Angriffsmöglichkeiten von PCs

Wie kann ein PC aus dem Internet angegriffen werden?

(a) **Über die automatische Ausführung von Programmen mit JavaScript, Java, ActiveX, VBScript, usw.**

(b) Über freigegebene Verzeichnisse

(c) Über offene Ports

Ports - ein offenes Tor

Jedes Programm, das eine Schnittstelle zum Internet bereit stellt, muss einen Port (eine Tür) öffnen, damit ihr PC Daten senden und empfangen kann. Ist so ein Port einmal geöffnet, kann er theoretisch von jedermann (auch missbräuchlich) benutzt werden. Allerdings kann ein Eindringling, um in diesem Bild zu bleiben, von außen dieses Tor nicht durchschreiten. Er benötigt einen 'Helfer im Haus', der für ihn Aufgaben wie Datendiebstahl oder Sabotage erledigt. Die Anweisungen an den 'Helfer' oder der Transport der gestohlenen Daten werden nur durch das geöffnete Tor ermöglicht. Ein geöffneter Port stellt also immer eine potentielle Gefahr dar.

Weshalb sind Ports geöffnet und wie kommen die internen 'Helfer' in den PC?

Wie oben beschrieben, benötigt das Betriebssystem Ports für die externe Kommunikation und erledigt bei Anfragen über diese Ports bestimmte Aufgaben. Einige 'Hacker' benutzen Insiderkenntnisse und missbrauchen (i.d.R. bei MS-Windows) das Betriebssystem für kriminelle Zugriffe. Wenn dies möglich ist, darf man das getrost als schwere Sicherheitslücke bezeichnen.

Solche Hacker verbreiten nun Programme, die sich als nette, kleine Spielerei, als Schutzsoftware (wie makaber) oder als kostenfreier Internetzugang usw. tarnen. AOL4FREE.EXE ist so ein Programm. Diese Programme haben oft nur die eine Aufgabe, sich fest in ihrem System zu installieren und einen Port (als Hintertür) zu öffnen. Ein Geschenk vom Gegner, das sich später als Falle herausstellt, kennt man aus der Geschichte als 'Trojanisches Pferd'. Odysseus besiegte mit dieser List die belagerte Stadt Troja. Programme, die nach dem gleichen Muster arbeiten, bezeichnet man ebenfalls als Trojaner oder als 'Backdoor', da sie dem Angreifer eine Hintertür öffnen.

Entsprechend ihrer Programmierung könne solche Trojaner Daten und Programme zerstören, vertrauliche Daten wie Geschäftsgeheimnisse, Kontonummern, Kennwörtet und PINs ausspionieren und damit erheblichen Schaden anrichten.

- Insgesamt stehen 65535 verschiedene Ports zur Verfügung.

Da es jedem Programmierer letztlich selbst überlassen ist, welchen Port er nutzt, könnte sich beispielsweise ein Trojaner hinter dem Port 80 verstecken, solange auf ihrem PC kein Webserver läuft. Port 80 ist ein „well known Port" und sollte eigentlich nur für die „http" Übertragung genutzt werden.

[aus: http://check.lfd.niedersachsen.de/start.php]

Aufgaben:

(a) Erkläre welche Gefahren die oben Beschriebenen Schwachstellen des Computers darstellen. Wie können Hacker sich diese Schwachstellen zunutze machen?

(b) Teste die Sicherheitseinstellungen deines Rechners über **http://check.lfd.niedersachsen.de/start.php** aus.

(c) Teste über http://www.hirnbrauser.de/ac/index.html welche Informationen man über einen Rechner (und seinen Benutzer) auf legale Weise erlangen kann.