6.3 IT-Sicherheit/Gefahren

6.3.1 Einfallstore: Viren, Würmer und Trojaner

Durch Viren, Würmer und Trojaner wird Schadsoftware auf einem System installiert. Zur Unterscheidung dienen die Fragen:

a) Wie bekommt man sie?

b) Wie wird sie verbreitet?

Damit Schadsoftware etwas bewirken kann, muss sie immer ausführbaren Code enthalten. Das können CPU-Befehle sein (Binärprogramme, z. B. EXE-Dateien), aber auch interpretierbarer Code (z. B. Java-Class-Dateien, Batch-Dateien, Skripte, Makros).

Dieser Code kann offen liegen (in einer EXE-Datei) oder versteckt sein. So gibt es speziell geformte Anwendungsdateien (Bilder, Texte, Sound), die in sich versteckt Code enthalten, der nur in Verbindung mit einem bestimmten Programmfehler ausgeführt wird. Diese Sachlage nennt man einen *exploit*.

Zweitens muss es etwas oder jemanden geben, der diesen ausführbaren Code startet. Das kann ein Benutzer sein, aber auch ein Systemdienst, der alles startet, was an einer bestimmten Stelle steht (z. B. Bootloader oder Autostart-Ordner).

6.3.2 Virus

Ein Virus wird in eine Datei (meist in eine Programmdatei) oder in einen Bootloader kopiert. Entsprechend handelt es sich dann um einen Datei- oder einen Bootvirus. Die Datei oder der Bootloader werden dabei in der Regel nur verändert, nicht aber komplett ersetzt. Beim Start des Bootloaders oder der Datei wird der Virus-Code mit ausgeführt. Damit kann der Virus auch weitere Dateien oder Bootloader des gleichen Systems befallen.

a) Infektion: Erwerb und Start einer befallenen Datei oder eines befallenen Systems

b) Verbreitung: Kopie auf weitere Dateien/Bootloader auf diesem System

Zur Erstellung eines Virus' sind Kenntnisse in Systemprogrammierung erforderlich.

6.3.3 Wurm

Ein Wurm ist in der Regel ein eigenständiges Programm. Nach dem Start versucht er selbständig, sich in andere per Netzwerk erreichbare Systeme zu kopieren und dort ausführen zu lassen.

a) Infektion: Erwerb und absichtlicher Start des Wurm-Programms auf einem System im Netzwerk

b) Verbreitung: Kopie auf weitere Systeme per Netzwerk mit dem Ziel, dass sie auch dort ausgeführt werden

Zur Erstellung eines Wurms sind Kenntnisse in Netzwerkprogrammierung erforderlich.

6.3.4 Trojaner

Ein Trojaner ist Programm oder ein anderer ausführbarer Code, der sich tarnt (dem Benutzer vorgibt, etwas Anderes zu sein), damit der Benutzer ihn ausführt.

a) Infektion: Erwerb und Start des Trojaner-Programms unter Täuschung des Benutzers

b) Verbreitung: keine

6.3.5 Hilfsmittel: Backdoors und Rootkits

Eine Backdoor ist ein Mechanismus, der einen Zugriff auf eine Ressource (ein System, eine Datei, ein Programm) ohne die vom Administrator gewünschte Authentifizierung ermöglicht.

Manchmal werden Backdoors verwendet, um die Wartung eines Systems zu erleichtern. Standard-Passworte für BIOS und für Telefon-Anlagen sind (leider) häufig anzutreffende Beispiele. Andere legale Backdoors erlauben es, Regierungsbehörden einen Zugriff zu verschaffen (Produkte der Fa. Cisco).

Aber auch Schadsoftware, die sich per Virus, Wurm oder Trojaner verbreitet, legt oft eine Backdoor an. Schon mit normalen Berechtigungen kann ein Prozess einen Server einrichten, der dauerhaft auf Anfragen von außen lauscht.

Wesentlich schlimmer ist die Lage, wenn ein Rootkit eingerichtet wurde. Dazu muss die Schadsoftware allerdings mindestens einmal Administratorrechte erlangt haben. Ein Rootkit ersetzt wichtige Systemdateien durch eigene Versionen und könnte sich damit (entsprechenden Aufwand des Programmierers vorausgesetzt) nahezu beliebig tarnen. Ein Rootkit kann dementsprechend schwierig zu bemerken sein, solange das System eingeschaltet ist.

Ein Rootkit *kann* eine Backdoor enthalten; dadurch wird die Funktionalität des Rootkits ja erweitert; das Rootkit kann dadurch aber auch leichter entdeckt werden. Wenn ein Rootkit entdeckt wurde, müssen sämtliche geänderten Systemdateien identifiziert und gegen die Originale getauscht werden.

6.3.6 Ebenen von Angriffen

a) Netzwerke und Protokolle

   1) DOS
   2) Sniffing
   3) Spoofing
   4) Man-in-the-Middle-Angriffe
   5) WLAN-Spezialitäten

   Abhilfe: Netzwerkstruktur verbessern

b) Benutzer, Social Engineering

   1) Phishing

   Abhilfe: Benutzer beraten

c) Anwendungssoftware

   1) Exploits (*buffer overflow*, Java-Applets und ActiveX)
   2) XSS
   3) Injection

   Abhilfe: Updates, Entwickler unterstützen

d) Einzelsystem

   1) Keylogger

   Abhilfe: Einzelsystem schützen