Cyberforensik-Report: Bequemlichkeit spielt Cyberkriminellen in die Karten

Der aktuelle Active Adversary Report von Sophos deckt eine interessante Trendwende auf, die ein allgemein verbreitetes Problem in der IT-Sicherheit betrifft: Bequemlichkeit.

In früheren Falldaten aus dem Report, der tatsächliche Cyberattacken analysiert, war die Ausnutzung von Sicherheitslücken die Hauptursache für Angriffe, dicht gefolgt von kompromittierten Zugangsdaten. In der ersten Jahreshälfte 2023 kehrt sich dieses Bild deutlich um, und zum ersten Mal standen mit 50% kompromittierte Zugangsdaten an erster Stelle der Ursachen. die Ausnutzung einer Schwachstelle lag bei 23%.
Auch wenn diese Momentaufnahme nicht umfassend belegen kann, dass Angreifer kompromittierte Anmeldeinformationen gegenüber Schwachstellen bevorzugen, lässt es sich nicht leugnen, dass die Nutzung illegal erworbener, gültiger Konten die Machenschaften der Angreifer erheblich erleichtert. Was die Kompromittierung von Anmeldedaten für die Cyberkriminellen noch einmal attraktiver macht, ist die in vielen Organisationen immer noch ganz fehlende oder nicht konsequent umgesetzte Multifaktor-Authentifizierung (MFA).
Bei der forensischen Aufarbeitung der Cyberattacken stellten die SophosLabs fest, dass MFA in 39 % der bisher untersuchten Fälle nicht umfassend konfiguriert war. „Das Entmutigendste an dieser Statistik ist, dass wir als Branche wissen, wie man dieses Problem löst, aber zu wenige Organisationen diesen Bereich priorisieren“, so Michael Veit, Cybersecurity-Experte bei Sophos. „Das Problem ist also nicht die Technologie, sondern die Durchsetzung. Oftmals werden die Authentifizierungsanforderungen gelockert, um ein besseres Benutzererlebnis zu bieten. Das öffnet Angreifern Tür und Tor und wenn es um menschliche Gegner geht, bieten diese kleinen Risse bereits beste Chancen, um in Netzwerke einzudringen.“

Authentifizierungstechnologien als Herausforderung
Auch im Bereich MFA (Multi Faktor Authentifizierung) findet ein ständiger Wettlauf statt. Da Unternehmen stärkere Authentifizierungsmechanismen einführen, reagieren Kriminelle mit der Entwicklung von Techniken, die die eingesetzten Technologien umgehen. „Dieser Zyklus wird sich auf absehbare Zeit fortsetzen“, so Veit „Wir haben jetzt den Punkt überschritten, an dem einfache SMS-Codes, zeitbasierte Einmalpasswörter (TOTP) oder sogar Push-Bashed-Authentifizierungen effektiv sind. Organisationen, die sich vor den neuesten Angriffstechniken schützen möchten, müssen auf Phishing-resistente MFA umsteigen. Und selbst hier sind die Kriminellen nicht untätig. Als Sophos X-Ops die Daten für den aktuellen Report analysierte, entdeckte das Team, dass eine der neuesten Social-Engineering-Taktiken zum Beispiel darin besteht, den Empfänger per SMS dazu zu bewegen, seinen Security Token zu deaktivieren.“

Moderne, phishing-resistente MFA-Technologien als Standardauthentifizierungsmodus für alle Dienste innerhalb einer Organisation inklusive entsprechender Schulungen sorgen aktuell für maximalen Schutz gegen kompromittierte Anmeldedaten. Dabei müssen die entstehenden Kosten auch an den Kosten einer potenziellen Sicherheitsverletzung und Wiederherstellung gemessen werden, die oft um ein Vielfaches teurer sind. Eine starke Authentifizierung allein kann jedoch nicht jeden Angriff stoppen, weshalb mehrschichtige Verteidigung und Telemetrie-Analyse von entscheidender Bedeutung sind. Beides verschafft Unternehmen Zeit und Gelegenheit, einen aktiven Angriff zu erkennen und abzuwehren.

Darüber hinaus können viele Authentifizierungssysteme für den adaptiven Zugriff konfiguriert werden. Dieses Vorgehen ändert die Zugriffs- oder Vertrauensebene basierend auf

Kontextdaten über den Benutzer oder das Gerät, das Zugriff anfordert. Außerdem wird der Zugriff auf diejenigen Benutzer beschränkt, die ihn wirklich benötigen. Mit adaptiven Zugriffsauthentifizierungssystemen können Unternehmen Zugriffsrichtlinien für bestimmte Anwendungen oder Benutzergruppen anpassen und dynamisch auf verdächtige Signale reagieren.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X (exTwitter): @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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