2. Praktikum

TSR-Programm

1. Aufgabe: Tastatur-Spion – Paßwort-Knacker

Die Funktion des nachfolgend zu entwerfenden Programms ist Bestandteil von Viren-Programmen, die z.B. das Paßwort eines ganz bestimmten Programms ausspionieren.

Es ist ein **speicherresidentes** TSR-Programm zu entwickeln, das **nur** während der Ausführung eines ganz bestimmten Programms (hier das Programm "PASSWORT") durch eine Manipulation der Tastencodeverarbeitung die Ausspähung der betätigten Tasten (und damit des verwendeten Paßwortes) ermöglicht.
Dies kann dadurch erreicht werden, daß die Tastenbetätigungen während der Ausführung des Programms gespeichert und nach Beendigung des Programms " PASSWORT" automatisch auf dem Bildschirm ausgegeben werden. Dann kann der Anwender aus der Codeabfolge das Paßwort ermitteln.
(Ein Virus würde die Tastencodes in eine Datei packen und an den Auftraggeber senden)

Für die Lösung dieser Aufgabe speichert dieses TSR-Programm nur nach dem Aufruf von "PASSWORT" (erfolgt durch COMMAND.COM mit DOS EXEC-Funktion 4Bh) alle Tastenbetätigungen in einen eigenen Ringpuffer und stellt dabei aber auch die normale Verarbeitung der Tastencodes sicher.
Nach Beendigung des Paßwort-Programms werde auch die Überwachung beendet und der gesamte Ringpufferinhalt auf dem Bildschirm dargestellt und daraus kann dann eventuell das gesuchte Paßwort ermittelt werden.

Für die Erkennung des Startens des auszuspionierenden Programms kann die **EXEC-Funktion 4Bh INT 21h** benutzt werden, mit deren Hilfe der DOS-Zeileninterpreter COMMAND.COM das Programm lädt und startet.
Es ist zu beachten, das COMMAND.COM den Namen des Programms nur in Großbuchstaben in den EXEC-Puffer überträgt, unabhängig von der Klein/Großschreibung der Tastatureingabe.
Außerdem trägt COMMAND.COM den gesamten Pfad in den EXEC-Puffer ein und deswegen sollte im Exec-Puffer nur nach dem nackten **Programmnamen in Großbuchstaben** als Teil des größeren Strings gesucht werden.
Skript zu EXEC-Fktn: Systemunterlagen Seite 28

Die Beendigung des auszuspionierenden Programms ("PASSWORT") kann mit Hilfe der Funktion 4Ch INT 21h erkannt werden. Obwohl natürlich noch andere Möglichkeiten der Programmbeendigung vorhanden sind, sollte aber im Rahmen dieser Praktikums-Aufgabe davon abgesehen werden.

Durch **Aufruf des TSR-Tastatur-Spions** werde das Programm im **Speicher resident** gemacht und ein nochmaliges Aufrufen soll dieses TSR-Programm dann wieder entfernen.
Skript: TSR-Programm

Optional: Der Name des auszuspähenden Programms soll in der Aufrufzeile nach einem Leerzeichen direkt hinter dem TSR-Programmnamen eingegeben werden.
Dadurch ist es dann möglich, beliebige Programme hinsichtlich der Tastatur-Eingabe auszuspionieren.

Das zur Verfügung stehende Programm **PASSWORT.EXE** fordert zur Paßworteingabe auf, verweigert den Zugriff bei einer falschen Eingabe, gibt bei korrektem Paßwort den Zugriff frei und beendet sich dann.