Spear-Phishing

Bei Spear-Phishing handelt es sich um eine neuere Methode des Phishing (Betrugsversuche per E-Mail) mit einem gezielteren persönlichen Ansatz. Spear-Phishing richtet sich meistens gegen konkrete Organisationen oder ein einzelnes Unternehmen.

Gezieltes Fischen nach Informationen

Spear-Phishing-Attacken (dt. „Speer-Fischen“) sind Angriffe per E-Mail, die sich im Gegensatz zum willkürlichen Phishing gegen ein konkretes Opfer richten. Spear-Phishing zielt darauf ab, nicht autorisierten Zugriff auf vertrauliche Daten wie etwa Finanzdaten, Geschäftsgeheimnisse, geistiges Eigentum oder militärische Informationen zu erhalten.

Vorgehensweise einer Attacke

Üblicherweise leitet eine E-Mail, die dem Anschein nach von einer vertrauenswürdigen Quelle stammt, den ahnungslosen Empfänger an eine gefälschte, oft mit Schadsoftware infizierte Webseite weiter. Um die Aufmerksamkeit des Opfers zu erregen und ihn dazu zu bringen, dem in der E-Mail aufgeführten Link zu folgen, gehen die Betrüger in der Regel sehr geschickt vor. So stammen die E-Mails angeblich von großen und bekannten Unternehmen (z. B. Ebay) oder offiziellen Organisationen wie etwa dem Nationalen Zentrum für vermisste und misshandelte Kinder. Ein weiterer Ansatz ist, das Vertrauen der Zielperson über Insider-Informationen aus sozialen Netzwerken zu erwecken – etwa über die Ausbildungsstätte, Sportaktivitäten oder den Inhalt einer zuletzt „geposteten“ Nachricht. Die E-Mails und verlinkten Webseiten sind oft derart auf den jeweiligen Empfänger zugeschnitten, dass dieser keinen unmittelbaren Verdacht schöpft. Klickt er den in der E-Mail enthaltenen Link aus Neugier, Mitleid, Angst oder sonstigem Interesse an, wird er auf einer realistisch erscheinenden Webseite schließlich dazu aufgefordert, bestimmte persönliche Daten wie Bankkontonummern, Identifikationsnummern oder Kennwörter preiszugeben.

Vorsicht, wenn…

- …Sie der Quelle der E-Mail nicht vollständig vertrauen – klicken Sie weder auf Weblinks noch auf E-Mail-Anhänge
- …der Absender der E-Mail sich als Freund, Bekannter, Arbeitgeber oder (ehemaliger) Kollege ausgibt
- …Sie in der E-Mail persönlich mit ihrem Vornamen (z. B. „Hallo Markus!“) angesprochen werden statt mit „Sehr geehrte(r) Herr/Frau…“
- …der Absender persönliche Details über Sie erwähnt – fragen Sie sich, woher die Person das wissen könnte
- …persönliche Daten wie Bankverbindung, Kreditkarteninformationen, Zugangscodes oder Passwörter abgefragt werden

Siehe auch:
Phishing

Zurück