Exploits

Exploits sind Computerprogramme oder Skripte, die gezielt Schwachstellen eines anderen Computerprogramms ausnutzen, um das betroffene System zu schädigen oder Zugang zu bestimmten Ressourcen zu erhalten.

Definition

Exploits (engl. to exploit = „ausnutzen“) machen sich spezifische Schwächen oder Fehlfunktionen anderer Computerprogramme zunutze, um beispielsweise an nicht freigegebene Daten zu gelangen oder DoS-Attacken auszuführen. Doch nicht alle Exploits haben einen kriminellen Hintergrund. In manchen Fällen werden sie ausdrücklich zur Demonstration von Sicherheitslücken („Proof of Concept“) geschrieben und veröffentlicht. Dadurch soll erreicht werden, dass Softwarehersteller möglichst schnell bekannt gewordene Schwachstellen in ihren Programmen beseitigen können.

Arten

Man unterscheidet Exploits in

- Lokale Exploits: können beim Öffnen scheinbar völlig harmloser Dateien (z. B. Bilddateien) aktiviert werden, insofern die dem Dateityp zugeordnete Anwendung eine Sicherheitslücke aufweist indem sie bei der Verarbeitung der Datei fehlerhaft bzw. unsauber arbeitet
- Remote Exploits: aktive Angriffe aus dem Internet mittels manipulierter Datenpakete oder spezieller Datenströme auf Schwachstellen in Netzwerksoftware
- DoS Exploits: überlasten die betroffene Anwendung, führen allerdings keinen fremdem Programmcode aus
- Command Execution Exploits: vom Angreifer steuerbare Ausführung von Programmcode auf dem Zielsystem
- SQL-Injection Exploits: finden sich in Bezug auf Webanwendungen, die eine SQL-Datenbank nutzen. Anfragen werden so gestellt, dass die fehlerhaft arbeitende Logikschicht Daten zurückliefert, die sie weder für den Lesezugriff noch den Schreibzugriff verfügbar machen sollte. (Beispielsweise können Eingaben in einem Log-In-Formular so gestaltet werden, dass die betroffene Anwendung einen ungültigen Benutzer dennoch erfolgreich einloggt)
- Zero-Day Exploits: erscheinen am selben Tag, an dem die Sicherheitslücke allgemein bekannt wird. (Zu diesem Zeitpunkt ist kaum ein Hersteller in der Lage, die Sicherheitslücke sinnvoll und umfassend mittels eines Patchs zu schließen)

Siehe auch:
Denial-of-Service-Angriff
Patch

Zurück