Buffer Overflow

Der Buffer Overflow (dt. Pufferüberlauf) schreibt durch einen Fehler im System zu viele Daten in den dafür vorgesehenen Speicherberiech, dem Puffer. Dadurch werden bestimmte Speicherstellen mit denen des Overflow überschrieben. So ist es dem Hacker möglich, seinen Code an den Puffer zu senden und dessen Prozess ausführen zu lassen.

Nachfolgend ein einfaches Beispiel, in der Programmiersprache C geschrieben (keine Angst, ich erkläre es gleich, so dass es jeder verstehen kann):

Quellcode

```
1. #include <string.h>
2. void main()
3. {
4. char buf[10];
5. strcpy(buf,"Dieser Virus ist ein Fake!!!");
6. }
```

Was passiert hier?
Nun, zuerst wollen wir eine Datei einbinden, in der so einige Mechanismen definiert sind, hier um mit Texten zu arbeiten. Danach folgt die Definition des Hauptprogramms, beginnend mit **void main()** und der **{**-Klammer. Wir reservieren in dem Notizbuch **buf** Platz für 10 Buchstaben oder andere Zeichen. Dann schreiben wir aber mithilfe der Funktion **strcopy()** (unser Stift) mehr Text rein als wir dafür in dem Notizbuch reserviert haben.

Die Folge: Wir schreiben über den uns zur Verfügung stehenden Platz im Notizbuch hinaus, was natürlich nicht schön aussieht. Und in Form eines Programms gibt das dann halt folgende Fehlermeldung:

Image not found or type unknown

Der Computer weiß nur, dass er Platz für 10 Zeichen zur Verfügung bekommt. Würde er versuchen auch nur 1 Zeichen mehr zu schreiben, würden andere Daten im Arbeitsspeicher überschrieben werden oder verloren gehen. Die mit dem Buffer Overflow verbundene Beendigung des Programms ist sozusagen eine Sicherheitsvorrichtung, damit andere Daten nicht ungewollt überschrieben werden und so andere Programme oder der ganze Rechner abstürzen.

Weiteres Beispiel:
Stellt euch vor, ihr esst ganz viele Äpfel bis ihr voll seid. Dann aber überkommt euch die Lust nach Birnen. Ihr esst so viele Birnen, dass das euer Magen nicht mitmacht, und alle Äpfel wieder auskotzt. Das, was übrig bleibt, sind die Birnen (Code des Hackers) die euer Magen nun verarbeitet (Code wird in den RAM geschrieben). Euer Körper ist von der ganzen Kotzerei erschöpft, und streikt nun (das Spiel crasht), und die Birnen lassen ihrer Wirkung freien Lauf. Glückwunsch, ihr habt einen Buffer Overflow in euch selbst erzeugt!