Privilegierte Konten im Visier: Fünf Best Practices gegen Identitätsdiebstahl durch Phishing

Für Cyberkriminelle bleibt Phishing eine der effizientesten Angriffsarten, um Log-in-Informationen abzugreifen. Besonders verheerend für Unternehmen ist die Kompromittierung privilegierter Benutzerkonten, die über hohe Berechtigungen verfügen. Hierdurch erhalten Hacker weitreichenden Zugriff auf Unternehmensressourcen und können unter dem Deckmantel der gestohlenen Identität lange unentdeckt agieren, um etwa Informationen wie Finanzdaten, Geschäftsgeheimnisse oder geistiges Eigentum zu exfiltrieren. Darüber hinaus können Cyberkriminelle die gestohlenen Zugangsdaten auch lukrativ im Darknet verkaufen.

Laut Forrester sind 80 Prozent der Sicherheitsverletzungen mit kompromittierten privilegierten Zugangsdaten verbunden. Um sich vor Identitätsdiebstahl und Kontenmissbrauch durch Phishing-Angriffe zu schützen, sollten Unternehmen deshalb einen mehrschichtigen Ansatz aus Mitarbeiteraufklärung und Technologien einsetzen.

Best Practices gegen Kontenmissbrauch durch Phishing - 1. Mitarbeiterschulungen
Die umfangreiche Aufklärung der Mitarbeiter über die Gefahr und Merkmale von Phishing zählt zu den Grundpfeilern, um sich vor Angriffen zu schützen. Generell sollten Nutzer folgende Punkte beachten:

• Persönliche Daten nicht öffentlich teilen: Nutzer sollten keine persönlichen Daten wie Geburtstage, Reisepläne oder persönliche Kontaktinformationen in sozialen Medien preisgeben, da diese von Angreifern für Social Engineering missbraucht werden können.

• Absenderadresse und Schreibstil prüfen: Bei verdächtigen E-Mails sollten Mitarbeiter stets die E-Mail-Adresse des Absenders kontrollieren, indem sie mit der Maus über die Absenderadresse fahren. Warnzeichen für Phishing sind zudem Rechtschreib- und Grammatikfehler sowie unübliche Formulierungen.

• Legitimität von Webseiten prüfen: Nutzer sollten nicht auf Links zu Webseiten in E-Mails klicken, sondern die Website direkt über den Browser aufrufen, um die Authentizität der in der E-Mail angegebenen Seite zu überprüfen.

• Neue Nachricht an bekannte Absender bei verdächtigen E-Mails: Wirkt eine E-Mail von einer scheinbar bekannten Quelle verdächtig, sollten Nutzer sich mit einer neuen E-Mail an diese Quelle wenden, anstatt auf „Antworten" zu klicken. Hierdurch kann die Legitimität der Nachricht kontrolliert werden.

• Ruhe walten lassen: Bei Phishing-Angriffen vermitteln Cyberkriminelle in ihren Nachrichten häufig Dringlichkeit, um ihre Opfer dazu zu bringen, rasch und unbedacht zu handeln. Nutzer sollten sich nicht aus der Ruhe bringen lassen und stets die oben genannten Schritte zur Überprüfung der Nachricht durchführen.

2. Vorsicht bei Web-Tools von Drittanbietern

Beim Einsatz von Drittanbieter-Web-Tools sollten Unternehmen deren Sicherheitsprotokolle untersuchen, um festzustellen, ob diese umfassend genug sind, um das Einschleusen von Malware zu minimieren. Natürlich muss bei der Beschränkung der Verwendung von Drittanbieter-Web-Tools ein Gleichgewicht zwischen Sicherheit und Nutzererfahrung ausgelotet werden.

3. E-Mail-Security-Software

Weiterhin ist eine E-Mail-Security-Software empfehlenswert, die eingehende E-Mails in einer Sandbox sammelt und validiert sowie bösartige Links erkennt und entfernt.

4. Multi-Faktor-Authentifizierung

Es sollte eine Multi-Faktor-Authentifizierung (MFA) eingesetzt werden, die mehrere Identifizierungsmethoden erfordert. Hierzu zählt etwas, das der Nutzer kennt (Passwort); etwas, das er besitzt (Gerät); sowie etwas, das er ist (biometrische Authentifizierung). Dies ist eine der besten Methoden, um zu verhindern, dass unautorisierte Benutzer auf sensible Daten zugreifen und sich lateral im Netzwerk bewegen können.

5. Risikobasierte Zugriffskontrollen

Unternehmen sollten zudem risikobasierte Zugriffskontrollen implementieren, um Zugriffsrichtlinien auf Grundlage des

Benutzerverhaltens zu definieren und durchzusetzen. Durch eine Kombination aus Analysen, maschinellem Lernen, Benutzerprofilen und der Durchsetzung von Richtlinien können Zugriffsentscheidungen in Echtzeit getroffen werden. Je nach Risiko-Level können dadurch die Authentifizierungsanforderungen verstärkt oder der Zugriff vollständig blockiert werden. Risikobasierte Zugriffskontrollen werden oft in Kombination mit MFA eingesetzt.

Die Flut an Phishing-Angriffen und damit einhergehende kompromittierte Zugangsdaten bleibt eine der größten Bedrohungen für die Unternehmenssicherheit. Die Aufklärung der Mitarbeiter und die Verbesserung der Authentifizierungssysteme einer Organisation sind wesentliche Schritte, um sich gegen Phishing und Identitätsdiebstahl zu schützen.