Was tun gegen Credential Stuffing-Angriffe?

Von Raymond Hartenstein – Malware, Ransomware, Datenlecks, App-Schwachstellen, Botnet-Attacken: Es gibt viele Möglichkeiten, unlautere Absichten im Internet mit kriminellen Methoden umzusetzen. Das notorische Phishing dient dabei oft als Schlüssel zum Erfolg: Allzu oft reagieren die Opfer wie gewünscht und geben ihre Daten mehr oder weniger bedenkenlos weiter. Gerade bei den Angestellten von Finanzinstituten und bei den Kunden nehmen solche „diskreten" Banküberfälle in letzter Zeit stark zu.

Damit in direktem Zusammenhang steht das sogenannte Credential Stuffing. Hierbei nutzen die Angreifer Usernamen und Passwörter, die sie aus anderen Quellen erbeutet haben, um an die Bankkonten zu gelangen. Das Prinzip ist einfach: Die Hacker entwenden die Login-Daten beziehungsweise Passwörter von Online-Händlern oder Mailservern. Besonders ergiebig wird diese Masche, wenn die Betroffenen ihre Passwörter gleich für mehrere Accounts bei anderen Institutionen einsetzen.

Tatsächlich kursieren zahlreiche Listen mit solchen Daten in den dunklen Kanälen des Internets. Weltweit wurden 2020 ganze 193 Milliarden Attacken registriert, 3,4 Milliarden davon galten Anbietern aus der Finanzbranche – eine Steigerung von 45 Prozent gegenüber dem Vorjahr. Der Schaden reicht von der Reputationsbeschädigung über Schadenersatzforderungen und Kundenverlust. Nicht zuletzt kann Credential Stuffing die Website- und Anwendungs-Performance durch Bot-Traffic-Überlastung beeinträchtigen. In der Hauptsache geht es Hackern, die sich auf die Finanzbranche konzentrieren, aber um die Übernahme von Konten und die Durchführung betrügerischer Transaktionen.

Die Cyberkriminellen nutzen Open-Source-Automatisierungstools, um die erbeuteten Anmeldedaten auf Hunderten von Websites auszuprobieren, und können sicher sein, früher oder später Erfolg zu haben. Die Angriffsszenarien erreichen einen beträchtlichen Komplexitätsgrad – bis hin zur weitgehenden Unsichtbarkeit sogar für IT-Sicherheitsverantwortliche. Kostenlose Automatisierungstools wie Sentry MBA oder SNIPR machen es den Angreifern leicht, gestohlene Anmeldedaten zu verifizieren. Mithilfe kostengünstiger Plattformen mit „Botnet as a Service"-Angeboten können sie auch groß angelegte und komplexe Credential-Stuffing-Attacken realisieren. Die immer höher entwickelten Tools haben diese Methode zu einem sehr beliebten Angriffsvektor gemacht.

MFA schützt nur bedingt

Viele Unternehmen nutzen eine Multi-Faktor-Authentifizierung (MFA), um ihre Daten zu sichern. Doch kann MFA allein nicht den benötigten Schutz bieten. Haben die Kriminellen erst einmal eine funktionierende Kombination aus Nutzer-ID und Passwort gefunden, suchen sie andere Möglichkeiten, um Zugriff auf die Konten zu bekommen. Dabei optimieren sie ständig ihre Methoden. So verteilen sie ihre Anmeldeversuche auf Tausende von Bots, setzen Proxyserver ein oder führen die Logins mit zeitlichen Abständen durch. Wer als Anwendungs- und Website-Entwickler unabsichtlich Nutzer-IDs oder andere Informationen bestätigt, spielt den Angreifern in die Hände. Melden sich diese beispielsweise mit einer bisher nicht verifizierten Kombination aus Nutzer-ID und Passwort an, können sie anhand der Passwort-Fehlermeldung erkennen, dass zumindest die Nutzer-ID funktioniert. Das Knacken des Passworts kann dann mit Brute-Force-Methoden erfolgen. Daher ist ein Check von Authentifizierungs-Workflows und Anmelde-Screens mehr als empfehlenswert.

Verfügen die Angreifer über die persönlichen (validen) Anmeldedaten ihrer Opfer, können Lösungen für eine Multi-Faktor-Authentifizierung den Zugriff auf Finanzanwendungen nicht sicher verhindern. Bei einigen MFA-Implementierungen geben Nutzer zunächst ihre Kombination aus ID und Passwort ein und bestätigen ihre Identität anschließend über einen dritten Faktor wie etwa einen SMS- oder einen E-Mail-Code. Hier können Cyberkriminelle die Eigenheiten der Lösung ausnutzen. Weil die meisten MFA-Lösungen die Kombination überprüfen, bevor sie den Sicherheitscode generieren, kann der Kriminelle, wenn Nutzer-ID und Passwort bestätigt wurden, sein Ziel durch das Spear-Phishing angreifen. Damit erbeutete verifizierte Daten bringen im Dark Web bares Geld.

Mehrschichtige Verteidigung

Besseren Schutz bietet eine netzwerkbasierte Bot-Management-Lösung im Rahmen einer mehrschichtigen Sicherheitsarchitektur. In der Regel verwenden die Angreifer verteilte Botnets für komplexe Credential-Stuffing-Angriffe. Eine leistungsfähige Bot-Management-Lösung kann illegitimen Bot Traffic am Netzwerkrand (Edge) erkennen, kontrollieren – und den Angriff abblocken. Künstliche Intelligenz und Machine Learning tragen dazu bei, die Management-Lösungen beziehungsweise die entsprechenden Plattformen smarter zu machen, sodass sie Credential-Stuffing-Angriffe erkennen und abwehren können, noch bevor sie die Anwendungen oder Rechenzentren erreichen können. Mehrschichtige Verteidigungsmaßnahmen und Segmentierung machen Webangriffe für Angreifer kostspielig, was sie dazu veranlasst, sich andere Ziele zu suchen. Finanzdienstleister sollten die neuesten Technologien nutzen, um sicherzustellen, dass sie den Angreifern im Jahr 2021 einen Schritt voraus sind.

Raymond Hartenstein,
Sales Manager Financial Services DACH,
Akamai, Frankfurt am Main

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH