verstecken der Seite *Druckereinstellungen*

System

- Verstecken der Seite mit den *virtuellen Speichereinstellungen*
- Verstecken der Seite *Hardwareprofileinstellungen*
- Verstecken der Option *Eigenschaften von System*
- Verstecken der Seite *Gerätmanager* in *Systemsteuerung - System*

Anwendungen

- Sperren der Verwendung der *MS-DOS-Eingabeaufforderung*
- Sperren der Verwendung von Anwendungen außer solchen, die speziell freigegeben werden

Explorer

- Entfernen des Kommandos *Ausführen* aus dem *Startmenü*
- Entfernen des Kommandos *Suchen* aus dem *Explorer*
- Entfernen des Kommandos *Systemsteuerung, Drucker* aus dem *Startmenü*
- Verstecken von Laufwerken

Anzeige

- Verstecken der Seite *Einstellungen* in der *Systemsteuerung - Anzeige*
- Verstecken aller Icons am Desktop
- Verhinderung des Sicherns der Desktop-Statusinstellungen beim Neustart

Fazit

Mit diesen neuen Programmfunktionen lassen sich also nun für einen Windows 9x, Windows 3.1 und DOS-Rechner ähnlich umfangreiche Restriktionen setzen, wie man das zum Beispiel von Windows NT her gewohnt ist. Das heißt, das Sicherheitskonzept kann mit diesen neuen Programmmöglichkeiten noch einmal verfeinert und auf die jeweiligen Bedürfnisse genau abgestimmt werden.

An dieser Stelle kann also nur noch einmal wiederholt werden, was in der letzten Ausgabe der PCNEWS zu diesem Thema schon zu lesen war.

Das Programm ist sehr einfach zu bedienen, arbeitet zuverlässig und schützt einen Windows-Rechner hervorragend vor unerwünschten Zugriffen. Das gleiche gilt natürlich für die Programmiererweiterung Extension, die genau so einfach zu bedienen und zu installieren, wie das restliche Programm. Die Programmiererweiterung kann ebenfalls mit üblichen Methoden nicht überlistet werden und es ist wirklich ein Produkt, das Systemadministratoren ein bisschen besser schlafen lässt.

Die Übersetzung der Menüpunkte aus dem Tschechischen könnte nach wie vor ein bisschen besser sein, stört aber die Funktionalität des Programms keineswegs.

Ausblick

Neben den beschriebenen Programmteilen, gibt es auch noch den Programmteil Remote Control. Damit kann man das Programm OA-Sodat32 von einem bestimmten Computer aus "fernbedienen". Dieser Programmteil bekommt von den Entwicklern gerade den letzten Schliff.

Autoren

SODAT software GmbH

- ✉ Sedláková33
CZ-602 00 Brno
Tschechische Republik
- ✉ support@sodatsw.cz

Bezugsquelle

PABLITOS Software GesmbH

- ✉ Edelsbacherstr. 50
8063 Eggersdorf
- ☎ 03117-5101-0, Fax: DW-90
- ✉ office@pablitos.co.at
- 🌐 <http://www.pablitos.co.at/>

Preise (in ATS, ohne MWST.)

	Einzel	Klasse	Schule
Basispaket	800,-	4158,-	8250,-
Extension	240,-	1250,-	2475,-

Klassenraum- und Schullizenzen inklusive Remote Control

➤ vor unerwünschten Zugriffen. Dadurch, dass die Attribute der Verzeichnisse und Dateien in einer Datei gespeichert werden können, können sie auch sehr leicht auf einen anderen Rechner mit einer ähnlichen Konfiguration übertragen werden. Der Verwaltungsaufwand ist daher auch bei mehreren Rechnern eher gering einzuschätzen.

Hervorzuheben ist auch, dass die verschiedenen Schutzmechanismen durch übliche Methoden nicht überlistet werden können. Es hilft bei installiertem Schutz weder eine Startdiskette noch die F8-Taste oder sonst ein üblicher „Trick“.

Die Übersetzung der Menüpunkte aus dem Tschechischen macht sich manchmal etwas bemerkbar, stört aber weder

die Funktionalität des Programms noch wirkt sie letztendlich sinnstörend.

Die mitgelieferten Booklets erklären die beiden Programme sehr gut und enthalten auch eine genaue Anleitung zur Installation.

Alles in allem handelt es sich hier um ein Produkt, das, wie die Autoren meinen, einen Systemadministrator wirklich ein bisschen besser schlafen lässt.