Social Engineering & Phishing

Problembeschreibung und Ursache

Täglich werden durch Social Engineering menschliche Eigenschaften, wie zum Beispiel Vertrauen, Angst und Hilfsbereitschaft, ausgenutzt, um Personen zu manipulieren. Dadurch werden die manipulierten Personen dazu gebracht, Sicherheitsfunktionen zu deaktivieren, Schadstoffe zu installieren usw.

Was ist Phishing

Phishing ist ein Beispiel für Social Engineering, in dem Angreifer gefälschte E-Mails versenden, die häufig nicht als solche auf den ersten Blick erkannt werden. Die Empfänger werden dazu verleitet, auf einen Betrug hereinzufallen.

Bedrohungsszenarien

Phishing hat mehrere Arten, die Angreifer verwenden, wie zum Beispiel:

- Chefmasche:
  Angreifer versuchen als falsche Führungskraft den Nutzer zu manipulieren.
- Link Manipulation:
  E-Mails/Nachrichten beinhalten einen Link, der zu einer schädlichen Webseite führen.
- Spear-Phishing:
  E-Mails werden gezielt an bestimmte Personen, die eine wichtige Rolle im Unternehmen und erweiterte Zugangsrechte haben, gesendet.
- Malware:
  Der Anhang der Mail beinhaltet schädliche Schadsoftware, die auf das Gerät der Nutzer geladen wird.

Typische Merkmale eines Phishing Angriffs

Bei den E-Mails gibt es einige Merkmale, die darauf hindeuten, dass es sich um einen Angriff handeln könnte:

- Fehlende persönliche Anrede
- Grammatikalische Fehler
- Fristen und Zeitdruck
- Merkwürdige Anhänge
- Links zu Fake-Webseiten

Dieses Dokument orientiert sich an der IEC-62443-3-2 Norm, BSI - Social Engineering - der Mensch als Schwachstelle, hornetsecurity-was ist phishing

https://www.hornetsecurity.com/de/wissensdatenbank/was-ist-phishing/?_adin=02021864894 , sowie proofpoint-phishing https://www.proofpoint.com/de/threat-reference/phishing