Wenn Cyberkriminelle ihre Köder auswerfen: Security-Grundlagen gegen Phishing-Angriffe

Cyberkriminelle sind oft nur einen Phishing-Angriff davon entfernt, ungehinderten Zugriff auf Geräte, Netzwerke und Unternehmensdaten zu erhalten. Dabei nutzen sie eine Vielzahl an Social-Engineering-Techniken. Diese reichen von Identitätsdiebstahl und Imitation bekannter Marken über gefälschte Stellenbewerbungen bis hin zu hochpersonalisiertem Spear-Phishing mithilfe privater Daten der Opfer. Phishing erfolgt meist per E-Mail, kann aber auch per Post, Telefon (Voice Phishing/Vishing), SMS (Smishing), Social Media sowie über Websites erfolgen, geht aber oft weit über die Verteilung verdächtiger Nachrichten hinaus. Zu weiteren Angriffstechniken zählen:
• DNS-basiertes Phishing gefährdet Hostdateien oder Domain-Namen eines Unternehmens und leitet dessen Kunden zu einer gefälschten Webseite weiter, um persönliche Daten oder Zahlungsinformationen abzugreifen.

• Phishing mit Content-Injection nutzt verseuchte Inhalte wie Codes oder Bilder, die zur Unternehmenswebsite oder Seiten von Partnern hinzugefügt werden, um persönliche Informationen von Mitarbeitern und Kunden wie etwa Log-in-Details zu stehlen. Diese Art von Phishing zielt besonders auf Personen ab, die auf verschiedenen Websites das gleiche Passwort verwenden.

• Man-in-the-Middle-Phishing: Hierbei stellen sich Kriminelle zwischen die Website des Unternehmens und dessen Kunden. So können sie alle Informationen, die der Kunde eingibt, erfassen.

Security-Best Practices gegen Phishing-Angriffe

Phishing birgt das Potenzial, viele der von Unternehmen eingesetzten Sicherheitsmaßnahmen zu umgehen und verheerende Auswirkungen auf sensible Daten und Ressourcen zu haben. Selbst für gut informierte User ist es mittlerweile schwierig, Phishing zu erkennen, da die Attacken immer ausgefeilter werden. Deshalb sind entsprechende Security-Best-Practices entscheidend, um sich gegen die Flut an Phishing-Angriffen zu verteidigen. Hierzu zählen:

Multi-Faktor-Authentifizierung: Es ist empfehlenswert, zwei Arten der Überprüfung durchzuführen, etwa ein Passwort und eine Sicherheitsfrage, wenn Nutzer sich bei sensiblen Konten anmelden. Die Zwei- oder Multifaktor-Authentifizierung trägt dazu bei, Cyberkriminellen, die sich Zugang zu Konten verschaffen wollen, die Arbeit zu erschweren. Selbst wenn ein Passwort im Besitz des Angreifers ist, bleibt das Konto durch eine zweite oder sogar dritte Authentifizierungsebene geschützt. Für die beste Verteidigung eignen sich Authentifizierungsebenen, die dem Benutzer physisch vorliegen, zum Beispiel ein Gerät, oder eine biometrische Authentifizierung.

Security-Schulungen und Simulationstrainings von Phishing-Angriffen: Der erste Schritt besteht darin, alle Mitarbeiter darin zu schulen, Phishing-E-Mails zu erkennen. Eine der besten Möglichkeiten, um sicherzustellen, dass Mitarbeiter bei der Erkennung potenzieller Phishing-E-Mails wachsam sind, sind Simulationstrainings. So kann das IT-Team zum Beispiel selbst Test-Phishing-Mails an die Mitarbeiter versenden und überwachen, welche und wie viele Personen auf den Köder anspringen.

VPN zum Schutz der Internetverbindung: Ein VPN verschlüsselt die Internetverbindung und hält die besuchten Websites und die vom Nutzer eingegebenen Informationen vor Angreifern geheim. Die Nutzung eines VPN verhindert, dass Angreifer den WLAN-Verkehr über öffentliche Netzwerke abfangen, eine gängige Technik, um Anmeldedaten oder andere sensible Informationen abzugreifen.

Sicherung von BYODs vor bösartigen Applikationen: Ein neuer Bedrohungsvektor, der durch den BYOD-Trend entstanden ist, sind bösartige Apps auf Mobilgeräten der Mitarbeiter, welche auf deren Adressbücher zugreifen und diese exportieren. Hierdurch erhalten Angreifer Kontakte, die sie für gezieltes Spear-Phishing missbrauchen können. Ein wichtiger Schritt für die Unternehmenssicherheit ist es, potenzielle Angreifer daran zu hindern, auf das Firmenverzeichnis zuzugreifen, welches Namen, E-Mail-Adressen und andere persönliche Mitarbeiterdaten enthält. So sollte eine mobile Sicherheitssoftware auf Endgeräte installiert werden, die Apps scannt und Benutzer daran hindert, auf die Unternehmensnetzwerke zuzugreifen, wenn sich auf ihren Mobilgeräten Applikationen befinden, die die Datensicherheit gefährden.

Phishing-Schutz beim mobilen Arbeiten: Ein weiterer Schritt besteht darin, mobile Benutzer vor dem Besuch von Phishing-Websites zu schützen, besonders, wenn sie sich in einem WLAN-Netzwerk befinden, welches das Unternehmen nicht kontrolliert. Diese Schutzmaßnahmen müssen auf Netzwerkebene durchgeführt werden, da eine bloße

E-Mail-Filterung hier nicht ausreicht. Phishing- und Spear-Phishing-Angriffe können sowohl über Firmen-Mails, die private E-Mail des Benutzers, als auch per SMS erfolgen. Mobile User sollten deshalb per VPN mit Diensten verbunden sein, die ein sicheres Domain Name System (DNS) und Blacklisting anbieten, um den Zugriff auf Phishing-Websites zu verhindern.

Ausgeklügelte Phishing-Angriffe stellen weiterhin eine der größten Bedrohungen für die Unternehmenssicherheit dar, weil sie auf das häufig schwächste Glied in der Security-Kette abzielen: den Menschen. Durch umfangreiche und kontinuierliche Mitarbeitertrainings und einen mehrschichtigen Ansatz aus Sicherheitstechnologien können jedoch die Risiken von Phishing deutlich gemindert werden.