proofpoint.

DATENBLATT

Proofpoint Account Takeover Protection

Erkennung, Untersuchung und Abwehr mehrstufiger Kontoübernahmen

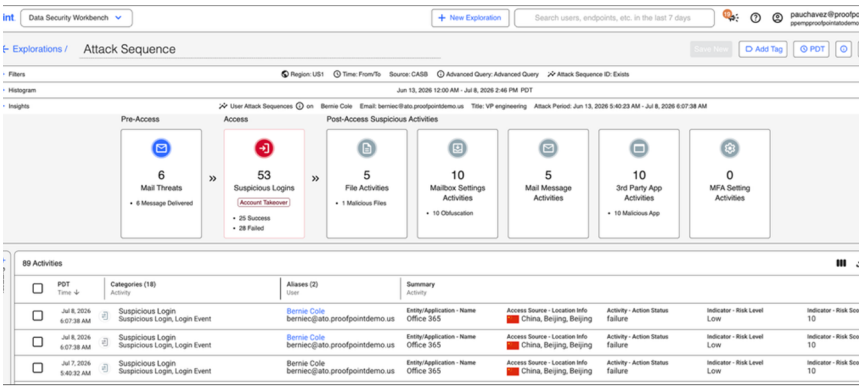
Wichtige Highlights

- **Hochpräzise Erkennung mehrstufiger Kontenkompromittierungen**
- **Schnellere Untersuchungen mit einheitlichem Überblick über den gesamten Angriffslebenszyklus**
- **Kürzere Verweildauer von Angreifern dank automatisierter Reaktions- und Behebungsmaßnahmen**
- **Minimierung von Betrug, Datenverlust und Betriebsunterbrechungen durch kompromittierte Konten**
- **Stärkung des mehrschichtigen Schutzansatzes mit Proofpoint Collaboration Security Prime**

Proofpoint Account Takeover Protection unterstützt Unternehmen bei der Erkennung, Untersuchung und Eindämmung kompromittierter Anwenderkonten im gesamten Lebenszyklus einer Kontoübernahme (ATO) – von Indikatoren vor dem Zugriff über erfolgreiche Kompromittierungen bis hin zu Aktivitäten von Angreifern nach dem Zugriff.

Proofpoint Account Takeover Protection basiert auf Proofpoint Nexus® AI und Bedrohungsdaten. Die Lösung bietet eine zuverlässige Erkennung bestätigter Kontenkompromittierungen und gleichzeitig einen vollständigen Überblick über das Verhalten von Angreifern. Sicherheitsteams können sich schnell einen Überblick über den Umfang eines Zwischenfalls verschaffen, Untersuchungen beschleunigen und Bedrohungen eindämmen, bevor sie zu Business Email Compromise (BEC), Datenverlust, lateralen Bewegungen oder anderen geschäftsschädigenden Angriffen führen.

Als Teil von Proofpoint Collaboration Security Prime integriert sich Proofpoint Account Takeover Protection in Proofpoint Threat Protection Workbench und Threat Interaction Map, um die Untersuchungen auf mehr als ein einzelnes kompromittiertes Konto auszudehnen. Durch die Korrelation von Identitätskompromittierungen mit E-Mail-Bedrohungen, Anwenderinteraktionen und Angreiferaktivitäten verhilft die Lösung Sicherheitsteams zu einem umfassenderen Verständnis der Angriffskampagne. Dies ermöglicht schnellere Untersuchungen, fundiertere Reaktionsentscheidungen und stärkere Behebungsmaßnahmen.



1. **Abb. 1:** Verschaffen Sie sich einen umfassenden Überblick über den gesamten Lebenszyklus von Kontoübernahme-Angriffen – von Aktivitäten vor dem Zugriff bis hin zu Aktivitäten nach dem Zugriff.

Zuverlässige Erkennung von Kontoübernahmen

Proofpoint Account Takeover Protection basiert auf Proofpoint Nexus AI und bietet eine zuverlässige Erkennung bestätigter Kontenkompromittierungen in Microsoft 365, Google Workspace und Okta.

Durch die kontinuierliche Analyse der Anwenderaktivitäten während des gesamten Lebenszyklus einer Kontoübernahme – von Indikatoren vor dem Zugriff bis hin zum Verhalten von Angreifern nach dem Zugriff – identifiziert Proofpoint Account Takeover Protection bestätigte Kontenkompromittierungen zuverlässig und priorisiert Erkennungen auf der Grundlage des Risiko-Schweregrads (Kritisch, Hoch und Mittel). Jede Erkennung umfasst die Verhaltensindikatoren und Beweise, die zu dem Ergebnis beigetragen haben. Auf diese Weise erhalten Analysten schnell einen Überblick darüber, warum ein Konto als kompromittiert identifiziert wurde, damit sie Reaktionen priorisieren und sichere Maßnahmen ergreifen können.

Vollständige Informationen über den Angriff

Sobald die Kontenkompromittierungen bestätigt ist, bietet Proofpoint Account Takeover Protection einen vollständigen Überblick über die Angriffssequenz. Dadurch können Sicherheitsteams nachvollziehen, wie sich der Angriff entwickelt hat und welche Schritte die Angreifer nach dem Zugriff unternommen haben.

Umfassende forensische Erkenntnisse liefern Informationen zu den Aktivitäten nach einem Zugriff. Dazu zählen zum Beispiel Manipulationen des Postfachs, schädliche Posteingangsregeln, OAuth-Missbrauch, Rechteänderungen, internes Phishing, verdächtige E-Mail-Aktivitäten und Persistenz-Techniken. Auf diese Weise können Analysten schnell den Umfang, die Raffinesse und die Reichweite eines Angriffs ermitteln. Proofpoint Account Takeover Protection rekonstruiert die Angriffssequenz und hebt betroffene Anwender und Ressourcen hervor. Dadurch können Untersuchungen beschleunigt, fundiertere Reaktionsentscheidungen unterstützt und Behebungsmaßnahmen verbessert werden.

Automatische Reaktionen auf Bedrohungen

Proofpoint Account Takeover Protection unterstützt Unternehmen bei der schnellen Eindämmung aktiver Bedrohungen. Dazu unterbrechen automatisierte Behebungsmaßnahmen den Zugriff der Angreifer und beschleunigen die Wiederherstellung. Mögliche Reaktionsmaßnahmen sind das Erzwingen von Kennwortänderungen, das Zurücksetzen von Anwenderkennwörtern, das Sperren aktiver Anwendersitzungen, das Entfernen schädlicher Postfachregeln, das Sperren nicht autorisierter OAuth-Anwendungen von Drittanbietern und andere Behebungsmaßnahmen, mit denen die Persistenz von Angreifern verhindert und die Kontointegrität wiederhergestellt werden soll.

Durch die Automatisierung kritischer Eindämmungsmaßnahmen können Sicherheitsteams die Verweildauer von Angreifern reduzieren, laterale Bewegungen einschränken, Geschäftsunterbrechungen minimieren und die Wiederherstellung nach einer Kontenkompromittierung beschleunigen.

Mehrschichtiger Schutzansatz mit Proofpoint Collaboration Security Prime

Als Teil von Proofpoint Collaboration Security Prime beschränkt sich Proofpoint Account Takeover Protection nicht nur auf Kontenkompromittierung, sondern bietet koordinierten Schutz für jede Phase des Lebenszyklus menschlicher Angriffe. Während Proofpoint Account Takeover Protection kompromittierte Konten erkennt, untersucht und eindämmt, verbessert Proofpoint Prime den Schutz, indem es Bedrohungen bereits vor einer Kontokompromittierung abwehrt, Angriffe über E-Mail- und Kollaborationskanäle hinweg korreliert, das Verhalten der Anwender durch adaptive Schulungen verbessert sowie mithilfe

Weitere Informationen finden Sie unter **proofpoint.com/de**.

proofpoint.