Social Engineering

Kriminelle wie auch Spione versuchen auf vielen Wegen, an Daten zu gelangen. Sie arbeiten dabei beispielsweise mit psychologischen Tricks, damit Personen von sich aus Daten preisgeben und Schutzmaßnahmen umgehen. Ihr Ziel ist es, an Daten und Informationen zu gelangen, interne Prozesse zu sabotieren, Schadcodes auf fremden Computern und mobilen Endgeräten zu installieren oder unautorisierte Finanztransfers in die Wege zu leiten. Diese Form von sozialer Manipulation nennt sich Social Engineering.

Die Kontaktaufnahme beim Social Engineering erfolgt häufig mehrstufig. Die Kriminellen bauen über mehrere Gespräche eine Vertrauensbasis auf, bevor sie dann Informationen fragen.

Jede und jeder einzelne Beschäftigte kann zum Ziel werden, da bereits kleinste Details wie Namen, Abwesenheiten oder Rufnummern Angreifern weiterhelfen können. Dabei sind die Angriffe nicht auf den Arbeitsplatz beschränkt. Spione und Kriminelle werden auch nach Feierabend aktiv, um weniger verdächtig zu wirken – zum Beispiel in Gesprächen an der Bushaltestelle, der Imbissbude oder in der Bahn.

Beschäftigte Ihres Unternehmens stehen besonders im Fokus von Social Engineering-Angriffen, da die Angreifer Unternehmensdaten nutzen du verkaufen. Seien Sie deshalb wachsam.

Lassen Sie sich in Gesprächen nicht unter Druck setzen. Haken Sie im Zweifelsfall nach. Bieten Sie in Telefongesprächen einen Rückruf an, um sich vorab intern abzustimmen.

So nehmen Spione und Kriminelle Kontakt auf

Ein Spion belauscht beispielsweise ein Gespräch zweier Angestellter über Sicherheitsvorschriften, die die Arbeit regeln. Er schaltet sich in das Gespräch ein, indem er von eigenen angeblichen Vorschriften erzählt. Durch geschicktes Nachfragen gelangt er an Informationen über interne Abläufe.

Ein Anrufer setzt Beschäftigte zum Beispiel durch fingierte Dringlichkeit unter Druck und gelangt so an die direkte Durchwahl der oder des Vorgesetzten. Diese kann er nutzen, um mit gefälschter Rufnummer an anderen Stellen einen Anruf aus deren oder dessen Büro vorzutäuschen.

Ein Hacker liest im Zug E-Mails auf dem Notebook mit, findet beispielsweise dann im Internet Stellenausschreibungen und formuliert zielgerichtet Virus infizierte Bewerbungsschreiben.

Ein Angreifer sammelt in sozialen Netzwerken Informationen, ergänzt diese durch Telefonate und spielt den Beschäftigten anschließend glaubhaft vor, er sei ein Vorgesetzter und autorisiert, Daten anzufordern oder freizugeben.

Soziale Netzwerke

Auch Details aus Profilen in sozialen Netzwerken können für
Social Engineering-Attacken genutzt werden – vor allem, wenn darin Details zur Arbeit angegeben werden. Angreifer recherchieren in den verschiedenen sozialen Netzwerken zu einer Person und erhalten so ein recht umfassendes Bild.

Ebenso können Kriminelle schnell und problemlos Fake-Profile erstellen. Sie vernetzen sich über diese Profile mit den Beschäftigten und starten dann ihre Angriffe.

Ein sparsamer Umgang mit Daten in sozialen Netzwerken schützt die Date Ihres Unternehmens.

Prüfen Sie, welche Daten Sie wo preisgeben und welches Gesamtbild sich daraus ergibt.

Geben Sie keine Informationen zu ihrer täglichen Arbeit oder zu konkreten Projekten an.

Veröffentlichen Sie keine dienstliche E-Mai-Adresse.

Prüfen Sie Anfragen in sozialen Netzwerken genau. Fragen Sie im Zweifelsfall nach.

Was ist bei Gefährdung oder Verdacht zu tun ?

Wenn Sie verdächtige E-Mails, Dateien oder Anrufe erhalten oder Sie auf anderem Wege kontaktiert werden, melden Sie sich bei den Ansprechpersonen der IT-Sicherheit, des Geheimschutzes oder des IT-Servicedesks. Selbstverständlich werden Ihre Angaben vertraulich behandelt.

Ansprechpersonen bei der IT-Sicherheit

Florian Thurmann
IT-Sicherheitsbeauftragter
Telefon: **0531 - 38728521**

E-Mail: Sicherheit@IT-Concepts.net

Herausgeber:
IT-Concepts.net
Am Horstbleek 53, 38116 Braunschweig

Fotos: Semisatch
Bild-Nr.: 76996819
Quelle: Shutterstock

Stand: 01/2019

IT – Concepts.net

Leistung & höchste Qualität sind unsere Stärke

Manipulation durch Social Engineering

IT-Sicherheit informiert