**Man-in-the-middle**

Ein Man-in-the-Middle-Angriff (MITM-Angriff) ist eine Art von Cyberangriff, bei dem ein Angreifer die Verbindung zwischen zwei Kommunikationspartnern abfängt und manipuliert. Der Angreifer kann dann in der Lage sein, Informationen zu stehlen, zu manipulieren oder zu injizieren, ohne dass die betroffenen Parteien davon erfahren.

Der Angreifer nutzt dabei eine Schwachstelle in der Netzwerksicherheit, um die Verbindung abzufangen und sich zwischen die beiden Parteien zu setzen. Sobald der Angreifer zwischen den beiden Parteien steht, kann er den Datenverkehr abfangen, analysieren und manipulieren, indem er z.B. Nachrichten löscht oder ändert.

Ein typisches Szenario für einen MITM-Angriff ist eine öffentliche WLAN-Verbindung, die von vielen Menschen genutzt wird. Der Angreifer kann sich in diesem Fall als ein legitimer Access Point ausgeben und die Verbindung abfangen, um Daten zu stehlen oder zu manipulieren.

Ein weiteres Beispiel für einen MITM-Angriff ist eine Phishing-E-Mail, die den Empfänger dazu bringt, auf einen bösartigen Link zu klicken. Der Angreifer kann dann den Datenverkehr zwischen dem Opfer und der angegriffenen Webseite abfangen und die Eingaben des Opfers, wie z.B. Benutzernamen und Passwörter, stehlen.

Um sich vor MITM-Angriffen zu schützen, sollten die Nutzer sicherstellen, dass sie ihre Verbindungen über sichere Protokolle wie HTTPS und SSL/TLS verschlüsseln und auf verdächtige E-Mails und Links achten.

**Einfache Definition:**

Ein Man-in-the-Middle-Angriff (MITM-Angriff) ist ein Cyberangriff, bei dem ein Angreifer die Verbindung zwischen zwei Kommunikationspartnern abfängt und manipuliert, um Informationen zu stehlen oder zu manipulieren. Der Angreifer nutzt dabei eine Schwachstelle in der Netzwerksicherheit, um sich zwischen die beiden Parteien zu setzen und den Datenverkehr abzufangen, zu analysieren oder zu manipulieren.

**Was ist zu tun bei sowas:**

Wenn eine Gesundheitsorganisation von einem Man-in-the-Middle-Angriff betroffen ist, sollte sie umgehend Maßnahmen ergreifen, um den Angriff zu stoppen und die betroffenen Systeme zu sichern. Hier sind einige Schritte, die die Organisation durchführen kann:

* Beenden Sie die Verbindung: Wenn eine verdächtige Verbindung oder ein verdächtiger Datenverkehr erkannt wird, sollten alle betroffenen Geräte oder Systeme sofort von der Netzwerkverbindung getrennt werden.
* Überprüfen Sie die Systeme: Überprüfen Sie alle betroffenen Systeme und Geräte, um festzustellen, ob sie infiziert sind oder Malware enthalten. Wenn eine Infektion festgestellt wird, sollte das betroffene System isoliert und untersucht werden.
* Ändern Sie Passwörter: Ändern Sie alle betroffenen Passwörter und stellen Sie sicher, dass sie sicher und einzigartig sind. Überprüfen Sie auch alle Konten und stellen Sie sicher, dass sie nicht unbefugt genutzt werden.
* Informieren Sie die Behörden: Wenn es sich um einen schwerwiegenden Vorfall handelt, sollten die zuständigen Behörden informiert werden, um eine Untersuchung einzuleiten und gegebenenfalls den Angriff zu stoppen.
* Verbessern Sie die Sicherheit: Stellen Sie sicher, dass alle Systeme und Geräte mit den neuesten Sicherheitsupdates und Patches aktualisiert sind und setzen Sie zusätzliche Sicherheitsmaßnahmen wie Firewalls und Intrusion Detection-Systeme ein, um zukünftige Angriffe zu verhindern.

Es ist wichtig, schnell zu handeln, um den Angriff zu stoppen und die Sicherheit des Systems wiederherzustellen, um weitere Schäden zu vermeiden.