Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (PCAD) schützt Microsoft 365- und Google Workspace-User vor der Kompromittierung von Cloud-Konten. Mit CAD können Sie Cyberkriminelle, die auf Ihre sensiblen Daten und vertrauenswürdigen Konten zugreifen, erkennen, untersuchen und abwehren. Unsere leistungsstarke Forensik und richtlinienbasierten Kontrollen helfen Ihnen, Bedrohungen auf der Grundlage der für Sie wichtigen Risikofaktoren zu überwachen und zu beheben.

WICHTIGE VORTEILE

- Identifizieren Sie die am meisten gefährdeten Benutzer und überwachen Sie Vorfälle über Drilldown-Dashboards
- Anpassung und Priorisierung von Warnmeldungen basierend auf den für Sie relevanten Risikofaktoren
- Korrelieren Sie Bedrohungen über E-Mail und Cloud, um gefährdete Konten genau zu erkennen
- Untersuchen Sie Sicherheitsvorfälle durch detaillierte Forensik und anpassbare Berichte
- Verhindern Sie unbefugten Zugriff auf Cloud-Apps und -Dienste mit adaptiven Zugriffskontrollen
- Automatisieren Sie Sicherheitsmaßnahmen mit flexiblen Richtlinienkontrollen
- Schnelle Bereitstellung in der Cloud
- Zuverlässiger preisgekrönter Kunden-Support

Die Anmeldedaten Ihrer Anwenderkonten sind der Schlüssel zu Ihrem Unternehmen. Wenn Cyberkriminelle Ihre Microsoft 365- oder Google Workspace-Konten kompromittieren, können diese gefährliche Angriffe inner- und außerhalb Ihres Unternehmens starten und Anwender davon überzeugen, Geld zu überweisen oder vertrauliche Informationen weiterzugeben. Zudem erhalten sie so möglicherweise Zugriff auf Ihre wichtigen Daten, Kunden- oder vertrauliche Finanzdaten etc. Das schadet nicht nur dem Ruf, sondern erzeugt auch einen finanziellen Schaden. Sobald die Angreifer einen Fuß in der Tür haben, installieren sie häufig Backdoor-Trojaner für zukünftige Angriffe. Die Kompromittierung der Konten erfolgt häufig per Phishing. Außerdem aber auch durch die folgenden Methoden:

- Brute-Force-Angriffe, bei denen die Anmeldedaten automatisiert „erraten“ werden
- Wiederverwendung von Anmeldedaten, wobei zuvor gestohlene Benutzernamen- und Kennwort-Paare verwendet werden
- Malware wie Keylogger-Programme und das Ausspähen von Anmeldedaten

Mit unserem integrierten, personenorientierten Ansatz, der Cloud- und E-Mail-Bedrohungsaktivitäten korreliert, können Sie sich gegen die Kompromittierung von Cloud-Konten schützen. Wir kombinieren Analysen – die auf Cloud-Zugriff und Benutzerverhalten basieren – mit unserer E-Mail-Threat-Intelligence. So können Sie gefährdete Benutzer identifizieren und kompromittierte Konten erkennen.

Zusätzlich werden mit unseren adaptiven Zugriffskontrollen für von der IT freigegebene Cloud-Anwendungen und -Services auch nicht autorisierte Zugriffe verhindert. Unsere personenorientierten Richtlinien warnen Sie in Echtzeit vor Problemen und wenden bei Bedarf risikobasierte Kontrollen an, z. B. VPN-Enforcement oder Multi-Faktor-Authentifizierung.

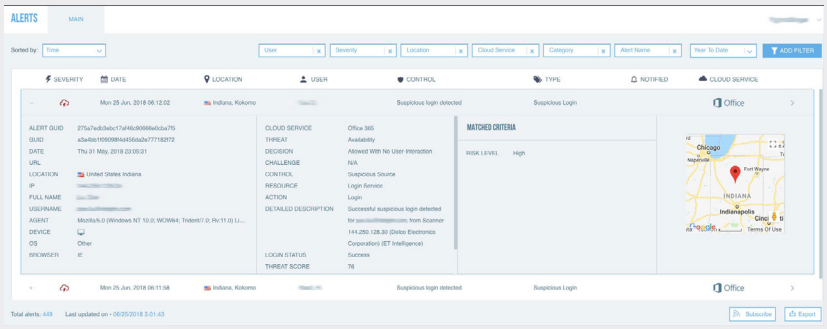
Erkennen Sie kompromittierte Konten

CAD bietet einen personenorientierten Einblick in E-Mail- und Cloud-Bedrohungen. Unsere Lösungen bieten folgende Vorteile:

- Identifizierung Ihrer Very Attacked People (VAPs) und Schutz ihrer Cloud-Konten
- Erkennung kompromittierter Konten mithilfe von Kontextdaten wie Anwenderstandort, Device, Netzwerk und Anmeldezeitpunkt
- Anwendung von Analysen zur Etablierung einer Basis, die sicheres Verhalten umschreibt
- Suche nach Anomalien anhand von erfassten Spuren, Schwellenwerten und hochentwickeltem Machine Learning sowie nach verdächtigen Aktivitäten wie extrem häufigen und ungewöhnlichen Anmeldeversuchen, nach typischem Brute-Force-Verhalten und Ereignissen, die objektiv zu schnell aufeinander erfolgen

Zudem kombiniert CAD unsere umfangreichen vektorübergreifenden Bedrohungsdaten aus Proofpoint Nexus Threat Graph mit benutzerspezifischen Risikoindikatoren. Dadurch können Sie Anmeldeversuche aus ungewöhnlichen Quellen erkennen.

Wir setzen unsere globalen Bedrohungsdaten auch für Reputationsprüfungen von IP-Adressen ein und korrelieren Bedrohungsaktivitäten von E-Mails bis zur Cloud. Zudem helfen unsere E-Mail-basierten Bedrohungsdaten, E-Mail-Angriffe per Anmeldedaten-Phishing und verdächtige Anmeldeversuche in Beziehung zu setzen. Angreifer können ein kompromittiertes Konto für einen Phishing-Angriff nutzen und andere Anwender in Ihrem Unternehmen kompromittieren. Um weitere kompromittierte Konten zu identifizieren, untersuchen wir die Spuren des Angreifers auf ungewöhnliche Benutzeragenten und Aktivitäten (z. B. E-Mail-Weiterleitungen).



Untersuchung von Zwischenfällen mit detaillierter Forensik

Wenn es zu einem Zwischenfall kommt, können Sie in unserem intuitiven Dashboard frühere Aktivitäten und Warnungen untersuchen. Hier können Sie detaillierte Forensikdaten zu Transaktionen überprüfen, z. B. Anwender, Datum und Uhrzeit, IP-Adresse, Gerät, Browser, Benutzeragent, Standort, Bedrohung und Bedrohungsbewertung sowie viele weitere. Sie können diese Daten auch über Drilldown-Grafiken und Protokollberichte anzeigen und analysieren. Außerdem können Sie Aktivitäts- und Warnungsprotokolle filtern und sortieren, um Ihre Untersuchungsberichte individuell anzupassen. Sie können aber auch unsere eigenen Berichte tages-, wochen- oder monatsweise abonnieren. Für weitere Analysen lassen sich die Forensik-Daten manuell oder per SIEM-Integration über REST-APIs exportieren.

Schutz von Microsoft 365- und Google Workspace-Konten mit flexiblen Richtlinien

Mit Informationen, die Sie dank unserer detaillierten Forensik erhalten, können Sie flexible Behebungsrichtlinien erstellen, die auf mehreren Parametern basieren (z. B. Anwender, Standort, Netzwerk, Gerät, verdächtige Aktivität). So können Sie beispielsweise Anmeldewarnungen für Länder auf der schwarzen Liste oder für Geräte, die nicht Ihren Unternehmensrichtlinien entsprechen, generieren. Wenn Sie einen stark genutzten Dienst wie Microsoft 365 oder Google Workspace überwachen, müssen Sie die Warnungen priorisieren, um eine Überflutung mit Meldungen zu vermeiden. Mit CAD können Sie Warnmeldungen anhand ihres Schweregrades generieren und dabei jede Benachrichtigung anpassen oder einfach die Standardvorlage nutzen. Und Sie können gefährdete Anwender genauer überwachen oder ihren Zugang sperren, wenn eine verdächtige Anmeldung erfolgreich ist.

Die adaptiven Zugriffskontrollen von CAD erlauben personenorientierte Echtzeit-Sicherheitsmaßnahmen auf Grundlage von Risiko, Kontext und Rolle. Sie können Zugriffsversuche von gefährlichen Standorten und Netzwerken oder Anmeldeversuche bekannter Bedrohungsakteure automatisch blockieren. Zudem können Sie risikobasierte Kontrollen – darunter starke Authentifizierung und VPN-Durchsetzung – auf stark gefährdete und umfassend berechtigte Anwender anwenden.

Schnelle Bereitstellung in der Cloud

Cloud-Plattformen benötigen Cloud-Schutz. Unsere Cloud-Architektur und die Schutzmaßnahmen über Microsoft 365- oder Google Workspace-APIs ermöglichen die schnelle Bereitstellung und liefern sofortigen Mehrwert.

Durch die Implementierung adaptiver Zugriffskontrollen können Sie Ihre Anmeldungen bei Cloud-Anwendungen an unser SAML-Gateway (Security Assertion Markup Language) weiterleiten. Dieses Gateway kontrolliert die föderierte Authentifizierung zwischen jedem Serviceanbieter und dem Identitätsanbieter. CAD unterstützt jeden von der IT-Abteilung genehmigten Cloud-Dienst, der mit SAML 2.0 verbunden ist. Für starke Authentifizierung können Sie Ihre Lösung für Multifaktor-Authentifizierung integrieren oder unsere Authentifizierungs-App Proofpoint Mobile Access verwenden, die in CAD enthalten ist. Sie können innerhalb von Tagen – nicht Wochen oder Monaten – hunderte oder tausende Anwender schützen.

Als einer der Branchenführer beim Bedrohungsschutz nutzen wir die Cloud, um unsere Software täglich zu aktualisieren, sodass Sie den Angreifern stets einen Schritt voraus bleiben. Unsere Cloud-Bereitstellung bietet auch die notwendige Flexibilität, um Anwender in jedem Netzwerk oder auf jedem Gerät zu schützen.

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. 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 personenorientierten 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**.