ANOMALI

Use Case

WIE SIE SICH MIT DEM MITRE ATT&CK® FRAMEWORK VOR ANGRIFFEN ÜBER KOMPROMITTIERTE ZUGANGSDATEN SCHÜTZEN

Kompromittierte Zugangsdaten – das sind legitime Zugangsdaten wie Benutzernamen und Passwörter, die in den Besitz von Angreifern gelangt sind – sind für Unternehmen heute die gängigste Bedrohung. Angriffe mithilfe kompromittierter Zugangsdaten stellen für Security-Teams dabei eine besondere Herausforderung dar, da sich Cyberkriminelle auf diese Weise als legitime User ausgeben und auf sensible Daten und Systeme zugreifen können, ohne von klassischen Security-Systemen wie Antivirus- und Anti-Malware-Lösungen entdeckt zu werden.

DER HOHE PREIS KOMPROMITTIERTER ZUGANGSDATEN

IBM und das Ponemon Institute beziffern die durchschnittlichen Kosten eines erfolgreichen Angriffs in den USA mit knapp 10 Millionen US-Dollar pro Incident. Bei einigen aktuellen, viel beachteten Breaches mithilfe kompromittierter Zugangsdaten gehen die Schäden allerdings deutlich über diese finanziellen Verluste hinaus.

- **Okta (2024):** Für Okta, einen führenden Anbieter im Bereich Identity & Access Management (IAM), war es besonders peinlich, einen umfangreichen Data Breach mithilfe kompromittierter Zugangsdaten zugeben zu müssen, die ein Mitarbeiter im persönlichen Google-Account gespeichert hatte. Da der Angriff eine Reihe renommierter Okta-Kunden wie Cloudflare und BeyondTrust betraf, war der Imageschaden enorm.
- **Norton (2023):** Angreifer verwendeten im Darkweb beschaffte Zugangsdaten, die schon vor einiger Zeit gestohlen worden waren, um Zugang zu den Systemen dieses Cybersecurity-Urgesteins zu erhalten. Über 925.000 Kunden waren betroffen – darunter einige, die ihre Passwörter im Passwort-Manager des Unternehmens gespeichert hatten.
- **23andMe (2023):** Dieser Angriff nahm besonders sensible personenbezogene Daten ins Visier: Die Cyberkriminellen griffen über kompromittierte Zugangsdaten auf mehr als 14.000 Benutzer-Accounts zu und verwendeten die dort gespeicherten genetischen und genealogischen Informationen, um sensible Daten von 6,9 Millionen Personen zu veröffentlichen. Das Unternehmen stand heftig in der Kritik und stimmte einer Einigung über 30 Millionen US-Dollar zu.
- **Colonial Pipeline (2021):** Bei einem der bekanntesten Angriffe der letzten Jahre nutzten die Angreifer ein kompromittiertes VPN-Passwort, um fast 100 GB Daten zu stehlen und Ransomware zu installieren. Das Unternehmen musste seine mehr als 9.000 Kilometer lange Pipeline vom Netz nehmen, was zu großflächigen Benzin-Engpässen und Preisspitzen führte. Außerdem zahlte der Betreiber 5 Millionen US-Dollar Lösegeld und musste erhebliche operative Einbußen und Reputationsschäden hinnehmen.

Die gute Nachricht ist, dass es mit dem MITRE ATT&CK Framework einen bewährten Ansatz gibt, der dabei hilft, genau diese Art von Schwachstellen besser zu verstehen – und tragfähige Strategien zu ihrer Behebung zu entwickeln.

DAS MITRE ATT&CK FRAMEWORK

MITRE ATT&CK betreibt als weltweit renommierte Organisation eine umfangreiche Wissensdatenbank, die allen Menschen und Einrichtungen zur Verfügung steht und hilft, die eigene Sicherheit stetig zu verbessern. ATT&CK steht dabei für „Adversarial Tactics, Techniques & Common Knowledge" – also eine umfassende, kontinuierlich gepflegte Liste gängiger Taktiken und Techniken, die Angreifer nutzen, um in Netzwerke oder Systeme einzudringen.

Das Framework ermöglicht es Unternehmen und Einrichtungen, sich besser vor Angriffen zu schützen. Es enthält:

- wertvolle Informationen zu den Techniken der Angreifer
- Details zu den Bedrohungsakteuren, die diese Techniken in der Vergangenheit verwendet haben
- Empfehlungen, um diese Taktiken und Techniken zu erkennen und zu stoppen

Der Begriff „Taktiken" beschreibt, was der Angreifer in einer bestimmten Phase des Angriffs zu tun versucht, während der Begriff „Techniken" die technischen Verfahren bezeichnet, mit denen Angreifer erfolgreich in Organisationen eindringen.

WARUM KOMPROMITTIERTE ZUGANGS-DATEN SO SCHWER ZU ERKENNEN SIND

Angesichts der Vielzahl von Techniken, die Angreifern heute zur Verfügung stehen, sind Attacken mit kompromittierten Zugangsdaten für Security-Experten in vielerlei Hinsicht besonders schwer zu verhindern.

- **Zugriffe wirken legitim:** Dank der kompromittierten Zugangsdaten können sich Angreifer als berechtigte User ausgeben, da ihre Aktivitäten für die Security-Systeme wie legitime Zugriffe aussehen. Dies ermöglicht es den Angreifern, eine lange Zeit im Netzwerk zu bleiben, ihre Zugriffsrechte sukzessive auszuweiten und sich lateral zu bewegen, ohne Verdacht zu erregen.
- **Die Angriffstechniken entwickeln sich dynamisch weiter:** Cyberkriminelle entwickeln immer neue Methoden, um an Zugangsdaten zu gelangen – etwa zunehmend raffinierte Phishing-, Social-Engineering- und MFA-Fatigue-Attacken. Bei Letzteren hebeln die Angreifer die Multi-Faktor-Authentifizierung aus, indem sie eine Flut an MFA-Abfragen an die Mailadresse, das Telefon oder andere registrierte Endgeräte des Anwenders schicken, bis dessen Aufmerksamkeit ermüdet.
- **Riesige und hochkomplexe Datenmengen:** Die schiere Zahl von Authentisierungsvorgängen und Benutzeraktivitäten in modernen Netzwerken macht es schwer, subtile Hinweise auf kompromittierte Zugangsdaten zu erkennen. Mit Blick auf die Unmengen an Logdaten und Alarmmeldungen in den komplexen Enterprise-Netzwerken von heute ist es für Security-Teams eine enorme Herausforderung, echte Bedrohungen und False Positives zu unterscheiden.

MITRE ATT&CK ENTERPRISE TACTICS

Das MITRE ATT&CK Framework unterscheidet 14 High-Level-Taktiken, die unterschiedliche Phasen eines Cyberangriffs repräsentieren. Kompromittierte Zugangsdaten gehören zur Kategorie TA0006: Credential Access.

ID	Taktik	Beschreibung
TA0003	Aufklärung	Sammlung von Informationen zur Planung der weiteren Schritte
TA0042	Ressourcenentwicklung	Bereitstellung der für die weiteren Schritte benötigten Ressourcen
TA0001	Erstzugang	Eindringen in das Netzwerk
TA0002	Ausführung	Ausführung von bösartigem Code
TA0003	Persistenz	Aufrechterhalten des Zugriffs
TA0004	Rechte-Eskalation	Ausweitung der Zugriffsberechtigungen
TA0005	Umgehung der Schutzmaßnahmen	Vermeidung der Entdeckung
TA0006	Zugriff auf Zugangsdaten	Diebstahl von Benutzernamen und Passwörtern
TA0007	Erkundung	Auskundschaften der Umgebung
TA0008	Laterale Bewegung	Bewegung durch das Netzwerk
TA0009	Datensammlung	Erfassung relevanter Daten
TA0011	Command and Control	Kommunikation und Steuerung des kompromittierten Systems
TA0010	Datenabzug	Diebstahl von Daten
TA0040	Einflussnahme	Manipulation, Störung oder Vernichtung von Systemen und Daten

Die Kategorie „TA0006: Credential Access“ umfasst laut ATT&CK Framework eine Vielzahl unterschiedlicher Techniken:

ID	Taktik	Beschreibung
T1110	Brute Force	• Ein Trial-&-Error-Verfahren, bei dem iterative Tools versuchen, das Passwort systematisch zu erraten, bis das richtige gefunden ist. • Erfordert hohe Rechenleistung
T1557	Adversary-in-the-Middle	• Richtet einen Server zwischen dem Ziel und der echten Website ein • Leitet den Benutzer zum Server statt zur tatsächlichen Website weiter • Fängt die ausgetauschten Informationen ab und verändert sie
T1555	Credentials from Password Stores	• Durchsucht gängige Speicherorte für Passwörter, um Zugangsdaten zu erhalten
T1212	Exploitation of Credential Access	• Nutzt Programmierfehler in Programmen, Diensten oder Betriebssystemen aus, um Code auszuführen
T1187	Forced Authentication	• Beispiel: Sendet einem Benutzer eine Spear-Phishing-Nachricht mit einem Anhang, der einen Link oder eine individuelle Datei enthält • Beim Öffnen des Dokuments oder Anklicken des Links wird eine Authentifizierung versucht • Die so erfassten Informationen, einschließlich der gehashten Zugangsdaten des Users, werden über SMB an den vom Angreifer kontrollierten Server gesendet
T1606	Forge Web Credentials	• Fälscht Zugangsdaten, die für Zugriffe auf Anwendungen oder Internetdienste verwendet werden können • Im Gegensatz zu anderen Taktiken sind die Zugangsdaten neu und werden vom Angreifer erstellt, nicht gestohlen
T1056	Input Capture	• Protokolliert Benutzereingaben, um Zugangsdaten zu erhalten oder Informationen zu sammeln – wahlweise durch transparente Tools oder indem der Benutzer verleitet wird, Informationen in einem scheinbar legitimen Dienst einzugeben
T1556	Modify Authentication Process	• Manipuliert Authentifizierungsprozesse und -mechanismen, um auf Zugangsdaten zuzugreifen oder Zugang zu Konten zu erhalten • Durch die Manipulation der Prozesse kann sich der Angreifer ohne gültiges Konto bei einem Dienst oder System anmelden
T1111	Multi-Factor Authentication (MFA) Interception	• Manipuliert die MFA, um Zugriff auf Zugangsdaten zu erhalten • Es gibt verschiedene Ansätze, um MFA abzufangen und zu umgehen
T1621	Multi-Factor Authentication (MFA) Request Generation	• Generiert multiple MFA-Anfragen, die an Benutzer gesendet werden, z. B., indem die Funktionen zur automatischen Generierung von Push-Benachrichtigungen wie Duo Push, Microsoft Authenticator, Okta oder ähnliche Dienste missbraucht werden
T1040	Network Sniffing	• Liest an der Netzwerkschnittstelle eines Systems Informationen aus, die über kabelgebundene oder kabellose Verbindungen gesendet werden • Spioniert passiv den Netzwerkverkehr aus, um Zugriff auf Daten zu erhalten, oder verwendet Span-Ports, um größere Datenmengen zu erfassen
T1003	OS Credential Dumping	• Dumping von Zugangsdaten, um Login- und Anmeldedaten zu erhalten, normalerweise in Form von Hash- oder Klartext-Passwörtern.
TA0040	Impact	• Manipulation, Störung oder Vernichtung von Systemen und Daten

ID	Taktik	Beschreibung
T1528	Steal Application Access Token	• Stiehlt Anwendungstoken, um Zugriff auf Remote-Systeme und Remote-Ressourcen zu erlangen • Der Diebstahl von Account-API-Token in Cloud- und Containerumgebungen ermöglicht es Angreifern oft, auf Daten zuzugreifen und mit den Berechtigungen dieser Accounts Aktivitäten zu initiieren
T1649	Steal or Forge Authentication Certificates	• Digitale Zertifikate werden zum Signieren und Verschlüsseln von Nachrichten und/oder Dateien oder Authentifizierungsressourcen verwendet • Gestohlene oder gefälschte Zertifikate können zur Authentifizierung für den Zugriff auf Remote-Systeme oder -Ressourcen verwendet werden
T1558	Steal or Forge Kerberos Tickets	• Kerberos ist ein in modernen Windows-Domänenumgebungen weit verbreitetes Authentifizierungsprotokoll • Die Kerberos-Authentifizierung kann ausgehebelt werden, indem Kerberos-Tickets gestohlen oder gefälscht werden – selbst ohne Zugriff auf das Passwort eines Kontos
T1539	Steal Web Session Cookie	• Viele Webanwendungen und Webdienste verwenden Session-Cookies als Authentifizierungstoken, nachdem sich ein Benutzer bei einer Website authentifiziert hat. Solche Cookies sind oft lange gültig, auch wenn die Webanwendung nicht aktiv genutzt wird. • Gestohlene Session-Cookies können verwendet werden, um als authentifizierter Benutzer Zugriff auf Anwendungen und Dienste zu erhalten, ohne dass eigene Zugangsdaten erforderlich wären
T1552	Unsecured Credentials	• Anmeldedaten können an vielen Stellen in einem System gespeichert oder abgelegt werden • Angreifer durchsuchen kompromittierte Systeme oft, um unsicher gespeicherte Anmeldedaten zu erhalten

INDIKATOREN FÜR KOMPROMITTIERTE ZUGANGSDATEN

Angreifer nutzen eine Vielzahl von Tools, um nicht entdeckt zu werden. Unternehmen und Benutzer müssen ihre Systeme daher kontinuierlich überwachen, um sofort zu erkennen, wenn ein Account kompromittiert wird. Typische Hinweise auf eine solche Kompromittierung sind:

- **Ungewöhnlicher Outbound-Traffic:** Von den typischen Nutzungsmustern abweichende Netzwerkaktivitäten, bei denen auffällig große Datenmengen von einem System oder Netzwerk gesendet werden
- **Login an ungewöhnlichen Orten und zu ungewöhnlichen Zeiten:** Anmeldeversuche an Accounts, bei denen die Standorte oder Uhrzeiten signifikant von den üblichen Anmeldezeiten des Benutzers abweichen
- **Nicht plausible Reiserouten:** Anmeldungen von verschiedenen Standorten in einer verdächtigen Zeitspanne
- **Multiple fehlgeschlagene Login-Versuche:** Mehrere aufeinanderfolgende fehlgeschlagene Anmeldeversuche am selben Konto
- **Ungewöhnlicher Zugriff auf sensible Daten:** Unbefugter oder ungewöhnlicher Zugriff auf vertrauliche Informationen ohne entsprechende Berechtigung
- **Verdächtige Konfigurationsänderungen:** Unerwartete oder nicht autorisierte Änderungen an den Systemeinstellungen

STRATEGIEN ZUR ERKENNUNG KOMPROMITTIERTER ZUGANGSDATEN

Organisationen werden den Missbrauch von Zugangsdaten vermutlich nie ganz verhindern können – ein unachtsamer Moment genügt, und schon fällt ein legitimer Zugang in die falschen Hände – aber die folgenden Strategien helfen Ihnen, das damit verbundene Risiko zu minimieren:

- **Aktivieren Sie Multi-Faktor-Authentifizierung:** MFA, auch als Zwei-Faktor-Authentifizierung bekannt, nimmt Benutzer in die Pflicht, sich mit mehr als einer Form der Identifizierung anzumelden. Neben dem Passwort, das digitale Assets schützt, hindert MFA als zusätzliche Sicherheitsebene unbefugte Benutzer daran, auf fremde Konten zuzugreifen – selbst, wenn ein Passwort gestohlen wurde.
- **Erstellen Sie Profile der Bedrohungsakteure:** Analysieren Sie Ihre Gegenspieler und deren Taktiken sowie deren Motivationen und Skills, die für Ihr Unternehmen relevant sind. Detaillierte Profile der Akteure ermöglichen es, Gemeinsamkeiten zwischen ihnen zu finden. So können sie Ihre Abwehrmaßnahmen an neue Bedrohungen anpassen, Ressourcen priorisieren und proaktive Maßnahmen ergreifen. Auch ATT&CK aktualisiert die Taktiken und Techniken bekannter und neuer Gegner kontinuierlich, um Unternehmen Echtzeit-Informationen über die Angreifer zu liefern.
- **Implementieren Sie UEBA-Funktionalitäten (User Entity & Behavior Analytics):** UEBA analysiert umfassende Informationen aus ihren Systemen, Anwendungen, Netzwerken und Geräten, um eine Baseline typischer Verhaltensmuster zu ermitteln. Mithilfe von Machine Learning und leistungsstarken Analysen ungewöhnlicher Muster ist UEBA in der Lage, viele komplexe Cyberangriffe zu erkennen. So lassen sich die in ATT&CK beschriebenen Techniken zur Kompromittierung von Zugangsdaten schneller identifizieren als mit regelbasierten Erkennungstechnologien.
- **Überwachen Sie durchgehend Ihre Angriffsfläche:** Ein aktives Monitoring Ihrer digitalen Ressourcen auf potenzielle Schwachstellen (etwa veraltete Software, Fehlkonfigurationen oder ungeschützte sensible Daten) ist unerlässlich, um neue Bedrohungen und Angriffspunkte zu identifizieren. Der Abgleich dieser Schwachstellen mit dem ATT&CK Framework zeigt anschließend auf, gegen welche Form von Angriffen ihre operativen Systeme unzureichend geschützt sind.
- **Beschleunigen Sie das Threat Hunting:** Suchen Sie nach Angriffen, indem Sie das Knowhow Ihrer Experten mit leistungsfähigen Analysen kombinieren, um Protokolle und Daten aktiv zu deuten, statt passiv auf Warnmeldungen zu reagieren. So können Ihre Analysten versteckte Bedrohungen identifizieren, die Ihre klassischen Security-Systeme umgangen und sich im Netzwerk Ihres Unternehmens eingenistet haben.
- **Informationen machen den Unterschied:** ATT&CK liefert Detailinformationen zu fast 70 Bedrohungsakteuren und Gruppierungen sowie zu den Techniken und Taktiken, die diese einsetzen, um Zugang zum Netzwerk Ihres Unternehmens zu erhalten. Threat Intelligence-Feeds helfen Ihnen dabei, potenzielle Indikatoren für Kompromittierungen (IoCs) – etwa kompromittierte Zugangsdaten – zuverlässig zu identifizieren, bevor es zu einem Angriff kommt. Dieser proaktive Ansatz ermöglicht es, Bedrohungen frühzeitig anhand der ATT&CK-TTPs, der Bedrohungsakteure, der Kampagnen, der Sicherheitsbulletins und der Schwachstellen zu identifizieren.

ERKENNUNG KOMPROMITTIERTER ZUGANGSDATEN MIT DER ANOMALI SECURITY AND IT OPERATIONS PLATFORM

Unternehmen, die sich umfassend mit dem MITRE ATT&CK-Framework auseinandersetzen, lernen, die gängigen Taktiken, Techniken und Prozesse (TTPs) ihrer Gegner besser zu verstehen. Ergänzend dazu bedarf es aber auch der richtigen Tools, etwa von Anomali, um dieses Verständnis auf einer robusten Datenbasis in konkrete Schutzmaßnahmen zu überführen.

Aufsetzend auf unsere tiefe Integration mit dem MITRE ATT&CK Framework und den größten, sorgfältig kuratierten Zugang zu Bedrohungsinformationen ist die Security and IT Operations Platform von Anomali in der Lage, ungewöhnliche Verhaltensweisen zuverlässig zu erkennen. Auf diese Weise stellt die Lösung die Weichen für eine schnelle und orchestrierte Reaktion – und sorgt dafür, dass selbst lückenlos authentifizierte Bedrohungsakteure Ihren Systemen, Ihren Daten und Ihrem Unternehmen keinen Schaden zuzufügen können.

ANOMALI: DIE ZUKUNFT DES SIEM

Anomali ist eine marktführende KI-gestützte Security and IT Operations Platform, die volle Transparenz, hohe Geschwindigkeit, innovative KI-Funktionalitäten und wertvolle Bedrohungsinformationen in einer benutzerfreundlichen, integrierten Plattform vereint. Dabei führt Anomali ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR und TIP in einer durchgängigen Lösung zusammen, um Ihren Technologie-Stack nachhaltig zu konsolidieren – und hilft Ihrem Team so, mit weniger Aufwand mehr zu erreichen.

INNOVATIVE UND EFFEKTIVE TECHNOLOGIE

Cybersecurity für Unternehmen jeder Größe. KI-gestützte, intelligente Lösungen für eine sicherere Welt. Das ist Anomali.

Erfahren Sie, wie Anomali Ihnen dabei hilft, Angriffe durch kompromittierte Zugangsdaten zu stoppen – vereinbaren Sie eine Demo.

ANOMALI IN ACTION

Jetzt Demo anfordern