Was versteht man unter den Begriff Phishing?

Phishing ist eine Form der Cyberkriminalität, bei der ein Gegner eine reale Person oder Institution imitiert und sich per E-Mail oder anderweitig als Agent oder Entität zeigt. Bei dieser Art von Cyberangriff sendet ein Angreifer bösartige Links oder Anhänge, die verschiedene Funktionen erfüllen können, einschließlich der Erfassung von Informationen über ein Opfer oder deren Konto. Diese Art von Nachrichten sind für die Opfer in Bezug auf Geldverlust und Identitätsdiebstahl schädlich.

Phishing ist definiert als die betrügerische Sammlung vertraulicher Daten durch die Empfänger und deren Missbrauch. Im Allgemeinen sind personenbezogene Daten wie Kreditkartennummern oder Passwort erforderlich. Wenn Benutzer diese Website besuchen, werden sie aufgefordert, persönliche Daten anzugeben, die an den Angreifer weitergeleitet werden.

Phishing ist eine weit verbreitete Form der Cyberattacke, vor der jeder lernen muss, sich selbst zu schützen. Es gibt verschiedene Möglichkeiten, wie die Angreifer die notwendigen Informationen für die betrügerische Handlung erhalten. In einigen Fällen wird die Malware direkt auf den Computer des Opfers heruntergeladen, und die Betrüger profitieren davon, dass sie ihre Kreditkartendaten oder anderen persönlichen Daten besitzen.

Häufig ist es der Fall, dass ein Unternehmen als Opfer dasteht und nicht eine einzelne Person. In einer solchen Situation werden E-Mails an Mitarbeiter gesendet, um Zugangsdaten oder andere vertrauliche Informationen zu erhalten, die für einen fortgeschrittenen Angriff erforderlich sind. Cyberangriffe wie Advanced Persistent Threats (APT) und Ransomware beginnen oft mit Phishing.

Damit ein Phishing-Versuch erfolgreich ist, muss die versendete E-Mail vertrauenswürdig und wichtig für das Opfer erscheinen. Daher nutzen Angreifer oft soziale Netzwerke, um so viele Informationen wie möglich über die Interessen ihrer Opfer, das soziale Umfeld, die persönliche und berufliche Entwicklung und so weiter herauszufinden. Nachdem sie diese Informationen gesammelt haben, sind sie in der Lage, die perfekte personalisierte E-Mail zu erstellen, die höchstwahrscheinlich eine Person täuschen würde.

Wie kann man so einen solchen Angriff rechtzeitig erkennen?

Abgesehen davon, dass wir immer wachsam sein und jede unerwartete E-Mail in Frage stellen sollten, insbesondere wenn wir aufgefordert werden, ein Programm/Software/Datei herunterzuladen oder die Anmeldeinformationen bestimmter Konten zu aktualisieren, kann man eine bösartige E-Mail auch durch genaue Inspektion identifizieren, da Rechtschreibfehler innerhalb ihres Inhalts oder sogar ihrer URL häufig vorkommen.

Wie kann man sich davor schützen?

Der erste Schritt, den man tun kann, um sich vor solchen Angriffen zu schützen, besteht darin, sich bewusst zu werden, was es impliziert und wie man es identifiziert. Es gibt natürlich Methoden wie die Verwendung eines E-Mail-Filters für das Netzwerk-Gateway, der die Anzahl der Phishing-E-Mails erfassen und reduzieren kann.