Weitreichende Folgen für Unternehmen und Nutzer: Fehler in öffentlichen Clouds

Öffentliche Clouds sind beliebt, um die stetig wachsenden Datenmengen zu verwalten. Für einen optimalen Schutz dieser Daten müssen Anbieter und Nutzer aber gleichermaßen ihren Sicherheitsrollen gerecht werden. Sophos hat sich Cyberangriffe auf Cloudplattformen mitsamt den Auswirkungen auf Unternehmen genauer angesehen.

Wer ist für die Sicherheit öffentlicher Clouds verantwortlich? Wenn man mit Cloudprovidern wie Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform zusammenarbeitet, ist es wichtig zu verstehen, dass Sicherheit eine Frage von gemeinsamer Verantwortung ist. Anbieter öffentlicher Clouds präsentieren ihren Kunden eine große Flexibilität, ihre Cloudumgebung zu gestalten. Die Konsequenz ist allerdings, dass Provider daher keinen umfassenden Schutz für virtuelle Netzwerke, virtuelle Maschinen oder Daten in der Cloud anbieten.

Das Modell der Mitverantwortung bedeutet, dass Cloudanbieter die Sicherheit der Cloud garantieren, während die Kunden des Anbieters für alles verantwortlich sind, was in der Cloud passiert. Jedoch wissen die Administratoren nicht immer, was der Cloudprovider verantwortet und welche Sicherheitskontrollen sie selbst anwenden müssen. Diese Unsicherheit führt zu ungeschützten Daten-, Datei-, Datenbank- und Festplatten-Snapshots.

Die Amazon S3 Bucket-Panne ist noch in Erinnerung und mittlerweile gibt es davon zahlreiche weitere. Diese Vorfälle weisen auf große Sicherheitsprobleme hin:

Öffentliche Amazon S3 Bucket – Enthüllung (mit neuer Wendung)
Man muss nicht lange suchen, um Vorfälle über S3-bezogene Datenverletzungen zu finden, die durch eine fehlerhafte Konfiguration (S3-Sicherheitseinstellungen auf „Public“ gesetzt), verursacht wurden. AWS (Amazon Web Services) haben sogar ein Update veröffentlicht, um dem Kunden zu helfen, damit nicht in Konflikt zu geraten – eine der größten Ursache der Cloud Daten-Verletzung. Ein Denkfehler ist es hier anzunehmen, dass Cyberkriminelle nur auf empfindliche Daten von Organisationen aus sind.

Zusätzlich zu finanziellen und persönlichen Daten – einer der Hauptnutzungsgründe für Cloudaufbewahrungsaccounts wie Amazon S3 Buckets – ist das Hosten von Content aus statischen Webseiten wie HTML-Dateien, JavaScript und Style Sheets (CSS). Angriffe, die diese Quellen betreffen, zielen nicht auf freigelegte Daten ab. Stattdessen streben sie an, Webseitendateien schadhaft zu manipulieren, um finanzielle Informationen der Nutzer zu entwenden.

Eine Kreuzung auf dem (Angriffs-) Weg
Beide Angriffsketten sehen zu Beginn gleich aus: Cyberkriminelle scannen das Internet mit automatisierten S3-Scannern nach fehlkonfigurierten S3 Buckets. Ab da gabeln sich die Angriffswege: Im typischen S3 Datenverstoß listen und synchronisieren die Angreifer wertvollen Inhalt mit der lokalen Festplatte und erreichen sämtliche Dateien, die im Public-Modus fehlkonfiguriert wurden.

Im Fall des Datenänderungsangriffs aber suchen die Kriminellen – nachdem sie Zugang erlangt haben – nach JavaScript Content und modifizieren ihn so, dass er schadhaften Code enthält. Besucht ein Nutzer nun die infizierte Webseite, lädt der schädliche JavaScript-Code

und protokolliert sämtliche in den Zahlungsformularen erfassten Kredit- und Debitkarten-Details. Diese Informationen werden dann an den Server des Angreifers geschickt.

Erkennen und schützen vor S3 Bucket-Enthüllungen (beide Varianten)
Versehentliche oder schädliche Änderungen an S3-Konfigurationen sind sehr verbreitet. Mittlerweile gibt es aber Cloudmanagement-Lösungen, die sich dieses Problems annehmen. Michael Veit, Sicherheitsexperte bei Sophos, erklärt, wie diese Lösungen arbeiten:

„Das Sophos Cloud Optix beispielsweise erkennt schnell sämtliche öffentlich zugänglichen Dateien oder Webseiten-Files, und deklariert sie als „privat“. Mithilfe dieser Funktion wird eine zusätzliche Sicherheitsebene gegenüber kritischen Services, wie zum Beispiel Guardrails, eingefügt, so dass keine Konfiguration ohne Erlaubnis möglich ist. Innerhalb von Minuten wäre der Kunde über das S3 Bucket-Datenproblem alarmiert worden. Unter Einsatz von AI-Methoden zur Aufspürung verdächtiger Nutzer-Logins benachrichtigt Cloud Optix die Unternehmen, wenn Inhalte von S3 Buckets von einem ungewöhnlichen Standort aus modifiziert werden – in der Annahme, dass geteilte oder gestohlene Nutzerdaten aus der Ferne eingesetzt werden.“

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de