**SQL-Injection**

SQL Injection ist eine Art von Cyberangriff, bei dem ein Angreifer bösartigen SQL-Code in eine Anwendung einschleust, um Zugriff auf vertrauliche Daten oder Systeme zu erlangen oder Schaden zu verursachen.

Der Angreifer nutzt dabei Schwachstellen in der Anwendung aus, um schädlichen SQL-Code einzuschleusen. Diese Schwachstellen können z.B. fehlende Validierung von Benutzereingaben oder unsichere Datenbankabfragen sein.

Durch die SQL Injection kann der Angreifer die Datenbank manipulieren und Abfragen ausführen, die er normalerweise nicht ausführen könnte. Beispielsweise kann ein Angreifer durch eine SQL Injection Zugriff auf Benutzerdaten erlangen, indem er eine Abfrage erstellt, die alle Benutzernamen und Passwörter in der Datenbank ausliest.

Ein weiteres Beispiel wäre die Änderung oder Löschung von Daten in der Datenbank. Hier könnte der Angreifer schädliche Abfragen erstellen, die es ihm ermöglichen, bestimmte Datensätze zu löschen oder zu manipulieren.

Um sich gegen SQL Injection-Angriffe zu schützen, sollten Entwickler sicherstellen, dass Benutzereingaben validiert werden und dass dynamisch generierte SQL-Abfragen sicher vorbereitet und ausgeführt werden. Es ist auch wichtig, dass alle Systeme und Anwendungen regelmäßig auf Schwachstellen überprüft und aktualisiert werden, um Angriffen vorzubeugen.

**Einfache Definition:**

SQL Injection ist eine Art von Cyberangriff, bei dem ein Angreifer schädlichen SQL-Code in eine Anwendung einschleust, um Zugriff auf vertrauliche Daten oder Systeme zu erlangen oder Schaden zu verursachen.

**Was ist zu tun bei sowas:**

Wenn eine Gesundheitsorganisation von einer SQL-Injection-Attacke betroffen ist, sollten 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: Trennen Sie alle betroffenen Geräte oder Systeme von der Netzwerkverbindung, um weitere Schäden zu vermeiden.
* Überprüfen Sie die Systeme: Überprüfen Sie alle betroffenen Systeme und Geräte, um festzustellen, ob sie infiziert sind oder SQL-Injection-Angriffe ausgesetzt sind. 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.
* Entfernen Sie den schädlichen SQL-Code: Entfernen Sie den schädlichen SQL-Code aus der Anwendung, indem Sie die Schwachstellen identifizieren und schließen, die den Angriff ermöglicht haben.
* 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.