proofpoint.

KURZVORSTELLUNG

SSO Password Guard

Erkennen Sie kompromittierte Kennwörter, bevor es zu einer Kontoübernahme kommt

Wichtige Highlights

- **Erkennt die Eingabe von Unternehmenskennwörtern auf nicht genehmigten Websites und warnt so vor Kompromittierungen von Anmeldedaten, bevor Angreifer diese verwenden können**
- **Bietet Echtzeit-Hinweise im Browser, wenn Anwender ihr Unternehmenskennwort wiederverwenden, was eine schnelle Korrektur ermöglicht und wiederholte Kompromittierungsrisiken reduziert**
- **Reduziert Anmeldedaten-bezogene Kompromittierungen, was zu weniger Kontoübernahmen, Untersuchungen und Kennwortrücksetzungen führt**

Überblick

Zu einer Kontoübernahme kann es kommen, wenn Anmeldedaten kompromittiert werden, zum Beispiel durch Angriffe, die Präventionskontrollen umgehen, oder durch alltägliches Anwenderverhalten, das gegen Unternehmensrichtlinien verstößt.

Mitarbeiter verwenden häufig dieselben Unternehmenskennwörter in SaaS-Apps, KI-Tools und externen Websites, sodass das Risiko weit außerhalb der Kontrolle des Unternehmens liegt. Sobald diese Anmeldedaten kompromittiert wurden, können sich Angreifer als legitime Anwender anmelden und herkömmliche Schutzmechanismen leicht umgehen. Diese klassischen Sicherheitskontrollen konzentrieren sich auf die Abwehr von Bedrohungen vor deren Eingang oder auf Benachrichtigungen über ungewöhnliche Aktivitäten nach einer Sicherheitsverletzung. Dadurch entsteht eine kritische Lücke, sobald Anmeldedaten auf einer nicht genehmigten oder schädlichen Website eingegeben werden.

SSO Password Guard hilft beim Schließen dieser Lücke.

Der Proofpoint-Kennwortschutz arbeitet direkt im Browser, erkennt die Wiederverwendung von Unternehmenskennwörtern während der Eingabe und weist Anwender darauf hin, dass sie ihr unsicheres Verhalten ändern sollten. Der Proofpoint Password Guard ist Teil von Proofpoint Collaboration Security Prime und dehnt den Schutz auf alle Kanäle und Angriffsphasen aus, um das Risiko einer Kontoübernahme und die Arbeitsbelastung Ihres Teams zu reduzieren.

Schutz vor Anmeldedatenkompromittierung im Moment des Risikos

SSO Password Guard setzt an einem kritischen Punkt in der Angriffskette an, d. h. der Schutz wird aktiv, nachdem eine Bedrohung den Anwender erreicht hat, aber bevor eine Kontoübernahme erfolgt.

Wenn Anwender Unternehmenskennwörter auf nicht genehmigten oder schädlichen Websites eingeben, erkennt Proofpoint das Verhalten in Echtzeit und bietet in diesem Fall im Browser sofortige Hilfestellungen – sowohl bei der Anmeldung als auch bei der Registrierung. Auf diese Weise wird die Kompromittierung von Anmeldedaten sofort gestoppt, bevor Kennwörter wiederverwendet oder in anderer Form ausgenutzt werden können.

Da der Kennwortmissbrauch während der Eingabe reduziert wird, schließen Unternehmen eine der zuverlässigsten Zugriffsmöglichkeiten für Angreifer. Dies reduziert das Risiko einer Kontoübernahme, bevor es zu einem Zwischenfall kommt.

Durchsetzung von Anmeldedaten-Richtlinien und Förderung von Verhaltensänderungen

Unternehmensrichtlinien allein hindern Anwender nicht daran, Unternehmenskennwörter wiederzuverwenden.

SSO Password Guard fördert sichere Verhaltensweisen, indem der Schutz genau in dem Moment eingreift, in dem Anwender unsichere Aktionen versuchen. Die Echtzeit-Hinweise im Browser verbinden das Verhalten des Anwenders direkt mit dem Risiko und wandeln unsichere Aktionen in unmittelbare Lernmomente um.

Gleichzeitig erhalten Sicherheitsteams Einblick in Wiederholungstäter und Gefahrenmuster. Dadurch können sie gezielte, evidenzbasierte Sensibilisierungsprogramme implementieren und von breit angelegten Schulungen zu fokussierten Maßnahmen übergehen sowie das Wiederholungsrisiko langfristig senken.

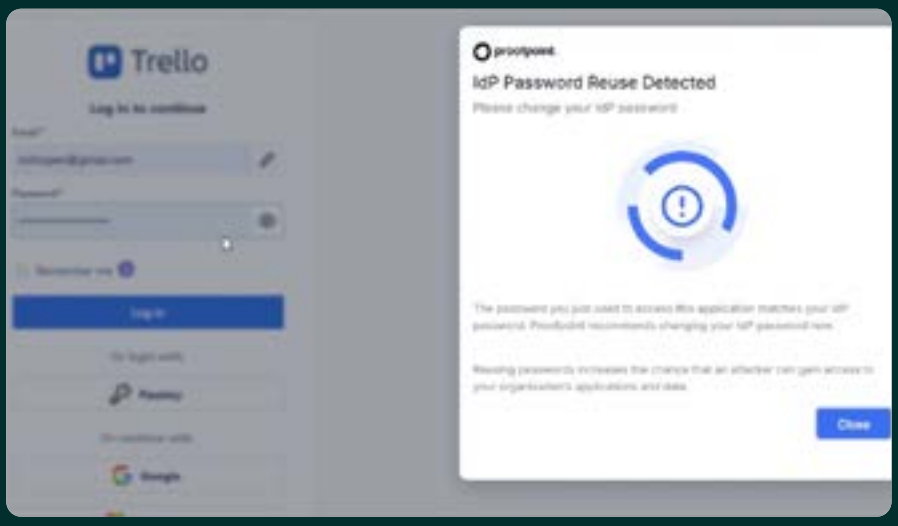

Abb. 1: Beispiel für eine Endnutzerwarnung von SSO Password Guard.

Reduzierung des betrieblichen Aufwands und der Komplexität

Die meisten Sicherheitsteams können Kontoübernahmen erst untersuchen, nachdem die Anmeldedaten bereits kompromittiert wurden. Oft fehlen ihnen klare Einblicke dazu, wo die Kompromittierung aufgetreten ist und welche Anwender das Risiko erhöhen.

SSO Password Guard reduziert diesen Aufwand, da die Kompromittierung von Kennwörtern verhindert wird, bevor Zwischenfälle entstehen. Gleichzeitig erhalten Sicherheitsteams detaillierte Einblicke in die Wiederverwendung von Anmeldedaten. Außerdem sehen sie, auf welchen Websites Unternehmenskennwörter verwendet werden. Sie können das Risiko dieser Websites abwägen und feststellen, welche Anwender wiederholt Anmeldedaten offenlegen und das größte Risiko darstellen.

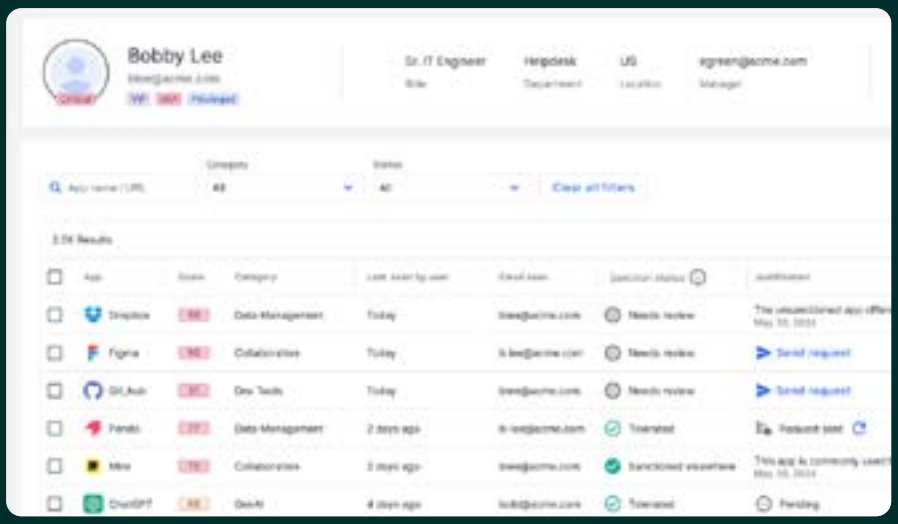

Abb. 2: Einblicke zu Kennwortoffenlegungen in SSO Password Guard.

Auf diese Weise werden die Zahl der Kontoübernahmen und der Zeitaufwand für Untersuchungen sowie für das Zurücksetzen und Bereinigen von Kennwörtern reduziert. Und im Falle einer erfolgten Kompromittierung erhalten die Teams den nötigen Kontext, sodass sie umgehend und ohne Rätselraten reagieren können.

Durch die Integration mit Proofpoint Collaboration Security Prime reduziert SSO Password Guard auch die Abhängigkeit von komplexen, signalgesteuerten Erkennungslösungen. Sicherheitsteams profitieren von zentralisierter Transparenz, zuverlässigen Signalen und kürzeren Reaktionszeiten. Dies trägt zur Senkung der Gesamtkosten und Verbesserung der Sicherheitsergebnisse bei.

proofpoint.