BEDROHUNG – SOCIAL ENGINEERING

VON DER KONTAKTANFRAGE ZUR INDIVIDUALISIERTEN PHISHING-ATTACKE

Viele Standards der Informationssicherheit fordern mindestens die Betrachtung der Vertraulichkeit, Integrität und Verfügbarkeit.

Das Schutzziel der Authentizität wird oft nicht berücksichtigt.

Der technische Schutz von Unternehmen wurde zunehmend verbessert – die menschlichen Aspekte und Social Engineering bzw. Social Hacking werden noch nicht ausreichend betrachtet.

Aktuelle Statistiken und bekannte Vorfälle weisen akuten Handlungsbedarf im Bereich des Social Engineering auf.

25 Autor: Prof. Christoph Thiel I Stand: 11/2022

TÜV NORD Akademie

Unter dem Begriff Social Engineering wird eine zwischenmenschliche Beeinflussung verstanden. Das Ziel hierbei ist, dass dabei Personen manipuliert werden und bestimmte Handlungen tätigen. Dabei werden menschliche Eigenschaften, wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autoritäten, ausgenutzt.

Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Oft werden dabei längerfristige Beziehungen zum Opfer aufgebaut. Social-Engineering-Angriffe laufen typischerweise in mehreren Stufen und über verschiedene Opfer ab. In jedem Schritt werden dabei für die Opfer häufig unwichtig erscheinende Teilinformationen ausspioniert, welche es in Gesamtheit einem Täter jedoch erlauben, weitere Informationsquellen im Unternehmen anzuzapfen. Fast immer werden falsche Tatsachen vorgespiegelt und die Opfer erfahren selten, dass sie angegriffen wurden.

Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Häufig dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen.

© TÜV NORD Akademie GmbH & Co. KG – Jede Art der Vervielfältigung ist nur mit Genehmigung der TÜV NORD Akademie gestattet.