heise Security

Gestohlener Microsoft-Schlüssel stammte aus einem Crash-Dump

07.09.2023 11:57 Uhr Dirk Knop

Angreifer konnten mit gestohlenem Schlüssel weitreichend auf Cloud-Ressourcen von Microsoft zugreifen. Der Schlüssel kam wohl aus einem Crash-Dump.

Der gestohlene Microsoft-Schlüssel, mit dem Angreifer Mitte Juni unter anderem E-Mails von Regierungsbehörden ausspähten, stammt wohl aus einem Crash-Dump. Dies hat Microsoft bei der Analyse des Vorfalls herausgefunden.

Wie Im Juli herauskam, konnten mutmaßlich chinesische Cyberkriminelle, die Microsoft der Gruppierung Storm-0558 zuordnet, einen OpenID Signing Key für das Azure Active Directory (Azure AD, AD) erlangen. Sie erstellten sich damit funktionierende Zugangstoken für Outlook Web Access (OWA) und Outlook.com und luden mit Skripten etwa Mails und Mail-Anhänge herunter. Mit dem gestohlenen Schlüssel ließen sich offenbar Zugangstoken und Benutzerkonten für nahezu alle Microsoft-Cloud-Dienste erstellen. Sofern Azure-AD-Instanzen und die Cloud-Apps darin anderen AAD-Instanzen vertrauen und beispielsweise "Login with Microsoft" ermöglichten, war damit auch dort der Zugriff möglich.

Microsofts Cloud-Schlüssel: Analysen führen zum Schlupfloch

Bei der Untersuchung des Vorfalls, woher der Schlüssel stammt und wie er in die Hände von Unbefugten gelangen konnte, stieß Microsoft schließlich auf Crash-Dumps. Dabei handelt es sich um Speicherbereiche, die in eine Datei geschrieben werden, falls eine Anwendung abstürzt.

Microsoft erklärt, dass das Unternehmen eine hochisolierte und Zugriffs-beschränkte Produktionsumgebung pflege. Dort arbeitende Mitarbeiter müssen Hintergrundprüfungen über sich ergehen lassen, erhalten dedizierte Konten, Workstations für den sicheren Zugriff sowie Multifaktorauthentifizierung mit Hardware-Dongles. Kontrollmechanismen verhindern dort die E-Mail-Nutzung, Konferenzen, Websuche oder andere Kollaborationstools, die zur Kompromittierung von Konten durch Malware oder Phishing führen könnten. In dieser Umgebung lief das fragliche Consumer-Signing-System.

Daneben gebe es die Unternehmensumgebung, die ebenfalls sichere Authentifizierung und sichere Geräte vorsieht, aber E-Mail, Konferenzen, Websuchen und andere Tools zur Zusammenarbeit erlaubt. Diese Tools sind wichtig, ermöglichen aber Angriffe wie Spear-Phishing, Token-stehlende Malware und andere Angriffsvektoren zur Kompromittierung von Zugängen. Die Regularien sehen daher vor, dass kein Material die hochgesicherte Produktionsumgebung verlassen dürfe.

Ein Absturz auf dem Consumer-Signing-System im April 2021 mündete in einem Speicherabzug des abgestürzten Prozesses. Eine Verkettung von Zufällen habe den Schlüssel darin belassen: Beim Anlegen von Crash-Dumps sollen sensible Informationen ausgeklammert werden. Aufgrund einer Race-Condition im Code landete der Key dennoch im Crash-Dump. Beim Verschieben von Daten sollen weitere Mechanismen dafür sorgen, dass keine sensiblen Daten wie Zugangsinformationen in weniger gesicherte Bereiche gelangen – diese hätten den Schlüssel jedoch nicht erkannt. Beides will das Unternehmen jetzt korrigiert haben.

Verkettung von Zufällen

Da der Crash-Dump vermeintlich keine sensiblen Daten enthielt, wurde er aus der isolierten Produktionsumgebung in die Debug-Umgebung im internetverbundenen Unternehmensnetz verschoben – ein Standardvorgang, betont Microsoft. Ein bösartiger Akteur der Storm-0558-Gruppe habe danach einen Unternehmensnetzzugang eines Microsoft-Ingenieurs kompromittiert. Das Konto hatte Zugriff auf die Debug-Umgebung mit dem Crash-Dump, der fälschlicherweise den Schlüssel enthielt. Belege habe man nicht, dass der Angreifer diese Daten ausgeschleust hat, da die Protokollierung nicht so weit reiche. Dies sei jedoch das wahrscheinlichste Szenario, wie die Cyberkriminellen an den Schlüssel gelangten.

Auch dafür, warum ein Consumer-Signing-Key den Zugang zu Enterprise-Mail erlaubt, haben die Redmonder eine Erklärung geliefert. Kunden hätten verstärkt die Unterstützung für Anwendungen nachgefragt, die sowohl mit Consumer- als auch mit Enterprise-Anwendungen funktionieren. Zwar habe man die Dokumentation aktualisiert, welche Schlüssel für Enterprise- und welche für Consumer-Konten zu verwenden seien. Allerdings wurde eine API, die die Signaturen kryptografisch überprüft, nicht automatisch um diese Erweitertung ergänzt. Die Mailsysteme wurden schließlich 2022 derart erweitert. Entwickler am Mailsystem gingen fälschlicherweise von einer kompletten Validierung durch die API aus, weshalb die Überprüfung nach Aussteller und Verwendungsbereich unterblieb. Deshalb akzeptierten die Mailsysteme Anfragen mit Sicherheitstoken zu Enterprise-Mail, die mit einem Consumer-Schlüssel signiert waren.

All diese Schwachstellen will Microsoft inzwischen ausgebessert haben. Weitere Abwehrmaßnahmen und Härtungen der Systeme hat Microsoft zudem in der ursprünglichen Analyse erwähnt.

(dmk)