proofpoint.

KURZINFORMATION ZU EINER BEDROHUNG

Kompromittierung und Übernahme von Cloud-Konten

Die Fakten

BESCHREIBUNG

Cloud-Kontenkompromittierung ist die böswillige Übernahme eines legitimen Anwenderkontos bei einem Cloud-basierten E-Mail- oder einem Collaboration-Dienst. Damit erhalten die Angreifer weitreichenden Zugriff auf Daten, Kontakte, Kalendereinträge, E-Mails und andere Systemtools. Neben den kompromittierten Anwenderdaten können die Angreifer das Konto auch zur Nachahmung des Anwenders per Social Engineering oder bei BEC-Angriffen (Business Email Compromise, auch als Chefmasche bezeichnet) nutzen – sowohl innerhalb als auch außerhalb des Unternehmens. Bedrohungsakteure können auf vertrauliche Daten zugreifen, andere Anwender oder externe Geschäftspartner zu Banküberweisungen verleiten oder den Ruf und die Finanzen eines Unternehmens ruinieren. Zudem können sie Backdoor-Trojaner installieren, die den Zugriff für weitere Angriffe aufrechterhalten.

DER WERKZEUGKASTEN

- Phishing-Angriffe, einschließlich OAuth-Token-Phishing
- Brute-Force-Angriffe, bei denen Anmeldedaten durch automatisiertes Ausprobieren geknackt werden, z. B. mit Aircrack-ng und Jack the Ripper
- Wiederverwendung von Anmeldedaten, wobei zuvor gestohlene Benutzernamen- und Kennwort-Paare verwendet werden
- Malware, einschließlich Keylogger und Anmeldedaten-Diebe wie PunkeyPOS und Spyrix

ANGRIFFSTYPEN

- Diebstahl von Anmeldedaten: Nutzung von schwachen bzw. auf anderen Websites verwendeten Kennwörtern oder unzureichenden Sicherheitssystemen, um in die Systeme einzudringen
- Schädliche OAuth-Anwendungen: OAuth-Token-Phishing und nachgeahmte Anwendungen, die die Kontobesitzer dazu bringen, Zugriffsberechtigungen für Systemressourcen zu delegieren
- Insider-Bedrohungen: Verlust von Anmeldedaten durch Fahrlässigkeit oder Böswilligkeit
- Malware: Auf Systemen installierte schädliche Software, die für lange Zeiträume unbemerkt bleiben und zum Teil Malware Anmeldedaten stehlen und mit dem Angreifer kommunizieren kann

RISIKOFAKTOREN

- Nutzung von Schatten-IT oder Cloud-Anwendungen und -Diensten ohne Einverständnis der IT-Abteilung
- Unzureichende Überwachungstools für E-Mail- und Cloud-Sicherheit
- Weitergabe von Anmeldedaten an andere Mitarbeiter oder externe Partner
- Unzureichende Kenntnisse über bewährte Sicherheitspraktiken und häufig genutzte Phishing-Techniken

Nach dem Umzug der Unternehmensressourcen in die Cloud haben Cyberangreifer nicht lange auf sich warten lassen. Angefangen von gehosteten E-Mail- und Webmail-Diensten über Cloud-Produktivitätsanwendungen wie Microsoft 365 und Google Workspace bis hin zu Cloud-Entwicklungsumgebungen wie AWS und Azure: Für Cyberkriminelle sind Anmeldedaten ein begehrte Beute, auf die sie mit zahllosen Phishing-Kampagnen Jagd machen. Und dank der Single Sign-On-Technologie, die lateralen Zugang zu vielen verschiedenen Systemen in einem Unternehmen gewährt, reicht ein einziges kompromittiertes Konto aus, um großen Schaden anzurichten.

Cloud-Kontenkompromittierung in den Schlagzeilen

Capital One muss nach Hack von 100 Mio. Kreditanträgen von 2019 80 Mio. USD Strafe zahlen

Das US-amerikanische Justizministerium verhaftete die ehemalige Amazon-Software-Entwicklerin Paige Thompson, klagte sie wegen Computerbetrug und -missbrauch an und warf ihr vor, auf Daten von Capital One zugegriffen zu haben. Mithilfe eines SSRF-Angriffs (Server-side Request Forgery) gelangte sie an die Anmeldedaten einer Rolle, mit der sie auf vertrauliche Informationen zugreifen konnte, die im S3-Dateispeicherdienst von Amazon aufbewahrt wurden. Der Anklage zufolge sprach Paige Thompson in ihrem Slack-Channel detailliert über ihre Taten und veröffentlichte Anleitungen auf GitHub, mit denen der Angriff nachgeahmt werden konnte.[1]

NSA und FBI geben Russland Schuld an massiven Brute-Force-Angriffen auf Microsoft 365

In einem gemeinsamen Bericht machten der britische Geheimdienst sowie die US-Behörden NSA (National Security Agency), FBI und Heimatschutzministerium eine Gruppe russischer Cyberkrimineller namens „Fancy Bear“ für die langfristig angelegte Kampagne mit Kompromittierungen von Microsoft 365-Konten verantwortlich. Die Angriffe setzten sogenanntes „Password Spraying“ ein, bei dem Computer mehrmals hintereinander mit stets anderen Kennwortkombinationen auf ein Konto zugreifen.[2]

1 Devling Barrett *(The Washington Post)*: „Capital One Fined $80 Million for 2019 Hack of 100 Million Credit Card Applications“ (Capital One muss nach Hack von 100 Mio. Kreditanträgen von 2019 80 Mio. USD Strafe zahlen), August 2020.

2 Thomas Brewster *(Forbes)*: „NSA and FBI Blame Russia for Massive ‘Brute Force’ Attacks On Microsoft 365“ (NSA und FBI geben Russland Schuld an massiven Brute-Force-Angriffen auf Microsoft 365), Juli 2021.

Der Ablauf einer Cloud-Kontoübernahme

Im Folgenden wird beschrieben, wie die Mehrzahl der Cloud-Kontenübernahmen abläuft.

1. **Diebstahl von Anmeldedaten:** Um Zugang zu den Anmeldedaten von Anwendern zu erhalten, nutzen Angreifer Techniken wie Anmeldedaten-Phishing, Brute-Force-Angriffe, Wiederverwendung von Anmeldedaten, schädliche OAuth-Anwendungen oder Malware, die Anmeldedaten erfasst (siehe „**Der Werkzeugkasten**“ auf Seite 1).
2. **Infiltration:** Nachdem sich der Angreifer beim Anwenderkonto anmelden konnte, hat er Zugriff auf E-Mails, Kontakte, Dateien und den Kalender des Opfers. Die Daten werden entweder gestohlen oder genutzt, um den Anwender glaubhaft zu imitieren.
3. **Persistenz und Ausbreitung:** Einige Betrüger antworten auf bestehende E-Mail-Threads oder verschicken E-Mails mit Malware oder gefährlichen URLs an Kollegen und externe Geschäftspartner. Der Angreifer imitiert den kompromittierten Anwender und wendet sich dann mit gefälschten Rechnungen oder Hinweisen zu geänderten Kontoverbindungen an andere Personen innerhalb oder außerhalb des Unternehmens. Mitunter lädt der Angreifer auch Malware auf interne Dateifreigaben hoch oder sabotiert das Unternehmen auf andere Weise. Häufig richtet der Angreifer automatische Weiterleitungsregeln ein, durch die er den Zugang zu den E-Mails eines Anwenders behält, selbst wenn dieser das Kennwort ändert. Durch den Einblick in alle eingehenden E-Mails und Kalendereinladungen erhält der Angreifer wichtige Informationen für spätere Nachahmer-Angriffe.
4. **Monetarisierung:** Wird ein Angriff nicht rechtzeitig erkannt und bleibt über längere Zeit unentdeckt, kann eine Kontenkompromittierung den Diebstahl von Geldern oder wertvollen Daten wie Finanzinformationen bzw. geistigem Eigentum ermöglichen.

Angriffe führen zu Datenverlust, Überweisungsbetrug und Systemmissbrauch

1	**AUFKLÄRUNG**
	Anmeldedaten-Phishing
	Daten-Leak oder -Dump
	Keylogger oder Malware
	Böswillige Insider
	Social Engineering
2	**INFILTRIERUNG**
	Abweichende Anmeldedaten
	Direkte Anmeldung
	Cloud-Malware (Drittanbieter-Anwendungen)
3	**EXPANSION, PERSISTENZ UND BEOBACHTUNG**
	Aufrechterhaltung des Zugriffs • Einrichtung von E-Mail-Weiterleitungsregeln • Änderung von Berechtigungen • Erstellung von Administratorkonten • Deaktivierung der Multifaktor-Authentifizierung • Einrichtung von Zugriff für Dritte
	Angriffe über vertrauenswürdige Konten • Versand interner und externer Phishing-E-Mails • Upload und Verbreitung von Malware
	Feststellung des Potenzials • Sichtung von E-Mails und Daten • Aufdeckung der Unternehmensstruktur • Kennenlernen der Geschäftsprozesse
4	**MONETARISIERUNG**
	E-Mail-Betrug (BEC) • Überweisungsbetrug • Betrug mit Gehaltszahlungen • Betrug mit Gutscheinkarten • Lieferkettenbetrug
	Datenexfiltration • E-Mails • Download • Weitergabe
	Sabotage • Cloud-Ransomware • Zerstörung
	Systemmissbrauch • Spam • Fraud-as-a-Service (Betrug als Service) • Schürfen von Krypto-Währungen

Risikofaktoren und Folgen durch Cloud-Kontenübernahme

So schützen Sie Ihr Unternehmen

- Blockieren Sie Anmeldedaten-Phishing-E-Mails vor der Zustellung an die Anwender.
- Schulen Sie Anwender in empfohlenen Vorgehensweisen für Kennwörter und im Erkennen von Phishing-E-Mails, damit sie zu einer starken Verteidigungslinie werden. Idealerweise sollten sie verdächtige Nachrichten auf einfache Weise melden können.
- Erwägen Sie den Einsatz einer CASB-Lösung (Cloud Access Security Broker), die Ihnen eine konsolidierte Ansicht der Cloud-Dienste Ihres Unternehmens liefert. Die Lösung sollte detaillierte Informationen über die Anwender und OAuth-Anwendungen enthalten, die Zugriff auf Daten in Cloud-Diensten haben – unabhängig von Gerät und Standort.
- Begrenzen Sie die Schäden durch ein kompromittiertes Konto, indem Sie für den Netzwerk- und Anwendungszugriff einen Zero-Trust-Ansatz implementieren.
- Prüfen Sie nicht nur eingehende, sondern auch interne E-Mails auf Bedrohungen wie Malware und E-Mail-Betrug.
- Verwenden Sie Multifaktor-Authentifizierung. Dies schützt Sie zwar nicht vollständig vor Kontoübernahmen, doch es erschwert den Kriminellen die Arbeit deutlich.
- Identifizieren Sie besonders gefährdete Anwender und überwachen Sie die Umgebung auf Zwischenfälle.
- Richten Sie Warnmeldungen ein und priorisieren Sie diese auf Basis der wichtigsten Risikofaktoren Ihres Unternehmens.
- Korrelieren Sie Bedrohungen über E-Mail und Cloud, um gefährdete Konten genau zu erkennen.
- Überwachen und kontrollieren Sie OAuth-Anwendungen und entziehen Sie schädlichen und anderen gefährlichen Anwendungen die Berechtigung.
- Verhindern Sie Klicks auf schädliche URLs und Malware-Downloads, indem Sie Browseraktivitäten isolieren.
- Untersuchen Sie Sicherheitszwischenfälle mit einer Lösung, die umfangreiche Forensik und anpassbare Berichte anbietet.
- Verhindern Sie unbefugten Zugriff auf Cloud-Apps und -Dienste mit adaptiven Zugriffskontrollen, ganz besonders für nicht verwaltete Geräte.
- Automatisieren Sie die Sicherheitsreaktionen mithilfe flexibler Richtlinienkontrollen, die auf Zwischenfälle oder Veränderungen in den Risikoprofilen von Anwendern reagieren. Anwender, die gerade angegriffen werden oder aufgrund ihrer digitalen Gewohnheiten bzw. Zugriffsberechtigungen ein höheres Risiko darstellen, müssen sich möglicherweise regelmäßig neu authentifizieren.

Forschungserkenntnisse

Proofpoint überwacht tausende Cloud-Mandanten und über 20 Millionen aktive Cloud-Anwender. In einer Untersuchung von Cloud-Bedrohungsdaten aus dem Jahr 2020 haben wir Folgendes festgestellt:

95 % der Unternehmen wurden angegriffen

52 % der Unternehmen verzeichneten mindestens ein kompromittiertes Konto

32 % der kompromittierten Unternehmen verzeichneten Aktivitäten wie Dateimanipulation, E-Mail-Weiterleitung und Aktivitäten bei OAuth-Anwendungen

10 % der Unternehmen verzeichneten autorisierte schädliche OAuth-Anwendungen

Bei einer Umfrage des Ponemon Institute von 2021, die von Proofpoint in Auftrag gegeben wurde, gaben 86 % der IT-Führungskräfte an, dass Cloud-Kontenkompromittierung die Unternehmen jährlich mehr als 500.000 US-Dollar kostet.[3] Die Umfrageteilnehmer berichteten von durchschnittlich 64 Cloud-Kontenkompromittierungen im Jahr, wobei in 30 % der Fälle vertrauliche Daten kompromittiert wurden.[4]

Fast 60 % der Teilnehmer erklärten, dass Konten von Microsoft 365 und Google Workspace besonders häufig durch Brute-Force- und Phishing-Angriffe ins Visier genommen wurden.

Insgesamt gaben mehr als 50 % der Befragten an, dass am häufigsten Phishing-Angriffe eingesetzt werden, um an legitime Cloud-Anmeldedaten zu gelangen.

3 Ponemon Institute: „Cost of Cloud Compromise and Shadow IT“ (Kosten durch Cloud-Kompromittierung und Schatten-IT), April 2021.
4 ebd.

Weitere Informationen

Um sich vor Cloud-Kontenkompromittierung zu schützen, müssen Unternehmen über robuste Sicherheitsmaßnahmen verfügen. Sicherheitsplattformen sollten eine umfassende Verschlüsselung und kontinuierliche Datenüberwachung ermöglichen. Zudem sollten sie Zwischenfälle schnell erkennen können, damit Administratoren jegliche Schäden begrenzen und beheben können.

Wenn Sie mehr darüber erfahren möchten, wie Sie Cloud-Kontenkompromittierung effektiv stoppen können, besuchen Sie **www.proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

1207-0001-01-01 11/21