So schützt Proofpoint vor Cloud-Kontoübernahmen

Potenziell verheerende Cloud-Kontoübernahmen verhindern und beheben

Produkte

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Zero Trust Network Access (ZTNA)
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Proofpoint Threat Protection-Plattform
- Proofpoint Targeted Attack Protection (TAP)

Wichtige Vorteile

- Verhinderung der Kontoübernahme durch Blockieren der Phishing-Angriffe, mit denen Anmeldedaten gestohlen werden sollen oder Malware aktiviert wird
- Erkennung und Behebung aller Vorkommen von Cloud-Kontoübernahmen
- Aufbau von zuverlässigem Schutz für Ihre wertvollen Ressourcen vor Bedrohungen
- Verhindern, dass Ihre Mitarbeiter unbeabsichtigt Bedrohungen in Ihre Umgebung hineinbringen
- Erfassung erstklassiger Bedrohungsdaten, damit Sie sich vor potenziellen Bedrohungen schützen können

Cyberkriminelle folgen Unternehmen in die Cloud. Da immer mehr Unternehmen auf gehostete E-Mails und Webmails, Cloud-basierte Produktivitätsanwendungen wie Microsoft 365 und Google Workspace sowie Cloud-basierte Entwicklungsumgebungen wie AWS und Azure umstellen, haben Cyberkriminelle schnell festgestellt, dass sich die grundlegenden Konto-Anmeldedaten eignen, um an Geld und Macht zu kommen. Diese Anmeldedaten sind daher das Ziel von immer mehr Bedrohungskampagnen – und die stetigen Bemühungen sind nur der erste Schritt zu Überweisungsbetrug, Industriespionage, Diebstahl von personenbezogenen Daten und anderen Aktionen.

Eine Cloud-Kontoübernahme beginnt damit, dass der Angreifer die Anmeldedaten eines Anwenders kompromittiert und so Zugriff auf Systeme erlangt. Diese Angriffe starten oft mit einer E-Mail, die Malware enthält oder den Anwender dazu verleitet, seine Anmeldedaten bereitzustellen. Sobald das Konto übernommen wurde, können sich die Angreifer als legitime oder vertrauenswürdige Person innerhalb des Unternehmens ausgeben. Dadurch erhalten sie die Möglichkeit, sich lateral im Netzwerk zu bewegen und Schaden anzurichten, beispielsweise indem sie wichtige Daten stehlen oder verschlüsseln. Ebenso können sie Malware hochladen, um Sync-and-Share-Funktionen zwischen Ihren Endpunkten, Microsoft 365 und anderen Cloud-Repositorys zu nutzen. Ab diesem Punkt können sie sich schnell im gesamten Unternehmen verbreiten oder vertrauliche Daten herunterladen, um Sie anschließend zu erpressen.

Da zunehmend Single Sign-On-Systeme verwendet werden, erhalten die Angreifer mit nur einem Satz Anmeldedaten umfassenden Zugriff auf verschiedenste Systeme im Unternehmen.

Eine der gefährlichsten Formen von Cloud-Kontoübernahme ist Ransomware. Bei dieser Cyberangriffsform werden Geschäftsabläufe unterbrochen, Krankenhäuser an der Behandlung von Patienten gehindert und ganze Behörden blockiert. Allein im letzten Jahr wurden in den USA mehr als 65.000 Ransomware-Angriffe verzeichnet. Und laut der Unit 42 von Palo Alto Networks begannen 75 % dieser Angriffe mit einer E-Mail.[1] Ransomware bereitet CISOs größte Sorgen – und wird als Sicherheitsproblem mit nationaler Tragweite eingestuft.

Proofpoint-Lösungen

Cyberkriminelle verwenden mehrere Strategien und Vektoren, um in Ihre Netzwerke zu gelangen. Sie nutzen häufig hybride Ansätze, um die gewünschten Informationen zu erhalten. Das Arsenal umfasst Brute-Force-Angriffe, Social-Engineering-Taktiken und Malware. Zur Abwehr benötigen Sie umfassenden mehrschichtigen Schutz. Proofpoint bietet zahlreiche Produkte und Services an, die Ihnen dabei helfen.

Gemeinsam eingesetzt können die Proofpoint-Lösungen Sie mit folgenden Vorteilen dabei unterstützen, Cloud-Kontoübernahmen abzuwehren:

- Verhinderung der Erst-Kontoübernahme
- Erkennung und Behebung von Cloud-Kontoübernahmen
- Aufbau von Schutz für Ihre wertvollen Ressourcen – Anwender sowie Systeme – zur Blockierung externer Bedrohungen
- Verhindern, dass Ihre Mitarbeiter unbeabsichtigt Bedrohungen in Ihre Umgebung hineinbringen
- Erfassung erstklassiger Bedrohungsdaten, damit Sie sich vor potenziellen neuen Bedrohungen schützen können

Prävention, Erkennung und Behebung

Die Proofpoint Threat Protection-Plattform ist eine integrierte, mehrschichtige Lösung, mit der das Risiko von Cloud-Kontoübernahmen reduziert wird. Sie umfasst branchenführende Erkennungsfunktionen, die verhindern, dass Anwender Malware, Anmeldedaten-Phishing und andere E-Mail-basierte Bedrohungen erhalten. Außerdem koordiniert sie die Sicherheitsmaßnahmen zur Behebung kompromittierter Konten. Das beschleunigt die Reaktion auf Zwischenfälle und verringert den Aufwand für die IT. Angegriffene Anwender sowie Anwender, die mit echten Bedrohungen für Anmeldedaten interagieren, erhalten kurze, zeitnahe Belehrungen per Sicherheitsschulung. Und mithilfe informativer und anpassbarer HTML-Banner können Sie Anwender auf potenziell schädliche E-Mails hinweisen. Die Plattform kann ein- und ausgehende Nachrichten per DMARC authentifizieren und kompromittierte Lieferantenkonten identifizieren. Dieser mehrschichtige Ansatz ist der Grund dafür, dass mehr als 60 % der Fortune 1000-Unternehmen beim Bedrohungsschutz und bei der Reduzierung des Risikos von Cloud-Kontoübernahmen auf Proofpoint vertrauen.

1 Unit 42, Palo Alto Networks *(https://unit42.paloaltonetworks.com/ransomware-families/)*: „Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report“ (Daten von 2021 zur Ergänzung des Ransomware-Bedrohungsberichts von Unit 42), Juli 2021.

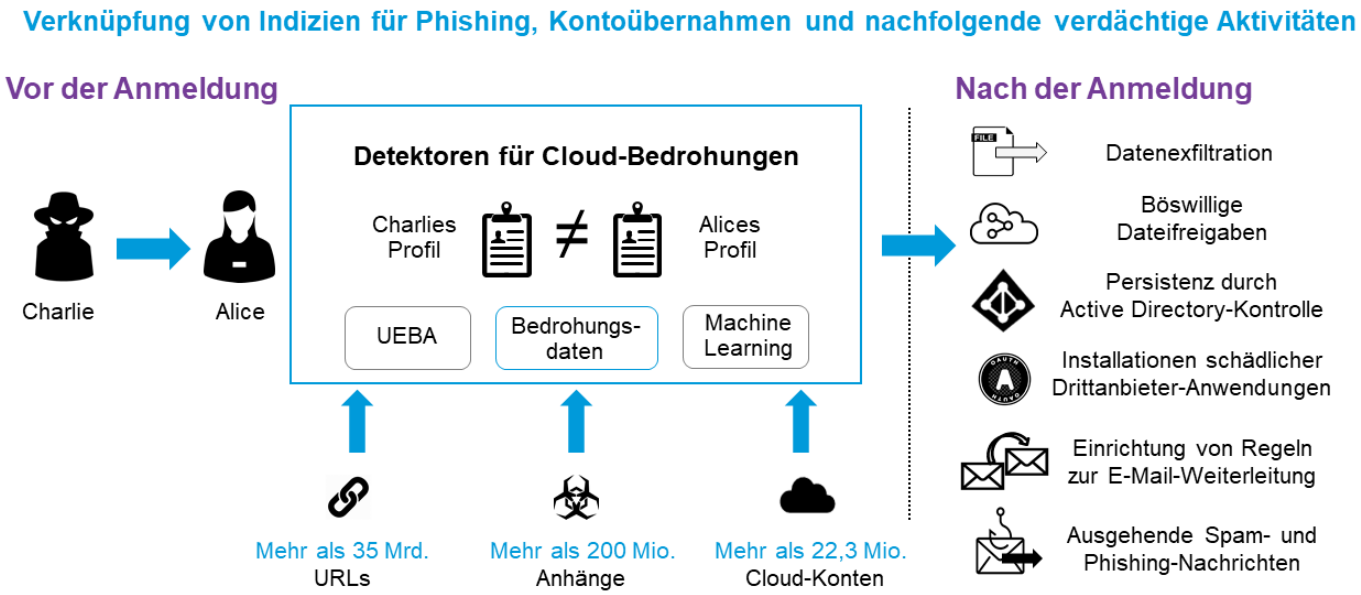

Abb. 1: Erkennung kompromittierter Konten durch CASB.

Proofpoint Cloud App Security Broker (CASB) ist unsere Komponente zum Schutz vor Cloud-Kontoübernahmen. Die Lösung nutzt einen personenzentrierten Ansatz, um Ihre Anwender vor Cloud-Bedrohungen und Ihre vertraulichen Daten zu schützen. Im ersten Schritt bietet sie Transparenz und Zugriffskontrolle. Denn nur wenn Sie Ihre Risiken kennen, können Sie einen effektiven Schutz vor Cloud-Kontoübernahmen aufbauen. Proofpoint CASB unterstützt Sie bei der Implementierung präventiver Sicherheitsmaßnahmen wie anpassbaren Zugriffskontrollen (z. B. erweiterte Authentifizierung). Wir erkennen alle Übernahmeversuche und weisen Sie auf Aktionen von Bedrohungsakteuren hin, sobald sie Zugriff auf ein Konto erlangen konnten. Proofpoint CASB sperrt kompromittierte Konten vorübergehend und behebt alle Bedrohungen nach einer Übernahme. Das bedeutet, dass die Lösung selbst nach einer erfolgreichen Übernahme verhindert, dass dieses Konto zur Weiterleitung von E-Mails, zur Extraktion von Daten und zum Versand von Phishing und Spam missbraucht werden kann.

Zero-Trust-Alternative für VPN

Mitarbeiter werden weltweit immer mobiler und arbeiten immer häufiger im Homeoffice. Zudem verschwindet der Netzwerk-Perimeter, da immer mehr Anwendungen in die Cloud migriert werden. Viele Unternehmen werden sich erst nach und nach der neuen Sicherheitsherausforderungen bewusst, die diese neue Situation mit sich bringt. Sie stellen erst jetzt fest, dass ihre herkömmlichen Sicherheitssysteme, die für standortzentrische Verbindungen und Sicherheitsprodukte ausgelegt sind, die dynamischen Cloud-basierten Bedrohungen nicht abwehren können.

Mit Proofpoint Zero Trust Network Access (ZTNA) können sich Ihre Anwender sicher mit Anwendungen verbinden – ganz gleich, ob diese im Rechenzentrum oder in der Cloud gehostet werden. Diese personenzentrierte Alternative zu VPN umfasst mikrosegmentierte Berechtigungen, sodass die Angriffsfläche Ihres Netzwerks stark reduziert wird. Sie erhalten einen Software-definierten Perimeter (SDP), mit dem Sie Zero-Trust-Netzwerkzugriff umsetzen können.

Browser- und E-Mail-Isolierung

IT- und Sicherheitsteams müssen eine sichere Arbeitsumgebung für ihre Anwender gewährleisten. Gleichzeitig sollen die Anwender effektiv mit Teammitgliedern forschen und zusammenarbeiten können. Das kann schwierig sein, wenn zwei Hauptvektoren für Cloud-Kontoübernahmen genau die Tools sind, die für Recherche und Kommunikation verwendet werden: Web und E-Mail. Proofpoint bietet zwei Lösungen an, mit denen Ihre Teams alle Vorteile sicher nutzen und nahtlos surfen können – und dennoch vor Cloud-Kontenkompromittierungen geschützt werden.

Proofpoint Browser Isolation schützt vor Cloud-Kontenkompromittierungen, indem verhindert wird, dass Anwender beim Surfen im Web versehentlich auf Phishing-Links klicken oder schädliche Daten auf Unternehmensgeräte herunterladen.

Proofpoint Email Isolation erweitert die Funktionen von Proofpoint Targeted Attack Protection (TAP) und ermöglicht die risikobasierte Isolierung von URL-Klicks in Unternehmens-E-Mails. Zudem kann sie Ihre am stärksten angegriffenen Mitarbeiter aufzeigen und die riskantesten URLs identifizieren, die in die Postfächer Ihrer Anwender gelangen.

Aktuelle Bedrohungsdaten

Mit detaillierten und umfassenden Einblicken in die Bedrohungslandschaft können Sie sich auf die nächste große Bedrohung vorbereiten. Proofpoint Nexus Threat Graph bietet die umfassenden Bedrohungsdaten, die Sie benötigen, um den größten aktuellen Bedrohungen einen Schritt voraus zu bleiben. Die Lösung kombiniert Milliarden Echtzeit-Datenpunkte aus der ganzen Welt zu mehreren Bedrohungsvektoren, erweiterte KI und Machine Learning sowie ein weltweites Team aus Cybersicherheitsforschern.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **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.

0205-005-01-01 11/21