BACKUP ONE

AWARENESS

IT-Gefahren, die Sie kennen sollten

SQL-Injection

Eine SQL-Injection ist eine Technik, bei der schädlicher SQL-Code in eine Datenbankanfrage eingefügt wird, um die Kontrolle über die Datenbank zu erlangen oder sie zu manipulieren.

ZIEL / SCHADEN

Angreifer können auf sensible Daten zugreifen, diese ändern oder löschen, die Datenbankstruktur verändern oder andere bösartige Aktivitäten ausführen.

INFEKTIONSWEG

Durch Eingabe von schädlichem SQL-Code in Formularen oder URL-Parametern, die auf eine Datenbank abzielen.

ABWEHR

Verwenden Sie Prepared Statements, nutzen Sie Datenbankzugriffssteuerungen und Validierungen und halten Sie Ihre Datenbank-Management-Systeme auf dem neuesten Stand.

BEFREIUNG MÖGLICH?

Nach einem erfolgreichen Angriff kann die Wiederherstellung schwierig sein. Backups und Audits können helfen, den Schaden zu beheben.

ANGRIFF - WAS NUN?

Wenn ein SQL-Injection-Angriff vermutet wird, sollten Sie die betroffene Anwendung sofort isolieren, Ihre Systeme prüfen, Ihre Passwörter ändern und einen Sicherheitsexperten hinzuziehen.