LU12b - Angriffsvarianten DOS/DDoS

Lernziele

1. Die grundlegende Funktionsweise von DoS/DDoS erklären und demonstrieren können.
2. Angriffsvektoren bzw. Angriffsarten für DoS/DDoS nennen können.
3. Nennen können wie eine DoS/DDoS-Attacke gegen die CIA-Triade wirkt und welches Schutzziel primär betroffen ist.

Grundlegende Funktionsweise

Die Angriffstechnik *DoS* nutzt eine simple Tatsache aus: Jeder Server verfügt nur über *begrenzte* Ressourcen (Rechenleistung, Arbeitsspeicher, Verbindungstabellen und Bandbreite). Werden diese Ressourcen schneller beansprucht als sie freigegeben werden können, bricht der Dienst für alle zusammen. In der nachfolgenden Abbildung wird gezeigt, wie legitime Anfragen echter Benutzer im Ansturm einer *Flood* untergehen und der Server dadurch nicht mehr antworten kann.

Das Grundprinzip einer Flood lässt sich stark vereinfacht so darstellen:

```
// von tausenden gekaperten Geräten gleichzeitig ausgeführt
while (true) {
    sende_anfrage(ziel_server);
}
```

Ein einzelner Rechner (DoS) richtet dabei meist wenig aus. Erst wenn dieselbe Schleife *verteilt* von tausenden Geräten eines *Botnets* ausgeführt wird (DDoS), summieren sich die Anfragen zu einer Last, die kein normaler Server mehr bewältigen kann. Die Verbindungstabelle läuft voll, sobald sie belegt ist, wird jede weitere Anfrage – auch die eines echten Kunden – abgewiesen.

CIA-Triade = Drei Dimensionen der IT-Sicherheit

Eine Applikation im Business-Umfeld hat grundsätzlich drei Dimensionen bzw. Ziele der Sicherheit zu gewährleisten:

- **Vertraulichkeit:** Userdaten sind weder bewusst noch unbewusst unbefugten zugänglich.
- **Verfügbarkeit:** Das System ist zu vereinbarten Zeiten vollumfänglich verfügbar.
- **Integrität:** Die Daten liegen unverfälscht vor.

Während eine *SQLi* potenziell alle drei Ziele verletzen kann, zielt eine DoS/DDoS-Attacke *primär und direkt* auf die **Verfügbarkeit** ab. Die beiden anderen Schutzziele können jedoch *indirekt* betroffen sein, wenn der Angriff als Ablenkung dient.

Angriff auf die Verfügbarkeit

Dies ist das eigentliche und direkte Ziel jeder DoS/DDoS-Attacke. Ein Angriff auf die Verfügbarkeit bedeutet, dass ein System zu vereinbarten Zeiten *nicht* mehr erreichbar ist. Je nach Geschäftsumfeld ist dies unterschiedlich kritisch: Der Lebensmittelladen um die Ecke kann sein Geschäft auch ohne IT-System betreiben. Ein Online-Shop hingegen verliert bei jedem Ausfall unmittelbar Umsatz.

Beispiel-Szenario	**Wirkung auf das Schutzziel**
HTTP-Flood gegen den Webshop kurz vor Weihnachten	Der Server ist überlastet, echte Kunden erhalten nur noch Timeouts und können nicht bestellen.

Angriff auf die Vertraulichkeit

Eine DoS/DDoS-Attacke selbst stiehlt keine Daten. Sie kann aber als *Ablenkungsmanöver* (engl. *Smokescreen*) dienen: Während das Sicherheitsteam alle Kräfte darauf verwendet, den Dienst wieder verfügbar zu machen, läuft im Hintergrund unbemerkt ein zweiter Angriff.

Beispiel-Szenario	**Wirkung auf das Schutzziel**
DDoS als Ablenkung, während parallel über eine andere Lücke Kundendaten exfiltriert werden	Der Datendiebstahl geht in der allgemeinen Aufregung unter und wird zu spät bemerkt.

Angriff auf die Integrität

Auch die Unverfälschtheit der Daten kann indirekt leiden. Sind Systeme überlastet, fallen mitunter Schutz- und Protokollmechanismen aus oder es kommt bei der überstürzten Wiederherstellung zu Fehlern.

Beispiel-Szenario	**Wirkung auf das Schutzziel**
Überlastung der Logging- und Monitoring-Systeme, während parallel Datensätze manipuliert werden	Die unbefugten Änderungen werden nicht protokolliert und bleiben dadurch unentdeckt.

---

olkan Demir

Volkan Demir