Was versteht man unter den Begriffen Denial-of-Service und Distributed-Denial-of-Service?

Denial-of-Service (DoS)- und Distributed Denial-of-Service (DDoS)-Angriffe sind vor allem für ihre Fähigkeit bekannt, den Zugriff auf mehrere Computerressourcen zu verweigern oder die Leistung eines bestimmten Dienstes oder einer bestimmten Konnektivität durch Überlastung der Netzwerk- oder Systemressourcen wie Netzwerkbandbreite, Router-Verarbeitungsfähigkeit usw. zu verringern.

Die DoS-Angriffe können in zwei Arten auftreten:

1.Der Angreifer verursacht, dass die Server abstürzen oder ihre Leistung verschlechtern, indem er die vorhandenen Softwarefehler ausnutzt.

2. Der Angreifer sendet eine große Anzahl von betrügerischen Anfragen, bis die CPU-, Speicher- oder Netzwerkressourcen des Opfers überlastet sind.

Die Distributed-Denial-of-Service (DDoS) sind eine aktualisierte Version der Denial-of-Service-Angriffe. Es verwendet Slave-Maschinen, auf die es die Verantwortlichkeiten verteilt und damit die Bedrohung erhöht. Die Auswirkungen mehrerer Angreifer sind nicht nur größer, sondern auch viel schwieriger zu erkennen.

Die DoS-Angriffe können je nach Anzahl der Angreifer und Paketvolumen wie folgt klassifiziert werden:

1. Software-Exploits: können ihr Ziel mit einem einzelnen oder wenigen Paket leicht deaktivieren, indem sie bestimmte Software-Bugs verwenden. Die einzige Möglichkeit, diese Art von DoS-Angriff zu verhindern, besteht darin, immer auf dem neuesten Stand der Software zu sein.

2.Überschwemmungsangriffe: Basierend auf der Anzahl der Angreifer können sie weiter in Single-Source- und Multi-Source-Angriffe unterteilt werden. Diese Art von Angriff funktioniert durch das Senden endloser Paketströme, bis alle Ressourcen überlastet sind.

Es gibt zwei Hauptkategorien, in denen wir die DDoS-Angriffe aufteilen können:

1. Bandbreitenverknappung: Das Netzwerk der Opfer wird mit unerwünschten Anfragen überflutet, so dass die legitimen nicht in das System gelangen können.

2. Ressourcenverknappung: Zielt auf einen Prozess oder einen Server auf dem System, der es nicht in der Lage ist, Anfragen zu bearbeiten, indem er seine Ressourcen bindet. Es verwendet entweder verwundbare Teile eines Protokolls oder sendet falsch gebildete IP-Pakete, um das System zum Absturz zu bringen.

Wie kann man so einen solchen Angriff rechtzeitig erkennen?

Es ist fast unmöglich, solche Angriffe zu erkennen. Die von den verfügbaren Tools generierten haben jedoch identifizierende Merkmale, die in einigen Fällen die Erkennung ermöglichen.

Erkennungsmechanismen wie entropiebasierte Erkennung, statistische und UNN-basierte Erkennung wurden vorgeschlagen.

Wie kann man sich davor schützen?

The first step you can take to protect yourself from such attacks is to become aware of what it implies and how to identify it. There are, of course, methods such as using an email filter for the network gateway that can capture and reduce the number of phishing emails.