**DDOS**

DDoS (Distributed Denial of Service) ist ein Angriff auf ein Computersystem, bei dem ein Netzwerk von vielen Computern verwendet wird, um das System durch eine Überlastung mit Anfragen lahmzulegen. Der Zweck eines DDoS-Angriffs ist es, die Verfügbarkeit des Systems zu beeinträchtigen, indem der Server mit einer hohen Anzahl von Anfragen überflutet wird, so dass er nicht mehr reagiert oder nicht mehr erreichbar ist.

Die DDoS-Attacke erfolgt in der Regel über eine Vielzahl von infizierten Geräten, die als "Botnet" bezeichnet werden. Diese Geräte können mit Malware infiziert werden, die es Angreifern ermöglicht, sie fernzusteuern, um Anfragen an das Ziel-System zu senden. Der Angreifer nutzt dabei die Tatsache aus, dass die Geräte in einem Botnet oft schlecht geschützt sind und häufig über eine schnelle Internetverbindung verfügen.

DDoS-Angriffe können erhebliche Schäden verursachen, insbesondere wenn sie auf kritische Systeme wie Banken, Regierungsbehörden oder Krankenhäuser abzielen. Die Systeme können durch die Überlastung mit Anfragen unzugänglich gemacht werden, was zu Ausfallzeiten, Datenverlusten und sogar finanziellen Verlusten führen kann.

Um sich vor DDoS-Angriffen zu schützen, ist es wichtig, geeignete Sicherheitsmaßnahmen zu ergreifen, wie z.B. die Verwendung von Firewalls, die Begrenzung der Bandbreite für den Netzwerkverkehr und die Überwachung des Netzwerkverkehrs auf Anomalien. Es ist auch wichtig, dass Unternehmen und Organisationen regelmäßig Backups von wichtigen Daten erstellen, um im Falle eines Angriffs eine schnelle Wiederherstellung zu ermöglichen.

**Einfache Definition**

Eine DDoS-Attacke (Distributed Denial of Service) ist ein Angriff auf ein Computersystem, bei dem ein Netzwerk von vielen Computern verwendet wird, um das System durch eine Überlastung mit Anfragen lahmzulegen. Das Ziel eines DDoS-Angriffs ist es, die Verfügbarkeit des Systems zu beeinträchtigen, indem der Server mit einer hohen Anzahl von Anfragen überflutet wird, so dass er nicht mehr reagiert oder nicht mehr erreichbar ist.

**Was tun, wenn sowas passiert:**

Im Falle einer DDoS-Attacke auf eine Gesundheitsorganisation gibt es mehrere Schritte, die unternommen werden sollten:

* Melden Sie den Angriff: Sobald eine DDoS-Attacke festgestellt wird, sollte das IT-Team der Organisation den Vorfall sofort melden. Sie können sich an spezialisierte Sicherheitsfirmen wenden, um Unterstützung bei der Bekämpfung des Angriffs zu erhalten.
* Bereiten Sie einen Notfallplan vor: Es ist wichtig, einen Notfallplan für DDoS-Attacken zu haben, der die erforderlichen Maßnahmen und Verfahren zur Eindämmung des Angriffs enthält. Die Mitarbeiter sollten über den Plan geschult und die notwendigen Ressourcen sollten zur Verfügung gestellt werden.
* Schützen Sie das Netzwerk: Es ist wichtig, das Netzwerk der Organisation zu schützen, indem geeignete Sicherheitsmaßnahmen ergriffen werden, wie z.B. die Verwendung von Firewalls, Intrusion-Detection-Systemen und anderen Sicherheitsvorkehrungen. Das Netzwerkverkehr sollte auch auf Anomalien überwacht werden, um mögliche Angriffe zu erkennen.
* Backup-Strategie: Eine regelmäßige Datensicherung sollte Teil des IT-Sicherheitskonzepts sein, um im Falle eines Angriffs die Daten wiederherstellen zu können. Die Backups sollten an einem sicheren Ort gespeichert werden.
* Kommunikation: Es ist wichtig, eine klare Kommunikationsstrategie zu haben, um die Kunden, Patienten und Mitarbeiter über den Angriff und die getroffenen Maßnahmen zu informieren. Eine transparente Kommunikation kann dazu beitragen, das Vertrauen der Öffentlichkeit wiederherzustellen und den Schaden zu begrenzen.
* Zusammenarbeit: Eine Zusammenarbeit mit anderen Organisationen und Sicherheitsfirmen kann bei der Bekämpfung des Angriffs helfen. Durch die Zusammenarbeit können Informationen und Ressourcen ausgetauscht werden, um den Angriff schnell zu bekämpfen.

DDoS-Attacken können schwerwiegende Auswirkungen auf Gesundheitsorganisationen haben und sollten daher ernst genommen werden. Eine schnelle Reaktion, eine angemessene Schulung der Mitarbeiter und die Umsetzung geeigneter Sicherheitsvorkehrungen können jedoch dazu beitragen, das Risiko von Angriffen zu minimieren und den Schaden zu begrenzen.