Social Engineering - Risikofaktor Mensch

Ein harmlos klingender Name bezeichnet eine der perfidesten zwischenmenschlichen Kommunikationstechniken, die seit Jahren weltweit existenzwichtiges unternehmerisches Kapital gefährdet!
Inzwischen geht man davon aus, dass etwa jedes 3. bis 5. Unternehmen (gleich welcher Größe) ein oder mehrmals pro Jahr Ausspähung ausgesetzt ist.
Meist ohne dies zu bemerken. Man wundert sich über Phänomene, hinterfragt diese jedoch nur sehr selten …

Von **"Social Engineering"** spricht man, wenn ganz normale menschliche Bedürfnisse und Verhaltensweisen ahnungsloser Menschen manipuliert werden, um diese zu bewegen Dinge zu tun, die sie bei ernsthaftem Nachdenken nie tun würden.

"Social Engineers" (meist beauftragte Profis) sammeln sensible Informationen wie Puzzle-Steinchen, deren Gesamtbild die Basis für weitergehende Ausspähung bildet.

Erste Angriffspunkte sind meist “unwichtig“ scheinende Unternehmensmitarbeiter oder deren Familienmitglieder. Benutzt werden menschliche Reaktionen und Verhaltensweisen wie beispielsweise Dankbarkeit, Hilfsbereitschaft, Einsamkeit, Autoritätshörigkeit, Geltungssucht, Stolz, Unsicherheit, Bequemlichkeit, Angst vor Konflikten oder Liebesbedürfnis und ähnliches mehr.
Strategien reichen von "zufälligen" Kontakten in Social Media, über direktes Kennenlernen und unauffälliges Ausfragen bis hin zum Einsatz personifizierter Mails mit täuschenden Links, deren Anklicken zusätzliche Spionagetechniken in Computern installiert.

Soziale Netzwerke, Firmenwebseiten und andere allgemein zugängliche Informationsquellen bieten dem Social Engineer umfangreiche Möglichkeiten, um sich auf seine Opfer umfassend vorzubereiten und mit diesem erste Kontakte zu knüpfen. Zu diesen "Vorfeld-Ermittlungen“ können auch Anrufe im Unternehmen gehören, die jedoch noch nicht die direkte Nachrichtenbeschaffung zum Ziel haben, sondern auf die Erlangung ergänzender Informationen zielen. Professionelle Stufenstrategien schließen sogar das Wühlen in Mülleimern oder die direkte Suche in Büros und Produktionsstätten mit ein!

Wenn nicht explizit geschult bemerken Menschen diese Methodik nur selten, weshalb unternehmensinterne Compliance-Regeln und andere Verhaltensvorschriften hierzu kaum Sicherheit bieten.

Finales Ziel der Angriffe ist zumeist das Erlangen von Firmeninterna oder sensiblen Daten, die eigene Strategien und Vorhaben erleichtern oder die zur Vorbereitung eines Eindringens in Firmennetzwerke oder Werksgelände selbst dienen.
Aber auch Unternehmen gefährdender "CEO-Fraud" (der "gute alte Oma-Trick" mit modernen Mitteln) wird durch Social Engineering vorbereitet.

Um sich vor Social-Engineer-Angriffen wirkungsvoll schützen zu können, muss man die Methoden und Techniken der angreifenden Profis ebenso verstehen, wie die Verhaltens-mechanismen der potentiellen Ziele und Opfer.
Standard-Schulungen und E-Learning können gegen SE-Angriffe nachweislich keinen ausreichenden Schutz bieten!

Die Teams von **FM-nøspy** sind erfahrene Kommunikationsprofis. Dieses Wissen - verbunden mit reicher internationaler Erfahrung im Behindern von Social-Engineering Angriffen - ist die Basis, auf der sie ihre Unterstützung für bedrohte Unternehmen weltweit erfolgreich aufbauen.

Bitte sprechen Sie mit uns, BEVOR Sie zu den Opfern gehören … info@fm-nospy.com