Pressemitteilung: Sentrigo Inc. 03.09.2009

Microsoft bestreitet die Gewichtung einer Sicherheitslücke in ihrer SQL Server-Datenbank, von der Sicherheitsfachleute sagen, dass dadurch Kennwörter zugänglich sind. Die Sicherheitslücke, die von Sentrigo aufgedeckt wurde, kann von remote über das Netzwerk in SQL Server 2000 und 2005 ausgenutzt werden.

Microsoft verharmlost diese SQL-Server-Sicherheitslücke, die von jemandem mit Administratorrechten ausgenutzt werden könnte, um die unverschlüsselten Passwörter der Nutzer anzusehen.

Die Sicherheitslücke wurde letztes Jahr vom Datenbank-Sicherheitsanbieter Sentrigo entdeckt, als einer ihrer Forscher bemerkte, dass sein persönliches Passwort im Speicher des SQL-Servers sichtbar wurde.

Seitdem gab es ein ständiges Hin und Her zwischen Microsoft und Sentrigo, da Microsoft behauptet, die Schwachstelle sei kein Thema, da sie ja administrativen Zugang erfordert.

Während Mitarbeiter von Sentrigo einräumen, dass administrativer Zugang notwendig sei, um ein Exploit zu auszunutzen, weisen sie auch darauf hin, dass viele Anwendungen mit Administratorrechten betrieben werden – und das bedeutet, dass Hacker möglicherweise eine SQL-Injektion Sicherheitslücke nutzen können, um Zugang zu administrativen Passwörtern zu bekommen.

„Passwörter, die zur Anmeldung an den SQL-Server verwendet werden, sind im Speicher als unverschlüsselte Daten hinterlegt", erklärte Slavik Markovich, CTO von Sentrigo. „Diese werden solange nicht gelöscht, bis der SQL-Server neu gestartet wird, deshalb können in vielen Fällen auch Passwörter noch Wochen oder Monate in Produktivumgebungen stehen. Ein einfaches Ausdrucken des Speicherinhaltes in eine Textdatei erlaubt die gezielte Suche nach Usernamen und den dazugehörigen Kennwörtern."

„Die Kenntnis dieser Passwörter kann weitreichende Auswirkungen haben, da viele Menschen die gleichen Passwörter für mehrere Systeme verwenden“, fügte er hinzu.

Im Fall von SQL Server 2000 und 2005, können Angreifer die Situation remote ausnutzen. Es gibt allerdings einen Lichtblick für Benutzer von SQL Server 2008, da Microsoft das „DBCC Utility“ entfernte. Lokale Verbindungen können jedoch diese Lücke noch weiterhin nutzen.

Trotzdem behauptet Microsoft, dass um diese Sicherheitslücke viel Lärm um nichts gemacht wird.

"Microsoft hat diese Sicherheitslücke in SQL Server gründlich untersucht und festgestellt, dass es sich nicht um eine Sicherheitslücke handelt, die ein Sicherheits-Update von Microsoft erfordert", sagte ein Sprecher. "Wie von den Sicherheitsexperten erwähnt, müsste ein Angreifer in diesem Szenario administrative Rechte auf das Zielsystem haben."

"Ein Angreifer, der administrative Rechte hat, hat bereits die vollständige Kontrolle über das System und kann Programme installieren, Daten ansehen, ändern oder löschen oder neue Konten mit vollen Benutzerrechten erstellen", fügte der Sprecher hinzu.

Während Administratoren normalerweise bei Bedarf ein Benutzerpasswort zurücksetzen können, erlauben es *Security Best Practices* sogar den Administratoren nicht, die aktuellen Passwörter anderer Benutzer zu sehen, sagen die Sentrigo Mitarbeiter. Das Problem wird dadurch noch verschärft, dass viele Unternehmen unterschiedliche Anforderungen und Vorschriften erfüllen müssen, die eine genaue Trennung der Aufgaben verlangen. Etwas, das eindeutig missachtet wird, durch die mögliche Kenntnis aller Anwenderpassworte durch die Administratoren, wie Sentrigo ergänzt.

Aufgrund dieser Situation, hat der Sicherheitsanbieter ein freies Dienstprogramm zum Löschen dieser Passwörter veröffentlicht. Das Programm kann ab heute von der Firmen-Website (http://www.sentrigo.com/passwords/) heruntergeladen werden.

Über Sentrigo

Sentrigo, Inc. ist ein anerkannter Spezialist für Datenbanksicherheit. Sentrigos Sicherheitslösung Hedgehog bietet ein weit reichendes Monitoring aller Datenbankaktivitäten und die Absicherung der Datenbanken in Real-Time. Die Software-basierte Lösung ist weltweit bei 2000 Firmen im Einsatz um unternehmenskritische Daten gegen Missbrauch durch Insider, aber auch gegen Angriffe von außen zu schützen. Unternehmen aus allen Industriesegmenten nutzen Hedgehog zur schnelleren Unterstützung und Umsetzung bei der Einführung und Überwachung von Regularien wie PCI DSS, Sarbanes-Oxley und HIPAA. Sentrigo wurde für die technologische Innovation von verschiedenen Publikationen, wie Network World und SC Magazine ausgezeichnet. Für weitere Informationen, oder um die frei verfügbare Testversion herunter zu laden, besuchen Sie www.sentrigo.com.

# # #

Medien Kontakt:
Caroline Kohn
Sentrigo, Inc.
Telefon: +49 (6821) 2079522
carolinek@sentrigo.com