beOnline
ict business consulting

Social Engineering

Social Engineering

Unter Social Engineering verstehen
wir das planen und Durchführen von Angriffen
auf Informationen und Systeme unter Ausnutzung
der “Schwachstelle Mensch”

beOnline
ict business consulting

Kevin Mitnick über Social Enginieering

«Mit dieser Art von Attacken war ich so erfolgreich, dass ich nur selten auf technische Attacken zurückgreifen musste. […] Der menschliche Bereich der IT-Sicherheit kann leicht ausgenutzt werden, wird aber ständig ignoriert. Unternehmen geben Millionen für Firewalls, Verschlüsselungen und sichere Zutrittssysteme aus. Dies ist Verschwendung, da keine dieser Massnahmen das schwächste Glied in der Kette angeht»

Was ist Social Engineering?

Social Engineering ist ein Methode, um nicht allgemein zugängliche Informationen durch «Aushorchen» zu erlangen.

Methodik: *Social Engineering*, Kryptocrew 20. Nov. 2002

Unter «Social Engineering» versteht man das Umgehen der IT-Sicherheitsvorkehrungen durch Manipulation der Computer-Anwender.

Social Engineering auch künftig das grösste Sicherheitsrisiko, 02.Nov. 2004

Ziele des Social Engineering

- Standortbestimmung im Bereich Sicherheit (IST-SOLL Vergleich)
- Aufzeigen und Bewerten neuer Schwachstellen/Risiken
- Bewusstseinsförderung und Sensibilisierung der Mitarbeitenden im Umgang mit Sicherheit
- Überprüfung des Verhaltens/der Reaktion von Mitarbeitenden
- Erhalt von Steuerungsinformationen für Awareness-Kampagnen im Bereich Sicherheit
- Überprüfung der Effektivität von Weisungen sowie organisatorischer, technischer und physischer Sicherheitsmassnahmen

Bereiche des Social Engineering

1. Human Based Social Engineering
2. Computer Based Social Engineering
3. Reverse Social Engineering

Unterschied

Die Art und Weise, wie Informationen gewonnen werden.

1. Human Based

Der Social Engineer versucht, Informationen auf direktem Wege zu erhalten.

Beispiele

Der Social Engineer

- tritt direkt mit einem Mitarbeitenden in Kontakt, z.B. als Lieferant, IT Support, um an Informationen zu gelangen.
- durchsucht die Mülltonnen einer Firma, um dort Informationen zu finden (sog. Dumpster Diving)
  verschafft sich Zutritt zum Geschäftsgebäude, z.B. als Reparaturdienst und versucht vor Ort an Informationen zu gelangen

2. Computer Based

Einsatz verschiedener Technologien, um Mitarbeitende auszutricksen, um so an Informationen heranzukommen

Beispiele

- „Phishing" (Versand eines E-Mails mit Hyperlink zu einer gefälschten Unternehmens-Webseite zwecks Passwortdiebstahl o.ä.)
- „Spoofing" (E-Mails mit gefälschter, vermeintlich interner Absenderadresse zwecks Erhalt von Informationen)

Durchführung einer Phishing-Attacke

Ziel

- Benutzer mittels gefälschter E-Mail auf eine gefälschte Website zu locken
- „Phishing" for personal information
- Authentisierungsdaten, Kreditkarten
  - Identitätsdiebstahl

3. Reverse

Der Social Engineer agiert als „Retter in Not"

Beispiele

- Social Engineer erzeugt ein Problem und gibt dann vor, derjenige zu sein, der dieses Problem beheben soll.
- Die Mitarbeitenden wenden sich an ihn und geben ihm alle Informationen, die er möchte.
- Hat er alle Informationen, die er haben wollte, behebt er das Problem wieder.
- Niemand schöpft direkt Verdacht, da alles wieder wie gewohnt funktioniert.

White Box versus Black Box Ansatz

White Box
Der Kunde stellt Insider-Informationen zur Verfügung, e.g. Lieferantenliste, Ferienliste der Mitarbeitenden, Namen von Mitarbeitenden, etc.

Black Box
Social Engineering Attacken werden ohne vorher bereitgestelltes Insider-Wissen durchgeführt

Die Wahl des Ansatzes hat Einfluss auf

- Zeitaufwand seitens Kunde
- Steuerungsmöglichkeit durch den Kunden
- Wahl der Methoden, Techniken und Hilfsmittel

Beispiel: Telefon-Attacke

White Box

- Benutzung von Namen und Identitäten von tatsächlichen Mitarbeitenden des Kunden
- Ausnützung von internem Wissen zur Szenario Erstellung

Black Box

- Gebrauch von falschen/erfundenen Namen und Identitäten
- Erstellung von realistischen Szenarien basierend auf vorgängigem Information Gathering

Methoden/Techniken I

Verlockung

- Überredungskunst
- Vertrauensgewinn durch Nutzen der Gutgläubigkeit
- Wecken des persönlichen Interesses
- Versprechen eines persönlichen Vorteils/Gewinns
- Schmeicheleien

Methoden/Techniken II

Täuschung

- Vorspiegeln falscher Tatsachen
- Vortäuschung eine Autoritätsperson zu sein unter Ausnutzung von Obrigkeitsgläubigkeit und der Macht der Hierarchie
- Vortäuschung der „Retter in Not" zu sein unter Ausnutzung von Inkompetenz und Unkenntnis

Methoden/Techniken III

Unter Druck setzen

- Einschüchterung
- Drohung
- Vortäuschung angeblicher Dringlichkeit/Zeitnot
- Hervorheben der Wichtigkeit (inhaltlicher Druck)

Hilfsmittel

- Technische Mittel
  - Kommunikation: E-Mail, Telefon, Fax, etc.
  - Dokumentation: Wanzen, Videokameras, etc.
- Verkleidung, Gegenstände
- Hintergrundinformationen
  - aus dem Müll (Dumpster Diving)
  - von der Website des Kunden
  - durch Mitarbeitende des Kunden
  - vom Kunden direkt
- Layout/Corporate Design von Briefen, Visitor Badges,etc.

Benötigte Hintergrundinformationen

- Namen von Mitarbeitenden und deren Funktion im Unternehmen
- Telefonlisten, E-Mail Adressen
- Abwesenheits- und Stellvertretungslisten
- Gebäudepläne und Raumlisten
- Gegenwärtige Anlässe/Umstände
- etc.

Zusammenarbeit mit dem Kunden

- klarer Vertrag mit Bevollmächtigung
- Definition eines Single Point Of Contact (SPOC)
- Geheimhaltungserklärung
- Fortwährende Optimierung durch formelle FeedbackMeetings und Zwischenberichte
- Bei einer Social Engineering Attacke vor Ort
    - Kooperationsvereinbarung oder ID für Social Engineering Team
    - Lokale Intervention durch vom Kunden bestimmte Person zum Zweck der Deeskalation

Reporting

Der umfassende Report enthält:

- Vorgehen/Drehbuch
- Ergebnisse
  - Resultat/ Aussage - Erkenntnis - Konsequenz
- Nachweise der Ergebnisse
  - anonymisierte Ton- und Bildaufzeichnungen
  - Transkripte (e.g. von Telefongesprächen)
  - Statistiken
  - Fotos
  - Protokolle

Referenzen

Sicherheitsaudits mittels Social Engineering bei

- mittelgrossen bis grossen Banken und Pensionskassen
- Energiewirtschaftsunternehmen
- staatlichen und kantonalen Institutionen
- Unternehmungen im Industriebereich

Sensibilisierungskampagnen bezüglich Social Engineering in

- der chemischen Industrie mit starken Forschungs- und Entwicklungsabteilungen
- Institutionen/ Unternehmungen mit wichtigen Beschaffungsaufgaben / Generalunternehmen
- Versicherungen

beOnline
ict business consulting

Telefon-Attacke

White Box

- Benutzung von Namen und Identitäten von tatsächlichen Mitarbeitenden des Kunden
- Ausnützung von internem Wissen zur Szenario Erstellung

Black Box

- Gebrauch von falschen/erfundenen Namen und Identitäten
- Erstellung von realistischen Szenarien basierend auf vorgängigem Information Gathering

Durchführung einer Phishing-Attacke

Ziel

- Benutzer mittels gefälschter E-Mail auf eine gefälschte Website zu locken
- „Phishing" for personal information
- Authentisierungsdaten, Kreditkarten

➢ Identitätsdiebstahl

Phishing: Wahl des Ansatzes I

White Box

- gemeinsame Festlegung von Absender, Inhalt und Ziel der Phishing Attacke

Black Box

- Kunde kaum involviert, wir erstellen Szenario ohne weiteres Insider-Wissen
- Design von der öffentlichen Kunden-Website wird adaptiert

Phishing: Wahl des Ansatzes II

Black Box Ansatz

- Versand von E-Mails an Ziele gemäss einer vom Kunden erstellten Adressliste
- E-Mail-Inhalt: Look and Feel des Kunden (CI; computer interaction), eine Aktion verlangend (e.g. Formular ausfüllen)
- Sender der E-Mail: interne Adresse, tatsächlich aber via Internet
- Formularwerte werden auf einen ‚bösartigen' Webserver über das Internet übermittelt

Ergebnisse der Phishing-Attacke

- Wie viele Zielpersonen griffen auf die ‚bösartige' Website zu?
- Wie viele Zielpersonen füllten das Formular tatsächlich aus?
- Hat jemand den Angriff bemerkt und Alarm geschlagen?

Praxisbeispiel einer kombinierten Attacke