Name
Markus Gladbach

0157 71446098
markus.gladbach@gladbach-consulting.com

Rapid7
Am Söldnermoos 17
85399 Hallbergmoos
rapid7.com

25. September 2019

Presseinformation

Hacker erraten 60 Prozent aller Passwörter

Nach neun Monaten Penetrationstests verdeutlicht eine Studie von Rapid7 die effektivsten Methoden, mit denen Hacker Passwörter knacken. 73 Prozent der Hackereinbrüche basieren auf gestohlenen Passwörtern. Die Hälfte von ihnen können zu 60 Prozent ganz einfach von Hackern erraten werden. Das zeigt die Studie „Under the Hoodie“ von Rapid7, die auf den Ergebnissen von 180 in neun Monaten durchgeführten Penetrationstests beruhen.

Trotz vieler Userschulungen, die die Bedeutung sicherer Passwörter zum Thema haben, konnten die Penetrationstester von Rapid7 60 Prozent aller Passwörter ganz einfach erraten, indem sie bekannte Standardwerte, Variationen des Wortes "Password", die aktuelle Jahreszeit, das aktuelle Jahr sowie leicht zu erratende, organisationsspezifische Passwörter ausprobierten.

Die beste Methode zur Erlangung von Benutzer-Anmeldeinformationen ist jedoch das Offline-Passwort-Hacking mit einer Hash-Datei. Die häufigste Quelle für Passwörter waren dieses Jahr erbeutete Hash-Dateien. Auch spezifischere Ursprünge für Hashes wie beispielsweise Challenge-Response-Traffic und /etc/shadow wurden gemeldet. Rapid7 stellte auch hier fest, dass viele der geknackten Passwörter mit etwas mehr Zeit leicht hätten erraten werden können. Besonders zu beachten sind die erbeuteten LM-Hashes. Diese sind extrem unsicher, laufen einigen grundlegenden empfohlenen Methoden der Kryptographie zuwider und wurden von Microsoft schon lange zugunsten stärkerer Hashing-Mechanismen verworfen. Doch obwohl sie in Microsoft-Umgebungen, die in den vergangenen zehn Jahren aktualisiert wurden, im Grunde keine Rolle mehr spielen, bestehen sie weiterhin hartnäckig und warten nur darauf, von Angreifern ausgenutzt zu werden. Domain-Administratoren werden nachdrücklich aufgefordert, diese LM-Hashes endgültig auszurotten, wobei zur Deaktivierung von LM-Hash-Speicher helfen können.

Dies sind die Ergebnisse des jährlichen Rapid7 Berichts „Under the Hoodie“ , der jetzt im dritten Jahr erscheint und sich auf die Erkenntnisse aus 180 Penetrationstests über einen Zeitraum von neun Monaten zwischen Mitte September 2018 und Ende Mai 2019 stützt. Mit den Erkenntnissen aus internen und externen Netzwerkanalysen, physischen Eindringversuchen und persönlichen sowie elektronischen Social-Engineering-Angriffen werden in dem Bericht die Schwachstellen aufgedeckt, die in Unternehmen am häufigsten zu finden sind.

Darüber hinaus beschreibt die Studie, warum die Transport-Schicht die häufigste Sicherheitsschwachstelle in Unternehmen ist (jedes fünfte Unternehmen ist betroffen). Besonderer Fokus wird auf die Verwendung veralteter Verschlüsselungsstandards bzw. unverschlüsselter Kommunikation von Systemen gelegt, die von extern erreichbar sind.

Tod Beardsley, Forschungsdirektor von Rapid7, sagte: "Es ist heute üblich, sicherzustellen, dass Passwörter einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten, und die Benutzer zu zwingen, ihr Passwort alle 90 Tage zu ändern. Aber solche Passwortregularien führen bei den Usern letztlich nur dazu, dass sie die Komplexität des Passworts reduzieren. Und so werden sie immer wieder von Schemata wie "Sommer2019!" oder "Herbst2019!", einsetzen. Unternehmen sollten daher ernsthaft in Erwägung ziehen, zufällige Passwörter über eine Lösung zur Passwortverwaltung zu vergeben, was deutlich besser wäre, als auf die Komplexität von Passwörtern und Rotationsregeln zu bestehen."

Über Rapid7

Unternehmen auf der ganzen Welt vertrauen auf Rapid7-Technologie, -Services und -Forschung, um ihre Sicherheit zu verbessern. Die Transparenz, Analyse und Automatisierung, die durch die rapid7 Insight-Cloud bereitgestellt wird, vereinfacht die Komplexität und hilft Sicherheitsteams, Schwachstellen zu reduzieren, bösartiges Verhalten zu erkennen, Angriffe zu untersuchen und abzuwehren sowie Routineaufgaben zu automatisieren. Mehr als 8.400 Kunden vertrauen auf Rapid7, um ihre Sicherheit zu verbessern und ihre Unternehmen sicher zu schützen.