

SOCIAL ENGINEERING



SZENARIO

Das Telefon klingelt und das Display zeigt eine unbekannte Nummer an. Am anderen Ende der Leitung meldet sich ein vermeintlicher Mitarbeiter von Microsoft und gibt Ihnen zu verstehen, dass Ihr Computer mit einem Schadprogramm infiziert ist, das bereits eine Vielzahl an Systemen lahmgelegt hat. Redegewandt erklärt er Ihnen, wie er Sie als Quelle des Übels identifiziert hat. Dann fordert der angebliche Experte Sie auf, sich auf einer Fernwartungsseite einzuloggen. Folgen Sie seinen Anweisungen? Wenn ja, überlassen Sie dem Angreifer damit die komplette Kontrolle über Ihren Computer.

Social Engineering ist die Gesamtheit der Manipulationstechniken, die menschliche Schwächen wie z.B. Leichtgläubigkeit oder Hilfsbereitschaft ausnutzen, um eine Information, ein Kapital oder einen Dienst zu erhalten.

GEWINN DES ANGREIFERS

- Geheimnisse aus Industrie, Diplomatie, Militär
- Wirtschaftliche Vorteile
- Sabotage der Konkurrenz
- Geld

Hinter Social Engineering versteckt sich meist ein wirtschaftlicher Beweggrund. Wer die Kunst der Manipulation beherrscht, kann sie nutzen, um Zugriff auf jede Information zu erhalten, unabhängig von Materialqualität und installierter Schutz-Software.

KONSEQUENZEN FÜR DAS OPFER

- Zusätzliche Arbeitszeit
- Produktionsstörung
- Einstellung der Aktivität
- Verbreitung von Geheimnissen
- Verlust von Glaubwürdigkeit
- Identitätsdiebstahl
- Kontrollverlust
- Direkte finanzielle Verluste
- Ruf- und Imageschäden

Die Mehrzahl der Menschen geht davon aus, dass Personen, von denen sie angesprochen werden, aufrichtig sind. Gleichzeitig geben jedoch die meisten Menschen zu, manchmal zu lügen...



DIE AUSGENUTZTE SCHWACHSTELLE

Einerseits macht uns unsere „technische Fahrlässigkeit“ angreifbar. Der Mensch verliert den Überblick über die Vielzahl an Informationen zu seiner Person, die dank der neuen Medien ohne sein Wissen kursieren. Auch geht er oft zu sorglos mit sensiblen Daten um, stellt Privates ins Netz und findet es zu anstrengend, sein Online-Ich regelmäßig zu „säubern“.

Andererseits sind wir eben auch nur Menschen. Auf der Suche nach Anerkennung, Schmeicheleien, Komplimenten, Freundschaft usw. ist der Mensch generell offen für Interesse, das seiner Person entgegengebracht wird. Menschliche Tugenden wie Hilfsbereitschaft oder Schwächen wie Eitelkeit, Ahnungslosigkeit und Naivität werden von Angreifern ausgenutzt, um ihre Opfer zu manipulieren. Den meisten Mitarbeitern einer Firma ist es wichtig, gute Team-Player und solidarisch mit den Kollegen zu sein. Dafür wird auf der Seite der Sicherheit oft eingebüßt.

Eine Tatsache, der man sich bewusst sein sollte: Keine Technologie der Welt ist in der Lage, Social Engineering abzuwenden!

SCHUTZMAßNAHMEN

- Jede Information, auch wenn sie noch so unbedeutend erscheint, muss als wichtig betrachtet werden.
- Seien Sie skeptisch, sobald eine Ihnen unbekannte Person zu neugierig wird.
- Klicken Sie nicht auf Links in E-Mails oder sozialen Netzwerken, die Sie nicht erwartet haben oder die Sie dubios finden. Seien Sie misstrauisch gegenüber „Freundschaftsanfragen“ von Unbekannten.

- Verraten Sie niemandem Ihren Benutzernamen und Ihr Passwort für Internet- und EDV-Anwendungen, auch wenn die Anfrage noch so glaubwürdig erscheint.
- Loggen Sie sich auf Webseiten und Online-Anwendungen stets mithilfe des dafür vorgesehenen Buttons aus.
- Lassen Sie Papierdokumente mit sensiblen Informationen nicht für andere sichtbar herumliegen.
- Treffen Sie keine impulsiven Entscheidungen - lassen Sie sich von Ihrem Gegenüber nicht unter Druck setzen.
- Haben Sie keine Angst, Anfragen abzulehnen, die Ihnen merkwürdig erscheinen.
- Überprüfen Sie im Zweifelsfall die Identität Ihres Gegenübers. Schlagen Sie vor, dass Sie ihn zurückrufen, damit Sie seine Nummer erhalten und seine Behauptungen überprüfen können.

SOS - WAS TUN, WENN ES PASSIERT?

- Klären Sie Kollegen und Mitarbeiter über Social Engineering auf
- Setzen Sie Sicherheitsmaßnahmen um
- Klassifizieren Sie Daten, um zu wissen, welche wichtig oder vital sind und dementsprechend geschützt werden müssen
- Ermitteln Sie nach einem Angriff den genauen Schaden
- Halten Sie die Auswirkungen möglichst gering
- Finden und schließen Sie die Sicherheitslücken in der Organisation

Weitere Tipps zur Informationssicherheit:

www.cases.lu · help@cases.lu