MS-SQL

MS-SQL ist der SQL-Server von Microsoft, welcher einen Browserdienst mitbringt, der standardmäßig auf Port 1434/udp lauscht [1]. Wird der Zugriff aus dem Internet auf diesen Dienst nicht unterbunden, können Angreifer dies ausnutzen, um Informationen über das Netzwerk auszuspähen, in dem der SQL-Server betrieben wird. Weiterhin kann der Dienst für DDoS-Amplification-Angriffe missbraucht werden.

Im Rahmen des Shadowserver "Open MS-SQL Server Resolution Service Scanning Projects" [2] werden MS-SQL-Server-Browserdienste identifiziert, welche offen aus dem Internet erreichbar sind. Der CERT-Bund erhält von Shadowserver die Testergebnisse für IP-Adressen in Deutschland, um betroffene Server-Betreiber benachrichtigen zu können.

Nachfolgend senden wir Ihnen eine Liste betroffener Systeme in Ihrem Netzbereich. Der Zeitstempel (Zeitzone UTC) gibt an, wann das System geprüft wurde und ein offener Browserdienst identifiziert wurde.

- "Server Name" entspricht üblicherweise dem NetBIOS-Namen des Systems.
- "Instance Name" gibt den Namen der SQL-Instanz auf dem Server an.
- "Amplification" gibt die Verstärkung an, welche von Angreifern bei Missbrauch des Browserdienstes auf diesem Server im Rahmen von DDoS-Angriffen erzielt werden kann. Diese errechnet sich durch die Größe der Antwort im Vergleich zur Größe der Anfrage an den Server.

Empfehlung von Microsoft

"Mit dem SQL Server-Browser-Dienst können Benutzer ohne Kenntnis der Portnummer Verbindungen mit Instanzen von Database Engine (Datenbankmodul) herstellen, die nicht den Port 1433 überwachen.

Wenn Sie SQL Server-Browser verwenden möchten, müssen Sie UDP-Port 1434 öffnen. Um eine möglichst sichere Umgebung zu erzielen, lassen Sie den SQL Server-Browser-Dienst beendet, und konfigurieren Sie die Clients so, dass sie Verbindungen mithilfe der Portnummer herstellen müssen." [3]

Referenzen

[1] Microsoft: SQL Server-Browserdienst [1]
[2] Shadowserver: Open MS-SQL Server Resolution Service Scanning Project [2]
[3] Microsoft: Konfigurieren einer Windows-Firewall für Datenbankmodulzugriff [3]

Links

[1] https://technet.microsoft.com/library/ms181087%28v=sql.105%29.aspx
[2] https://scan.shadowserver.org/mssql/
[3] https://msdn.microsoft.com/de-de/library/ms175043.aspx

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/ms-sql/